MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIAS E TECNOLOGIA DO SERTÃO PERNAMBUCANO
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

WILLIAM DA SILVA MELO

MODELO DE FORMAÇÃO PARA EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA BASEADA EM pMOOC: UMA EXPERIÊNCIA COM SEGURANÇA DA INFORMAÇÃO

SALGUEIRO-PE
2020

WILLIAM DA SILVA MELO

MODELO DE FORMAÇÃO PARA EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA BASEADA EM pMOOC: UMA EXPERIÊNCIA COM SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Educação Profissional e Tecnológica, ofertado pelo Instituto Federal do Sertão Pernambucano, como parte dos requisitos para obtenção do título de Mestre em Educação Profissional e Tecnológica.

Orientador: Prof. Dr. Francisco Kelsen de Oliveira.

SALGUEIRO-PE
2020

Melo, William da Silva
M528p Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: uma Experiência com Segurança da Informação. X, 149f.

Dissertação (Mestrado) – Programa de Pós-Graduação em Educação Profissional e Tecnológica, Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF Sertão PE) / Campus Salgueiro, Salgueiro, PE, 2020.
Orientador (a): Prof. Dr. Francisco Kelsen de Oliveira

1. MOOC 2. Segurança da Informação 3. Educação Profissional e Tecnológica 4. Ensino Médio 5. Aprendizado em Computação Integrado I. Título II. Oliveira, Francisco Kelsen de.

CDD 371.33

WILLIAM DA SILVA MELO

MODELO DE FORMAÇÃO PARA EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA BASEADA EM pMOOC: UMA EXPERIÊNCIA COM SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Educação Profissional e Tecnológica, ofertado pelo Instituto Federal do Sertão Pernambucano, como parte dos requisitos para obtenção do título de Mestre em Educação Profissional e Tecnológica.

Orientador: Prof. Dr. Francisco Kelsen de Oliveira

BANCA EXAMINADORA

_____

Prof. Dr. Francisco Kelsen de Oliveira
Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano
(Orientador)

_____

Profa. Dra. Josilene Almeida Brito
Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano
(Membro interno)

_____

Prof. Dr. Alex Sandro Gomes
Universidade Federal do Pernambuco
(Membro externo)

AGRADECIMENTOS

Impossível não reconhecer a importância dEle em todo esse processo, me dando forças nos momentos de cansaço; fôlego, quando as lutas pareciam grandes demais; fé, quando precisei de ajuda pra acreditar, e alegria pra comemorar essa conquista. A Deus seja dada toda honra e toda glória!

A minha esposa, Camila, pela paciência (aturando meu mau humor nesse período), pela disposição em me ouvir, por toda ajuda, consolo e conselhos.

Aos meus familiares, em especial a meus pais, Manuel e Raquel, e irmãos, Alex e Cristiane, por todo o apoio, carinho e palavras de incentivo.

Ao meu orientador, Prof. Dr. Francisco Kelsen de Oliveira, por ter sido tão acessível, presente e solícito nas orientações, por sua dedicação, humildade, paciência e por ser esse ser humano tão bacana que nos inspira a acreditar numa educação de excelência.

Aos meus colegas do mestrado, em especial aos colegas de estrada, Carol, Edmilson, Fernando, João e Plínia, por todas as caronas, trabalhos em grupo, momentos de descontração, desabafos e cumplicidade.

A todos os servidores do IF Sertão e aos professores, em especial, Francisco Júnior da Silva Fernandes, Marcelo Anderson Batista dos Santos, Orlando Silva de Oliveira, pelas contribuições em minha pesquisa, e também Alex Sandro Gomes e Josilene Almeida Brito, pelas valiosas sugestões nas bancas de avaliação.

A todos os alunos do Ensino Médio Integrado ao Técnico de Informática, participantes ou não desta pesquisa.

Enfim, a todos que contribuíram direta ou indiretamente para a realização desta dissertação, meu muito obrigado!

RESUMO

O presente estudo teve como objetivo elaborar um modelo de formação *on-line*, aberto e massivo capaz de aliar teoria e prática na promoção da aprendizagem na educação profissional e tecnológica. A metodologia utilizada para identificar as principais estratégias, abordagens e instrumentos utilizados nos MOOCs foi a revisão sistemática de literatura. Na fase de elaboração do modelo de formação e da criação do MOOC, foi adotada a pesquisa-ação. Para tal, as análises das opiniões, desempenho e experiências dos estudantes foram observadas no âmbito qualitativo e quantitativo. Os sujeitos de pesquisa são professores e alunos dos cursos do Ensino Médio Integrado ao Técnico em Informática (EMITI) do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, campus Salgueiro. Os instrumentos e procedimentos utilizados para coleta de dados foram questionários, roteiro de entrevistas, grupos de discussão, testes e formulário de satisfação. O método para análise e interpretação dos dados foi a análise de conteúdo. O modelo de formação abrange elementos e diretrizes categorizadas em três perspectivas: tecnológica, pedagógica e contextual. Com base nesse modelo, foi criado e aplicado o pMOOC Segurança da informação – aliando teoria e prática. Nas avaliações, percebeu-se uma grande evolução nos alunos, considerando o desenvolvimento de conhecimentos com base nas categorias do domínio cognitivo definido na taxonomia de Bloom. Houve melhoria no desempenho relativo às categorias lembrar e entender, sendo que a análise dos resultados nas categorias aplicar, analisar e sintetizar demonstram 100% de efetividade. Já a taxa de participantes que concluíram o curso foi de 47%. O resultado da pesquisa de satisfação com o curso recebeu avaliação de 9,5, considerando-se uma escala de 0,0 a 10,0. Desse modo, percebeu-se, por parte dos alunos, uma grande aceitação do modelo de formação *on-line* com ênfase na prática, pMOOC, que, no âmbito deste estudo, foi aplicado na área da segurança da informação. A melhoria no desempenho dos alunos indica que houve aprendizado em computação e, nesse sentido, essa experiência apresenta-se com possibilidade de ser aplicada nas mais diversas áreas dos ensinos profissional e tecnológico.

Palavras-chave: MOOC. Segurança da informação. Educação Profissional e Tecnológica. Ensino Médio Integrado. Aprendizado em computação.

ABSTRACT

The present study aimed to develop an online, open and massive training model capable of combining theory and practice in promoting learning in professional and technological education. The methodology used to identify the main strategies, approaches and instruments used in MOOCs was a systematic literature review. In the phase of preparing the training model and creating the MOOC, action research was adopted. To this end, the analysis of students' opinions, performance and experiences were observed in the qualitative and quantitative scope. The research subjects are teachers and students of the courses of the Integrated High School to the Technician in Computer Science (EMITI) of the Federal Institute of Education, Science and Technology of the Sertão Pernambucano, campus Salgueiro. The instruments and procedures used for data collection were questionnaires, interview scripts, discussion groups, tests and satisfaction form. The method for analyzing and interpreting the data was content analysis. The training model includes elements and guidelines categorized in three perspectives: technological, pedagogical and contextual. Based on this model, the Information Security pMOOC was created and applied - combining theory and practice. In the evaluations, a great evolution was noticed in the students, considering the development of knowledge based on the categories of the cognitive domain defined in Bloom's taxonomy. There was an improvement in the performance related to the remember and understand categories, and the analysis of the results in the apply, analyze and synthesize categories demonstrates 100% effectiveness. The rate of participants who completed the course was 47%. The result of the satisfaction survey with the course received an evaluation of 9.5, considering a scale ranging from 0 to 10.0. Thus, it was noticed, by the students, a great acceptance of the online training model with an emphasis on practice, pMOOC, which, in the scope of this study, was applied in the area of information security. The improvement in students' performance indicates that there was learning in computing and, in this sense, this experience presents itself with the possibility of being applied in the most diverse areas of professional and technological teaching.

Keywords: MOOC. Information security. Professional and Technological Education. Integrated High School. Computer Learning.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AAD	Aprendizagem aberta e a distância
APF	Administração Pública Federal
AVAs	Ambientes Virtuais de Aprendizagem
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DCN	Diretrizes Curriculares Nacionais
EAD	Educação a Distância
EMITI	Ensino Médio Integrado ao Técnico de Informática
EPT	Educação Profissional e Tecnológica
IFES	Instituições Federais de Ensino Superior
LDB	Lei de Diretrizes e Bases da Educação Nacional
MOOC	Cursos *on-line* abertos e massivos
MEC	Ministério da Educação
POSIC	Política de Segurança da Informação e Comunicação
REA	Recurso Educacional Aberto
RNA	Redes Neurais Artificiais
RSL	Revisão Sistemática da Literatura
SVM	Máquinas de Vetor de Suporte
SPOC	Curso *on-line* pequeno e privado
TCU	Tribunal de Contas da União
TDIC	Tecnologias Digitais de Informação e Comunicação
TI	Tecnologia da Informação
WEF	*World Economic Forum*

SUMÁRIO

1 INTRODUÇÃO

O uso das ferramentas de tecnologias digitais de informação e comunicação (TDIC) e a popularização do acesso à internet trouxeram inúmeros benefícios para as pessoas, salientando-se que o espaço cibernético tem se mostrado um meio repleto de perigos, com potencial danoso muito alto. Como exemplos de ameaças que permeiam o ciberespaço, têm-se os seguintes: disseminação de vírus, acesso indevido a dados sigilosos, fraudes financeiras, *cyberbullying* e sequestro de dados (*ransomwere*). Com isso, vulnerabilidades do ponto de vista físico, lógico ou pessoal podem ser exploradas e tornar o ambiente mais suscetível a ataques, o que resulta em exposição de ativos de informação.

Nesse sentido, a informação vem assumindo um caráter estratégico e tem sido considerada 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 valor 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 crescente com a segurança da informação, como também a necessidade de educação para que indivíduos e instituições possam se proteger desses riscos. De acordo com Lyra (2015), as pessoas devem ser educadas para compreenderem o valor das informações e saber como protegê-las, sendo que, para isso, são necessários programas de treinamento e conscientização constantes.

A cada ano, o fórum econômico mundial, em inglês *World Economic Forum* (WEF), elabora um relatório em que constam os principais riscos que podem interferir no crescimento global. As cinco primeiras posições nesse ranking estão relacionadas a questões climáticas, desastres naturais e perda de biodiversidade. As fraudes de dados ocupam a sexta posição na lista de ameaças com maior probabilidade de causar impactos, seguidas pelos ataques cibernéticos (sétima posição), que também têm relação direta com a segurança cibernética (WEF, 2020).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), grupo responsável por tratar de 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 2018 para 2019, totalizando, apenas em 2019, 875.327 (oitocentos e setenta e cinco mil, trezentos e vinte e sete) incidentes (PONTOBR, 2020).

As alternativas para capacitação na modalidade educação à distância (EAD) têm se destacado por oferecer flexibilidade de horários e menor custo, se comparadas ao ensino presencial, por isso, segundo Nór (2018), entre 2011 a 2015, a modalidade EAD cresceu 51% nas instituições privadas. Ainda, considerando-se a iniciativa pública, uma reformulação ocorreu em 2019, com base na Lei de Diretrizes Bases da Educação (LDB), art. 80, que afirma o incentivo ao desenvolvimento e à veiculação de programas de ensino a distância (BRASIL, 1996).

A atualização feita pela Resolução nº 3, de 21 de novembro de 2018 nas Diretrizes Curriculares Nacionais (DCNs) para o Ensino Médio afirma que a educação a distância pode ter uma abrangência de até 20% da carga horária total, devendo incidir, preferencialmente, nos itinerários formativos do currículo (BRASIL, 2018b). Diante das inovações que têm se popularizado no contexto da EAD, destacam-se os cursos *on-line* abertos e massivos (MOOC) por possibilitarem o atendimento de um número exponencial de pessoas, independentemente de composição formal em turmas, além de permitirem formação gratuita e aberta.

Como aponta Silva (2017), os MOOCs possibilitam acesso a diversas mídias interativas e digitais, como vídeos, animações, textos, imagens, utilizando-se para tal a multimídia e a internet. Já de acordo com Alves (2010), deve existir um plano de treinamento para alertar sobre segurança da informação em que se utilizem estratégias como seminários e cursos de capacitação. Nesse sentido, este trabalho pesquisou as possibilidades de formação *on-line* baseada em MOOC em que se aliam teoria e prática com o fim de se desenvolver aprendizado em computação na temática da segurança da informação.

1.1 Questão norteadora

A motivação para este estudo se baseia em nossa visão acerca da importância da educação para se utilizarem os meios digitais com segurança, bem como da necessidade de se aliarem teoria e prática para o alcance desse propósito. Nessa perspectiva, partiu-se da hipótese de que um modelo de formação baseado num MOOC que alie teoria e prática é capaz de promover aprendizagem em segurança da informação. Assim, este estudo foi norteado pela seguinte questão: como é possível aliar aspectos teóricos e práticos para desenvolver aprendizagem na área da segurança da informação em um ambiente *on-line*, aberto e massivo criado para alunos de cursos do Ensino Médio Integrado ao Técnico (EMITI) ao técnico de informática do Campus Salgueiro do Instituto Federal de Educação, Ciências e Tecnologia do Sertão Pernambucano (IFSERTÃO-PE)?

1.2 Justificativa e motivação

Nos estudos relativos a segurança da informação, observa-se uma predominância de foco em gestores de tecnologia da informação (TI) e/ou funcionários de organizações que fazem uso ativo de TI. Por outro lado, de acordo com Lyra (2015), as pesquisas que têm estudantes como sujeitos são quase inexistentes. Ressalta-se que o Ensino Profissional e Tecnológico (EPT), segundo o Ministério da Educação (MEC), “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”. (BRASIL, 2018a). Sendo assim, de acordo com as perspectivas profissionais e tecnológicas do EPT estabelecidas pelo MEC, entende-se que esses alunos precisam ser preparados para ingressar no mundo do trabalho, onde eles farão uso ativo de TDICs e terão a necessidade de lidar com diversas questões relativas à segurança da informação.

Em relação às possibilidades de formação, a EAD, com todos os seus inerentes recursos de multimídia e inovação, trata-se de uma alternativa que tem o poder de romper com propostas de currículo engessadas e objetivistas do ensino tradicional. Especificamente, os MOOCs se mostram adequados para capacitar profissionais de T.I. na área da segurança da informação, visto que conseguem acompanhar a rapidez

com que se desenvolvem os ataques e artifícios maliciosos que permeiam o meio digital.

1.3 Objetivos

1.3.1 Objetivo geral

O objetivo geral desta pesquisa é propor um modelo de formação *on-line*, aberto e massivo capaz de aliar teoria e prática na promoção da aprendizagem em segurança da informação.

1.3.2 Objetivos específicos

Com o intuito de alcançar objetivo geral, foram estabelecidos os seguintes objetivos específicos:

- analisar a oferta de cursos abertos e massivos (MOOCs), identificando as principais ferramentas, abordagens e metodologias de ensino e aprendizagem empregadas;
- identificar as características necessárias para um curso *on-line* com ênfase numa formação técnica que alie os aspectos teóricos e práticos;
- avaliar a aprendizagem em segurança da informação, considerando o percurso formativo proposto nesta pesquisa.

2 REVISÃO DE LITERATURA

O modo como a informação é manipulada contribui diretamente para tratar impactos relativos à sua confidencialidade, integridade e disponibilidade. Nesse sentido, nas sessões de 2.1 a 2.5, são levantadas questões relativas ao papel da educação a distância e dos recursos educacionais abertos na educação relativa à segurança da informação. Para tal, são investigadas as abordagens, estratégias e instrumentos de ensino utilizadas nos cursos *on-line* abertos e massivos (MOOC).

2.1 Segurança da informação

A informação vem assumindo um caráter estratégico e tem sido considerada 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 nos bens tangíveis, sendo que, hoje em dia, veem a informação como o principal ativo. De fato, com o tempo, passou-se a dedicar especial atenção ao valor da informação, visto que, o bom uso dela possibilita subsidiar processos de tomada de decisão, melhorar a produtividade, otimizar tarefas, reduzir custos, obter vantagem competitiva e tratar continuidade de uma instituição (SÊMOLA, 2014).

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 na imagem ou na reputação da instituição. De acordo com Foina (2015), uma informação terá maior probabilidade de ser atacada quanto maior valor tiver. Dantas (2011) acrescenta que a informação é um ativo essencial que ocupa posição de destaque, portanto protegê-la tornou-se algo vital.

No cenário da atualidade, a segurança da informação envolve muito mais do que ferramentas para a detecção de invasão e proteção antivírus, consistindo num arcabouço de medidas voltadas para garantir confidencialidade, disponibilidade e integridade das informações, o que inclui prevenção, detecção, resposta, recuperação e continuidade de um negócio. (DANTAS, 2011).

O crescente uso da tecnologia e sua má utilização têm 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 é um documento que institui diretrizes e normas de segurança da informação nas mais diversas instituições, incluindo os órgãos da Administração Pública Federal (APF) direta e indireta, sendo que a ausência dessa política causa preocupação (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) (apud RIOS; TEIXEIRA FILHO; RIOS, 2017).

Em se tratando mais especificamente das Instituições Federais de Ensino Superior (IFES), em 2016, foi realizada uma pesquisa em 98 delas, constatando-se que apenas 34% possuem e utilizam de forma integral a POSIC, enquanto 51% sequer elaboraram uma política de segurança da informação para sua comunidade acadêmica (BRASIL, 2016). Nesse sentido, considerando as ameaças que circundam o meio digital, torna-se necessária uma conscientização sobre o uso seguro das ferramentas de TDICs. Para isso, as estratégias EAD tratadas nas sessões posteriores figuram como uma excelente alternativa.

2.2 Educação a distância

As possibilidades de educação a distância (EAD) estão evoluindo e se diversificando devido, dentre outros fatores, à popularização do acesso à internet e à disseminação de ferramentas TDICs no cotidiano das pessoas. Atualmente, está em plena expansão a sexta geração da EAD, caracterizada pela disponibilidade de ambientes virtuais de aprendizagem (AVAs) na *web* 4.0, adoção de tecnologias e possibilidades de comunicação contínua, mesmo em condição de deslocamento. Simultaneamente, convivemos com o conjunto de recursos da quinta geração, também conhecida como *mobile learning (m-learning*), em que a mediação do conteúdo é marcada pela multimídia móvel, utilizando-se equipamentos como computadores portáteis, *smartphones* e *tablets* (TUMBO, 2018).

A primeira geração EAD adveio quando o meio de comunicação era o texto impresso, cuja distribuição ocorria por correspondência; na segunda geração, o meio de difusão passou a ser o rádio e a televisão; a terceira geração girou em torno da

multimídia estática, disponibilizando conteúdos por meio de CDs e DVDs; já, na quarta geração, ocorreu a primeira experiência de interação de um grupo em tempo real a distância, utilizando-se a internet e a *web*.

Apesar de toda a inovação, tecnologia e multimídia envolvidas, a ideia básica da educação a distância é muito simples: alunos e professores estão em locais diferentes durante todo o tempo (ou em grande parte) em que aprendem e ensinam. Estando em locais distintos, eles dependem de algum tipo de tecnologia para transmitir informações e lhes proporcionar um meio para interagir (MOORE; KEARSLEY, 2008).

O censo da educação superior realizado pelo Ministério da Educação (MEC) mostra que, no Brasil, a educação a distância tem crescido nos últimos anos. Em 2007, representava 7,0% das matrículas de graduação; já em 2017, a EAD aumentou para 17,6%, atendendo a mais de 1,7 milhão de alunos, o que representou uma participação de 21,2% dos graduandos no país. A modalidade presencial, por seu turno, apresenta o segundo ano de queda no número de matrículas (BRASIL, 2018c).

Todo esse crescimento na EAD tem relação com diversos fatores, entre os quais, romper barreiras espaciais e temporais entre professor e aluno, oferecer flexibilidade nos horários de estudo e apresentar baixo custo, se comparada ao ensino presencial. Ainda, por se relacionar também à popularização do acesso a recursos tecnológicos, com possibilidade de utilização de diversas mídias interativas (mensagens instantâneas, *chats*, fóruns de discussão e videoconferências), essa modalidade de educação tem despertado interesse nos alunos.

O Decreto nº 5622, que regulamenta as diretrizes para o desenvolvimento de programas de ensino a distância, em seu artigo 2º, inclui a modalidade de Educação Básica como uma possibilidade (BRASIL, 2005). A atualização feita pela Resolução nº 3, de 21 de novembro de 2018, nas Diretrizes Curriculares Nacionais (DCNs) para o Ensino Médio afirma que a educação a distância pode ter uma abrangência de até 20% da carga horária total, devendo incidir, preferencialmente, nos itinerários formativos do currículo (BRASIL, 2018b). Logo, para que isso seja implementado de maneira efetiva, torna-se indispensável o bom uso das ferramentas de TDICs aliadas a abordagens e metodologias de aprendizagem mais adequadas à modalidade de ensino a distância.

Entre os fatores importantes para se trabalhar com EAD no ensino básico, se incluem a faixa etária e a maturidade dos aprendizes, além do desenvolvimento de

habilidades como autonomia, gerenciamento do tempo e disciplina. Com isso, diante de toda inovação, tecnologias, multimídia e abordagens de ensino aprendizado, a educação a distância deve estar mais acessível e ao alcance de todos. Nesse sentido, a subseção seguinte apresenta as possibilidades de contribuições dos recursos educacionais abertos (REA) no contexto da EAD.

2.3 Recursos educacionais abertos (REAs)

A educação como uma garantia para os indivíduos é citada na Declaração Universal dos Direitos Humanos. Nossa Constituição Federal também afirma, no art. 205, que se trata de um direito de todos, dever do Estado e da família, e que será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho (BRASIL, 1988).

Todavia, apesar do reconhecimento da importância da educação para o desenvolvimento integral do indivíduo, ainda existem muitas barreiras que dificultam o acesso das pessoas à formação. Custo de apostilas e livros, preço de mensalidade no ensino privado, requisitos iniciais de formação, falta de estrutura tecnológica, condições geográficas, ausência ou carência de programas para inclusão de pessoas com deficiência, adultos sem acesso à educação ao longo da vida são situações que produzem desigualdades no acesso aos processos educacionais (PEREIRA, 2015).

Nesse panorama, os recursos educacionais abertos (REAs) visam promover maior equidade na educação e diminuir as barreiras que restringem as oportunidades de aprendizagem, por meio da disponibilização de materiais e tecnologias produzidas com licenças abertas. Ressalta-se que esses recursos não se restringem a mídias digitais, usadas na EAD, podendo incluir também livros, apostilas e outros materiais usados na educação presencial, sendo que, em função das tecnologias, ferramentas e variedades de mídias, os REAs utilizam predominantemente o meio digital. Esses elementos estão tão ligados ao termo, que originaram a aprendizagem aberta e a distância (AAD), a qual “caracteriza-se essencialmente pela flexibilidade, pela abertura dos sistemas e pela maior autonomia do estudante”. (BELLONI, 2012, p. 30).

Sob a perspectiva da abertura, para Pereira (2015), em se tratando de um REA, qualquer pessoa tem a liberdade de usar, personalizar, melhorar e redistribuir os recursos educacionais a fim de atender as mais diversas necessidades. Para tal, é

necessário que esse conteúdo apresente uma autorização que conceda o licenciamento necessário para os níveis de uso, de alteração e de distribuição ou não, de forma *on-line* e simplificada. Um bom exemplo de licença é a *creative commons*, na qual o autor concede os níveis de autorização de forma *on-line* e simplificada, a fim de disponibilizar a obra pela internet. Dessa forma, a autoria de citação continua tendo garantia, mesmo permitindo a distribuição, modificação, personalização para os mais variados fins.

Da perspectiva legal e técnica, os REAs são materiais de ensino, aprendizado e pesquisa em qualquer suporte ou mídia de domínio público, ou licenciados de maneira aberta. Com isso, torna-se possível a utilização ou adaptação por terceiros, a qual pode incidir em cursos completos, partes de cursos, módulos, livros didáticos, artigos de pesquisa, vídeos, testes, software e qualquer outra ferramenta, material ou técnica que possam apoiar o acesso ao conhecimento (UNESCO, 2016).

Conforme Pereira (2015), a ênfase na abertura de materiais implica livre disponibilidade na internet e o mínimo de restrições possível sobre o uso dos recursos. Assim, eles não podem ter barreiras técnicas e econômicas, devendo também as barreiras legais ser as mínimas possíveis para o usuário final, que poderá não apenas ler ou usar o recurso, mas também adaptá-lo e construir algo a partir disso.

Li (2018) enfatiza que o acesso aberto significa que qualquer pessoa pode participar de cursos, independentemente da idade, capacidade e situação financeira, devendo ser removidas ou minimizadas as barreiras físicas, de tempo, currículo, falta de autoconfiança e financeiras; os métodos de estudos devem ser flexíveis e manter foco no aluno; as tarefas de ensino devem incluir aconselhamento, motivação e a individualização de módulos de aprendizagem para diferentes pessoas, que em sua maioria estudam *on-line*.

Em síntese, os REAs geralmente estão disponíveis na rede, promovendo uma maior democratização do acesso e garantindo proteção de autoria. Em função disso, muitos MOOCs utilizam esses recursos por agregarem materiais de qualidade que não impõem violações do ponto de vista da propriedade intelectual.

2.4 Curso *on-line* aberto e massivo (MOOC)

Os recursos da EAD visam romper as barreiras espaciais e temporais entre professor e aluno, com o uso de redes sociais e de ambientes virtuais de

aprendizagem (AVAs). Os cursos *on-line* abertos e massivos (do inglês *massive open online course, ou* MOOC) surgiram de uma iniciativa de George Siemens, que, ao ministrar 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 *on-line* (SOUZA; CYPRIANO, 2016).

Os MOOCs têm ganhado espaço no mundo todo, possibilitando ofertar educação por meio da *web*, porém se diferenciam da educação a distância tradicional em vários aspectos, tais como oferta massiva, independência de composição formal em turmas e custo reduzido. Para Forno e Knoll (2013), os MOOCs constituem uma categoria de educação à parte, afinal, eles podem ser acessados por qualquer pessoa conectada à internet. Huang (2018) diferencia os MOOCs pelo fato de não estarem restritos a dezenas ou centenas de pessoas, como ocorre na EAD, e também por não estarem limitados no tempo e no espaço (o que reduz significativamente o limiar de aprendizagem).

Holanda e Tedesco (2017) enfatizam a massividade como um dos principais diferenciais entre os cursos *on-line* tradicionais e os MOOCs. Já Siemens (2013) e Aretio (2013) sustentam que os MOOCs são uma forma evoluída de educação a distância, pois inovam com a utilização da tecnologia da informação *on-line,* só que de forma massiva e aberta. Muitos especialistas acreditam que os MOOCs constituem uma “revolução na educação”, uma tendência tecnológica e pedagógica emergente, um fenômeno relativamente novo e que está sendo tratado como algo generalizado (FASSBINDER; DELAMARO; BARBOSA, 2014).

Não existe um consenso sobre a quantidade de participantes que um curso MOOC pode ter ou se o número deve necessariamente ser ilimitado ou não, entretanto, independente do limite máximo de participantes, no que diz respeito à massividade, fica claro que os MOOCs possuem uma larga abrangência. Além da experiência realizada por George Siemens, Alcock, Dufton e Durusu-Tanrıöver (2015) citam outro exemplo de curso que manteve 60.000 estudantes inscritos, mantendo-se mais de 30.000 ativos. Para se ter um senso de escala, se numa universidade 100 graduados fossem ensinados numa classe por ano (uma suposição generosa para a maioria das faculdades), demoraria cerca de 300 anos para se atingir a formação que o MOOC citado obteve.

Outro requisito marcante no formato dos MOOCs é a abertura do acesso. De acordo com Toven-Lindsey, Rhoads e Lozano (2015), ser aberto é permitir que

qualquer um possa participar, ou seja, não exigir pré-requisito para matrícula. Da mesma direção, Fassbinder, Delamaro e Barbosa (2014) salientam que o currículo do MOOC deve ser compartilhado publicamente. Todavia, mesmo vencida a barreira da imposição de pré-requisitos educacionais, que propicia facilidade de acesso, ainda se esbarra no fator custo. Pérez-Sanagustín et al. (2017) destacam que a produção de MOOCs é onerosa para as instituições, havendo vários custos envolvidos no planejamento, capacitação e elaboração dos cursos, favorecendo as universidades de elite, que têm liderado a produção dos MOOCs pelo fato de possuírem capacidade de investimento. Em face dessa realidade, a gratuidade do acesso aos MOOCs é algo bem discutido, sendo que muitos estudiosos, como Fassbinder, Delamaro e Barbosa (2014), Alcock, Dufton e Durusu-Tanrıöver (2015), Chauhan, Taneja e Goel (2015) e Gené et al. (2014) propugnam que, para ser realmente aberto e possibilitar o acesso de todos à educação, o MOOC deve ser gratuito.

Importante ressaltar que, considerando os custos envolvidos na criação de diversas mídias interativas e digitais, capacitação de pessoal, entre outras despesas incluídas na elaboração de um curso on-line aberto e massivo, autores como Forno e Knoll (2013) admitem que podem existir taxas de matrícula. Toven-Lindsey, Rhoads e Lozano (2015) e Cilesiz (2014), por sua vez, afirmam que existe inclusive um grande potencial de geração de receita sendo explorado nos MOOCs.

Características como abertura e massividade representam muito bem os MOOCs, os quais incluem ainda outras vantagens, como independência de composição formal em turmas, participação assíncrona (podendo ser iniciada a qualquer momento pelo estudante), escalabilidade para quantidade de alunos e alcance abrangente de público, possibilidade de acesso a mídias interativas e digitais, diferentes mecanismos de avaliação e recursos colaboração (ALMENARA; CEJUDO; MARTÍNEZ , 2014, SILVA, 2017).

Equilibrando a grande expectativa gerada em torno dos MOOCs enquanto alternativa real de educação de qualidade, inclusive em nível de graduação e pós-graduação, Toven-Lindsey, Rhoads e Lozano (2015) afirmam que muitos professores e analistas da educação duvidam da capacidade de esses cursos oferecerem uma alternativa viável aos modelos tradicionais de educação presencial ou *on-line*. Desse modo, Almenara, Cejudo e Martínez (2014) apontam uma dicotomia nas perspectivas acerca dos MOOCs, isto é, enquanto uns os consideram a melhor tecnologia educacional existente, outros membros da comunidade acadêmica mostram-se

céticos em relação a seus benefícios e viabilidades. Para estes, o novo meio não tem nada de novo, tratando-se apenas de uma nova roupagem dada a uma EAD disfarçada num modelo de negócio para universidades e outras instituições. Dizem ainda que a qualidade dos MOOCs deixa muito a desejar.

Interessante observar que todo esse cenário de supervalorização e críticas em torno dos MOOCs comprova que, no mínimo, essa tecnologia provocou uma grande reflexão no meio acadêmico. A empresa de consultoria Gartner (2019)[1] explica a dicotomia entre opiniões dos profissionais da educação, mostrando que toda tecnologia passa por fases distintas: lançamento da tecnologia, pico de expectativas superdimensionadas, declive de desilusão, inclinação de iluminação e platô de produtividade, como se mostra na figura 1, a seguir.

Figura 1 – Fases da tecnologia

Fonte: Adaptada de Gartner (2019).

Conforme a figura 1, inicialmente, existe uma expectativa muito alta quanto ao impacto que a tecnologia pode causar, sendo que muita publicidade pode estar baseada apenas nessa expectativa. Posteriormente, o declive de desilusão pode surgir quando experiências malsucedidas geram frustrações; já a inclinação de iluminação acontece quando as vantagens de utilizar a tecnologia são mais bem compreendidas e começam a se solidificar.

Para Almenara, Cejudo e Martínez (2014), antes de se aderir a um discurso alarmista, deve-se abrir uma linha de investigação sobre as possibilidades e limitações

[1] Gartner Group é uma consultoria americana de tecnologia que analisa mercados de vários setores e suas tendências.

reais que o modelo educacional oferece, sendo que, de acordo com Alcock, Dufton e Durusu-tanrıöver (2015), os MOOCs podem ser bastante recompensadores, porém estão longe de ser a maneira mais fácil de ensinar. Com isso, em relação à fase de platô de produtividade (figura 1), nota-se que a consolidação do uso da tecnologia MOOC ocorre quando são aplicados critérios bem definidos para avaliar qualidade, viabilidade, aplicabilidade e relevância para os objetivos educacionais visados.

Promover aprendizagem colaborativa, conforme a concepção de Holanda e Tedesco (2017), é um desafio, o que é corroborado por Cilesiz (2014), que critica experiências que não promovem interação entre estudantes e professor, gerando uma dificuldade de comunicação entre eles. Já Almenara, Cejudo e Martínez (2014) acrescentam que os estudantes não desenvolvem bem as habilidades de trabalho em equipe e colaboração, afinal isso nem sempre é experimentado por eles da maneira adequada.

Algumas atividades, como formação de grupos de estudo, participação em *chats web*, redes sociais, gamificação e fórum de discussão, constituem tentativas de promover uma maior colaboração no processo de aprendizagem (AUH; SIM, 2018, MELLATI; KHADEMI; ABOLHASSANI, 2018, TOVEN-LINDSEY; RHOADS; LOZANO, 2015). Nesse sentido, observa-se que alcançar a colaboração num ambiente virtual de aprendizagem *on-line* não é tarefa simples. Holanda e Tedesco (2017) identificam várias condições para tal: existência de um objetivo comum, interdependência positiva entre pares, mecanismos de coordenação e comunicação e responsabilidade individual.

Outra questão crucial que tem gerado grande preocupação na implementação dos MOOC é a taxa de abandono. Quanto a isso, Lee e Pak (2018) e Almenara, bem como Cejudo e Martínez (2014) expõem situações que registram menos de 10% de conclusão do curso. Numa delas, as matrículas chegaram a 12.725 alunos, dos quais apenas 8.000 assistiram a algum vídeo, 346 realizaram o exame final, e somente 261 obtiveram certificação, ou seja, pouco mais de 2%. Por outro lado, Alcock, Dufton e Durusu-tanrıöver (2015) afirmam que os cálculos de conclusão devem ser feitos com clareza, não devendo se ater a uma simples comparação entre os que se matriculam e os que concluem, afinal esse resultado pode alardear uma percepção negativa e precipitada sobre evasão.

Considerando ser provável que pouco mais da metade das pessoas que se inscrevem, possivelmente com um único clique, realmente participe da turma, o modo

mais realista de calcular taxas de conclusão seria considerando “aprendizes ativos”, em vez dos matriculados, ou seja, identificar os alunos que realmente iniciaram o curso, acessaram o site, assistiram a um vídeo ou responderam a questionários. Com isso, os resultados que antes demonstram taxas de conclusão entre 10 a 17 % atingem o patamar de cerca de 54% (ALCOCK; DUFTON; DURUSU-TANRIÖVER, 2015).

Acerca das questões didático-pedagógicas em um cenário de diversas influências, como internet, multimídia, conectivismo e interatividade, de acordo com Riedo et al. (2014), é preciso adotar uma orientação pedagógica em que o aluno se torne um participante ativo, praticando ações mais refletidas na construção do seu conhecimento. Nesse sentido, para Holanda e Tedesco (2017), os modernos métodos educacionais sugerem que os aprendizes devem desenvolver habilidades como criatividade, pensamento crítico, colaboração e resolução de problemas.

A categorização dos MOOCs mais comum elabora com base em dois grandes grupos: os cMOOCs e os xMOOCs (ALMENARA; CEJUDO; MARTÍNEZ, 2014, FASSBINDER; DELAMARO; BARBOSA, 2014, HOLANDA; TEDESCO, 2017, HUISMAN et al., 2018, WU, 2017). Nos xMOOCs, considerados mais instrucionais, os alunos participam de uma experiência individualizada e massiva marcada por uma série de conteúdos. O curso é centrado no professor, que assume papel de perito, selecionando o conteúdo e as ferramentas de avaliação, padronizadas e automatizadas (banco de questões) até certo ponto. Esse modelo de MOOC é considerado uma versão repaginada e *on-line* do modelo de ensino tradicional.

Os cMOOCs, de forma preponderante, se ancoram na aplicação da teoria cognitivista de Siemens (2013), focando em comunidades de discussão, vários tipos de aplicativos e serviços da *web*, como *blogs, wikis, podcasts* e agendas colaborativas. O fluxo de informações e conhecimento é, pois, distribuído; os horários de aula desaparecem; grupos de trabalho são espontâneos e direcionados de acordo com o interesse do aluno e, além disso, o currículo é negociado com os estudantes. Sendo assim, nos xMOOCs, o foco está no processo de instrução e nos conteúdos, enquanto, nos cMOOCs, a interação é um elemento chave, com os estudantes assumindo um papel mais significativo no processo de formação.

Além dos xMMOCs e dos cMOOCs, Fassbinder, Delamaro e Barbosa (2014) identificam outras três categorias: aMOOCs, que têm a capacidade de se adaptar às preferências de aprendizagem do aluno e contam com *feedback* inteligente e em

tempo real; mMOOCs (o *m* da sigla refere-se à ausência de professor ou tutor), de curto prazo e sem exigência de pré-requisitos, podendo ser considerados um modo de educação não formal, e os quasi-MOOCs, que abrangem tutoriais da *web*, com uso de recursos educacionais abertos que apoiam tarefas específicas de aprendizagem, de forma que não chegam a ser um curso. Wu (2017) conceitua ainda o SPOC, curso *on-line* pequeno e privado de curta duração, com um público mais fechado, sendo por vezes corporativo e podendo complementar o ensino tradicional.

No que diz respeito à perspectiva pedagógica e sua funcionalidade na aprendizagem, Clark (2013) categoriza ainda os seguintes tipos de MOOCs: Transfer MOOCs, que transferem cursos existentes para uma plataforma MOOC, imitando cursos acadêmicos tradicionais, com palestras, testes curtos, textos e avaliações; madeMOOCs, em que se usam vídeos, com ênfase na qualidade da criação de tarefas interativas baseadas em *software* e vídeos; VOOCs, os quais tendem a ser mais vocacionais; synchMOOCs são síncronos, com data fixa de início, trabalhos e fim; asynchMOOCs são assíncronos, sem datas fixadas para término, sendo os prazos relaxados.

Os MOOCs adaptativos (adaptiveMOOCs - aMOOCs) usam algoritmos adaptativos para apresentar experiências de aprendizagem personalizadas, levando os alunos a trilhas de aprendizagem personalizadas; os groupMOOCs começam com grupos pequenos e colaborativos baseados em localidade, habilidade e desempenho, os quais podem ser dissolvidos e reformulados com o objetivo de aumentar a permanência no curso; os connectivistMOOCs buscam colher e compartilhar conhecimentos compartilhados pelos participantes, que não veem o curso como uma receita de conhecimento fixo e justo; miniMOOCs são mais curtos, focados em conteúdos e habilidades que não requerem prazos tão longos (CLARK, 2013).

Ribeiro e Catapan (2018) identificam ainda o que consideram ser variantes conceituais dos MOOCs: o LOOC, ou SMOOC – *little* ou *small* se referem a MOOCs pequenos, com menos de 100 alunos; SPOC – com ritmo autogerido pelo aluno; sMOOC – acessível por mídias sociais e dispositivos móveis; COOC – curso *on-line* aberto à comunidade; BOOC (*big open on-line course)* – tenta unir aprendizado cMOOC com *feedback* personalizado xMOOC; DOCC – curso colaborativo aberto distribuído; MOOR – pesquisa *on-line* aberta e massiva; POOC – curso *on-line* aberto e personalizado, e mobileMOOC – demonstra sinergia entre MOOC e *mLearning* (Quadro 1, a seguir).

Quadro 1 – Tipos de MOOC

Tipos de MOOC	Descrição
aMOOC	MOOC adaptativo, permite trilhas de aprendizagem personalizadas
asynchMOOC	Assíncrono sem cronograma fixo
BOOC	Une cMOOC com *feedback* personalizado xMOOC
cMOOC	MOOC conectivista
COOC	Curso *on-line* aberto à comunidade
DOCC	Curso colaborativo aberto distribuído
groupMOOC	Trabalha com grupos
LOOC ou SMOOC	MOOCs pequenos
madeMOOC	Interativos baseados em *software* e vídeos
miniMOOC	MOOC curto
mMOOC	MOOC sem tutor/professor
mobileMOOC	Demonstra sinergia entre MOOC e o *mLearning*
MOOR	Pesquisa on-line aberta e massiva
POOC	Curso on-line aberto e personalizado
quasi-MOOC	Apoiam tarefas específicas de aprendizagem
sMOOC	Acessível por mídias sociais
SPOC	Curso *on-line* pequeno e privado
SPOC	*Self-pacedon-linecourse* ritmo autogerido pelo aluno
synchMOOC	Síncrono com cronograma fixo
Transfer MOOC	Transferem cursos para versão MOOC
VOOC	Vocacionais
xMOOC	MOOC instrucional

Fonte: Elaborado pelo autor.

Para criar MOOCs podem ser utilizadas plataformas também denominadas *massive open on-line education platform* (MOOEP), a exemplo do Google *Course Builder* (https://code.google.com/p/course-builder), edX Platform (code.edx.org), openMOOC (openmooc.org) e openHPI (https://openhpi.de). Além disso, é comum se utilizarem provedores MOOC (MOOC Provider), como Cousera, Udacity, edX, Udemy, Veduca e MiríadaX para disponibilizar esses serviços (FASSBINDER; DELAMARO; BARBOSA, 2014). Esses autores indicam que a criação de um MOOC envolve basicamente quatro conjuntos de atividades: análise de necessidades; planejamento; implementação e execução, conforme o quadro 2, a seguir.

Quadro 2 - Criação de um MOOC

Fases da criação de um MOOC	
1	**Análise das necessidades** - levantar as demandas existentes e, com base no tempo e recursos disponíveis, será possível elaborar uma proposta de MOOC
2	**Planejamento** - definição dos objetivos, abordagem de armazenamento e entrega, padrões de qualidade para mídias, estilo de apresentação de conteúdo, planejamento de atividades *on-line*, métodos de avaliação, formas de promoção e divulgação do curso
3	**Implementação** - elaboração de materiais didáticos, atividades e serviços
4	**Execução** - marcada pela abertura do período de inscrições, dentre outras atividades inerentes ao contexto da instituição à qual o MOOC será vinculado

Fonte: Adaptado de Fassbinder, Delamaro e Barbosa (2014).

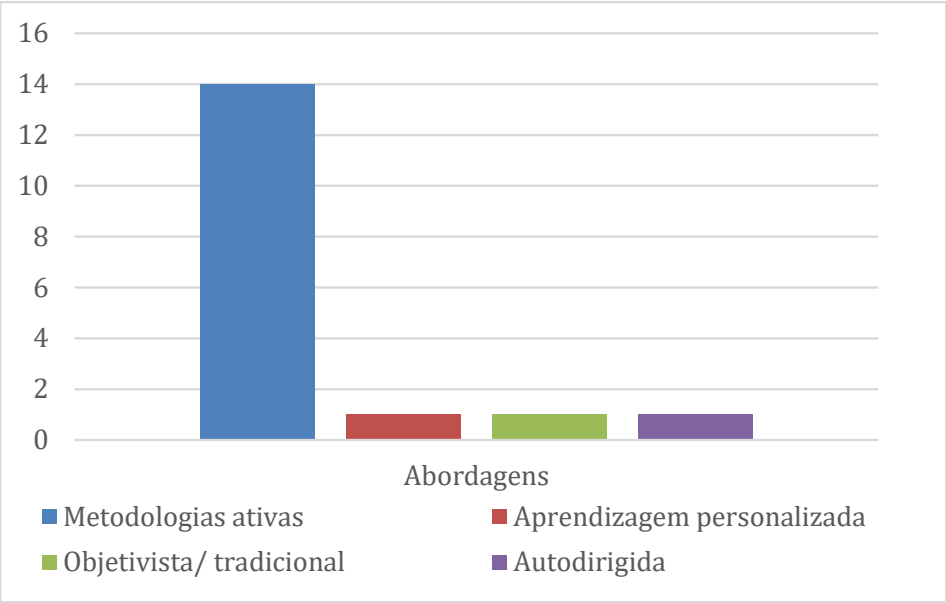
2.5 Abordagens, estratégias e instrumentos utilizados nos MOOCs

De acordo com os resultados da revisão sistemática da literatura (RSL) realizada neste trabalho, foi possível observar que, dentre as abordagens de ensino identificadas, essencialmente o ensino tradicional não se encaixa nos moldes dos cursos *on-line* abertos e massivos, visto que, independentemente de sua modalidade ou especificidade, o professor não é o centro do processo educativo, até porque, em muitos casos, essa figura é substituída pela do tutor ou instrutor.

De acordo com Toven-Lindsey, Rhoads e Lozano (2015), quando um MOOC é criado, ainda pode ocorrer uma certa confusão, pois algumas experiências (objetivistas) mostram que sequências instrucionais são simplesmente submetidas como uma verdade absoluta na educação a distância, impondo uma realidade pré-concebida que o estudante precisa apenas absorver, situação que se assemelha muito ao ensino tradicional desenvolvido em sala de aula presencial. Entretanto, de acordo com Alcock, Dufton e Durusu-tanrıöver (2015), para que o processo de aprendizagem dê bons resultados, é essencial uma interação eficaz do aluno com o grupo e com o instrutor. Em outras palavras, não é aceitável simplesmente colocar os recursos *on-line* e depois desaparecer.

Na contramão do ensino tradicional presencial, o gráfico 1 mostra outras abordagens de ensino, mais utilizadas nos MOOCs. Toven-Lindsey, Rhoads e Lozano (2015) observam que a presença da abordagem objetivista subdivide-se entre *individual*, quando o aluno consome alguma mídia do curso, e *em grupo*, a qual nem sempre demonstra efetividade.

Gráfico 1 – Abordagens de ensino



Fonte: Elaborado pelo autor.

De acordo com Luo et al. (2018), a abordagem de aprendizagem autodirigida envolve autogerenciamento, automonitoramento e automotivação, sendo que determinadas características do projeto de ensino, como diagnósticos, recursos, estratégias e avaliações de aprendizagem, devem ser adequadas para o alcance dessa autonomia. Já a aprendizagem personalizada procura utilizar a tecnologia da informação com a orientação dos professores, para responder à necessidade de cada estudante de forma adaptativa. Desse modo, adiciona ou exclui conteúdo; seleciona materiais e propõe questões considerando um aluno ou grupo de alunos específicos (TORRES; GONZÁLEZ; YAGO, 2017).

É possível observar no gráfico 1 que as metodologias ativas de aprendizagem têm uma participação muito relevante nos estudos identificados, uma vez que encorajam o envolvimento do aluno, deslocando-o da posição de receptor passivo para o centro de processo de aprendizagem. Nesse sentido, o aluno não fica limitado aos recursos fornecidos pelo professor.

Uma proposta de ensino, independentemente da modalidade escolhida, deve permitir que os alunos construam seu próprio conhecimento, vivenciando suas próprias experiências a partir das suas compreensões. Segundo Piaget (1973), os métodos didáticos são de fundamental importância para despertar o interesse e desenvolver o aprendizado dos alunos, fazendo com que reconstruam seus

esquemas de comportamento, interiorizem os assuntos e consequentemente, construam o conhecimento.

Toven-Lindsey, Rhoads e Lozano (2015) esclarecem que a educação centrada no aluno tem raízes na teoria construtivista, que se tornou uma característica importante em muitos ambientes virtuais de aprendizagem *on-line,* podendo ocorrer de forma individual (construtivismo cognitivo) ou em grupo (construtivismo social). Assim, a aprendizagem sofre influências singulares, de acordo com uma percepção de cada indivíduo, mas também apresenta uma perspectiva social, com diálogo, interação e colaboração no contexto social em que a aprendizagem ocorre, ou seja, na abordagem construtivista individual, o conhecimento é construído nos alunos, enquanto que a construtivista em grupo pressupõe que o conhecimento é socialmente construído no mundo.

De acordo com Feng e Qu (2018), a *web* pode atuar no sentido de transformar a abordagem de ensino de modo que seja orientada ao estudante, diferente do que ocorre no ensino tradicional. Para isso, conforme Alcock, Dufton e Durusu-Tanrđöver (2015), o papel do professor ou instrutor precisa mudar de um a voz única e amplamente autoritária para o de organizador, tutor corretor, comentarista, intérprete, líder de torcida e, ocasionalmente, apologista. Corroborando essa visão, Toven-Lindsey, Rhoads e Lozano (2015), Freitas e Paredes (2018) e Feng e Qu (2018) e Wu (2017), destacam que, numa abordagem centrada no aluno, o instrutor deve atuar como um guia, prestando suporte ao corpo estudantil, utilizando metodologias ativas apoiadas por tecnologias e recursos de alta qualidade a fim de envolver os alunos e promover a construção do conhecimento.

No contexto das metodologias ativas de aprendizagem representado no gráfico 1, o ensino híbrido ou *blended learning,* demonstra grande representatividade nos MOOCs. De acordo com Pérez-Sanagustín et al. (2017), o conceito *híbrido* é de grande alcance e pode ser compreendido como qualquer iniciativa, estratégia ou modelo de aprendizagem que integre MOOCs ou tecnologias relacionadas a MOOCs em um currículo tradicional.

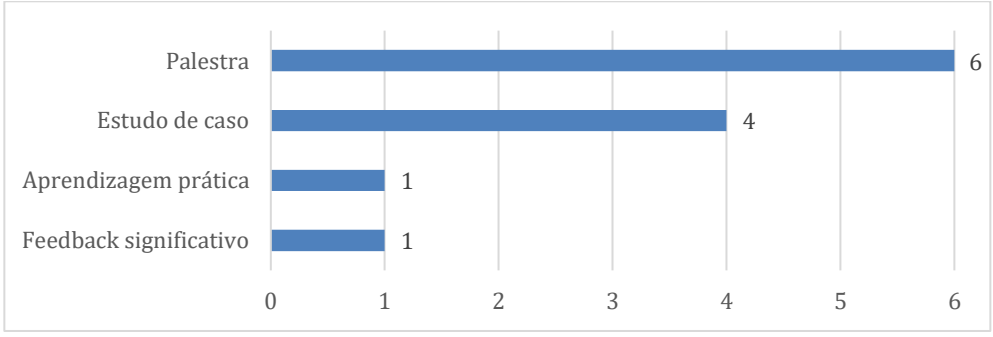
Complementando o conceito do ensino híbrido, Park, Yu e Jo (2015) esclarecem que o mesmo combina atividades em sala de aula com atividades *on-line*, sendo que muitas instituições de ensino superior consideram o ensino híbrido uma maneira de transformar a pedagogia tradicional. De fato, muitas aplicações do ensino híbrido se utilizam do modelo da sala de aula invertida (*flipped classroom*), onde os

alunos são primeiramente expostos ao conteúdo por meio de recursos *on-line*, tendo acesso a leituras, vídeos ou outras atividades em meios eletrônicos. Posteriormente, há um tempo dedicado à aula presencial, com uma abordagem centrada no aluno, capaz de promover uma aprendizagem ativa. (RAMNANAN; POUND, 2017). Nesse sentido, o encontro presencial na sala de aula invertida, de acordo com Ramnanan e Pound (2017), Torres, González e Yago (2017) e Ziegenfuss e Furse (2015), deve permitir que o aluno aplique seus conhecimentos a problemas desafiadores e envolventes em um ambiente que promova a colaboração com os colegas e o *feedback* e a orientação dos professores.

Lee e Pak (2018) advertem que, quando os alunos têm o hábito de receber instruções de maneira passiva, por conta do modelo de ensino tradicional ao qual foram condicionados, existe uma barreira natural na transição para o método ativo, no qual o aluno é o centro do processo. Por isso, nos encontros presenciais do ensino híbrido, os professores precisam trabalhar com atenção detalhada e aconselhamento a fim de facilitar a aprendizagem através do MOOC, pois o objetivo é promover, nos estudantes, aprendizagem autodirigida.

De acordo com Klooss et al. (2015), o ensino híbrido pode ser integrado com um curso MOOC, usando a sala de aula invertida, mas também pode utilizar outros modelos, como prelúdio digital, sendo a primeira parte do curso toda *on-line* (MOOC), ocorrendo, em seguida, o ensino *face to face (f2f);* ensino digital combinado com tutoria presencial ou remota, no qual o conteúdo é baseado em MOOC, sendo que, nos semestres em que não há encontro f2f, o corpo docente fica disponível para tutoria no horário de expediente. No que diz respeito às estratégias de ensino utilizadas nos MOOCs, notam-se várias iniciativas relevantes, conforme o gráfico 2, a seguir, em que é possível perceber um evidente destaque para as palestras.

Gráfico 2 – Estratégias de ensino



Fonte: Elaborado pelo autor.

Cilesiz (2014) chama a atenção para predominância das palestras na educação a distância em todo mundo, destacando ainda uma tendência de continuidade e crescimento do uso desse recurso, o qual, segundo o autor, permite acesso a um número muito grande de alunos, reduz a necessidade de múltiplos instrutores e uso de instalações físicas, chegando, em alguns casos, até a substituir o ensino presencial regular em cursos superiores.

O fenômeno das palestras pode aparecer sobre vários formatos: vídeo unidirecional, televisão instrucional, *webcasting*, *podecasting* (vídeo), gravações de aula. A transmissão pode se realizar por diversos meios de comunicação, como circuito fechado em várias salas de aula, canais de televisão a cabo, vídeos digitais disponíveis na internet (CILESIZ, 2014).

Há muitas vantagens em se inserirem palestras nos cursos MOOC, visto que, segundo Herala et al. (2017), elas têm um impacto positivo na preparação dos alunos, pois permitem que gerenciem seu tempo e ritmo de acordo com suas conveniências, bem como motivam e propiciam mais independência. Acrescentam os autores que, com as palestras em vídeo, o desempenho dos alunos parece melhorar quando comparado com outros cursos similares sem componentes de vídeo de aula.

Entretanto, do ponto de vista pedagógico, para Alcock, Dufton e Durusu-tanrıöver (2015), há um aspecto preocupante nas palestras: a falta de interação entre estudantes e instrutor, ou seja, incomoda os alunos o fato de o professor não os conhecer, estar distante e pouco acessível. Acrescenta-se ainda a dificuldade de concentração, baixa autodisciplina e inexistência de contato social (CILESIZ, 2014). Por isso, as plataformas MOOC precisam evitar essas deficiências por meio de uma proposta de aprendizagem que inclua recursos capazes de suprir as expectativas.

Uma característica marcante na estratégia de aprendizagem prática, segundo Freitas e Paredes (2018), é juntar à teoria sua aplicação, para expor o aluno a uma situação real muitas vezes centrada no contexto da profissão que ele irá exercer. De modo semelhante, Luo et al. (2018) consideram que o método baseado em casos melhora a qualidade da instrução *on-line* autodirigida e prepara os alunos para o que encontrarão em suas profissões.

A forma, teórica ou prática, como as habilidades, atitudes e conhecimentos em computação são inicialmente desenvolvidos desempenha um papel importante no grau em que podem ser utilizadas em outros contextos. Logo, se forem aprendidos em um contexto prático, poderão ser usados mais facilmente em experiências

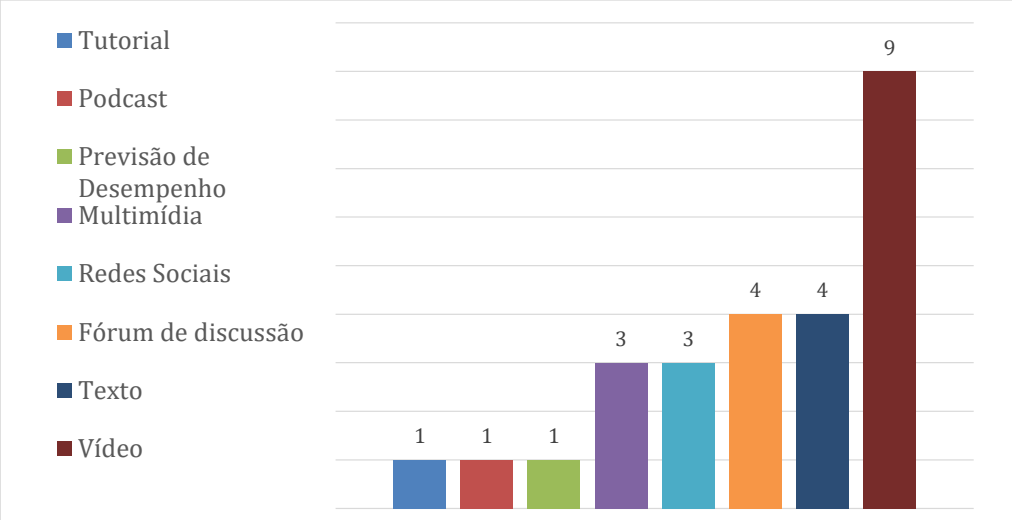
similares, o que é especialmente importante na educação profissional (REEVES, 1994). Nesse sentido, a educação em computação deve estar situada em contextos significativos, interessantes, orientados para problemas e desafiador.

Para Feng e Qu (2018), o estudo de caso é capaz de estimular o entusiasmo dos alunos e testar sua capacidade. Esses autores destacam três principais finalidades para utilizar estudos de caso: aplicar exemplos; praticar a análise e ação e estimular a reflexão pessoal, sendo que, em qualquer uma delas e independentemente de seu propósito, um caso de qualidade deve incluir um contexto complexo, pontos de vista diferentes, uma teia de decisões e um tema amplo. O aluno é orientado a analisar, interpretar e discernir elementos chave, coletar e processar dados de diferentes fontes a fim de formular soluções para o caso.

Algumas implementações de MOOCs podem levar o aluno a acreditar que o acesso ao instrutor ou ao grupo ao qual pertence é difícil, sendo essa ausência de interação e *feedback* uma grande barreira enfrentada na EAD. Em contraponto, Rasi e Vuojärvi (2018) orientam que a estratégia do *feedback* significativo deve propiciar informações sobre a compreensão ou desempenho de alguém, sendo um dos meios mais poderosos de capacitar e melhorar o desempenho dos alunos. Consideram ainda que, num mundo digitalizado, as práticas de *feedback* devem promover conectividade e flexibilidade, sendo que uma aplicação promissora utiliza dispositivos móveis com *feedback* em áudio, que, se comparado ao baseado em texto, é mais fácil de entender e mais pessoal, conseguindo mediar mais informações e transmitir mais nuances e emoções.

A relação dos instrumentos, ou ferramentas, identificados como recursos importantes para subsidiar a educação nos MOOCs pode ser vista no gráfico 3, seguinte.

Gráfico 3 – Instrumentos



Fonte: Elaborado pelo autor.

Como mostra o gráfico 3, categoria mais destacada é a dos vídeos, que inclui aulas gravadas, pequenas palestras, apresentação de *slides* com narração, gravações da fala de instrutores, quadro de animações, além de gravação de apresentações com lousa mágica. Wachtler et al. (2016) apontam que o vídeo é uma das mídias digitais mais utilizadas na internet, sendo que um estudo realizado por Feng e Qu (2018) mostra que a taxa de aceitação desse recurso por estudantes chega a 75%, ou seja, trata-se do mais popular entre os universitários.

Alguns fatores, porém, pesam negativamente quanto ao recurso de vídeo. Feng e Qu (2018) ressaltam que, por falta de tempo, esse instrumento nem sempre é utilizado no currículo regular, enquanto Wachtler et al. (2016) chamam atenção para o estado de passividade que alguns alunos experimentam ao assistir um vídeo, havendo, entretanto, iniciativas que prometem fornecer maior interação nesse processo. Um exemplo são ferramentas como *zaption, edpuzzele* e *teded*, capazes de acrescentar caixas de diálogo, perguntas e testes de múltipla escolha, para que a comunicação flua em ambas as direções do vídeo. Os autores apontam para necessidade de considerar intervalos e maneiras adequadas de incluir essas interações.

No que diz respeito às características dos vídeos, estudos realizados por Herala et al. (2017) sugerem que, em MOOC, a duração deve ser menos de dez minutos. Já em mídia para celular, o vídeo deve durar menos de cinco minutos. Em caso de sala de aula invertida, no entanto, a recomendação é que essa duração se

estenda de quinze a trinta minutos. Koppelman (2016) considera também importante mostrar a face humana, pois proporciona uma sensação mais pessoal, ou seja, os alunos devem sentir que aquilo foi personalizado e produzido para eles, de preferência num ambiente informal, onde o instrutor pode fazer um bom contato visual. Caso sejam utilizados slides, as lâminas devem ser exibidas adicionando-se ênfase ao se mostrarem os slides.

É possível disponibilizar os vídeos em plataformas como *Youtube* ou *Vimeo.* Também alguns ambientes virtuais de aprendizagem educacionais, como o *Moodle,* hospedam gravações, que ficam à disposição do estudante. Importante ressaltar que fatores como disponibilidade e acessibilidade nos vídeos são mais importantes para o aluno do que a alta qualidade na imagem (HERALA et al., 2017). Nesse sentido, nota-se também que os alunos gostam de estudar com diferentes tipos de mídia, pois, para eles, isso torna mais fácil lembrar e compreender, visto que mantêm a atenção focada. O fato de poder escolher o local e momento adequados para assistir ao vídeo proporciona comodidade e flexibilidade no gerenciamento do tempo. (KOPPELMAN, 2016)

Sobre a utilização de texto, Wu (2017) afirma que se trata do material mais fácil de ser obtido, sendo extremamente confortável e conveniente para os alunos, pelo hábito de utilizá-lo. Além disso, Toven-Lindsey, Rhoads e Lozano (2015), Ziegenfuss e Furse (2015) e Ramnanan e Pound (2017) afirmam que podem ser disponibilizados diversos tipos de arquivos no formato de texto: *ebooks*, cartilhas, artigos de pesquisa, materiais de leitura complementar.

Na visão de Toven-Lindsey, Rhoads e Lozano (2015), a utilização da multimídia pode ajudar a explicar conceitos do currículo com imagens digitais interativas, animações, avatar, já que os alunos são mais propensos a lembrar do conteúdo exposto em imagens e vídeos do que apenas no texto escrito. A multimídia é, assim, eficaz para comunicar conceitos difíceis de maneira simples, ativando vários sentidos, aprimorando as experiências de aprendizagem, reforçando conceitos de maneira dinâmica (AUH; SIM, 2018)

O fórum de discussão *on-line*, segundo Toven-Lindsey, Rhoads e Lozano (2015), é uma ferramenta pedagógica utilizada com bastante frequência, demonstrando ser um recurso valioso. Apesar de ser usada ativamente por poucos estudantes, incentiva a interação entre os alunos em tempo real e permite consultar *posts* antigos de acordo com o tema de interesse.

No fórum, alguns instrutores postam dúvidas ou questões abertas para estimular o diálogo, com a intenção de estimular uma colaboração significativa na construção do conhecimento orientada para o grupo. De acordo com Wu (2017), professores podem selecionar pontos importantes no fórum e explicá-los em detalhes, porém o autor considera que a utilização de grupos de *webchats* é mais eficiente, por serem mais populares entre os jovens.

Os *podcasts* e os tutoriais são adequados para autoaprendizagem. Segundo Eranki e Moudgalya (2016), o tutorial estimula o estudante a reproduzir a ação demonstrada, caracterizando um método de ensino ativo em que o ritmo conveniente permite reflexão e revisão, bem como aplicação de conceitos complexos que nem sempre são possíveis no ensino síncrono tradicional.

Na experiência de Hussain et al. (2018), a previsão de desempenho utilizou redes neurais artificiais (RNA) e máquinas de vetor de suporte (SVMs) para treinar algoritmos com aprendizagem de máquina e prever as dificuldades que os estudantes irão encontrar em uma sessão posterior do curso. O objetivo foi identificar os alunos que precisavam de ajuda adicional e atuar numa intervenção a fim de satisfazer essas necessidades de aprendizado.

As redes sociais utilizadas no contexto da educação têm ênfase em aprender e incorporar mecanismos para compartilhar o que é aprendido, sendo os grupos formados por pessoas que têm interesses em comum, interação essa de fundamental importância para a construção do conhecimento. Auh e Sim (2018) consideram alguns requisitos para que as redes sociais alcancem abrangência educacional: liderança entre um grupo disperso, trabalho em equipe, credibilidade dos participantes responsáveis e proatividade na busca por conhecimento.

Essa tendência nova de utilizar aplicativos de redes sociais, como *whatsapp, viber* e *telegrama,* abriu novas oportunidades interativas entre alunos e professores, pois essas tecnologias facilitam a interação e o livre compartilhamento de ideias. É também comum se utilizar uma linguagem popular nesses contextos, o que deixa os alunos ainda mais à vontade, evitando-se a ansiedade causada pelo contato visual. Por isso a interação por meio de redes sociais é considerada totalmente diferente, inovadora e capaz de estabelecer relações fortes entre aluno/aluno e aluno/professor (MELLATI; KHADEMI; ABOLHASSANI, 2017).

A quadro 3 mostra os trabalhos que comprovam êxito nos processos de ensino e aprendizagem os quais, em sua maioria, adotaram métodos de verificação que

realizaram testes de desempenho com turmas tradicionais e piloto, nas quais foi aplicada a abordagem, estratégia ou instrumento estudado. Ao final da experiência, foi realizado um comparativo de desempenho entre as duas turmas com o objetivo de se chegarem a conclusões relativas às estratégias utilizadas.

Para comprovar o êxito das estratégias aplicadas e representadas no quadro 3, foram utilizadas entrevistas, coleta de *feedback* de alunos e professores, bem como comparativo de taxas de conclusão, para se mensurar a efetividade da aplicação adotada.

Quadro 3 - Trabalhos que relataram êxito (continua)

Título do artigo	**Citação**	**Abordagem/ estratégia/ instrumentos**	**Alia teoria e prática?**
A study on SPOC assisted college oral English teaching strategies.	Wu (2017)	Mooc, texto, vídeos, fórum de discussões, slides, palestras.	Sim
Advances in medical education and practice: student perceptions of the flipped classroom.	Ramnanan e Pound (2017)	Ensino híbrido, palestras, slides com narração, texto, estudo de caso	Sim
An analysis of the use and effect of questions in interactive learning-videos.	Wachtler et al. (2016)	Vídeo	Não
Application of hybrid teaching method using the MOOC and verification of its effectiveness.	Lee e Pak (2018)	Ensino híbrido, palestras, estudo de caso, fórum de discussão	Sim
Applying case-based method in designing self-directed on-line instruction: a formative research study	Luo et al. (2018)	Método baseado em casos; multimídia, vídeo, áudio, imagens, animação, avatar	Sim
Archaeology and the Mooc: Massive, open, on-line, and opportunistic	Durusu-tanriöver (2015)	Vídeo, estudo de caso, fórum de discussão	Não
Comparing the effectiveness of self-learning Java workshops with traditional classrooms	Eranki e Moudgalya (2016)	Tutorial falado	Sim
Creative interaction in social networks: Multi-synchronous language learning environments	Mellati, Khademi e Abolhassani (2018)	Redes sociais	Não
Experiences with using videos in distance education: a pilot study: a course on human-computer interaction.	Koppelman (2016)	Vídeos, estudo de caso	Sim
Opening up collaboration and partnership possibilities	Ziegenfuss e Furse (2015)	Mooc, híbrido, texto, vídeos *on-line*, encontros face-a-face e palestras.	Sim

Título do artigo	Citação	Abordagem/ estratégia/ instrumentos	Alia teoria e prática?
Toward personal and emotional connectivity in mobile higher education through has ynchronous formative audio feedback.	Rasi e Vuojärvi (2018)	*Feedback* significativo, fórum de discussão, redes sociais	Sim
Web GIS and Geospatial Technologies for Landscape Education on Personalized Learning Contexts	Torres, González e Yago (2017)	Ensino híbrido, vídeo, redes sociais, *feedback* significativo	Sim

Fonte: Elaborado pelo autor.

Na opinião de Freitas e Paredes (2018), para que a aprendizagem seja efetiva, as lições devem misturar teoria e prática, a fim de levar para a sala de aula uma realidade que pode ser encontrada mais tarde no ambiente de trabalho, como é possível comprovar nos estudos identificados no quadro 3. Notamos que a grande maioria dos estudos que comprovaram êxito no processo de ensino/aprendizagem procuraram aliar teoria e prática.

Além disso, no quadro 3, fica claro que a utilização de várias abordagens, estratégias e instrumentos colabora para o bom desempenho dos alunos. Nesse sentido, Koppelman (2016) corrobora a opinião de Freitas e Paredes (2018). ao afirmar que os alunos gostam de estudar com diferentes tipos de mídia (vídeos, apresentações e imagens, animações). Wu (2017) complementa que o suporte das redes sociais pode oferecer muito por agregar na interação entre professores e alunos.

2.6 Avaliações

A avaliação educacional pode ocorrer em várias fases do processo formativo, podendo assumir intenções e objetivos distintos. Para Abreu (2011), no ato de avaliar, buscam-se captar maiores informações sobre a realidade da aprendizagem, a fim de estabelecer melhores formas de atingir resultados no contexto de ensino e aprendizagem. Nesse sentido, o educador deve estar sempre ajustando uma definição clara e estruturada dos objetivos instrucionais, considerando a aquisição de conhecimento e de competências adequados ao perfil profissional a ser formado, o que irá direcionar o processo de ensino para a escolha das melhores estratégias. (FERRAZ; BELHOT, 2010).

Ao se considerar a avaliação não só como um processo somativo e classificatório, mas na perspectiva da análise de informações dos alunos com o objetivo de melhorar o aprendizado, muito pode contribuir a taxonomia de Bloom. De acordo com Ferraz e Belhot (2010), essa taxonomia oferece uma base para o desenvolvimento de instrumentos de avaliação e utilização de estratégias diferenciadas para avaliar e estimular o desempenho dos alunos em diferentes níveis de aquisição de conhecimento.

Uma convenção da Associação Norte Americana de Psicologia (APA), ocorrida no ano de 1948, em Boston, reuniu psicólogos interessados em elaborar uma metodologia para sistematizar melhor o processo de avaliação, sendo que a forma mais adequada para realizar tal tarefa foi a elaboração de um sistema de classificação de objetivos que se tornasse ponto de partida e base para o planejamento educacional (TREVISAN; AMARAL, 2016).

Com a liderança de Benjamin S. Bloom, foi formado um grupo de trabalho que elaborou uma estrutura de organização hierárquica de objetivos educacionais baseada em três domínios: i) cognitivo - desenvolvimento intelectual de habilidades e atitudes; ii) afetivo - desenvolvimento da área emocional e afetiva; iii) psicomotor - desenvolvimento de habilidades físicas. Atente-se que, apesar de esses três domínios terem sido amplamente discutidos e divulgados, o domínio cognitivo é mais conhecido e utilizado, sendo a partir dele que muitos educadores definem planejamentos educacionais, objetivos, estratégias e sistemas de avaliação (FERRAZ; BELHOT, 2010).

A construção de habilidades e conhecimentos abordados no domínio cognitivo é definida em objetivos instrucionais, que, por sua vez, retratam o desempenho que os educadores gostariam de desenvolver nos educandos. Nesse sentido, esse processo é baseado em níveis hierárquicos de complexidade crescente, do mais simples para o mais complexo, ou seja, para adquirir uma nova habilidade pertencente ao próximo nível, o aluno deve ter dominado e adquirido a habilidade do nível anterior. Sendo assim, a taxonomia de Bloom não é apenas um esquema para classificação, mas “Uma possibilidade de organização hierárquica dos processos cognitivos de acordo com níveis de complexidade e objetivos do desenvolvimento cognitivo desejado e planejado” (FERRAZ; BELHOT, 2010, p. 424). As categorias originais definidas no domínio cognitivo são conhecimento, compreensão, aplicação, análise, síntese e avaliação.

Em outra ocasião, no ano de 2001, foi publicada por Lorin Anderson uma revisão da taxonomia na qual foram combinados o tipo de conhecimento a ser adquirido e o processo utilizado para a aquisição desse conhecimento. As categorias também foram então renomeadas e passaram a ser descritas pelos seguintes verbos: lembrar, entender, aplicar, analisar, avaliar e criar. Sendo assim, as categorias são relacionadas com ações (verbos) que irão auxiliar na classificação das questões da avaliação em um dos níveis da taxonomia. (TREVISAN; AMARAL, 2016).

Tratando mais especificamente dos instrumentos de avaliação da aprendizagem, nos cursos *on-line*, é muito comum se utilizarem testes de múltipla escolha. Segundo Cilesiz (2014), é insuficiente e arbitrário usar apenas esse método para verificação de aprendizagem, visto que os alunos precisam experimentar formas variadas de avaliação, a fim de que seja possível se obter uma visão fundamentada do desempenho deles.

É possível identificar vários formatos de avaliação utilizados nos cursos MOOC, tais como preencher campo vazio – os alunos preenchem a resposta num campo vazio; resposta curta – capta a resposta do aluno e exibe a resposta padrão para que seja possível fazer comparações; autoteste – que exibe automaticamente o resultado do teste, fornecendo explicações sobre respostas erradas; verdadeiro ou falso (ALCOCK; DUFTON; DURUSU-TANRIÖVER, 2015, TOVEN-LINDSEY; RHOADS; LOZANO, 2015, WU, 2017). Alcock, Dufton e Durusu-tanrıöver (2015) complementam afirmando que a variedade de exercícios permite que os alunos se alinhem aos estilos de aprendizagem com que tenham mais afinidade, proporcionando encontrar a forma de expressão mais confortável para cada um.

Quando um MOOC, que trabalha com centenas ou milhares de alunos e prazos dispersos de avaliação, precisa utilizar questões abertas no seu método de avaliação, de acordo com Huisman et al. (2018), a avaliação por pares se mostra uma alternativa válida, confiável e equivalente à avaliação feita por um perito. Nela, outros estudantes (revisores) analisam as respostas, dando *feedback* e realizando a avaliação, o que exige que critérios e padrões claros sejam definidos no curso. Nesse sentido, não só ganha o avaliado, como também o revisor, considerando que este é exposto a outros exemplos de resposta, o que lhe faculta melhorar seu senso de aprendizagem e desempenho.

Ao utilizar os instrumentos de avaliação como uma possibilidade de mensurar o alcance dos objetivos instrucionais definidos pelo educador, considerando as

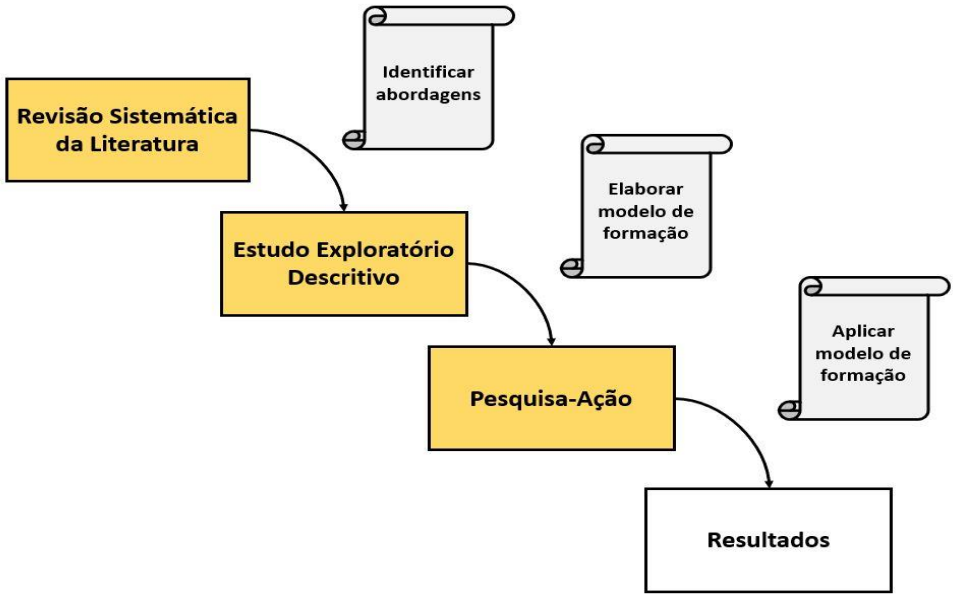
categorias do domínio cognitivo definidas na taxonomia de Bloom e o desenvolvimento de habilidades e conhecimentos, a avaliação pode funcionar como um mecanismo de apoio didático-pedagógico no processo de ensino aprendizagem que busca continuamente a sua melhoria. Nesse sentido, para avaliar o desenvolvimento de habilidades e conhecimentos nos alunos, considerando a aplicação do modelo de formação elaborado nesta pesquisa, foi utilizada a taxonomia de Bloom.

3 METODOLOGIA

A metodologia de pesquisa definida em um projeto científico contribui para evolução do estudo proposto como um meio para se chegar a possíveis soluções de uma situação abordada. De acordo com Minayo (2010), a metodologia inclui a teoria da abordagem (método), os instrumentos de operacionalização (técnicas) e a criatividade do pesquisador para fazer com que o caminho do pensamento chegue na abordagem prática da realidade.

Inicialmente, essa pesquisa realizou uma revisão sistemática da literatura (RSL) para analisar as abordagens, estratégias e instrumentos de ensino/aprendizagem capazes de aliar teoria e prática. Para investigar os sujeitos da pesquisa, a fim de elaborar o modelo de formação, adotou-se um estudo exploratório e descritivo de caráter qualitativo e quantitativo, o mesmo está disponível em formato de produto educacional na plataforma Educapes pelo Link: http://educapes.capes.gov.br/handle/capes/567384. Já na implementação desse modelo de formação voltado para temática da segurança da informação, utilizou-se a pesquisa-ação, conforme mostra a figura 2.

Figura 2 - Fases da metodologia



Fonte: Elaborada pelo autor.

Nas sessões subsequentes serão explicitados todos os recursos metodológicos utilizadas nesta pesquisa, tais como: Tipo de estudo (3.1); Sujeitos e cenário de estudo (3.2); Instrumentos de coleta de dados (3.3); Procedimento para análise de dados (3.4) e aspectos éticos envolvidos na pesquisa.

3.1 Tipo de estudo

O modelo de revisão sistemática da literatura (RSL) proposto por Kitchenham e Charters (2007) foi utilizado com a finalidade de investigar os estudos primários que abordam a aplicação dos cursos *on-line* abertos e massivos. Com isso, foi possível identificar as principais abordagens, estratégias e metodologias de ensino/aprendizagem empregadas, especialmente as que demonstraram efetividade e que conseguiram aliar teoria e prática.

A RSL adota um caminho metodológico bem definido, envolvendo três fases principais: planejamento da revisão, condução da revisão e publicação dos resultados. Sendo assim, evidencia as contribuições relativas a um assunto ou fenômeno de forma imparcial e repetível, analisando determinadas questões de pesquisa (KITCHENHAM; CHARTERS, 2007). De acordo com Falbo (2017), o protocolo da RSL é fundamental, pois especifica as questões de pesquisa, a estratégia que será utilizada para conduzir a RSL, os critérios para a seleção dos estudos, bem como os dados que serão extraídos e sintetizados.

Considerando o exposto, na fase de planejamento da RSL foi definido como objetivo analisar as estratégias de ensino que conseguem aliar teoria e prática nos cursos *on-line* abertos e massivos (MOOC). As questões de pesquisa estão descritas no quadro 4; os critérios de inclusão, no quadro 5; os de exclusão, no quadro 6, e a classificação de qualidade, no quadro 7.

As bases de dados utilizadas foram Science Direct, IEE Explorer, ACM, Scopus e Springer, devido à importância e abrangência que possuem na área estudada.

Quadro 4 - Questões de pesquisa

Questões de Pesquisa		**Motivações**
QP1	Quais abordagens, estratégias ou instrumentos de ensino aprendizagem têm sido utilizados nos MOOCs?	Familiarizar-se com as abordagens, estratégias ou instrumentos utilizados nos MOOCs.

QP2	Quais abordagens, estratégias ou instrumentos têm alcançado êxito no processo de ensino aprendizagem?	Escolher as abordagens, estratégias ou instrumentos de acordo com o resultado.
QP2	Quais abordagens de ensino e aprendizagem conseguem aliar teoria e prática em cursos ofertados por ambientes *on-line*?	Direcionar a abordagem para uma perspectiva prática.

Fonte: Elaborado pelo autor.

Conforme é possível observar no quadro 5, consideraram-se como critérios de inclusão artigos completos e publicados, ou seja, trabalhos com base científica comprovada. Os idiomas português e espanhol incluídos serviram para abranger estudos regionais, além do inglês, que é considerado por muitos autores a língua franca da ciência mundial. Buscou-se identificar, nos trabalhos analisados, as abordagens, estratégias ou instrumentos utilizados nos MOOCs.

Quadro 5 – Critérios de inclusão

Critérios de inclusão	
I1	Artigos completos publicados em periódicos ou anais.
I2	Textos escritos em português, espanhol ou inglês.
I3	Trabalhos que apliquem abordagens, estratégias ou instrumentos de ensino por meio de MOOC.

Fonte: Elaborado pelo autor.

Foram excluídos do escopo deste estudo trabalhos incompletos e que não foram publicados, devido ao fato de não ser possível garantir o rigor científico de um trabalho que não foi publicado (quadro 6). Além disso, , em um trabalho incompleto, não se podem analisar com profundidade os aspectos abordados. Da mesma forma, foram excluídos artigos que não aplicaram abordagem, estratégias ou instrumentos, visto que o resultado dessa aplicação necessitaria ser analisado, em função dos objetivos propostos.

Quadro 6 – Critérios de exclusão

Critérios de exclusão	
E1	Artigos incompletos.
E2	Trabalhos que não foram publicados em periódicos ou anais.
E3	Trabalhos que não apliquem alguma abordagem, estratégias ou instrumentos de ensino.

Fonte: Elaborado pelo autor.

Os critérios de qualidade serviram para classificar os estudos no tocante aos objetivos da RSL, visto que os critérios de inclusão e exclusão já fazem uma seleção

dos artigos. Nesse sentido, a classificação proposta varia de baixa para alta conforme se aproximam das abordagens que conseguem aliar teoria e prática nos MOOCs.

Quadro 7 – Classificação de qualidade

Níveis de qualidade	Descrição
Alta	Abordagens que conseguem aliar teoria e prática em MOOC.
Média	Abordagens de ensino aplicadas em MOOC.
Baixa	Abordagens de ensino aplicadas em ambientes *on-line*.

Fonte: Elaborado pelo autor.

O método de busca utilizado foi a busca automática no portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), com a utilização da combinação de *strings,* conforme descrito no quadro 8. Importante ressaltar que a mesma foi previamente avaliada com o teste piloto e aplicada com perfil de assinante. Posteriormente, na fase de condução, foram identificados os estudos com base nos critérios de seleção, sendo os dados extraídos, analisados e sintetizados a fim de se descreverem e divulgarem os resultados.

Quadro 8 – Combinação das *strings* de busca

1ª ordem	2ª ordem	3ª ordem	***Strings* de busca**
“open and massive on-line course” ”MOOC”	"teaching strategy" "teaching approach" "teaching method" "teaching process" "teaching technique"	"case-based learning" "case-based instruction" "case study" “theory and practice”	(“Open and massive on-line course” OR ”MOOC”) AND ("Teaching strategy" OR "teaching approach" OR "teaching method" OR "teaching process" OR "teaching technique") AND ("Case-based learning" OR "Case-based instruction" OR "case study" OR “theory and practice”)

Fonte: Elaborado pelo autor.

Na fase de elaboração do modelo de formação, no que diz respeito à investigação do perfil e das opiniões dos sujeitos da pesquisa, foi utilizada uma abordagem qualitativa e quantitativa, de caráter exploratório e descritivo, a fim de se alcançarem os objetivos deste estudo. As visões metodológicas qualitativas e quantitativas, no decorrer da história, trouxeram norte pesquisa científica e são correntes pragmáticas baseadas essencialmente no realismo/objetivismo (quantitativa) e no idealismo/subjetivismo, usadas pela metodologia qualitativa (QUEIROZ, 2006).

A pesquisa exploratória e descritiva utiliza uma série de informações sobre o objeto de estudo retiradas da realidade vivenciada por determinada população ou de determinado fenômeno (VERGARA, 2012). Assim, podemos entender também o método da pesquisa qualitativa de acordo com uma perspectiva exploratória e descritiva, que visa interpretar uma realidade sociocultural, levando em conta valores da subjetividade e da variabilidade do comportamento.

A pesquisa qualitativa responde a questões muito particulares, se preocupando, nas ciências sociais, com um nível de realidade que não pode ser quantificado, ou seja, trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um universo mais profundo das relações dos processos e dos fenômenos que não podem ser reduzidos a simples operacionalização de variáveis (MINAYO, 2004).

O intuito da abordagem qualitativa nesta pesquisa se justifica pela necessidade de abstração interpretativa no estudo das percepções individuais e coletivas que não leva em conta somente generalizações e estatísticas, mas também a compreensão das singularidades e dos significados de acordo com as condições apresentadas pelos entrevistados.

Em consonância com o método qualitativo, utilizamos também uma abordagem que visou mensurar e classificar as opiniões de acordo com um cenário que considera a quantificação de amostras comparáveis entre si: a abordagem quantitativa. Assim, a partir do pressuposto de que as amostragens representam um dado contexto similar, é comum, na metodologia quantitativa, a utilização de questões fechadas que permitem aos entrevistados darem uma opinião mais específica e direcionada ao tema estudado. Segundo Oliveira (2001), para quantificar opiniões coletadas, o método quantitativo pode utilizar técnicas estatísticas, como porcentagem, média, desvio padrão, coeficiente de correlação.

Após a elaboração do modelo de formação *on-line* aberto e massivo, considerando a investigação das problemáticas envolvidas, a definição da abordagem usada no curso, sua construção, carga horária, mídias, conteúdos, entre outras questões, optou-se por uma abordagem de pesquisa-ação na fase de implantação do pMOOC Segurança da informação: aliando teoria e prática, construído a partir do modelo de formação desenvolvido nesta pesquisa.

A pesquisa-ação, segundo Tripp (2005), é participativa à medida que inclui os que, de um modo ou outro, estão envolvidos nela e é colaborativa em seu modo de

trabalhar. Franco (2005), corrobora a visão 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 concepção da pesquisa ação, o pesquisador assume dois papéis: de pesquisador e de participante, gerenciando os ciclos de planejamento de uma ação, implementação, monitoramento e avaliação de sua eficácia, caminhando na direção da transformação da realidade objetivada (FRANCO, 2005). Nesse sentido, os professores e alunos do curso EMITI do Instituto Federal do Sertão Pernambucano - *Campus* Salgueiro, foram convidados a contribuir na elaboração do modelo de formação. Para tal, foram aplicados questionários e realizadas entrevistas com grupos focais (professores e alunos) para discutir e avaliar os requisitos e elementos presentes no modelo de formação proposto nesta pesquisa.

A pesquisa-ação foi escolhida neste estudo pois investiga uma situação social concreta, visando à melhoria de determinada conjuntura, com a resolução dos problemas ou produção de conhecimentos, contemplando a união sinérgica entre pesquisa e ação. Além disso, essa pesquisa utiliza princípios do *design* participativo (ou pesquisa-ação participativa) no qual os sujeitos envolvidos participam ativamente do processo de escolha das metodologias, organização, materiais, conceitos abordados e *design* da ferramenta educacional a ser elaborada (SANTA-ROSA; STRUCHINER, 2011).

Sendo assim, após levantamento bibliográfico feito na RSL, foram identificados caminhos, práticas e metodologias que, por sua vez, foram discutidos com os envolvidos para que se chegasse a uma definição das diretrizes e ações a serem realizadas no processo de elaboração do modelo de formação definido nesta pesquisa.

Foi feito o dimensionamento do cenário estudado a partir da coleta, análise e representação estatística dos dados levantados. Assim, puderam ser realizados agrupamentos, observação de variáveis de estudo, procedimentos matemáticos, utilização de gráficos e números com o objetivo de mensurar as opiniões coletadas.

Ao analisar a quantificação, categorização e cruzamento dos dados, foi possível também tirar conclusões que incorrem em significado de caráter qualitativo, fazendo com que haja convergência entre os métodos usados nesta pesquisa. Pretendeu-se assim agregar as vantagens das metodologias qualitativa e quantitativa

no estudo, de forma a entender as opiniões dos informantes, subsidiando a construção deste trabalho.

3.2 Sujeitos e cenário de estudo

Trentini e Paim (2004 p. 73 e 74) definem o cenário do estudo, "[...] como aquele onde ocorrem as relações sociais inerentes ao propósito da pesquisa [...]". Portanto, o espaço físico é aquele onde foi identificado o problema a ser solucionado ou as mudanças a serem feitas". Nesse contexto, a pesquisa ocorreu no Instituto Federal do Sertão Pernambucano - *Campus* Salgueiro.

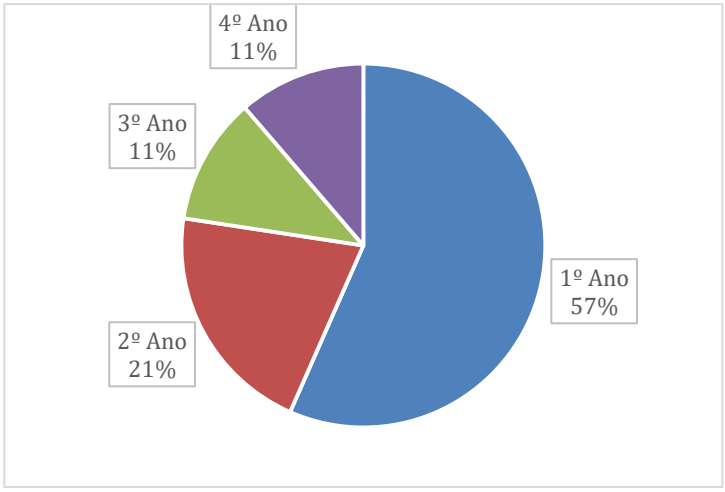
Considerando que o estudo se refere a questões intimamente ligadas ao contexto dos alunos, os sujeitos da pesquisa não poderiam deixar de ser eles mesmos. Foi, pois, delimitado como público os alunos dos cursos do EMITI. Ainda, considerando a importância dos professores de informática no processo formativo, eles também foram incluídos nas entrevistas.

Para elaboração do modelo de formação, foram aplicados questionários com 53 alunos do EMITI. Além disso, nas reuniões da pesquisa ação, foram realizadas entrevistas com dois grupos focais: 12 alunos do 4º ano e 3 professores de informática que ministram ou já ministraram a disciplina Segurança da Informação. Já que o estudo foi condicionado a investigar a aplicação do modelo de formação ligado à área segurança da informação foram excluídos como sujeitos da pesquisa alunos e professores de outras áreas.

A amostra contou com 79,2% de alunos do sexo masculino e 20,8% do sexo feminino. As idades variaram entre 15 a 23 anos, sendo que a média ponderada das idades, considerando a quantidade de alunos, foi de 16 anos.

O gráfico 4, a seguir, mostra o ano que os alunos estavam cursando no período da elaboração e aplicação do modelo de formação.

Gráfico 4 - Ano cursado pelos alunos



Fonte: Elaborado pelo autor.

3.3 Instrumentos de coleta de dados

Antes da elaboração do modelo de formação, os alunos EMITI no Instituto Federal do Sertão Pernambucano - *Campus* Salgueiro responderam a um questionário *on-line* (Apêndice D), cujo objetivo foi analisar o perfil dos alunos, incluindo idade, dedicação e disciplina nos estudos, disponibilidade de tempo e acesso a recursos tecnológicos, além de percepções sobre o ensino a distância e a disciplina Segurança da Informação.

Na fase de elaboração da proposta de formação, as contribuições dos envolvidos foram captadas por meio de entrevistas semiestruturadas, que, segundo Richardson et al. (2014), são técnicas importantes que permitem o desenvolvimento de uma estreita relação entre as pessoas e visam obter do participante o que ele considera aspectos mais relevantes em uma situação de estudo.

As entrevistas foram do tipo reuniões com grupo focal, que, segundo Dias (2000), é realizado com até doze participantes e um moderador (que elabora uma lista de questões para discussão, compondo um guia de entrevista). Objetiva identificar percepções, sentimentos, atitudes e ideias relativos a determinado assunto, produto ou atividade, com o pesquisador assumindo a função de moderador nas entrevistas.

O processo de aplicação dos questionários e entrevistas ocorreu da seguinte maneira: após recolhimento dos termos de autorização (Apêndices A, B e C), os alunos e professores que concordaram em participar da pesquisa e [os alunos] que

tiveram autorização dos pais ou responsáveis foram convidados a responder ao questionário *on-line* e às entrevistas no laboratório de informática da instituição.

As entrevistas foram gravadas em áudio e transcritas textualmente. As discussões, avaliações, decisões e encaminhamentos feitos pelo grupo na pesquisa ação foram feitos considerando os objetivos, motivações e referencial teórico levantados. Também foram consideradas as opiniões de todos os alunos que responderam ao questionário perfil do aluno (Apêndice D).

Antes de iniciarem o curso no formato de MOOC, os alunos foram submetidos a um pré-teste (Apêndice E), o qual teve como objetivo investigar o nível do conhecimento na temática abordada (segurança da informação). Nesse sentido, após terem experimentado a formação proposta, responderam o mesmo questionário no formato de prova final, ou pós-teste (Apêndice E).

Também foram utilizadas, para efeito de interpretação do desempenho do aluno, a participação no grupo de interação e nas atividades propostas. Após a conclusão da capacitação, os alunos responderam a um questionário de satisfação (Apêndice J) que avaliou suas experiências no curso, em diversas perspectivas tais como: material didático, conteúdo e interatividade.

Todos os instrumentos utilizados na coleta de dados estão disponíveis nos apêndices desta dissertação.

3.4 Análise dos dados

A análise de conteúdo foi utilizada para preparar as informações coletadas, categorizá-las, descrever os resultados encontrados e interpretá-los. De acordo com Moraes (1999), a análise de conteúdo pode ser usada para descrever e interpretar o conteúdo de toda classe de documentos e textos, conduzindo a descrições sistemáticas qualitativas e quantitativas. Desse modo, foi necessário tabulação em números e gráficos, além de se fazer a classificação em categorias a fim de se compreender o que os dados representam. A análise de dados então, pode ser compreendida como o processo pelo qual se dá ordem, estrutura e significado aos dados coletados, transformando-os em conclusões úteis, fidedignas e dotadas de significado (MOÇAMBIQUE, 2008).

As informações obtidas nos instrumentos de coleta de dados foram transcritas textualmente e, durante a análise, buscou-se entender de maneira aprofundada o

conteúdo das mensagens, expondo-se fidedignamente os documentos apresentados. A perspectiva quantitativa incluiu percentuais, escalas de respostas, utilizando-se tabelas, quadros ou gráficos. A visão qualitativa expressou o conjunto de significados presentes nos dados, captando as motivações, percepções e opiniões reveladas pelos sujeitos, na tentativa de evidenciar as relações existentes entre a teoria estudada, a prática das relações estabelecidas na proposta de formação e outros fatores.

3.5 Aspectos éticos

Foi garantido aos entrevistados, no decorrer da pesquisa, total sigilo, anonimato, privacidade e acesso dos resultados. Também foi observado o previsto na Resolução 196/96, que trata sobre as diretrizes e normas regulamentadoras de pesquisas que envolvam seres humanos (BRASIL, 1996). Nessa Resolução, é exigido que todo o entrevistado comprove seu consentimento na participação da pesquisa, assinando o Termo de Consentimento Livre e Esclarecido - TCLE (Apêndice A). Caso o entrevistado seja menor de idade, concordará com a participação por meio do Termo de Assentimento Livre e Esclarecido (TALE) (Apêndice C), havendo ainda a necessidade de um responsável assinar o TCLE (Apêndice B).

Nesse sentido, antes de aplicar o questionário aos sujeitos, realizou-se uma orientação completa sobre a natureza do trabalho, os objetivos, benefícios, métodos utilizados e possíveis prejuízos que podiam afetar os participantes. Logo após, os sujeitos da pesquisa que aceitaram participar forneceram TCLE assinado.

De acordo com a interpretação do Conselho Nacional de Saúde expressa em sua Resolução 466/12, não existe interação entre seres humanos sem a ocorrência de riscos, mesmo que sejam mínimos (BRASIL, 2012). Nesse sentido, os riscos identificados nesta pesquisa não ameaçavam a integridade física, liberdade ou dignidade dos sujeitos. Por outro lado, aspectos psicológicos, como exposição e constrangimento, foram identificados como possíveis riscos. Afinal, o sujeito da pesquisa pode considerar as informações que está fornecendo como muito pessoais ou se sentir incomodado com determinados questionamentos. Sendo assim, as medidas tomadas para amenizar os riscos de constrangimento e exposição foram as seguintes: garantia do sigilo de todas as informações e o respeito à privacidade, ou

seja, o nome ou qualquer outro dado ou elemento que pudesse, de qualquer forma, identificar o participante foi mantido em sigilo.

Sempre que foi necessário citar algum participante ou suas respostas, utilizou-se um pseudônimo para que não houvesse exposição ou constrangimento. Ademais foi esclarecido aos sujeitos que a participação na pesquisa seria voluntária e que poderiam se recusar a participar, ou retirar seu consentimento a qualquer momento, sem precisar justificar o porquê da saída.

Apesar dos riscos envolvidos e das medidas realizadas para atenuá-los, devem ser levados em consideração os benefícios gerados com esta pesquisa: além de promover uma conscientização acerca do uso seguro do meio digital, foi promovida uma capacitação acerca da temática segurança da informação para os sujeitos da pesquisa. Partindo do princípio de que a educação a distância (EAD) está sendo pouco abordada na Educação Profissional e Tecnológica (EPT), este estudo representa uma experiência com a aplicação de um modelo de formação *on-line* aberta e massiva que servirá como subsídio para comunidade científica na compreensão da efetividade da modalidade de ensino adotada.

4 RESULTADOS E DISCUSSÃO

De acordo como público alvo selecionado no escopo deste estudo, alunos do EMITI do Instituto Federal do Sertão Pernambucano - *Campus* Salgueiro, a elaboração do modelo de formação considerou satisfazer as expectativas educacionais dessa comunidade acadêmica, incluindo as opiniões dos professores e o levantamento feito RSL. Nesse sentido, seguindo as recomendações de Fassbinder, Delamaro e Barbosa (2014), as fases percorridas para construir o MOOC Segurança da Informação – aliando teoria e prática foram as seguintes: análises de necessidades, planejamento, implementação e execução.

Durante a elaboração do MOOC, foram formuladas diversas diretrizes que compõem o modelo de formação, as quais foram subdivididas em três categorias: *perspectiva pedagógica*, que trata sobre questões relativas a abordagens de ensino e a estratégias para desenvolver aprendizagem; *perspectiva contextual*, que descreve requisitos adequados para as necessidades do público em questão, e *perspectiva tecnológica*, que envolve as questões ligadas a tecnologia, mídias e interatividade, conforme os quadros 14, 15 e 16. Assim, essas perspectivas servirão também como subsídio para outras iniciativas de cursos *on-line* abertos e massivos aplicados no EMI ao Técnico.

Para subsidiar a definição das diretrizes estabelecidas no modelo de formação, foi considerado o arcabouço teórico levantado nesta pesquisa, as opiniões dos 53 alunos que cursam entre o 1º e o 4º ano do EMITI, as entrevistas realizadas nas reuniões de pesquisa-ação com professores e alunos do IF SERTÃO-PE - *Campus* Salgueiro, bem como as experiências vivenciadas durante a elaboração e implementação do modelo.

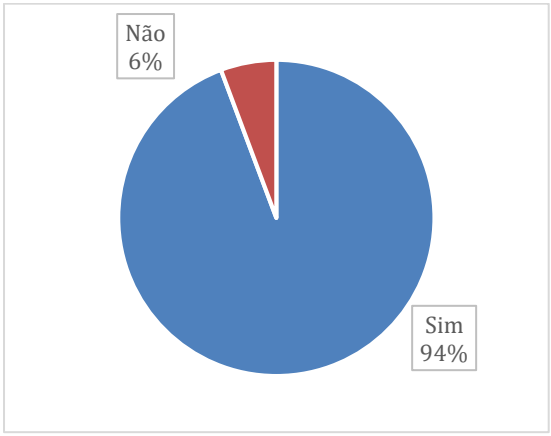
No que diz respeito ao nível de dedicação e disciplina nos estudos, considerando uma escala de 0 a 10, os alunos se autoavaliaram, indicando estar nos níveis 5,9 e 5,3. Essa informação nos revela que os próprios alunos consideram ter um nível baixo de dedicação e disciplina nos estudos. Salienta-se que, para Belloni (2012), a autonomia do estudante é um fator imprescindível para o sucesso do ensino e aprendizagem nos cursos de educação aberta e a distância. Já de acordo com Moore e Kearsley (2008), a capacidade de um aluno desenvolver bem o plano de aprendizado, encontrar recursos para o estudo e decidir sozinho sobre seu progresso deve ser uma preocupação relevante em um sistema de ensino.

Diante dos resultados relativos à autonomia, disciplina e dedicação nos estudos, foram levantadas as primeiras perspectivas contextuais: PC1 – se faz necessário um método de acompanhamento da evolução dos alunos no MOOC – e PC2 – é necessário utilizar estratégias para motivar o aluno a se dedicar ao curso. Afinal de contas, se os alunos afirmam ter um baixo nível de dedicação e disciplina nos estudos, ao se programar em um curso *on-line* onde não existe a figura do professor, se faz necessário um método para acompanhar e motivar os estudantes durante o processo de aprendizagem.

Além da autonomia, dedicação e disciplina, outros fatores importantes a serem considerados foram disponibilidade de tempo e acesso a recursos tecnológicos, como computador e internet. Quanto a tempo livre para estudar, os alunos relataram que teriam em média uma hora disponível diariamente. Por outro lado, quando os professores foram questionados a respeito do tempo que os alunos teriam para se dedicar a um curso *on-line*, considerando as atividades que já realizam na escola, os docentes afirmaram acreditar que os estudantes disporiam de apenas trinta minutos diários.

Os dados apontam que os esses convivem com uma carga elevada de atividades e tarefas escolares, logo, caso o MOOC desenvolvido fosse muito abrangente e extenso, incorrer-se-ia no risco de haver uma sobrecarga de atividades, situação que poderia resultar em evasão dos estudantes. Nesse sentido, formulamos a PC3 – o plano de estudos definido para o curso não deve comprometer mais do que 60 minutos diários do tempo do aluno.

Gráfico 5 - Acesso a TDICs em casa



Fonte: Elaborado pelo autor.

O gráfico 5 mostra a disponibilidade de acesso a TDIC para os alunos no ambiente doméstico, evidenciando que a maioria tem acesso facilitado a computador e internet. Esse dado comprova que o fator acesso a recursos de tecnologia não é um impeditivo para que eles cursem o MOOC. Ressalta-se que os 3 alunos que relataram não ter acesso a TDICs em casas poderiam utilizar o laboratório de informática do *campus*, nos horários em que não estejam ocorrendo em aulas regulares de outras disciplinas. Nesse sentido, formulamos a primeira perspectiva tecnológica: PT1 – é necessário fornecer acesso aos recursos de TDICs e internet do *campus* para possibilitar aos alunos oportunidade de realizarem o curso.

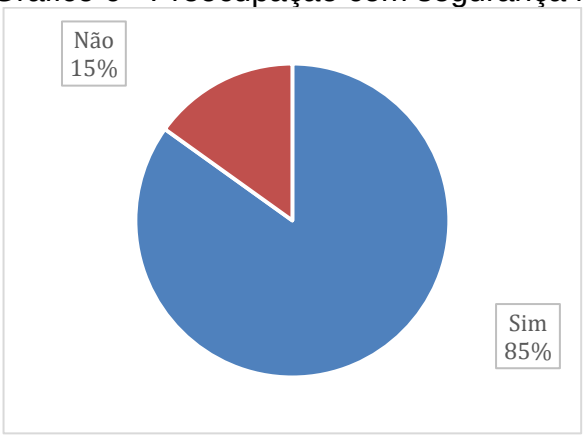
Quanto à finalidade de uso dos recursos de TDICs, de acordo com o público investigado, aproximadamente 50% do tempo em que os alunos estão no computador, *smartphone* ou *tablet* é destinado a estudos. Essa informação nos levou a formular a PT2 – o uso de TDICs é incentivado, visto que os estudantes estão familiarizados com a utilização dessas ferramentas, que se tornam aliadas no processo de ensino e aprendizagem.

No que diz respeito a ferramentas utilizadas para comunicação em grupo com fins educacionais, os alunos relataram quase nunca utilizar fóruns de discussão e *chats* de plataformas, sendo que quase sempre utilizam redes sociais como *whatsapp, telegram* e *facebook* para fins educacionais, o que nos levou à terceira perspectiva tecnológica: PT3 – os alunos não estão familiarizados com fóruns de discussão, mas, por outro lado, é incentivada a utilização de rede social como ferramenta para comunicação em grupo.

4.1 Análise de necessidades

Sobre o interesse no tema segurança da informação, numa escala de 0 a 10, o público investigado indicou 7, ou seja, um alto grau de interesse no tema. Já quando questionados sobre a preocupação com segurança ao utilizar *sites*, aplicativos, *e-mail*, a grande maioria dos entrevistados (85%) demonstrou grande preocupação com isso, conforme mostra o gráfico 6, a seguir.

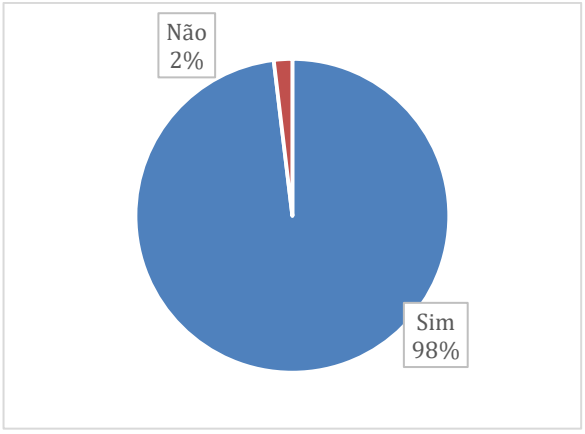
Gráfico 6 - Preocupação com segurança na navegação.



Fonte: Elaborado pelo autor.

No que diz respeito ao nível de conhecimento sobre o tema que consideravam ter, numa escala de 0 a 10, as respostas dos alunos apontaram 4, ou seja, um nível baixo. Em relação à capacidade para se proteger de ataques ou fraudes no meio digital, considerando uma escala de 0 a 10, a resposta dos alunos foi 5. Já quando foram questionados sobre terem fornecido, na internet, dados pessoais, como endereço, telefone e CPF, praticamente todos já o fizeram (98%), conforme se verifica no gráfico 7, a seguir.

Gráfico 7 - Fornecimento de dados pessoais



Fonte: Elaborado pelo autor.

Diante do grande interesse pelo tema, da ampla preocupação com o assunto durante a navegação, da baixa capacidade para se proteger de ataques e complementando com as informações do gráfico 7 (98% dos alunos já forneceram dados pessoais na internet), percebe-se claramente que eles estão vulneráveis a diversos riscos no meio digital.

Depreende-se, pois, que existe a necessidade e expectativa de capacitação em segurança da informação, ou seja, fica comprovada a demanda existente, caracterizando a 1ª fase da criação de um MOOC: análise das necessidades, mesmo nas séries iniciais, como o 1º e 2º anos do EMITI. Com isso, formulamos a PC4 - na elaboração do curso, devem ser levados em consideração aspectos como expectativa de formação e interesse nos temas abordados para MOOC.

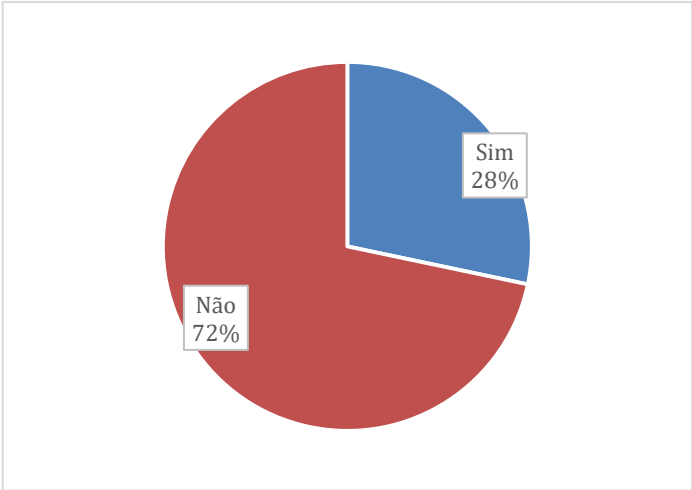
4.2 Planejamento

Uma vez comprovada a necessidade de capacitação na área segurança da informação e seguindo a proposta de desenvolver um modelo de formação *on-line* aberta e massiva capaz de aliar teoria e prática e de promover aprendizado com significado, o planejamento sobre como deveria ser esse modelo de formação considerou as informações levantadas na revisão de literatura, no estudo exploratório descritivo, sendo que, com a pesquisa-ação, foi possível implementar tal modelo. Assim, foi garantida a participação dos alunos e professores no processo de elaboração do MOOC Segurança da Informação – aliando teoria e prática.

As opiniões a respeito de questões como conteúdo a ser abordado; mídias e elementos que estarão presentes; métodos de avaliação; duração e cronograma; metodologia utilizada para aliar teoria e prática, entre outros assuntos, foram captados em entrevistas semiestruturadas realizadas com dois grupos focais: o grupo 1 – professores de informática e grupo 2 – alunos. Além das entrevistas também foram consideradas as opiniões coletadas em um questionário aplicado com todos os alunos de todas as turmas do EMITI do Campus Salgueiro.

Quando os alunos foram questionados sobre já terem feito qualquer tipo de curso a distância, 72% responderam que não, conforme se vê no gráfico 8, a seguir.

Gráfico 8 – Experiência com EAD

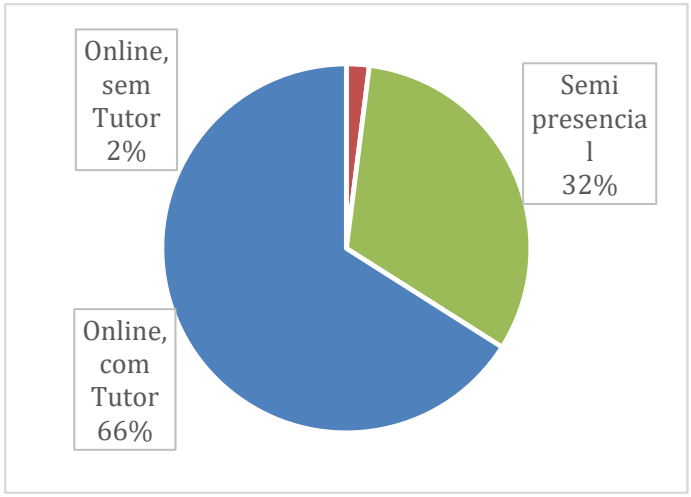


Fonte: Elaborado pelo autor.

Os dados do gráfico 8 revelam que, apesar de os alunos utilizarem amplamente recursos de TDIC e redes sociais com fins educacionais, não estão familiarizados com o formato de EAD. Isso nos levou a concluir que a maioria não estava familiarizada com o formato dos cursos MOOC, logo formulamos a PC5 – os estudantes devem ser familiarizados com o formato do curso. Para tal, além de um momento presencial de apresentação, o MOOC elaborado nesta pesquisa continha um vídeo de boas-vindas que orientou os estudantes sobre o curso e a plataforma utilizada. Complementarmente, formulamos a PT4 – a plataforma utilizada para hospedar o curso deve ter boa usabilidade (fácil e intuitiva para utilizar).

Sobre assistência de um tutor ou professor especialista na área, conforme mostra o gráfico 9, seguinte, a maioria dos alunos (66%) acredita que ela deve ser feita *on-line,* sem a necessidade de encontros presenciais. Já os outros (32,1%) esperam ter encontros presenciais, enquanto apenas um aluno entrevistado acredita que não é necessário tutor/professor, seja presencial ou *on-line*.

Gráfico 9 – Contato com tutor/professor



Fonte: Elaborado pelo autor.

Os dados do gráfico 9 evidenciam que os alunos estão divididos sobre a forma como o tutor/professor deve dar assistência (presencial ou *on-line*) durante o curso, ficando claro que a maioria dos entrevistados (98%) acredita que é necessário haver um tutor/professor. Com isso, pudemos formular as seguintes perspectivas pedagógicas: PP1 – é necessário assistência de um tutor/professor especializado na área para dar assistência aos alunos do curso; PP2 – é necessário assistência do tutor/professor de forma *on-line* – e PP3 – é necessário que o plano de ensino contemple encontros presenciais com professor especializado na área.

No que diz respeito ao conteúdo do curso, para o aluno 13, deve ser abordada uma parte sobre introdução a segurança da informação, considerando a baixa propriedade que os alunos têm do tema. Os três professores entrevistados também chamaram a atenção para a necessidade de se ter uma abordagem introdutória. Com isso, conseguimos formular a perspectivas pedagógica PP4 – é necessário considerar uma abordagem introdutória sobre o conteúdo abordado no curso.

Para que aluno evolua continuamente em seu processo de aprendizagem, os objetivos que norteiam a estruturação do curso, incluindo materiais didáticos, atividades e métodos de avaliação devem seguir uma ordem crescente de complexidade, com base nas habilidades e competências a ser desenvolvidas. Para tal, a taxonomia de Bloom é uma possibilidade para a organização hierárquica dos objetivos de desenvolvimento cognitivo, sendo que as habilidades desenvolvidas aumentam em complexidade dentro das categorias lembrar, entender, aplicar, analisar, sintetizar e criar (FERRAZ; BELHOT, 2010). Com base nisso, formulamos a

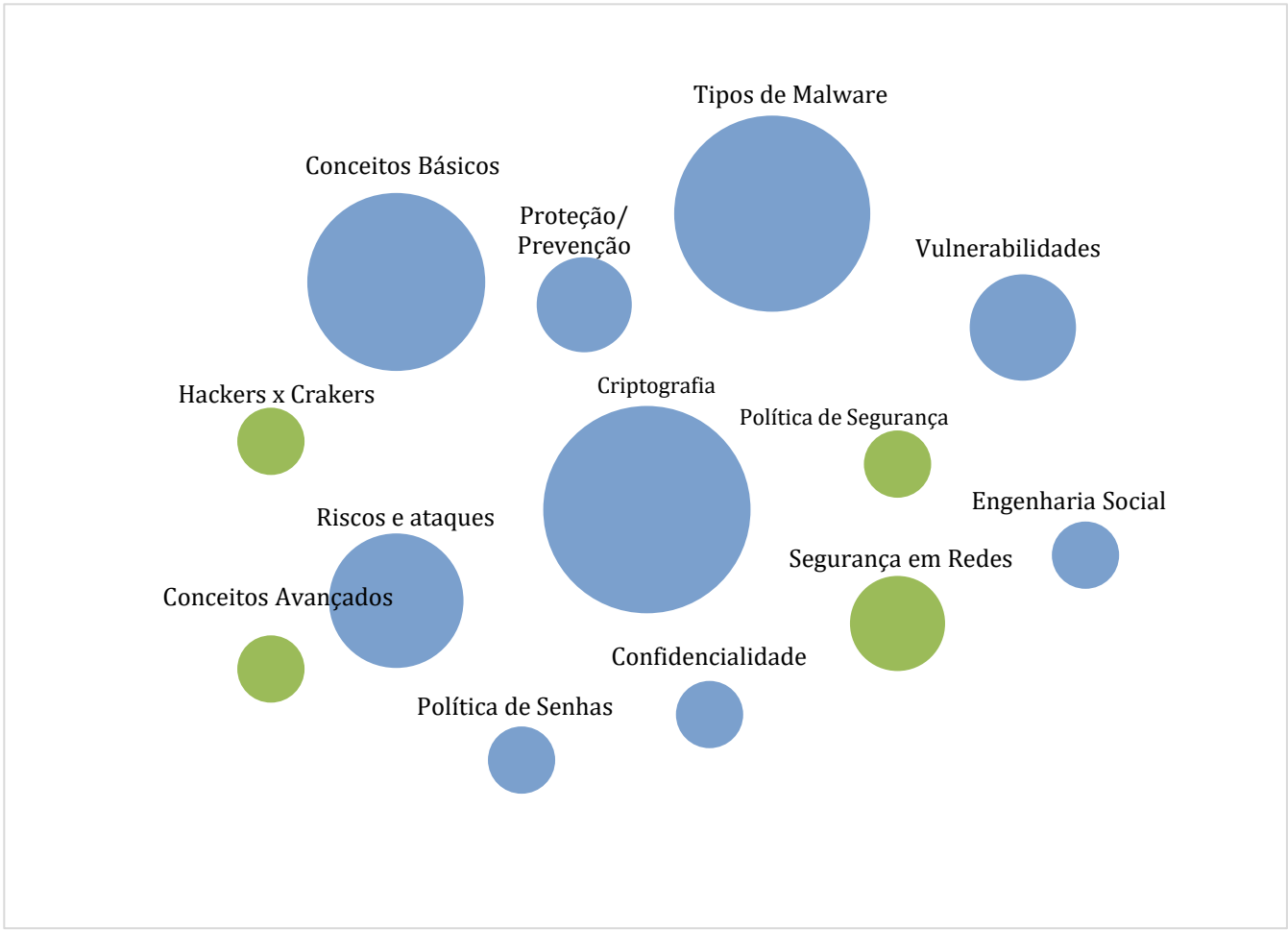
PP5 – os objetivos instrucionais do curso devem seguir uma ordem crescente de complexidade, com base nas categorias estabelecidas pela taxonomia de Bloom.

De acordo com o professor 1, não deve ser adotada uma abordagem avançada do conteúdo, mas sim do nível básico ao intermediário, o que foi corroborado pelo professor 2, o qual afirmou que não ministrava determinados assuntos mais avançados por conta da limitação técnica dos alunos. Com base nesses dados, compreende-se que a abordagem adequada para o conteúdo do curso deve iniciar de forma introdutória a intermediária, sendo os conteúdos avançados monitorados pelo tutor. Assim, formulou-se a perspectiva pedagógica PP6 - a abrangência do conteúdo deve ter uma abordagem que avance de básica para intermediária.

A importância de orientar pessoas leigas com relação à segurança da informação foi ressaltada pelo professor 1, seja numa compra na internet ou nos demais cuidados que a pessoa deve tomar no meio digital. Além disso, foi revelada a importância da contribuição de o aluno contribuir para o plano de segurança da informação da empresa em que ingressar. Tal preocupação também foi ressaltada pelo professor 3, o que remete à expectativa no desenvolvimento das capacidades de lidar com o mundo do trabalho, Isso nos levou à PC6 – é necessário contextualizar o conteúdo com o mundo do trabalho.

Ainda no que diz respeito ao conteúdo, existe uma demanda de que se aproxime da realidade dos jovens, para que lhes desperte interesse, ainda que ainda não esteja nas ementas institucionalizadas e nos livros didáticos consagrados, a exemplo das redes sociais. Acredita-se também que o conteúdo clássico deve ser contextualizado com a realidade dos estudantes, considerando-se a vivência empresarial que eles terão no futuro. Nesse sentido, corroborando a visão dos professores 1 e 3 acerca do conteúdo, o aluno 13 afirma que devem ser utilizados no curso exemplos reais de ataques que ocorreram ao longo da história, para se entender como eles se concretizaram, conforme descreve a PP7 – é necessário aproximar o conteúdo da realidade do aluno, trazendo exemplo reais de situações alinhadas com os assuntos abordados.

Gráfico 10 - Conteúdos sugeridos



Fonte: Elaborado pelo autor.

O gráfico 10 demonstra os conteúdos mais sugeridos para compor o MOOC Segurança da informação – aliando teoria e prática, segundo a opinião dos alunos e professores entrevistados. É possível observar que conteúdos como criptografia, tipos de *malware*, conceitos básicos de segurança da informação, riscos e ataques no meio digital, detecção de vulnerabilidades e prevenção/proteção contra riscos no foram, respectivamente, os mais sugeridos pelos entrevistados. Nesse sentido, foi possível captar os tópicos de maior foco interesse dos alunos no curso (representados entre os que estão marcados em azul no gráfico 10), além de outros conteúdos também contemplados na aplicação do modelo de formação.

Os conteúdos representados em verde no gráfico 10 também foram sugeridos, porém com um grau menor de representação. Sendo assim, devido às limitações de tempo, cronograma e abrangência estabelecidos e considerando as preferências dos usuários esses conteúdos não foram contemplados no curso.

O quadro 9 apresenta um resumo dos conteúdos abordados no curso Segurança da informação – aliando teoria e prática, observando-se que tais conteúdos estão alinhados com as sugestões feitas pela comunidade acadêmica. Assim, além de ressaltar a PC4, concluímos que os conteúdos abordados no curso deveriam ser de interesse dos estudantes, circunstância que contribuiu muito para adesão à capacitação. Com isso, formulamos a PC7 – a comunidade acadêmica deve ser consultada sobre os conteúdos abordados no curso, a fim de garantir o interesse dos alunos.

Quadro 9 – Conteúdos do MOOC

Conceitos e princípios da segurança da informação	Confidencialidade; integridade; disponibilidade; autenticidade; não repúdio; legalidade; privacidade; auditoria; vulnerabilidades; ameaças; riscos; ataques; engenharia social.
Redes sociais	Riscos e prevenção.
Criptografia	Cifra de césar; criptografia de chave simétrica e assimétrica; função *hash*; assinatura digital; certificado digital; programas de criptografia; prevenção.
Programas maliciosos	Vírus; *worms; bot* e *botnet; spyware; backdoor*; cavalo de tróia; *ransomware*.
Golpes e ataques na internet	Varredura em redes (*scan*); falsificação de *e-mail (e-mail spoofing); spam*; furto de identidade; política de senhas; fraude de antecipação de recursos (*advance fee fraud*); *phishing*; golpes de comércio eletrônico; interceptação de tráfego (*sniffing*); força bruta (*brute force*); desfiguração de página (*defacement*); negação de serviço (DoS e DDoS).

Fonte: Elaborado pelo autor.

Sobre as mídias, de acordo com os professores 1 e 2, deve ser utilizada uma variedade delas, contanto que sejam interativas, tais como vídeos, áudios, situações reais exploradas pela mídia, *sites* com páginas que dão retorno automatizado ao usuário, e que tragam elementos de multimídia, a fim de se promover atuação do aluno em desafios propostos. Nessa perspectiva, formulamos a PT5 – devem ser utilizadas uma diversidade de mídias interativas e digitais, tais como vídeos, animações, textos e imagens –, corroborando a afirmação de Silva (2017) de que, nos MOOCs, é possível acessar diversas mídias interativas e digitais, como vídeos, animações, textos, imagens, utilizando-se para tal a multimídia e a internet.

No que diz respeito à interatividade e à multimídia, o professor 3 se alinhou com o que disseram os professores 1, 2 e ainda com a visão Silva (2014), para quem o potencial da tecnologia deve ser explorado de maneira a enriquecer o curso. Assim, considerando as possibilidades que os recursos de TDICs podem inserir no contexto

do ensino e aprendizado, formulam-se as diretrizes tecnológicas PT6 – a multimídia e as redes sociais devem apoiar o processo de ensino/aprendizado – e PT7 – as mídias utilizadas devem ser dinâmicas e interativas.

Como resultado do planejamento desenvolvido e seguindo as sugestões apontadas pelos entrevistados, foram definidos vários elementos, incluindo mídias, como textos, imagens, vídeos, jogos e animações. A figura 15 mostra os elementos que devem compor o modelo de formação e, consequentemente, o MOOC Segurança da informação – aliando teoria e prática. Todos são discutidos nos tópicos posteriores.

4.3 Implementação e execução

A elaboração dos materiais didáticos, mídias e atividades foi desenvolvida pelo pesquisador, que também se utilizou de vídeos disponíveis em repositórios da internet. O curso foi disponibilizado na plataforma de educação *on-line* de código aberto da Google denominada *Course Builder*.

Figura 3 – Plataforma *Course Builder*

Fonte: Elaborada pelo autor.

Na figura 3 é possível notar que a plataforma exige um registro para que o aluno se inscreva no curso (botão Registrar-se). A partir daí, ele tem acesso ao conteúdo do curso, sendo possível acompanhar sua evolução e desempenho com sua conta de usuário. Essa plataforma foi escolhida pelo fato de ser gratuita, permitir acesso

simultâneo a diversos usuários e se encaixar nos moldes da educação *on-line* e aberta estabelecidos nesta pesquisa.

No que diz respeito aos vídeos, o aluno 13 afirmou que são muito importantes os vídeos tutoriais disponíveis no *Youtube*. Segundo o aluno 14, eles devem utilizar uma abordagem que demonstre a prática de dada situação. Já o aluno 10 salientou a importância dos vídeos, mas disse sentir falta de um conteúdo textual consistente para efetivamente compreender os artifícios utilizados na abordagem prática que os vídeos costumam trazer. Assim, levando em consideração a abordagem prática, porém informal que alguns recursos em vídeo tutoriais trazem, formulou-se a PC8 – o conteúdo textual deve ser consistente, deixando claros os conceitos envolvidos nas práticas realizadas.

As opiniões dos alunos 2, 7 e 8 confirmam a PT7 – as mídias utilizadas devem ser dinâmicas e interativas – e corroboram ainda o ponto de vista de Auh e Sim (2018) sobre os alunos serem mais propensos a lembrar do conteúdo apresentado em imagens e vídeos do que somente no texto escrito. Sendo assim, os vídeos utilizados no MOOC, em sua maioria do tipo quadro de animações e minipalestras, foram disponibilizados no Youtube com, no máximo, 8 minutos, conforme mostra a figura 4.

Figura 4 – Vídeos

Fonte: Elaborada pelo autor.

Todos os envolvidos chamaram a atenção para a complexibilidade de se utilizarem métodos de avaliação, ainda mais se tratando de um ambiente *on-line*. Segundo o professor 3, é complexo avaliar, pensamento corroborado pelos professores 1 e 2, que discorreram também sobre a dificuldade de se utilizarem métodos de avaliação em cursos EAD, o que acreditam ser ainda mais complexo.

Os professores foram unânimes em afirmar que devem ser utilizados métodos diferentes de avaliação em um curso *on-line*, o que só reforça a visão de Cilezes (2014) sobre ser insuficiente e arbitrário usar apenas questões fechadas para verificação de aprendizagem. Segundo esse autor, os alunos precisam experimentar formas variadas de avaliação, o que torna possível obter uma visão fundamentada do estudante. Assim, fica clara a necessidade de avaliação abrangente, que possibilite as várias perspectivas de aproveitamento do conteúdo de maneira aprofundada e sistêmica. Com isso, foi possível formular a PP8 – devem ser utilizados métodos de avaliação diversificados.

A respeito dos aspectos práticos, na fala do aluno 10, ficou evidenciada importância de se avaliar a prática, mesmo que isso ocorra de forma simplificada. Tal posicionamento foi corroborado pelo professor 1, que reforçou a necessidade de avaliação prática por se tratar de uma área técnica, que exigirá do aluno habilidades aplicadas quando ele ingressar no mundo do trabalho. Nesse sentido, compreendendo a importância da avaliação prática no contexto da EPT, formulou-se a perspectiva contextual PP9 – é necessário que os métodos de avaliação abordem questões teóricas e práticas.

Importante salientar que as opiniões dos envolvidos na pesquisa apontam que as atividades não devem ser muito complexas, devendo oferecer um nível de desafio que estimule a resolução da situação proposta. Outra aspectos destacado foi a regularidade planejada das atividades, assim, o aluno deverá manter o compromisso e continuar focado no curso, conforme a fala do aluno 13: “Eu acredito que, como se trata de um curso a distância, teria que ter uma frequência muito boa das unidades”. Tal visão foi complementada pelo aluno 10, que ressaltou a importância dos desafios para manter a pessoa focada no curso.

Considerando as questões discutidas sobre atividades no âmbito das avaliações e levando em consideração a forma como isso impacta na permanência e êxito no curso, pudemos formular as seguintes perspectivas contextuais: PP10 – as atividades propostas devem evoluir em sua complexidade do nível básico para intermediário, no entanto devem oferecer um desafio para o estudante; PC9 – o curso deve incluir uma regularidade nas atividades propostas, de modo que o estudante possa se manter comprometido e focado no curso.

Na figura 5, é possível observar uma atividade que consiste em um desafio proposto no MOOC Segurança da informação – aliando teoria e prática: os alunos devem criar um vírus utilizando os conhecimentos adquiridos no curso.

Figura 5 - Desafio prático

Fonte: Elaborada pelo autor.

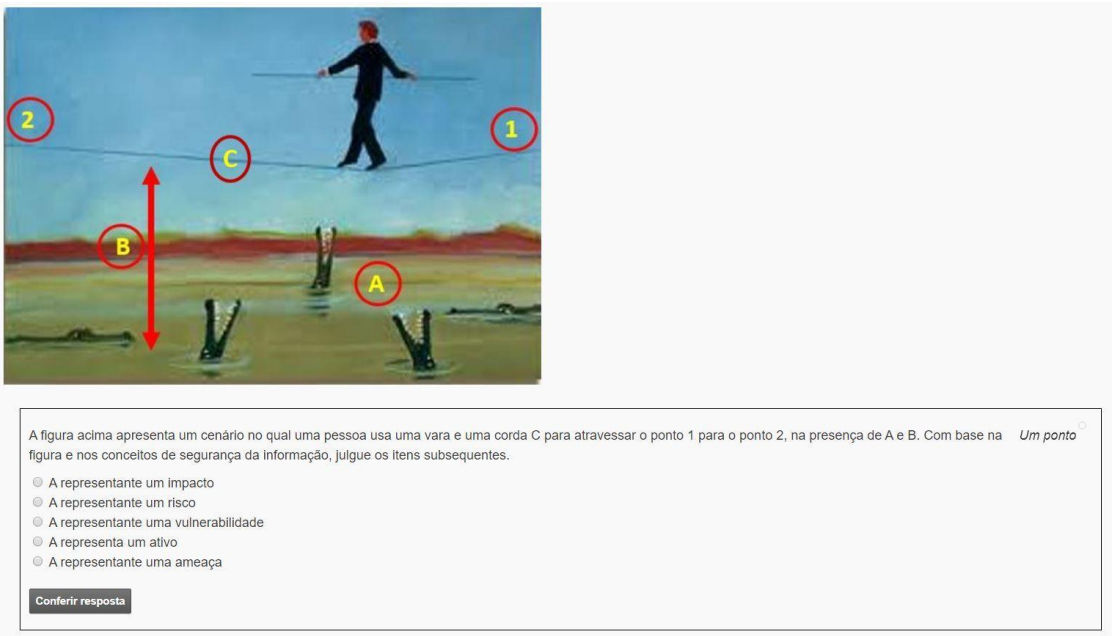
Os desafios práticos representam uma possibilidade para os alunos experimentarem o que aprenderam em situações novas e desafiadoras. Importante ressaltar que o sucesso em atividades como a representada na figura 5 causa uma sensação de realização no estudante e promove um estímulo para que continue avançando, conforme a fala do aluno 10: “Mas que ele possa dizer: nossa eu fiz! sei lá, o cara ter, sei lá, doutorado, manja, mas eu também consegui. Para instigar mais ainda ele a continuar focado no curso”. Assim, buscando estimular o interesse do aluno no curso, foi possível formular a PP11 – os desafios práticos devem abordar questões atuais, interessantes para o aluno e que possam ser aplicadas em situações diferentes das abordadas no conteúdo do MOOC.

Diversas alternativas para técnicas de avaliação foram levantadas pelos professores, como as questões objetivas (com tempo estabelecido para responder), atividades práticas, nível de interação no fórum de discussão, tempo de conexão nas páginas, questionários, questões-problema, questões reflexivas ou subjetivas e avaliação em grupo.

As diversas opções de avaliação da aprendizagem confirmam a PP8 – devem ser utilizados métodos de avaliação diversificados. Nesse sentido, no MOOC Segurança da informação – aliando teoria e prática, como técnicas de avaliação, foram utilizadas questões objetivas, questões subjetivas, estudos de caso, desafios práticos, trabalhos em grupo e prova final.

Conforme mostra a figura 6, as questões objetivas foram formuladas com 5 alternativas, sendo que somente uma é correta. Assim, no decorrer do curso, foram inseridas atividades formativas de fixação com questões objetivas, além de atividades avaliativas ao final de cada uma das unidades, contendo desafio prático, estudo de caso e jogos, além do pós-teste, realizado no fim do curso. Todos esses instrumentos de avaliação foram considerados para definir a aprovação do aluno no MOOC, sendo considerada para aprovação média maior ou igual a 6.

Figura 6 - Questão objetiva



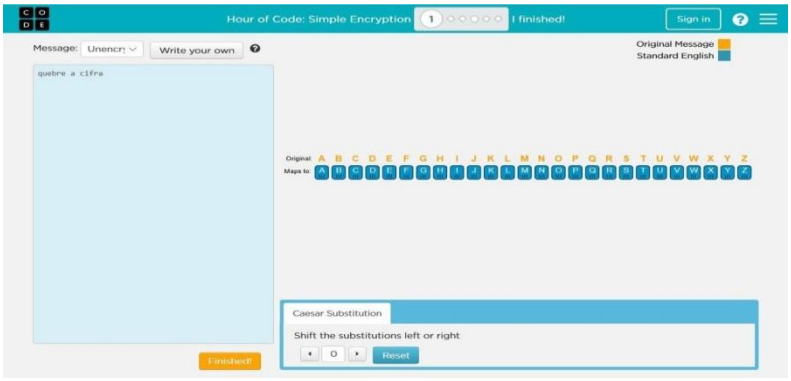
Fonte: Elaborada pelo autor.

Diante da demanda de se utilizarem recursos de multimídia que ofereçam desafios para o aluno, uma abordagem interessante é a da gamificação, como podemos ver na figura 7, que mostra um jogo utilizado como atividade de fixação. Essa atividade permite que os alunos exercitem os conceitos e a implementação de cifragem e decifragem de mensagens, utilizando várias chaves criptográficas, tais como cifra de césar e algoritmos de substituição aleatória. Nesse sentido, busca-se atender, de forma lúdica, interativa e desafiadora, as demandas de aprendizagem no modelo de formação.

Apesar de a interface do jogo ser intuitiva, o idioma padrão é o inglês, portanto os alunos foram orientados a utilizar um navegador que permitisse tradução a fim de que pudessem compreender melhor as fases e desafios. Além disso, considerando mitigar quaisquer dificuldades que poderiam ser vivenciadas na compreensão do jogo,

foram postadas orientações no grupo de interação. Assim, em situações como essa, seguindo as recomendações relativas a acompanhamento e monitoramento dos alunos no curso, é requisitada a atuação do tutor.

Figura 7 – Jogo criptografia



Fonte: Site studio.code.org.

Quando os entrevistados foram questionados a respeito de alternativas que permitiriam aliar teoria e prática, tanto professores quanto alunos compartilham a ideia de serem utilizados como exemplos situações reais, de preferência aquelas que tiveram uma boa cobertura da mídia e que são de conhecimento geral, conforme ressaltaram os alunos 10 e 14.

O aluno 4 concordou com as falas dos demais colegas e acrescentou que os desafios práticos propostos para os estudantes devem ter um grau de complexidade menor do que os explorados no conteúdo. É possível notar a preocupação dos discentes com a complexidade do tema tratado no curso, ficando evidenciada a necessidade do acompanhamento do tutor em conteúdos mais avançados, conforme evidencia a PP15, abordada no final da sessão implementação e execução.

Ainda em relação à possibilidade de aliar teoria e prática, confirmando os relatos apresentados na revisão da literatura, o professor 1 chamou a atenção para os estudos de caso, aprendizagem baseada em problemas e gamificação, sugerindo a criação de ambientes que produzam problemas reais a serem resolvidos pelos estudantes. O professor 2 complementou com os seguintes exemplos: verificação da robustez de senhas e exemplificação de alguns tipos de ataques, como DOS, DDOS e *ipspoofing*.

Nesse sentido, no que diz respeito à escolha das metodologias que demonstram efetividade em aliar teoria e prática, formularam-se as perspectivas

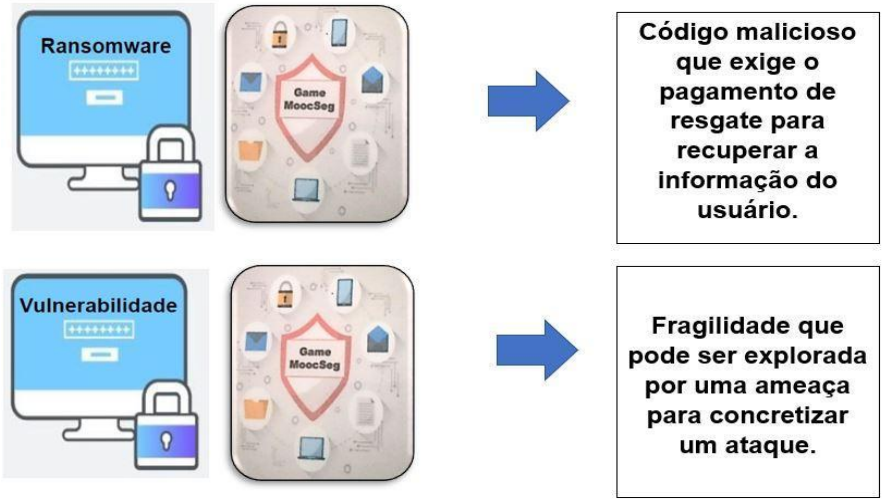
pedagógicas PP12 – devem ser utilizadas metodologias ativas de ensino aprendizagem – e PP13 – os alunos devem aplicar de modo prático o conhecimento adquirido no curso.

Como abordagem de ensino adotada no MOOC Segurança da informação - aliando teoria e prática, buscou-se evitar ao máximo as metodologias tradicionais de ensino, como a objetivista, a instrucional ou xMOOC, que mantêm o professor como centro do processo de ensino. Optou-se por metodologias ativas de aprendizagem, como gamificação, estudos de caso, aprendizagem prática e inserção de elementos dos cMOOCs: jogo em grupo e grupo de interação. Os elementos que compõem o modelo de formação podem ser vistos na figura 15.

As metodologias utilizadas no modelo de formação favorecem deslocar os alunos para o centro do processo educativo, estimulando seu interesse e autonomia, contribuindo também para que vivenciem suas próprias experiências na construção do conhecimento de forma individualizada e em grupo. É possível notar, no capítulo dos Resultados, a evolução dos alunos após realizarem a formação desenvolvida nesta pesquisa.

Antes de iniciar o curso *on-line* aberto e massivo Segurança da informação – aliando teoria e prática, os alunos participaram de um jogo de cartas, desenvolvido neste projeto para ser aplicado em grupo. Nesse jogo, foram abordados princípios da segurança da informação e tipos de *malware*. A figura 8, a seguir, apresenta exemplos dos pares de cartas utilizadas no jogo, sendo que todas as regras e cartas utilizadas estão disponíveis no apêndice F, podendo ser adaptadas para qualquer outra área.

Figura 8 – Jogo MOOCSEG



Fonte: Elaborada pelo autor.

A figura 9 mostra a execução do jogo MOOCSEG, sendo possível perceber a satisfação de uma das equipes que venceu o desafio pelas suas expressões e pela forma como erguem o prêmio. Durante a aplicação do jogo, cada turma (1º ao 4º anos) foi dividida em dois grupos e, por sua vez, cada grupo recebeu um baralho que continha 15 pares de cartas. Um par trazia um conceito (ex.: *ransoware*) e sua definição (ex.: código malicioso que exige o pagamento de resgate para recuperar a informação do usuário).

Figura 9 - Execução do jogo MOOCSEG

Fonte: Acervo do autor.

As cartas foram misturadas, e os grupos tiveram quinze minutos para discutir entre si o que consideravam ser os pares corretos para então montar os pares no quadro, entregando sua resposta. Posteriormente, foi feita a conferência, e o grupo

que fez mais pontos venceu o jogo. O quadro 10 mostra todas as definições e os conceitos utilizados como pares no jogo MOOCSEG (Apêndice F).

Quadro 10 – Pares de cartas MOOCSEG

Vulnerabilidade	Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.
Ameaça	Possível evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso.
Risco	Possível evento potencialmente danoso a uma organização, isto é, um evento hipotético que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante.
Vírus	Programa ou parte de um programa de computador, normalmente malicioso, que permite inserir as seguintes cópias e se tornar parte de outros programas e arquivos.
Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
Bot	Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente.
Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
Backdoor	Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
Trojan	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.
Ransomware	Código malicioso que exige o pagamento de resgate para recuperar a informação do usuário.
Phishing	Golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.
Sniffing	Inspeciona os dados trafegados em redes de computadores.
Adware	*Spyware* projetado especificamente para apresentar propagandas.
Screenlogger	*Spyware* capaz de armazenar a posição do cursor e a tela apresentada no monitor.
Keylogger	*Spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

Fonte: Elaborado pelo autor.

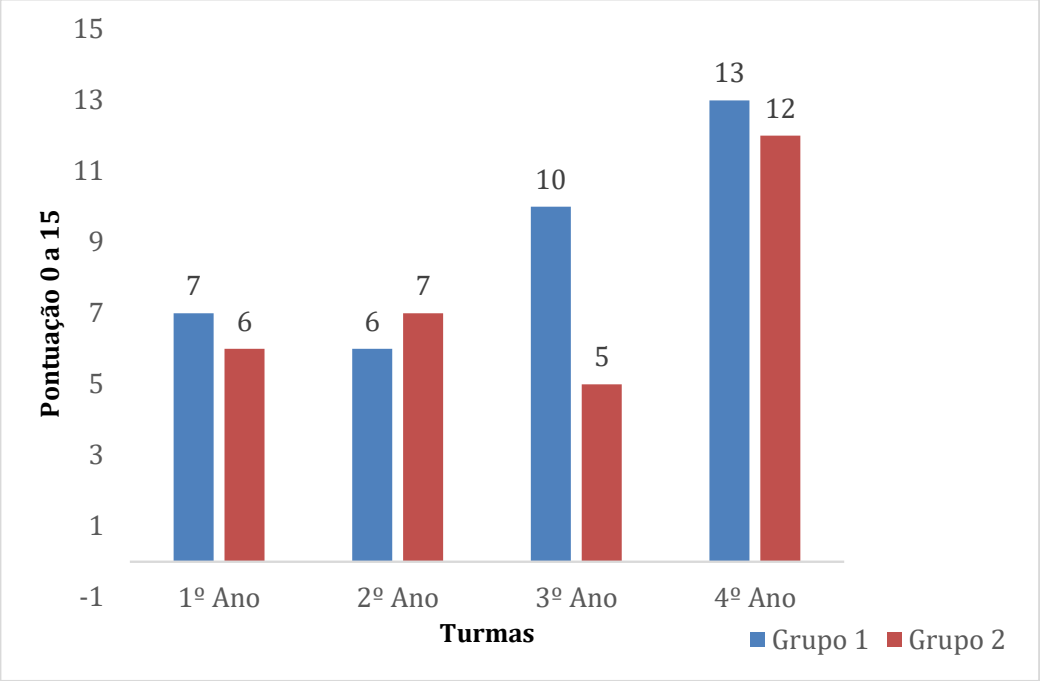
O gráfico 11 mostra o desempenho das turmas no jogo. No 1º e no 2º ano, a média de acertos foi de 46%, enquanto no 3º ano o resultado foi um pouco melhor (50%). Já no 4º ano, período em que os alunos estão cursando, presencial e formalmente, a disciplina Segurança da Informação, a quantidade de acertos foi bem maior (83%).

Com esses resultados, ficou evidenciada uma diferença muito pequena entre os desempenhos do 1º, 2º e 3º anos (apenas de 4%). Considerando o grau de interesse que os alunos demonstraram pelo tema segurança da informação, infere-se

que haverá uma evolução no domínio dos conceitos iniciais relativo ao conteúdo trabalhado no jogo, caso os alunos façam o MOOC desenvolvido nesta pesquisa.

O desempenho dos alunos do 4º ano, por sua vez, mostra que já possuem um maior domínio dos conceitos iniciais relativos ao tema, logo poderão revisar esses conceitos e avançar no restante do curso a partir das abordagens intermediária, avançada e prática.

Gráfico 11 - Resultados do jogo MOOCSEG



Fonte: Elaborado pelo autor.

A disciplina Segurança da Informação não está presente nas ementas de todos os cursos técnicos integrados ao médio de informática na rede dos institutos federais de educação ciência e tecnologia. Nesse sentido, o MOOC Segurança da informação – aliando teoria e prática pode ser utilizado por qualquer instituição ou indivíduo que tenha interesse em cursar essa disciplina de modo prático, levando em consideração que o curso é gratuito e aberto, estando disponível para acesso por meio da internet. O MOOC também se mostra uma possibilidade para o ensino híbrido.

A fim de incentivar a colaboração e interação aos alunos que se matricularam no MOOC, foi criado um grupo de interação na rede social whatsapp. Os alunos puderam ingressar no grupo através de um *link* disponível na plataforma *Course Builder* ou por meio de convite enviado, conforme a figura 10.

Figura 10 - Grupo de interação

Fonte: Elaborada pelo autor.

No primeiro momento, o contato com os alunos no grupo de interação foi mais no sentido de dar as boas-vindas e de explicar a finalidade do grupo. Interessante observar que nem todos os que entraram no grupo e interagiram estavam matriculados no curso. Logo de início, o aluno 13 pediu que fossem encaminhadas as fotos dos grupos que venceram o jogo MOOCSEG: “Professor, manda as fotos dos ganhadores ”, o que demonstra o sentimento de pertencimento e adesão à proposta de formação, além de orgulho e satisfação por fazer parte de uma das equipes que venceram o jogo.

Na conversa inicial realizada no grupo, se tratou das opiniões relativas ao jogo MOOCSEG, sendo registradas 17 interações, o que foi compreendido como uma participação considerável, afinal 22% dos membros manifestaram suas percepções. As opiniões expressas foram muito positivas, por terem gostado do jogo, e surpreendentes, por terem errado vários pares de *cards*, conforme relato dos alunos 14 e 20. Já o aluno 24 informou que conhecia poucos conceitos de segurança da informação, enquanto o aluno 4 afirmou ter confundido conceitos. Por sua vez, os alunos 3, 21, 22, 23 e 25 definiram o jogo como envolvente, construtivo, legal e interessante.

Considerando o *feedback* dos alunos, percebemos que o jogo MOOCSEG envolveu e despertou o interesse para o curso, além de promover o engajamento da turma. Com isso, a PP14 ressalta o efeito positivo que atividades que utilizam

gamificação em grupo despertam (PP14 – os jogos em grupo devem fazer parte do plano de ensino do curso).

Na contramão da considerável colaboração percebida inicialmente no grupo de discussão, a partir do momento em que foram postadas as enquetes abordando o conteúdo do curso, percebeu-se uma participação muito baixa dos alunos, apenas 5% dos membros. Analisando essa situação, percebeu-se que muitos alunos que estavam no grupo de discussão não estavam matriculados e ativos na plataforma do curso. Com isso, depreende-se que, pelo fato de não estarem estudando conteúdo, por desinteresse, ou por receio de dar resposta errada e vivenciarem um constrangimento perante os outros membros do grupo, pode ter ocorrido uma inibição naquelas colaborações.

Figura 11 - Enquete grupo de discussão

Fonte: Elaborada pelo autor.

Quadro 11 - Enquete grupo de discussão

Considerando os conceitos sobre segurança da informação abordados na primeira unidade, relacione a figura acima (1 - Entrada, 2 - Tiro e 3 – Assaltante) com os seguintes conceitos: Ameaça, Risco e Vulnerabilidade.

Fonte: Elaborado pelo autor.

Após a enquete ter sido postada, conforme a figura 11 e o quadro 11, somente deram respostas os alunos 16, 23 e 13, os quais estavam matriculados e ativos no curso. Nesse sentido, apesar de 52 alunos estarem participando do grupo de interação, apenas 17 (32%) estavam matriculados e ativos no curso, sendo que somente 3 deles responderam à enquete. Dessa forma, percebe-se que a baixa

participação relativa às respostas obtidas nas enquetes deve-se também à baixa adesão dos alunos ao curso.

Interessante observar que a rede social utilizada como ferramenta para o grupo de interação também serviu para estimular a participação dos membros do grupo no curso, de acordo com as intervenções feitas pelo pesquisador: “Aqui você pode tirar suas dúvidas, fazer comentários, conversar com os colegas...”; “Essa semana tentem concluir ao menos a Unidade 1.”; “Pessoal, quero parabenizar os que já conseguiram concluir o curso. Aluno 4, Aluno 6 e Aluno 1 (tempo recorde em dois dias kkk)”. Com isso, formulamos a PC10 - as redes sociais podem ser utilizadas para interagir, questionar, motivar e alertar os alunos sobre questões relativas ao curso (Apêndice I).

Como estratégia para estimular a adesão dos alunos ao MOOC, alguns professores concordaram em disponibilizar pontuação extra para aqueles que o concluíssem dentro do cronograma estabelecido. Após esse anúncio ter sido feito pelo pesquisador, imediatamente o aluno 2 demonstrou interesse. Diante dessa reação, fica evidenciada a efetividade da estratégia, especialmente, quando o professor de Física (considerada uma matéria difícil por boa parte dos alunos) concordou em atribuir pontuação extra. Com isso, formulamos a PC11 – gratificar o aluno com pontuação extra estimula sua adesão ao curso.

Diante das cerca de quinze disciplinas que os alunos já tinham que lidar no EMITI, a possibilidade de assumir mais uma responsabilidade com o MOOC causou-lhes um certo receio, afinal cursar o MOOC não agregava nenhum requisito para aprovação no ano corrente, mas, ainda assim, 17 alunos iniciaram o curso. Desse modo, levando em conta a prioridade que os alunos dão para as disciplinas que atribuem pontuação e, consequentemente, peso na avaliação relativa à sua aprovação no ano letivo, depreendeu-se que, caso o MOOC fizesse parte da grade curricular formal do curso, teria uma maior aceitação por parte dos estudantes.

Analisando as interações feitas no grupo de discussão, percebe-se que foram utilizadas basicamente quatro tipos de mensagens: interação, enquete, lembrete e estímulo, conforme o quadro 12. As mensagens do tipo interação incentivavam os alunos a expressarem suas opiniões, traziam orientações e *feedbacks* individuais e coletivos sobre atividades e expressavam a disponibilidade do tutor em atender possíveis dúvidas ou necessidades que os alunos tivessem. Assim, essas mensagens serviram também para construir um senso de presença do tutor junto à turma.

Quadro 12 - Tipos de mensagens

Tipos de mensagem	Descrição	Periodicidade
Interação	*Feedbacks* do tutor para a turma.	Semanal.
Enquete	Questionamentos relativos ao conteúdo.	1 enquete por unidade, seguindo o cronograma.
Lembrete	Avisos relacionados a prazos de entrega das atividades.	3 dias antes e na data de entrega das atividades ou avaliações.
Estímulo	Incentivo à evolução e conclusão do curso.	Semanal.

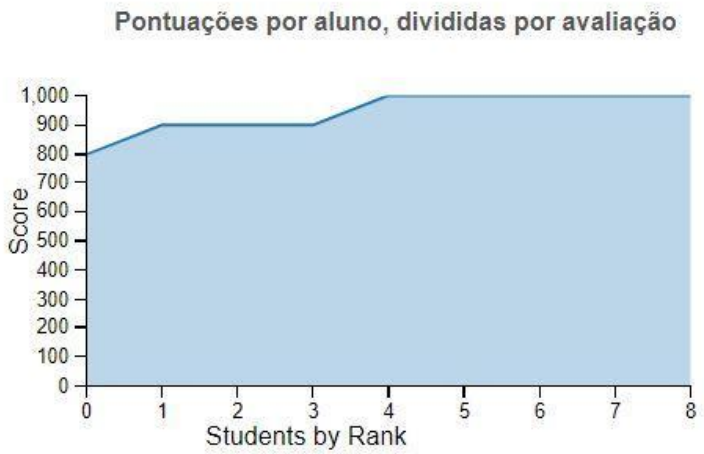
Fonte: Elaborado pelo autor.

A mensagens do tipo *enquete* questionavam os alunos acerca do conteúdo presente no curso e evoluíram de acordo com a progressão das unidades, considerando o cronograma. Nesse sentido, a primeira enquete abordou o conteúdo da unidade 1; posteriormente, o tema passou a ser a unidade 2, e assim sucessivamente. Já os *lembretes* traziam avisos relativos aos prazos de entrega das atividades e à disponibilidade do curso. Importante salientar que, para acompanhar a evolução dos alunos no curso, seu processo de matrícula, evolução nas unidades e desempenho nas avaliações, foi utilizada a análise integrada da ferramenta *Course Builder*, conforme se observa na figura 12.

As mensagens do tipo *estímulo* tiveram a função de estimular o estudante a fazer e concluir o curso, reforçando a importância da capacitação e parabenizando a evolução dos alunos diante do grupo. Periodicamente era publicada uma lista com os alunos que conseguiram evoluir nas unidades. Tais mensagens geraram um sentimento de incentivo à participação e engajamento no curso. Sendo assim, nota-se que as mensagens construíram um processo de interação bilateral entre o tutor/pesquisador e os alunos, bem como entre os próprios alunos.

Além das interações que ocorreram no grupo, os estudantes ainda tiveram a opção de tirar suas dúvidas em particular (privado), contatando o pesquisador por meio da rede social *whatsapp*. Nesse sentido, ocorreu o processo de tutoria utilizando-se a comunicação dos tipos *enquetes, lembretes, estímulo* e *interação*, conforme mostra o quadro 12, sendo que a periodicidade dessas mensagens ocorreu conforme a conveniência e necessidade de cada aluno.

Figura 12 - Analisador de desempenho no curso



Fonte: Ferramenta Google *Course Builder*.

A experiência com a videoconferência, em que se abordaram conteúdos avançados, ocorreu a partir da segunda unidade do MOOC, sucedendo a familiarização com o curso e com o conteúdo introdutório. Os alunos foram consultados sobre o melhor horário para fazer a videoconferência, que abordou conceitos e a prática de um ataque de negação de serviço (DOS), utilizando o sistema operacional Kali Linux. No momento da videoconferência, houve o incentivo por parte dos próprios alunos para que os outros membros do grupo também participassem.

A resposta rápida dos alunos à videoconferência e o incentivo que eles deram aos outros membros do grupo para que também participassem demonstram o efeito positivo da abordagem de um assunto relevante e prático do conteúdo em estudo.

O contato multimídia e interativo representou uma injeção de ânimo e um estímulo para os alunos, uma vez que foram abordados tópicos avançados, desafiantes e amplamente explorados pela mídia. Além disso, a comunicação síncrono permitiu contato visual, compartilhamento de arquivos e demonstração de práticas em tempo real, propiciando maior interação e colaboração entre os alunos. Com isso, foi formulada a PP15 - os conteúdos avançados devem ser abordados de modo prático pelo tutor de maneira síncrona e interativa.

A abordagem de estudo de caso foi inserida como estratégia para aproximar o conteúdo da realidade do estudante, fazendo-o se deparar com situação prática que precisava ser solucionada com base no conteúdo do curso. Sendo assim, o quadro

13 apresenta o estudo de caso presente na unidade 3, o qual trata sobre golpes e ataques na internet.

Quadro 13 - Estudo de caso

Você está acessando uma rede social, logado em sua conta pessoal e de repente visualiza um anúncio do site Americanas contendo uma promoção “imperdível” de uma máquina de lavar. Como tinha feito recentemente uma pesquisa, comparando preços e marcas desse produto, percebe que o valor do anúncio se encontra muito abaixo do praticado no mercado. Ao clicar, é redirecionado para uma página muito semelhante à da Americanas, que detalha melhor a promoção, explica que você deve aproveitar a oportunidade relâmpago, que é possível comprar com apenas um clique (não é necessário cadastro) e afirma que a única modalidade de pagamento é por meio de boleto bancário. Sendo assim, salienta que a promoção está acabando e que restam apenas poucas unidades do produto em estoque. Após gerar o boleto bancário e efetuar o pagamento da compra, você tenta acompanhar o envio do produto pelo número do pedido descrito no boleto, porém não consegue visualizar o pedido cadastrado para sua compra no site. Entra em contato telefônico pelo canal de atendimento ao cliente e percebe que foi vítima de um golpe. De acordo com os conhecimentos adquiridos no curso, identifique quais vulnerabilidades podem ter sido exploradas para enganar o usuário. Identifique quais estratégias de golpe foram utilizadas. Explique quais ações o usuário deveria ter adotado para identificar a fraude. O que deve ser feito caso o usuário efetue o pagamento do boleto fraudulento?

Fonte: Elaborado pelo autor.

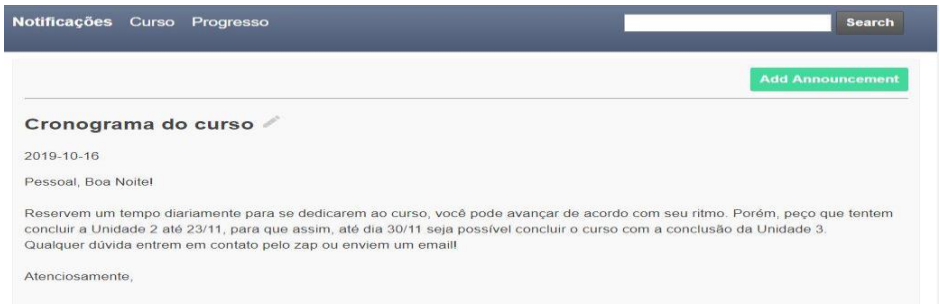
Os estudos de caso propostos representaram desafios para os estudantes, pois eles precisavam não somente compreender o conteúdo, mas também as relações entre vulnerabilidades e ataques, além de formular medidas para mitigar os possíveis danos ocorridos em situações que exigem um profissional técnico em informática atuar de forma intempestiva. Nesse sentido, considerando as finalidades para utilização dos estudos de caso trazidas por Feng e Qu (2018), tais como aplicar exemplos, praticar a análise e ação e estimular a reflexão pessoal, foi formulada a PC12 - os estudos de caso devem representar situações práticas que envolvam o cotidiano do mundo do trabalho.

No que diz respeito à duração e cronograma do curso, considerando as outras atribuições dos alunos na escola, de acordo com o professor 3, a sugestão foi de 40 (quarenta horas) horas, realizada em cerca de duas semanas. O professor 1 complementou, afirmando que deveriam ser estabelecidos claramente os prazos para o aluno (datas de início, entrega das atividades e final do curso), o que foi confirmado pelo aluno 13. Nesse sentido, tanto o professor 1 quanto o aluno 13 ressaltaram a

necessidade de fixação dos prazos, assim, foi formulada a PC13 – o cronograma deve fixar claramente prazos de início, datas de entregas de atividades e final do curso.

O prazo definido para realização do MOOC foi de um mês, totalizando 40 horas de carga horária. O plano de estudo foi executado de acordo com a conveniência dos estudantes, dentro do período estabelecido (11/11/2019 até 11/12/2019). Ainda no que diz respeito ao cronograma, relacionando a PC13 com a PC1 (se faz necessário um método de acompanhamento da evolução dos alunos no MOOC), foi utilizada a funcionalidade *notificações* da plataforma *Course Builder*, a qual envia um lembrete, conforme se mostra na figura 13.

Figura 13 – Lembretes



Fonte: Elaborada pelo autor.

Os prazos do cronograma proposto também foram reafirmados periodicamente para os alunos no grupo de interação, como é possível observar no diálogo estabelecido entre o pesquisador e o aluno 2 (cf. Apêndice I). Interessante observar que, apesar de serem estabelecidos prazos para o estudante evoluir no curso, eles tinham autonomia para utilizar o tempo de acordo com sua conveniência e interesse. As avaliações também tinham um prazo, visível aos alunos durante o acesso, como demonstra a figura 14.

Figura 14 - Prazos cronograma

Fonte: Elaborada pelo autor.

No que diz respeito a adesão, interesse e conclusão no curso, independentemente do cronograma, para o professor 1, se o aluno gostar da proposta, irá avançar nas unidades, mesmo antes do prazo definido, situação que se confirmou quando o aluno 1 conseguiu, em apenas dois dias, concluir o MOOC Segurança da Informação: aliando teoria e prática, passando por todas as etapas e respondendo a todas as atividades, mesmo o prazo do cronograma sendo de um mês. Esse comportamento do aluno 1 demonstra profundo interesse pelo MOOC Segurança da informação - aliando teoria e prática, revelando que, além da motivação para iniciar o curso, a abordagem, a metodologia e os elementos que compuseram a capacitação instigaram o aluno a avançar e concluir o treinamento muito antes do prazo.

No que diz respeito à aplicação do curso ser realizada no primeiro ou no segundo semestre do ano, assim como nas férias, as opiniões dos professores e dos alunos divergiram. Para os professores 1 e 2, o período ideal de aplicação seria nas férias, sugestão dada também pela aluna 9. Já quando a questão foi discutida entre os estudantes, tal proposta foi veementemente rejeitada. Durante a reunião, foi realizada até uma enquete que evidenciou as férias como sendo a pior opção para eles, visto que se trata de um período de descanso, portanto incompatível com a realização de atividades escolares. Nesse sentido, a fala do aluno 10 ironiza a opção de realização do curso nas férias, afirmando que nenhum aluno da sala faria o curso nesse período. Toda a turma riu, concordando com a afirmação do colega. O aluno 14 complementou que não teria tempo nem de cumprir as tarefas regulares da escola, quanto mais fazer um curso extra, concluindo que o melhor período seria o primeiro semestre.

Contrariando o consenso obtido entre os estudantes, o professor 3 afirmou que, para os alunos do 1º ano, seria mais interessante aplicar o curso no segundo semestre, considerando que, quando eles ingressam na instituição, precisam de um tempo para se adaptar à rotina de atividades. Essa opinião foi também a do aluno 13. Por outro lado, o professor 3 ponderou que, para os alunos do último ano, o primeiro semestre seria a melhor opção, visto que, no fim do ano, eles estão preocupados com as provas finais e com o ENEM.

Diante do impasse com relação ao cronograma, percebeu-se que o período ideal para realização do curso varia conforme a evolução da turma, sendo mais delicado definir um período para os primeiros e últimos anos do Ensino Médio, já que a turma do 1º ano ainda está se ambientando, e a do 4º ano está muito concentrada

no ENEM. Como o objetivo deste projeto foi disponibilizar o curso para todas as turmas (do 1º ao 4º ano), o período estabelecido foi o segundo semestre, tendo início após a aplicação da prova do ENEM. Assim, MOOC Segurança da informação – aliando teoria e prática foi aplicado entre os dias 11/11/2019 até 11/12/2019, totalizando 40 horas de curso, distribuindo-se o conteúdo e as atividades nesse período. Com isso, formulamos a PC14 – o período ideal para aplicar um curso *on-line* na turma do Médio Integrado varia conforme a evolução da turma.

Os quadros 14, 15 e 16 mostram, como resultados desta pesquisa, as diretrizes das perspectivas pedagógicas, contextuais e tecnológicas elaboradas, as quais foram construídas com base nos questionários, entrevistas e interações realizadas entre o pesquisador e os sujeitos da pesquisa (professores e alunos do curso EMITI). Nesse sentido, as diretrizes retratam o resultado e as experiências vivenciadas durante a elaboração de um curso *on-line* aberto e massivo na área da informática, abordando o tema da segurança da informação.

Espera-se que as lições aprendidas e descritas nesse modelo de formação possam servir como base para auxiliar outras iniciativas que pretendam aliar teoria e prática e desenvolver aprendizado, mesmo as que se vinculem a outras áreas do conhecimento. Afinal, os elementos que compõem o modelo de formação, suas perspectivas e diretrizes independem de uma área específica de conhecimento.

Figura 15 - Elementos do pMOOC

Fonte: Elaborada pelo autor.

A figura 15 apresenta os elementos que compõem o pMOOC, como resultado do modelo de formação elaborado nesta pesquisa, o qual alia os aspectos teóricos e práticos de um conteúdo, de forma a sistematizar aplicações práticas cotidianas,

experiências profissionais, estudos de casos, simulações, entrevistas com especialistas, enfim recursos que aproximem o aprendiz da prática à luz da teoria em estudo. Esse novo formato de MOOC, apesar de considerar aspectos já contemplados em cMOOC e synchMOOC, apresenta as inovações relativas a desenvolver aprendizado prático. Com isso, o pMOOC difere dos todos outros tipos de MOOC identificados na literatura científica.

Diante dos resultados evidenciados na sessão desempenho dos alunos, o pMOOC se mostra capaz de aliar teoria e prática e de promover aprendizado com base nas relações estabelecidas nas perspectivas pedagógicas, contextuais e tecnológicas, bem como nas diretrizes definidas para esse modelo de formação.

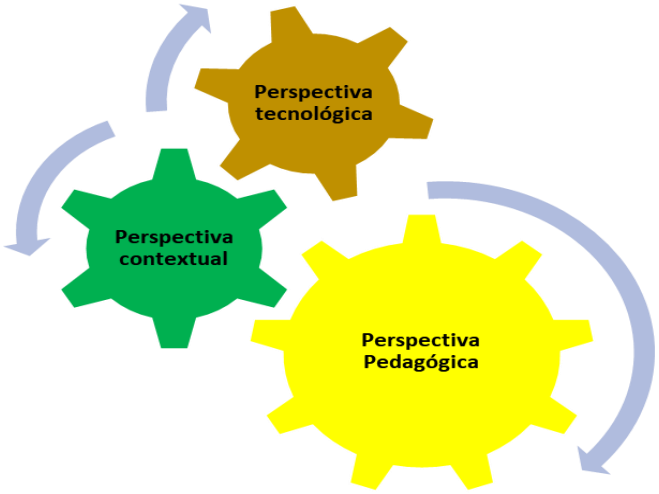
Conforme os relatos de experiência relativos à elaboração e implementação do MOOC descritos neste estudo, na unidade 1 ocorre o pré-teste, com intuito de realizar uma avaliação diagnóstica da turma e gerar informações que possam nortear o processo individualizado e coletivo de ensino. São abordados os conteúdos introdutórios, utilizando-se diversas mídias: textos, vídeos, animações e atividades formativas de fixação e de avaliação. Sendo assim, ocorrem encontros presenciais para familiarizar os alunos com o formato do curso e com a plataforma utilizada, bem como para aplicar o jogo MOOCSEG (Apêndice F).

A unidade 1 também inclui o desafio prático, fase em que o objetivo é desenvolver conhecimentos e habilidades crescentes no domínio cognitivo definidos pela taxonomia de Bloom, tais como lembrar, entender e aplicar. Para realizar a verificação de aprendizagem, os recursos usados são as atividades avaliativas, o jogo e o desafio prático.

Já na unidade 2, além dos elementos evidenciados na unidade 1, são desenvolvidas as habilidades de analisar e sintetizar, assim como na unidade 3. Para tal, ocorre um aprofundamento na abordagem utilizada no conteúdo e são adicionados os elementos estudo de caso e videoconferência. Para realizar a verificação de aprendizagem, os recursos são as atividades avaliativas, o jogo, o desafio prático e o estudo de caso.

Durante todo o percurso formativo, o tutor interagiu tanto com o grupo quanto, individualmente, com os alunos, na rede social escolhida. Com isso, depois que o estudante realiza todo o curso, considerando seu desempenho nas atividades, desafios práticos, estudos de caso e a aprovação no pós-teste, está apto a concluir a formação.

Figura 16 – Perspectivas do pMOOC



Fonte: Elaborada pelo autor.

Quadro 14 - Perspectiva pedagógica do pMOOC

ID	Diretrizes pedagógicas
PP1	É necessário tutor/professor especializado na área para dar assistência aos alunos do curso.
PP2	É necessário assistência do tutor/professor de forma *on-line*.
PP3	É necessário que o plano de ensino contemple encontros presenciais com professor especializado na área.
PP4	É necessário considerar uma abordagem introdutória sobre o conteúdo abordado no curso.
PP5	Os objetivos instrucionais do curso devem seguir uma ordem crescente de complexidade, com base na taxonomia de Bloom.
PP6	A abrangência do conteúdo deve seguir uma abordagem de básica a intermediária.
PP7	É necessário aproximar o conteúdo da realidade do aluno, trazendo exemplos reais de situações alinhadas com os assuntos abordados.
PP8	Devem ser utilizados métodos de avaliação diversificados.
PP9	É necessário que os métodos de avaliação abordem questões teóricas e práticas.
PP10	As atividades propostas devem evoluir em complexidade, do nível básico para intermediário.
PP11	Os desafios práticos devem abordar questões atuais, interessantes para o aluno e que possam ser aplicadas em situações diferentes das abordadas no conteúdo.
PP12	Devem ser utilizadas metodologias ativas de ensino e aprendizagem.
PP13	Os alunos devem aplicar na prática o conhecimento adquirido no curso.
PP14	Os jogos em grupo devem fazer parte do plano de ensino do curso.
PP15	Os conteúdos avançados devem ser abordados pelo tutor de maneira síncrona e interativa.

Fonte: Elaborado pelo autor.

Quadro 15 – Perspectiva contextual do pMOOC

ID	Diretrizes contextuais
PC1	Se faz necessário um método de acompanhamento da evolução dos alunos no MOOC.
PC2	É necessário utilizar estratégias para motivar o aluno a se dedicar ao curso.
PC3	O plano de estudos definido para o curso não deve comprometer mais do que 60 minutos diários do tempo do aluno.
PC4	Na elaboração do curso, devem ser levados em consideração aspectos como expectativa de formação e interesse nos temas abordados para MOOC.
PC5	Os estudantes devem ser familiarizados com o formato do curso.
PC6	É necessário contextualizar o conteúdo com o mundo do trabalho.
PC7	A comunidade acadêmica deve ser consultada sobre os conteúdos abordados no curso, a fim de garantir interesse dos alunos.
PC8	O conteúdo textual deve ser consistente, deixando claros os conceitos envolvidos nas práticas realizadas.
PC9	O curso deve ter uma regularidade nas atividades propostas.
PC10	As redes sociais podem ser utilizadas para interagir, questionar, motivar e alertar os alunos sobre questões relativas ao curso.
PC11	Gratificar o aluno com pontuação extra estimula sua adesão ao curso.
PC12	Os estudos de caso devem representar situações práticas que envolvam o cotidiano do mundo do trabalho.
PC13	O cronograma deve fixar claramente prazos de início, datas de entregas de atividades e data do final do curso.
PC14	O período ideal para aplicar um curso *on-line* na turma do EMI varia conforme a evolução da turma.

Fonte: Elaborado pelo autor.

Quadro 16 – Perspectiva tecnológica do pMOOC

ID	Diretrizes tecnológicas
PT1	É necessário fornecer acesso aos recursos de TDICs do *campus*, para possibilitar aos alunos oportunidade de realização do curso.
PT2	O uso de TDICs é incentivado, visto que os alunos estão familiarizados com essas ferramentas, as quais são aliadas no processo de ensino/aprendizagem.
PT3	Os alunos não estão familiarizados com fóruns de discussão, sendo incentivada a utilização de rede social como ferramenta para comunicação em grupo.
PT4	A plataforma utilizada para hospedar o curso deve ter boa usabilidade (fácil, intuitiva para utilizar).
PT5	Deve ser utilizada uma diversidade de mídias interativas e digitais, tais como vídeos, animações, textos e imagens.
PT6	A multimídia e as redes sociais devem apoiar o processo de ensino e aprendizagem.
PT7	As mídias utilizadas devem ser dinâmicas e interativas.

Fonte: Elaborado pelo autor.

4.4 O desempenho dos alunos

O pMOOC Segurança da informação – aliando teoria e prática está disponível para matrículas continuamente, ou seja, a qualquer momento, é possível realizar a

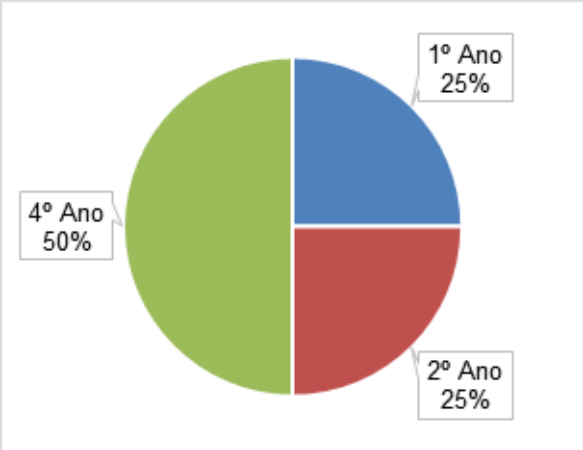
capacitação, cujo acesso se dá por meio do link: https://mooc-seginfo.appspot.com/moocseg/course, disponível na plataforma Google *Course Builder*. Em formato de produto educacional esse conteúdo também está disponível na plataforma Educapes pelo link: http://educapes.capes.gov.br/handle/capes/567384. Atente-se que, nesta pesquisa, para avaliar o desempenho dos alunos, foi considerado o período estabelecido no cronograma de aplicação - de 11/11/2019 até 11/12/2019.

O curso foi disponibilizado para alunos do EMITI como uma oferta optativa, podendo se matricular os que manifestaram interesse na temática abordada. Considerando o total dos 56 alunos, 17 foram matriculados e permaneceram ativos no MOOC, sendo que 8 (47%) dos matriculados conseguiram concluir todas as etapas do pMOOC, incluindo realização das atividades e avaliações, dentro do período estabelecido.

Foram comparados os resultados das atividades realizadas no pré-teste (Apêndice E), aplicado com os alunos antes da participação no curso, com o resultado obtido no pós-teste (Apêndice E), mesmo teste realizado após a participação no curso.

O gráfico 12, a seguir, mostra a porcentagem equivalente ao ano escolar que os alunos estavam cursando no período que concluíram o curso. É possível observar que houve maior adesão por parte dos alunos do 4º ano, sendo importante salientar que o fato de eles estarem cursando a disciplina presencialmente não foi um fator impeditivo para que realizassem o curso; pelo contrário, encararam o curso como uma oportunidade para complementar o conhecimento obtido na área. Para o aluno 1, o MOOC contribuiu com o agregou no conhecimento que já tinha sobre o tema, como ele mesmo frisou: “mesmo eu tendo um conhecimento sobre esse curso me mostrou coisas que eu não conhecia ainda”.

Gráfico 12 - Alunos concluintes



Fonte: Elaborado pelo autor.

Nesta pesquisa, a análise da aprendizagem alcançada visa mensurar o desempenho dos estudantes quanto ao aprendizado relativo a vulnerabilidades em segurança da informação, apesar de não ter se limitado a esse tema em sua abordagem. Sendo assim, as avaliações consideraram conhecimentos e habilidades crescentes no domínio cognitivo definidos pela taxonomia de Bloom, sendo eles: lembrar (6.1), entender (6.2), aplicar (6.3), além de analisar e sintetizar (6.4).

4.4.1 Categoria lembrar

No que diz respeito aos conceitos relacionados à segurança da informação, vulnerabilidade está atrelada a uma falha ou fraqueza de procedimento, *design*, implementação ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema. A partir desse conceito, a avaliação focada na categoria lembrar visou verificar se o aluno era capaz de identificar o conceito de vulnerabilidade por meio do questionamento reproduzido no quadro 17.

Quadro 17 - Identificando vulnerabilidades

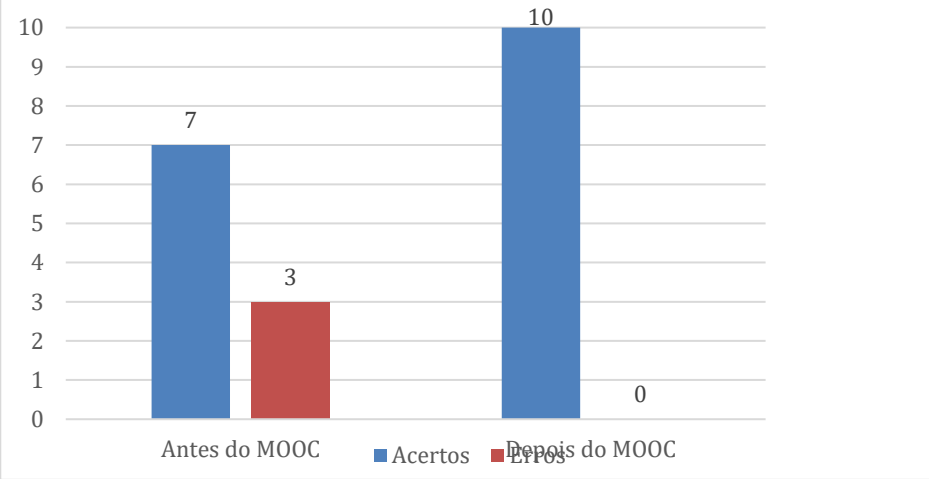
01 - Considerando os conceitos relacionados à segurança da informação e o texto a seguir: “É uma falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema”, pode-se afirmar que essa definição de se refere a a) risco b) fragilidade

c) ameaça
d) impacto
e) vulnerabilidade

Fonte: Elaborado pelo autor.

Analisando os resultados das respostas individuais no pré-teste (antes da aplicação do curso), percebe-se uma taxa de erros de 30% na identificação do conceito de vulnerabilidade, o que demonstra a falta de domínio por parte da turma na identificação desse conceito. Por outro lado, quando verificamos o resultado desse mesmo questionamento feito aos alunos que fizeram o pMOOC Segurança da informação – aliando teoria e prática, notamos que todos eles (100%) identificaram corretamente o conceito de vulnerabilidade. Nesse sentido, fica evidenciado que o domínio *lembrar* aplicado ao conceito tratado no curso foi desenvolvido.

Gráfico 13 – Desempenho lembrar

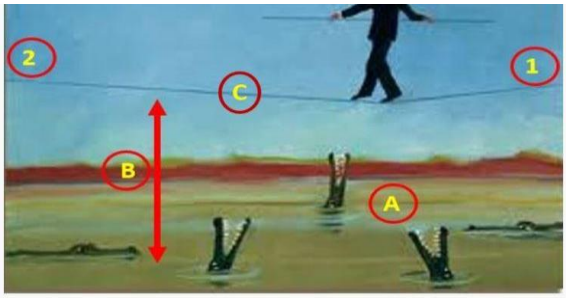


Fonte: Elaborado pelo autor.

4.4.2 Categoria entender

Para verificação da aprendizagem no nível do domínio cognitivo *entender*, os questionamentos feitos aos alunos buscaram verificar se eles tinham a capacidade de compreender o significado de vulnerabilidade em segurança da informação e utilizá-lo em contextos diferentes. Assim, no quadro 18, mostra-se um homem tentando se equilibrar em C para atravessar do ponto 1 para o ponto 2, na presença de A e considerando a possibilidade de ocorrer B.

Quadro 18 – Reconhecendo vulnerabilidades

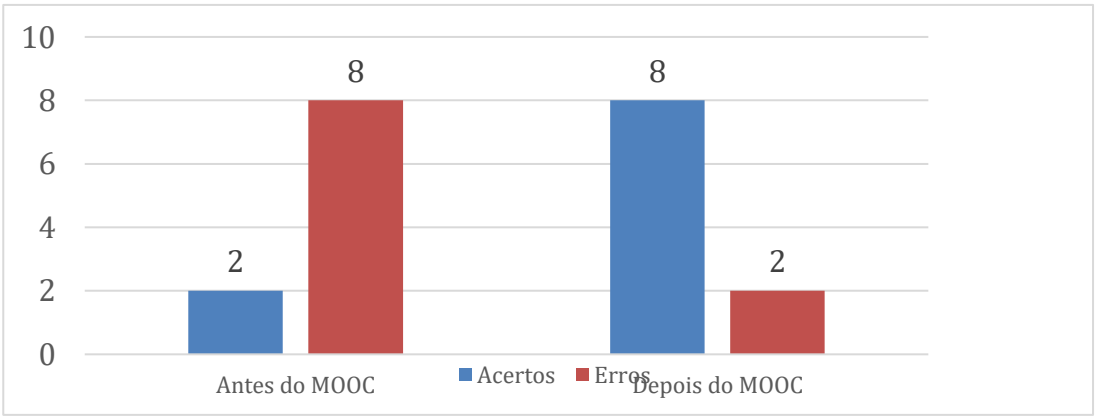


a) C representa uma ameaça
b) C representa um risco
c) C representa uma vulnerabilidade
d) C representa um ataque
e) C representa um ativo

Fonte: Elaborado pelo autor.

Analisando o desempenho dos estudantes nesse questionamento, percebemos que, no conjunto dos 15 alunos (que responderam tanto o pré-teste quanto o pós-teste), houve uma taxa de acertos de 20% (três alunos) antes da aplicação do MOOC. Após realizarem o curso, 12 alunos (80%) responderam corretamente o questionamento, como se verifica no gráfico 14. Esse resultado demonstra que a grande maioria dos estudantes que realizaram o pMOOC Segurança da informação – aliando teoria e prática conseguiu desenvolver a capacidade esperada no domínio cognitivo entender.

Gráfico 14 – Desempenho entender



Fonte: Elaborado pelo autor.

A fim de complementar a verificação de aprendizagem relativa ao domínio cognitivo entender, foi publicada uma enquete na rede social whatsapp, utilizada nesta

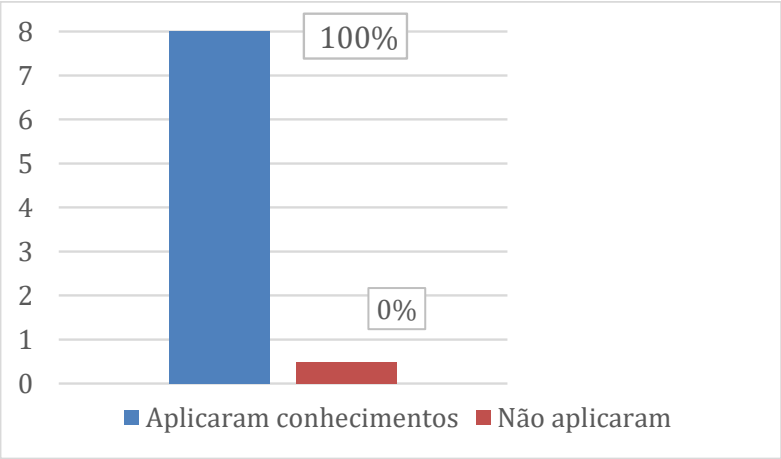
pesquisa como grupo de interação, para reafirmar a capacidade de os alunos compreenderem os princípios da segurança da informação e utilizá-los em contextos diferentes. Conforme podemos observar na figura 11, foi solicitado que comparassem, na figura, 1 - Entrada, 2 - Tiro e 3 - Assaltante com os seguintes conceitos: Ameaça, Risco e Vulnerabilidade. Três estudantes responderam a enquete, sendo todos eles assertivos em suas respostas.

Nesse sentido, além da avaliação formal retratada no gráfico 14, que demonstra uma evolução nos acertos de 20% para 80% durante a execução do pMOOC por meio do grupo de interação, as respostas da enquete revelam que 100% dos estudantes que deram respostas foram assertivos. Depreende-se, então, que o domínio entender foi desenvolvido.

4.4.3 Categoria aplicar

Para verificação da aprendizagem no nível do domínio cognitivo *aplicar,* o objetivo foi avaliar se os alunos desenvolveram a habilidade de usar informações, métodos e conteúdos aprendidos em situações concretas. Importante destacar que chegaram nessa fase do curso 8 alunos, portanto as análises de desempenho estão baseadas nesse quantitativo. Para tal, como demonstrando na figura 5, foi solicitado que os estudantes criassem um “vírus” capaz de desligar a máquina do usuário quando o arquivo fosse executado, explorando vulnerabilidades do sistema operacional Windows.

Gráfico 15 - Desempenho aplicar



Fonte: Elaborado pelo autor.

O segundo desafio prático abordou golpes no comércio eletrônico: o aluno precisava clonar o site de uma empresa de vendas conhecido, para simular um ataque de *phishing*. Da mesma forma que ocorreu no desafio 1, todos conseguiram realizar a clonagem do site, demonstrando a capacidade de realizar ou aplicar procedimentos em situações novas e específicas. Além dos desafios práticos, o nível do domínio cognitivo *aplicar* foi desenvolvido nos jogos MOOCSEG e jogo *on-line* de criptografia.

É possível notar, de acordo com o desempenho dos estudantes, que 100% deles, conforme mostra o gráfico 15, ou seja, os oito alunos que chegaram a essa fase do curso conseguiram completar com sucesso os desafios práticos e os jogos. Com isso, depreende-se que o curso possibilitou que desenvolvessem a capacidade de aplicar de forma prática o que aprenderam no MOOC.

4.4.4 Categorias analisar e sintetizar

Com os estudos de caso, os alunos chegaram à fase de verificação da aprendizagem relativa aos níveis do domínio cognitivo analisar e sintetizar, que contemplam as habilidades de subdividir uma estrutura final em partes menores, examinando o relacionamento entre elas e a capacidade de combinar partes não organizadas para formar um novo todo.

Como pode-se observar no quadro 13, o estudo de caso que aborda golpes no comércio eletrônico retrata a ocorrência de uma fraude no meio digital, sendo os alunos estimulados a analisar a situação e a responder a questionamentos que diziam respeito às vulnerabilidades exploradas e às técnicas utilizadas no golpe (analisar). Também foram solicitados a descrever como o usuário deveria se comportar nessas situações (sintetizar).

Após realizar as análises das respostas concluímos que os domínios cognitivos analisar e sintetizar foram desenvolvidos pelos estudantes. O aluno 6, por exemplo, afirmou que “*Phishing* ou *cookies* não autorizados permitiram identificar o tipo de produto que a vítima tinha interesse de adquirir...”. Disse ainda que a técnica utilizada foi “Engenharia social, a vítima teria que perceber o preço fora do normal, além de que o site não teria um certificado digital”, lembrando que cabe ressarcimento: “Nessas situações a vítima está protegida por lei e pode ser ressarcida”.

O aluno 4, em sua resposta, ressaltou a importância de se ter um mecanismo de proteção atualizado: “Não ter um mecanismo de proteção ou podem estar desatualizadas”. Também correlacionou a estratégia utilizada como “engenharia social ” e afirmou ainda que, quando o usuário desconfia de algum *link*, deve consultar o site original: “Uma vez que o usuário suspeite da oferta a um preço muito mais baixo do que o mercado e outros recursos, como pagamento e falta de entrada de pedidos, deve ir ao site original dos EUA e procurar o produto”.

O quadro 19, a seguir, mostra outro exemplo de estudo de caso aplicado no MOOC em que computadores de um laboratório foram infectados por um Worm. Nesse sentido, os alunos são questionados a examinar quais foram as vulnerabilidades exploradas e explicar as medidas que devem ser adotadas para conter e se recuperar do incidente.

Quadro 19 – Domínios analisar e sintetizar

Na quinta-feira de manhã, John, um empregado da universidade XYZ, notou uma mensagem de aviso em seu computador dizendo que o sistema foi atacado por um Win32.VB worm. Mesmo com o software antivírus presente no sistema, o software não conseguiu detectar o novo worm porque não foi atualizado para a versão mais recente. Quando John tentou abrir seu e-mail, ele experimentou uma conexão de internet lenta. Ele percebeu que havia alguns nomes de arquivo incomuns no disco. John imediatamente informou seu amigo Bob, que também era um empregado XYZ, do problema. Bob checou seu computador em seu escritório e experimentou o mesmo problema que John. John e Bob verificaram vários computadores nos laboratórios, e descobriram que Win32.VB verme havia infectado muitos outros computadores no laboratório. Eles contataram o setor de TI da Universidade XYZ. O administrador do sistema verificou os computadores, constatando o incidente de segurança da informação. Como um resultado do ataque verme, as atividades no laboratório da Universidade XYZ foram suspensas, o que causou um grande inconveniente.
Na sua opinião, qual foi a vulnerabilidade explorada? Quais medidas devem ser adotadas para conter e se recuperar do incidente de segurança da informação relatado no estudo de caso acima?

Fonte: Adaptado de He, Yuan e Yang (2013).

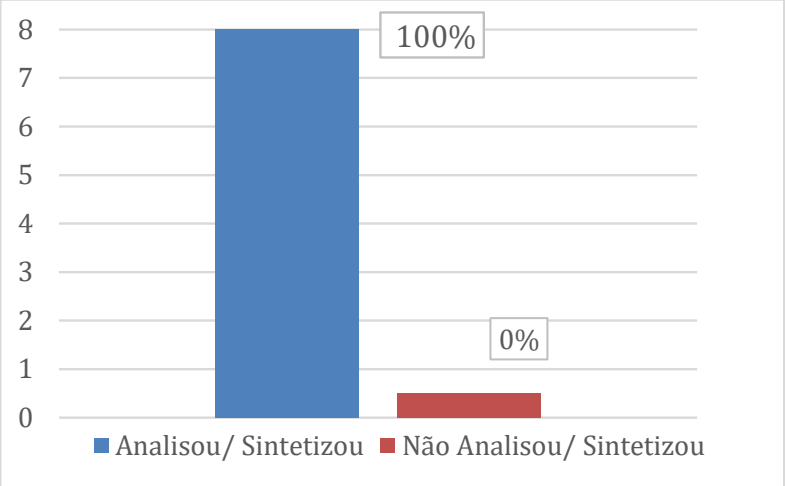
Ao avaliar as respostas dos estudantes, mais uma vez verificamos que eles conseguiram analisar a situação, apontar as vulnerabilidades exploradas e sintetizar a proposição das medidas a serem adotadas. Conforme se vê no gráfico 16, 100% dos alunos desenvolveram as categorias dos domínios cognitivos analisar e sintetizar.

O aluno 4, por exemplo, afirmou o seguinte:

> Você pode perceber que o antivírus do seu computador não foi atualizado; nesse caso, a primeira coisa a fazer é executar esta atualização. Posteriormente, o técnico de TI deve iniciar uma verificação completa do sistema e executar a remoção de malware. Para evitar mais incidentes, você pode ativar uma rotina de atualização automática de segurança no sistema operacional.

O aluno 3 fez uma análise parecida: “O que causou a vulnerabilidade foi a falta de atualização do software (antivírus), ele deverá atualizar para a versão mais recente”. Com isso, podemos notar que os alunos tiveram êxito nas análises e sínteses, o que mostra que essas habilidades foram desenvolvidas no decorrer do curso.

Gráfico 16 – Desempenho analisar e sintetizar



Fonte: Elaborado pelo autor.

4.5 Avaliação de satisfação com o curso

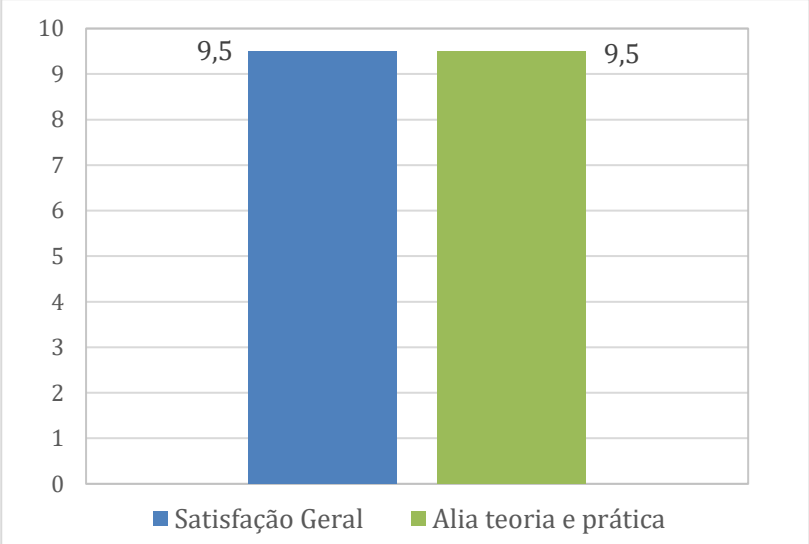
Diante do modelo de formação proposto e considerando todos os elementos didáticos pedagógicos que o compõem, para os alunos que concluíram o pMOOC Segurança da Informação – aliando teoria e prática, foi disponibilizada uma avaliação de satisfação cujo objetivo foi captar opiniões e avaliar se os recursos aplicados foram adequados para o público do EMITI. Essa avaliação abordou todos os elementos

planejados e implementados no MOOC, conforme podemos observar nos gráficos 17 e 18, sendo captadas as opiniões referentes a avaliação geral do curso, estratégias para aliar teoria e prática, conteúdo, mídias, material de leitura, vídeos, desafios práticos, estudos de caso, grupo de discussão, interatividade, duração.

Como evidenciado no gráfico 17, considerando uma escala de 0 a 10, os alunos avaliaram em 9,5 a satisfação geral com o pMOOC Segurança da Informação – aliando teoria e prática. Quando questionados se a abordagem utilizada no MOOC possibilitou aliar teoria e prática, considerando a mesma escala, o resultado também foi 9,5. Nessa perspectiva, entende-se que o modelo de formação proposto foi assertivo em corresponder às expectativas de formação técnica, com ênfase em aliar teoria e prática para os alunos do EMI.

Além da avaliação de satisfação, conforme resultados da sessão desempenho dos alunos, depreende-se que as diretrizes estabelecidas nas perspectivas pedagógicas, contextuais e tecnológicas, de modo geral, foram validadas no pMOOC Segurança da Informação – aliando teoria e prática.

Gráfico 17 – Avaliação de satisfação



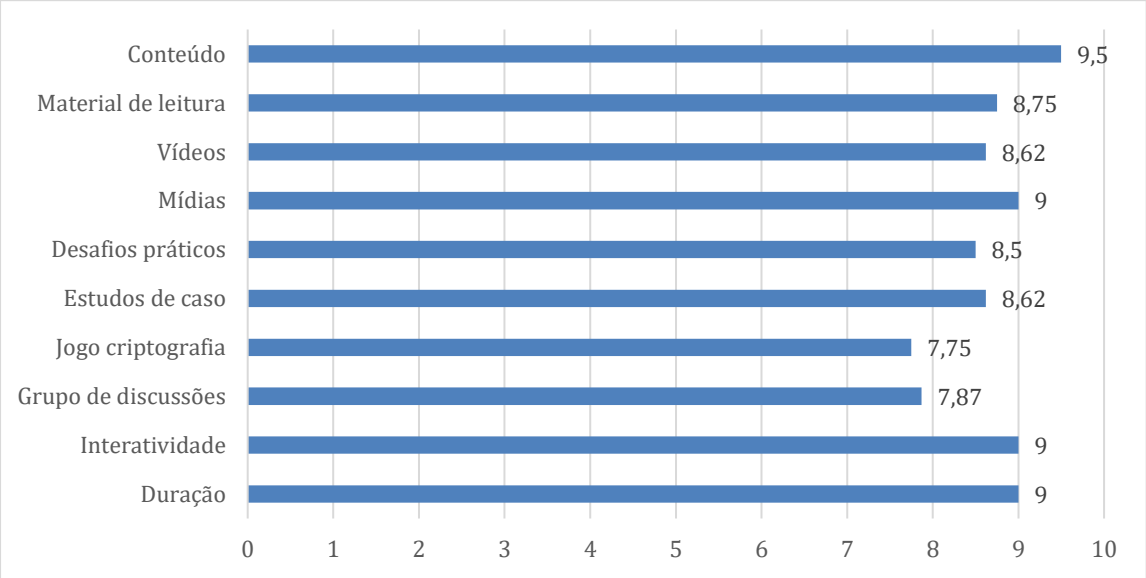
Fonte: Elaborado pelo autor.

Como podemos observar no gráfico 18, segundo as respostas dos alunos considerando uma escala de 0 a 10, de modo geral, o *feedback* relativo aos elementos do pMOOC Segurança da Informação – aliando teoria e prática foi positivo, já que todos os elementos receberam uma nota maior que 7,75. Houve um destaque para o conteúdo abordado, com índice de satisfação de 9,5, resultado que reforça as

diretrizes PP4, PP7, PP14, PP6, PC6 e PC8, elaboradas no modelo de formação, as quais, de alguma forma, versam sobre o conteúdo do curso.

Outros elementos que mereceram destaque positivo na avaliação dos alunos foram as mídias utilizadas, que receberam conceito 9, confirmando-se as diretrizes elaboradas nas PT5 e PT7. Da mesma forma, a PC13, que trata da duração ou cronograma do curso, e a PT7, que fala se refere à interatividade, foram validadas nas avaliações. Os desafios práticos, vídeos e estudos de casos propostos também foram bem aceitos pelos alunos, recebendo, respectivamente, os escores 8,5, 8,62 e 8,62, que validam as diretrizes da PP13 e da PP9.

Gráfico 18 – Detalhamento da avaliação de satisfação



Fonte: Elaborado pelo autor.

Nas avaliações, o jogo de criptografia e o grupo de discussão foram os que receberam escores mais baixos: 7,75 e 7,87, respectivamente. Ainda assim, essa é uma avaliação que representa um resultado positivo, o que valida as diretrizes PP14, PT6 e PC10. No que diz respeito ao jogo de criptografia, como fora desenvolvido em inglês, os alunos foram orientados a acessá-lo com um navegador que permitisse tradução. Depreende-se então que essa tenha sido uma dificuldade enfrentada pelos estudantes, o que justifica a avaliação um pouco mais baixa do jogo. Sobre o grupo de interação, como poucos alunos concluíram o curso, as interações relativas às enquetes que diziam respeito ao conteúdo foram baixas, o que também justifica a avaliação com escore de 7,87.

5 CONSIDERAÇÕES FINAIS

O crescimento da educação a distância impressiona e não se destaca somente no âmbito dos cursos superiores, visto que a popularização do acesso à internet e às TDICs abriu um “mundo” de possibilidades para capacitação ao alcance de apenas alguns cliques. Os cursos *on-line* abertos e massivos (MOOCs) contribuem grandemente para a expansão da EAD, com seus variados formatos que agradam aos mais diversos tipos de público.

Considerando as novas tecnológicas aplicadas à educação e as modernas funcionalidades disponibilizadas pelas plataformas MOOEP (plataformas massivas de educação *on-line* e aberta) não se podem desprezar as possibilidades de multimídia e interatividade. Por outro lado, continua sendo imprescindível para o processo de ensino aprendizagem a escolha da abordagem didático-pedagógica adequada, a estruturação, organização e aplicação dos objetivos instrucionais e dos métodos de avaliação.

As propostas de ensino que deslocam o aluno da posição de receptor passivo para o centro do processo de aprendizagem, apesar de ainda representarem um esforço e uma mudança de paradigma, se mostram extremamente eficazes e quase sempre bem aceitas pelos estudantes. Além de empreender esse esforço, o pMOOC proposto como modelo de formação teve como missão desenvolver habilidades e conhecimentos práticos nos alunos da educação profissional e tecnológica, dando voz ativa e efetiva a eles na formulação do seu percurso formativo.

O modelo de formação pMOOC, curso *on-line* aberto e massivo prático, desenvolvido nesta pesquisa se apresenta como um novo tipo de MOOC, pois, apesar de considerar aspectos conectivistas e síncronos, como o grupo de interação que usa redes sociais, os jogos e o acompanhamento do tutor, já contemplados em outros formatos, difere dos demais por desenvolver aprendizado prático, com base em uma série de diretrizes e perspectivas pedagógicas, contextuais e tecnológicas que alia os aspectos teóricos de um conteúdo aos práticos. De tal forma, sistematiza aplicações práticas cotidianas, experiências profissionais, estudos de casos, simulações, entrevistas com especialistas, enfim recursos que aproximam o aprendiz da prática à luz da teoria em estudo.

As colaborações advindas dos alunos e professores foram primordiais para a elaboração do modelo de formação proposto e, por conseguinte, para o

aprimoramento de conhecimentos e habilidades do domínio cognitivo nos estudantes. Os resultados de aprendizagem demonstram que o curso *on-line* aberto e massivo prático Segurança da Informação – aliando teoria e prática foi eficaz para o público do EMITI. Apesar de não ter sido feita uma análise estatística e de se pesquisar uma amostragem limitada, existem evidências consistentes nos resultados das análises dos dados.

Embora o modelo de formação não esteja restrito a uma área, outras iniciativas que se propuserem a implementar MOOCs no EMI e que tomem como base os resultados desta pesquisa terão que investigar e delimitar detalhadamente seu público a fim de alcançar satisfatoriamente os objetivos de aprendizagem definidos, principalmente no que diz respeito às perspectivas contextuais elaboradas. Como possibilidade para futuras análises, o pMOOC Segurança da informação: aliando teoria e prática está disponível na plataforma *Course Builder*, possibilitando o acesso de novos alunos.

O índice de concluintes de 47% no pMOOC implementado nesta pesquisa foi interpretado como um bom resultado, considerando-se que diversas outras iniciativas alcançam uma taxa de conclusão que varia entre 10 a 17%, de acordo com Almenara, Cejudo e Martínez (2014) e Alcock, Dufton e Durusu-tanriöver (2015). Da mesma forma, os resultados de aprendizagem e a excelente avaliação de satisfação com o curso são efeitos do engajamento dos professores e alunos na proposta de elaboração de um pMOOC que fosse adequado às suas necessidades instrucionais.

Levando em consideração as estratégias que precisaram ser implementadas para estimular a adesão dos alunos, diante da grande prioridade que dão às disciplinas que atribuem pontuação e, consequentemente, peso na avaliação relativa à sua aprovação no ano letivo, depreende-se que, caso o MOOC fizesse parte da grade curricular formal do curso, teria ainda uma maior aceitação por parte dos estudantes.

Com os resultados desta pesquisa, espera-se que seja possível formar melhor os alunos da EPT com um aprendizado prático, significativo e em consonância ao seu contexto de cidadão e profissional, contribuindo assim com as atuais discussões que envolvem as novas Diretrizes Curriculares Nacionais (DCNs) para o Ensino Médio, visto que, segundo a atualização feita pela Resolução nº 3, de 2018, a educação a distância pode ter uma abrangência de até 20% da carga horária total, devendo incidir, preferencialmente, nos itinerários formativos do currículo (BRASIL, 2018b). Sendo

assim, a experiência da aplicação de um curso *on-line* aberto e massivo prático junto ao público do EMITI traz uma visão validada pelo desempenho e pelas opiniões dos alunos, aplicada de uma maneira que pode ser utilizada em diversas áreas do conhecimento.

REFERÊNCIAS

ABREU, K. F. **Concepções de leitura e de texto subjacentes às provas de vestibular:** constatações e implicações para o ensino da língua espanhola. 2011. 271 f. Dissertação (Mestrado em Linguística – Departamento de Letras Vernáculas, Universidade Federal do Ceará, Fortaleza, 2011. Disponível em: http://www.repositorio.ufc.br/handle/riufc/8284. Acesso em: 26 mar. 2020.

ALCOCK, S.; DUFTON, J. A.; DURUSU-TANRđÖVER, M. Archaeology and the MOOC: Massive, open, on-line, and opportunistic. **Journal of Social Archaeology**, SAGE Publications, v. 16, n. 1, p.3-31, 12 out. 2015. Disponível em: http://dx.doi.org/10.1177/1469605315609017. Acesso em: 30 mar. 2019.

ALMENARA, C.; CEJUDO, M. C. L.; MARTÍNEZ, A. I. V. Las tipologías de MOOC: su diseño e implicaciones educativas. **Professorado**: Revista de Currículum y Formación de Profesorado, Granada, v. 18, n. 1, p.12-26, 2014. Disponível em: https://www.redalyc.org/pdf/567/56730662002.pdf. Acesso em: 3 jul. 2019.

ALVES, C. 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: 7 abr. 2019.

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

ARETIO, G. **MOOC. ¿SonEaD, igual que el e-learning?** 2013. Disponível em: https://aretio.hypotheses.org/736. Acesso em: 1º jul. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **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.

AUH, Y.; SIM, H. R. Uses of social network topology and network-integrated multimedia for designing a large-scale open learning system: case studies of unsupervised featured learning platform Design in South Korea. **Multimedia tools and applications**, v. 78, n. 5, p. 5445-62, 21 set. 2018. Disponível em: http://dx.doi.org/10.1007/s11042-018-6658-1. Acesso em: 24 ago. 2019.

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.

BELLONI, M. L. **Educação à Distância.** 6. ed. Campinas, SP: Autores Associados, 2012.

BRASIL. Conselho Nacional de Saúde. Resolução n° 466, de 12 de dezembro de 2012. Aprova normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília: **Diário Oficial da União**, 2013.

BRASIL. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. **Educação Profissional e Tecnológica (EPT)**. Brasília, 2018a.

Disponível em: http://portal.mec.gov.br/component/content/article?id=65251:educacao-profissional-e-tecnologica-ept. Acesso em: 17 nov. 2018.

BRASIL. Ministério da Educação. **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.

BRASIL. Ministério da Educação. **Decreto 5.622**, **de 19 de dezembro de 2005**. Regulamenta o art. 80 da LDB. Brasília: MEC, 2005. Disponível em: http://portal.mec.gov.br/seed/arquivos/pdf/dec_5622.pdf. Acesso em: 25 out. 2019.

BRASIL. Ministério da Educação. Conselho Nacional de Educação. **Resolução 3, de 21 de novembro de 2018**. Atualiza as Diretrizes Curriculares Nacionais para o Ensino Médio. Brasília: MEC, 2018b. Disponível em: http://portal.mec.gov.br/docman/novembro-2018-pdf/102481-rceb003-18/file. Acesso em: 13 jan. 2020.

BRASIL. Ministério da Educação. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Censo da Educação Superior 2017**. Brasília: Setembro, 2018c. Disponível em: http://portal.mec.gov.br/docman/setembro-2018-pdf/97041-apresentac-a-o-censo-superior-u-ltimo/file. Acesso em: 30 mar. 2019.

BRASIL. Ministério da Saúde. Conselho Nacional de Educação. **Resolução 196, de 10 de outubro de 1996**. Diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília, 1996. Disponível em: http://conselho.saude.gov.br/resolucoes/reso_96.htm. Acesso em: 17 nov. 2018.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização e Tecnologia da Informação. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Sumário Executivo, 2008. Disponível em: http://portal2.tcu.gov.br/portal/pls/portal/docs/2515176.PDF. Acesso em: 16 ago. 2018.

CHAUHAN, J.; TANEJA, S.; GOEL, A. Enhancing MOOC with Augmented Reality, Adaptive Learning and Gamification. *In*: INTERNATIONAL CONFERENCE ON MOOCS, INNOVATION AND TECHNOLOGY IN EDUCATION (MITE), 3., 2015. Proceedings […], 2015, p. 348-353. Disponível em: http://dx.doi.org/10.1109/mite.2015.7375343. Acesso em: 17 ago. 2019.

CILESIZ, S. Under graduate students' experiences with recorded lectures: towards a theory of acculturation. **Higher Education**, v. 69, n. 3, p. 471-93, 27 jun. 2014. Springer Science and Business Media LLC. Disponível em: http://dx.doi.org/10.1007/s10734-014-9786-1. Acesso em: 17 ago. 2019.

CLARK, D. **MOOCs**: taxonomy of 8 types of MOOC. 2013. Disponível em: http://donaldclarkplanb.blogspot.com/2013/04/moocs-taxonomy-of-8-types-of-mooc.html. Acesso em: 28 jun. 2019.

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

DECLARAÇÃO Universal dos Direitos Humanos. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 9 nov. 2018.

DIAS, C. A. **Grupo focal:** técnica de coleta de dados em pesquisas qualitativas. 2000. Disponível em: http://periodicos.ufpb.br/index.php/ies/article/download/330/252. Acesso em: 9 nov. 2018.

ERANKI, K. L. N.; MOUDGALYA, K. M. Comparing the Effectiveness of Self-Learning Java Workshops with Traditional Classrooms. **Journal of Educational Technology & Society**, p. 59-74, 29 mar. 2016.

FALBO, R. A. **Mapeamento Sistemático**. 2017. Disponível em: https://inf.ufes.br/~falbo/files/MP/TP/Sobre_MS.pdf. Acesso em: 27 out. 2018

FASSBINDER, A.; DELAMARO, M. E.; BARBOSA, E. F. Construção e uso de MOOCs: uma revisão sistemática. *In*: SIMPÓSIO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO, 25., 2014. **Anais [...]**, p. 332-341, 3 nov. 2014. Disponível em: http://dx.doi.org/10.5753/cbie.sbie.2014.332. Acesso em: 17 ago. 2019.

FENG, Y.; QU, G. Study on MOOC-based Blended Teaching Method in the University's Ideological & Political Education. **Educational Sciences**: Theory & Practice, v. 18, n. 5, p.1701-11, 31 out. 2018. Disponível em: http://dx.doi.org/10.12738/estp.2018.5.069. Acesso em: 17 ago. 2019.

FERRAZ, A. P. C. M.; BELHOT, R. V. Taxonomia de Bloom: revisão teórica e apresentação das adequações do instrumento para definição de objetivos instrucionais. **Gestão e produção,** São Carlos, v. 17, n. 2, p. 421-31, 2010. Disponível em: http://www.scielo.br/pdf/gp/v17n2/a15v17n2.pdf. Acesso em: 10 jan. 2020.

FOINA, P. R. Estratégia e segurança de informação. *In*: LYRA, Maurício 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. 2019.

FORNO, J. P.; KNOLL, G. F. Os MOOCS no mundo: um levantamento de cursos on-line abertos massivos. **Nuances**: estudos sobre Educação, Presidente Prudente, v. 24, n. 3, p. 178-94, set./dez., 2013. Disponível em: http://reaparana.com.br/portal/wp-content/uploads/2014/10/Os-MOOCs-no-mundo-2013.pdf. Acesso em: 17 ago. 2019.

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

FREITAS, A.; PAREDES, J. Understanding the faculty perspectives influencing their innovative practices in MOOCs/SPOCs: a case study. **International Journal of Educational Technology in Higher Education**, v. 15, n. 1, p. 2-13, 5 abr. 2018. Disponível em: http://dx.doi.org/10.1186/s41239-017-0086-6. Acesso em: 25 ago. 2019.

GENÉ, O. B.; NUNES, M. M.; FIDALGO, Á. Gamification in MOOC: challenges, opportunities and proposals for advancing MOOC Model. *In*: INTERNATIONAL CONFERENCE ON TECHNOLOGICAL ECOSYSTEMS FOR ENHANCING MULTICULTURALITY, 2., 2014. **Proceedings [...]**, 2014.

HE, W.; YUAN, X.; YANG, L. Supporting case-based learning in information security with web-based technology. **Journal of Information Systems Education**, v. 24, n. 1, p. 31-40, 2013. Disponível em:

https://pdfs.semanticscholar.org/f8ab/e022d666a7289e139fe5c2585f6697ba275f.pdf. Acesso em: 10 jan. 2020.

HERALA, A. et al. Experiences from Video Lectures in Software Engineering Education. **International Journal of Modern Education and Computer Science**, MECS Publisher, v. 9, n. 5, p.17-26, 8 maio 2017. Disponível em: http://dx.doi.org/10.5815/ijmecs.2017.05.03. Acesso em: 25 ago. 2019.

HOLANDA, A. C.; TEDESCO, P. MOOCs e Colaboração: definição, desafios, tendências e perspectivas. *In*: SIMPÓSIO BRASILEIRO DE INFORMÁTICA NA EDUCAÇÃO, 28., 2017. **Anais [...]**, Porto Alegre: Sociedade Brasileira de Computação, 2017. p. 243-252. Disponível em: http://dx.doi.org/10.5753/cbie.sbie.2017.243. Acesso em: 25 ago. 2019.

HUANG, Y. Construction of the Discipline System of Art The oryunder the Concept of Major Discipline. **Educational Sciences:** theory & practice, v. 18, n. 6, p.3777-83, 30 dez. 2018. Disponível em: http://dx.doi.org/10.12738/estp.2018.6.290. Acesso em: 25 ago. 2019.

HUISMAN, B. et al. Peer assessment in MOOCs: The relation ship between peer reviewers' ability and authors' essay performance. **British Journal of Educational Technology**, v. 49, n. 1, p.101-10, 1º dez. 2016. Disponível em: http://dx.doi.org/10.1111/bjet.12520. Acesso em: 25 ago. 2019.

HUSSAIN, M. et al. Using machine learning to predict student difficulties from learning session data. **Artificial Intelligence Review**, v. 52, n. 1, p. 381-407, 10 fev. 2018. Disponível em: http://dx.doi.org/10.1007/s10462-018-9620-8. Acesso em: 16 jan. 2020.

KITCHENHAM, B. A.; CHARTERS, S. **Guidelines for performing systematic literature reviews in software engineering**. Keele: Keele University; Durham: University of Durham 2007.

KLOOS, C. D. et al. Mixingand blending MOOC technologies with face-to-face pedagogies. *In:* IEEE GLOBAL ENGINEERING EDUCATION CONFERENCE (EDUCON), 2015, Tallin, Estonia. **Proceedings […]**, 2015, p. 967–71.

KOPPELMAN, H. Experiences with using videos in distance education. A pilot study: A course on human-computer interaction. **Issues in informing science and information technology**, n. 13, p. 269-77, 2016. Disponível em: http://www.informingscience.org/Publications/3472. Acesso em: 5 jul. 2019.

LEE, M.; PAK, J. Application of Hybrid Teaching Method Using the MOOC and Verification of its Effectiveness. **Journal of problem-based Learning**, p. 8-20, 14 jun. 2018.

LI, K. C. The evolution of open learning: A review of the transition from pre-e-learning to the era of e-learning. **Knowledge management & e-learning**, Hong Kong, v. 10, n. 4, p. 408-25, 2018. Disponível em: http://www.kmel-journal.org/ojs/index.php/on-line-publication/article/view/36. Acesso em: 2 abr. 2019

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.

LUO, H. et al. Applying case-based method in designing self-direct edon-line instruction: a formative research study. **Educational technology research and development**, v. 66, n. 2, p. 515-44, 16 fev. 2018. Disponível em: http://dx.doi.org/10.1007/s11423-018-9572-3. Acesso em: 4 abr. 2019.

LYRA, M. R. (org.). **Governança da Segurança da Informação.** Brasília: Edição do Autor, 2015. 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.

MELLATI, M; KHADEMI, M.; ABOLHASSANI, M. Creative interaction in social networks: multi-synchrono us language learning environments. **Education and information technologies**, v. 23, n. 5, p. 2053-71, 19 mar. 2018. Disponível em: http://dx.doi.org/10.1007/s10639-018-9703-9. Acesso em: 4 abr. 2019.

MINAYO, M. C. de S. Trabalho de campo: contexto de observação, interação e descoberta. *In*: MINAYO, M. C. de S.; DESLANDES, Suely F.; GOMES, Romeu (org). **Pesquisa social**: teoria, método e criatividade. 29. ed. Petrópolis, RJ: Vozes, 2010. p. 61-77.

MINAYO, M. C. de S. **O desafio do conhecimento**; pesquisa qualitativa em saúde. 3. ed. São Paulo; Rio de Janeiro: Hucitec-Abrasco, 2004.

MOÇAMBIQUE. Maputo. **Análise de dados**. CPC, 2008. Disponível em: http://www.cpc.unc.edu/measure/training/materials/data-quality-portuguese/modulo3_capa.pdf. Acesso em: 4 abr. 2019.

MOORE, M. G.; KEARSLEY, G. **Educação a distância:** uma visão integrada. Tradução: Roberto Galman. São Paulo: Cengage Learning, 2008. Disponível em: https://www.academia.edu/5116276/Uma_Vis%C3%A3o_Integrada. Acesso em: 30 mar. 2019.

MORAES, R. Análise de conteúdo. **Revista Educação**, Porto Alegre, v. 22, n. 37, p. 7-32, 1999. Disponível em: http://pesquisaemeducacaoufrgs.pbworks.com/w/file/fetch/60815562/Analise%20de%20conte%C3%BAdo.pdf. Acesso em: 4 abr. 2019.

NÓR, B. Cursos EAD estão crescendo no Brasil. **Revista Você S/A**, 1º fev. 2018. Disponível em: https://vocesa.abril.com.br/carreira/cursos-ead-estao-crescendo-no-brasil/. Acesso em: 5 out. 2018.

OLIVEIRA, S. L. de. **Tratado de metodologia científica**: projetos de pesquisas, TGI, TCC, monografias, dissertações e teses. 2. ed. São Paulo: Pioneira Thomson Learning, 2001.

PARK, Y.; YU, J. H.; JO, I. Clustering blended learning courses byon-line behavior data: a case study in a Korean Higher Education Institute. **The internet and higher education**, v. 29, p.1-11, abr. 2016. Disponível em: http://dx.doi.org/10.1016/j.iheduc.2015.11.001. Acesso em: 17 ago. 2019.

PEREIRA, A. M. de A. **Uso de recursos educacionais abertos (REA) na educação superior/UAB:** sonho ou realidade?. 2015. 163 f. Dissertação (Mestrado em Educação Matemática e Tecnológica) – Universidade Federal de Pernambuco,

Recife, 2015. Disponível em: https://repositorio.ufpe.br/handle/123456789/13845. Acesso em: 1º abr. 2019.

PÉREZ-SANAGUSTÍN, M. et al. H-MOOC framework: reusing MOOCs for hybrid education. **Journal of computing in higher education**, v. 29, n. 1, p. 47-64, 24 jan. 2017. Disponível em: http://dx.doi.org/10.1007/s12528-017-9133-5. Acesso em: 17 Ago. 2019.

PIAGET, J. **Estudos sociológicos**. Rio de Janeiro: Forense, 1973.

PONTOBR (Brasil). Núcleo de informação e Coordenação. **Estatísticas dos incidentes reportados ao CERT.br:** total de incidentes reportados por ano. 2020. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 11 fev. 2020.

QUEIROZ, L. R. S. **Pesquisa quantitativa e pesquisa qualitativa:** perspectivas para o campo da etnomusicologia. UFBP, 2006. Disponível em: http://periodicos.ufpb.br/ojs/index.php/claves/article/view/2719/2324. Acesso em: 10 abr. 2013.

QUINTELLA, H. L. M. de M. ; BRANCO, M. P. de O. **Fatores críticos de sucesso em segurança da informação em um órgão da Administração Pública Federal.** *In*: SIMPÓSIO NACIONAL DE INOVAÇÃO E SUSTENTABILIDADE (SINGEP), 2., 2013, São Paulo. Anais do II SINGEP e I S2IS. São Paulo: Uninove, 2013. p. 1-16. Disponível em:<http://repositorio.uninove.br/xmlui/handle/123456789/494>. Acesso em: 17Ago. 2018.

RAMNANAN, C.; POUND, L. Advances in medical education and practice: student perceptions of the flipped classroom. **Advances in Medical Education and Practice**, v. 8, p.63-73, jan. 2017. Disponível em: http://dx.doi.org/10.2147/amep.s109037. Acesso em: 14 nov. 2018.

RASI, P.; VUOJÄRVI, H. Toward personal and emotional connectivity in mobile higher education through a synchronous formative audio feedback. **British Journal of Educational Technology**, v. 49, n. 2, p. 292-304, 3 out. 2017. Disponível em: http://dx.doi.org/10.1111/bjet.12587. Acesso em: 17 go. 2019.

REEVES. T. Evaluating what really matters in computer-based education. *In*: WILD, M.; KIRKPATRICK, D. **Computer education**: new perspectives. Perth: Mathematics, Science & Technology Education Centre.1994. Disponível em: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7865&context=ecuworks#page=2. Acesso em: 16 jan. 2020.

RIBEIRO, L. O. M.; CATAPAN, A. H. Plataformas MOOC e redes de cooperação na EAD. **Revista de Educação A Distância**: Caminhos da autoria e criatividade na EAD, Porto Alegre, v. 5, n. 1, p.45-62, 15 jan. 2018. Disponível em: https://www.auniredе.org.br/revista/index.php/emrede/issue/viewFile/9/4. Acesso em: 23 jan. 2020.

RICHARDSON, R. J. et al. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas S.A., 2014.

RIEDO, C. R. F.; PEREIRA, E. M. de A.; WASSEM, J.; GARCIA, M. F. O desenvolvimento de um MOOC (Massive Open On-line 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: Qualidade na Educação: convergências de sujeitos, conhecimentos, práticas e tecnologias. 2014. **Anais [...]**. 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. 2019.

RIOS, O. K. L.; TEIXEIRA FILHO, J. G. de A.; RIOS, V. P. da S. 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, p. 49-65, 10 abr. 2017. Disponível em: http://navus.sc.senac.br/index.php/navus/article/ view/482. Acesso em: 17 ago. 2018.

SANTA-ROSA, J. G.; STRUCHINER, M. Design Participativo de um Ambiente Virtual de Aprendizagem de Histologia. **Revista Brasileira de Pesquisa em Educação em Ciências**, v. 10, n. 2, p.1-19, 2 dez. 2011. Disponível em: https://periodicos.ufmg.br/index.php/rbpec/article/view/3979. Acesso em: 25 mar. 2020.

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

SIEMENS, G. Massive Open On-line Courses: Innovation in Education?. *In*: MCGREAL R.; KINUTHIA W.; MARSHALL S. **Open Educational Resources:** Innovation, Research and Practice. Vancouver: Commonwealth of learning (COL), 2013. p. 5-16. Disponível em: https://oerknowledgecloud.org/content/massive-open-on-line-courses-innovation-education. Acesso em: 1º set. 2019.

SILVA, H. S. **Revisão sistemática sobre uso de MOOCS no Brasil.** 2017. 19 f. TCC (Especialização em Tecnologias da Informação e da Comunicação Aplicadas à Educação [EAD]), Universidade Federal de Santa Maria, Constantina, 2017. Disponível em: https://repositorio.ufsm.br/handle/1/12046. Acesso em: 17 ago. 2018.

SOUZA, R. de; CYPRIANO, E. F. MOOC: uma alternativa contemporânea para o ensino de astronomia. **Ciência & Educação**, Bauru, v. 22, n. 1, p. 65-80. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-73132016000100065. Acesso em: 17 Ago. 2019.

TORRES, M. de L.; GONZÁLEZ, R. M.; YAGO, F. M. WebGIS and Geospatial Technologies for Landscape Education on Personalized Learning Contexts. **Isprs International Journal of Geo-information**, v. 6, n. 11, p. 350-68, 8 nov. 2017. Disponível em: MDPI AG. http://dx.doi.org/10.3390/ijgi6110350. Acesso em: 25 ago. 2019.

TOVEN-LINDSEY, B.; RHOADS, R. A.; LOZANO, J. B. Virtually unlimited classrooms: Pedagogical practices in massive open on-line courses. **The Internet and Higher Education**, v. 24, p.1-12, jan. 2015. Disponível em: http://dx.doi.org/10.1016/j.iheduc.2014.07.001. Acesso em: 17 ago. 2019.

TRENTINI, M. ; PAIM, L. **Pesquisa convergente-assistencial:** um desenho que une o fazer e o pensar na prática assistencial em saúde-enfermagem. 2. ed. rev. e ampl. Florianópolis: Insular, 2004.

TREVISAN, A. L.; AMARAL, R. G. do. A Taxionomia revisada de Bloom aplicada à avaliação: um estudo de provas escritas de Matemática. **Ciência & Educação**, Bauru, v. 22, n. 2, p.451-64, jun. 2016. Disponível em:

http://www.scielo.br/scielo.php?script=sci_abstract&pid=S1516-73132016000200451&lng=en&nrm=iso&tlng=pt. Acesso em: 26 mar. 2020.

TRIPP, D. Pesquisa-ação: Uma introdução metodológica. **Educação e Pesquisa**, São Paulo, v.31, n.3, p.443-66, 2005.

TUMBO, D. L. **A Educação a Distância suportada por Tecnologias Digitais de Informação e Comunicação na Universidade Pedagógica de Moçambique:** proposta de indicadores de qualidade a considerar na implementação. 2018. 350 f. Tese (Doutorado em Ciências da Educação) – Instituto de Educação, Universidade do Minho, Braga, 2018. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/59045/1/Dion%C3%ADsio%20Lu%C3%ADs%20Tumbo.pdf. Acesso em: 30 mar. 2019.

UNESCO. Commonwealth of learning (COL). **Taking OER beyondthe OER Community.** Disponível em: http://oerworkshop.weebly.com/. Acesso em: 2 abr. 2019.

WACHTLER, J. et al. Ananalysis of the use and effect of questions in interactive learning-videos. **Smart Learning Environments**, p. 6-16, 2016. Disponível em: https://slejournal.springeropen.com/articles/10.1186/s40561-016-0033-3. Acesso em: 05 jul. 2019.

WORLD ECONOMIC FORUM (WEF). **Risks Report**. 15. ed. Davos, 2020. Disponível em: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Acesso em: 11 fev. 2020.

WU, R. A Studyon SPOC Assisted College Oral English Teaching Strategies. **Theory And Practice In Language Studies**, v. 7, n. 9, p.756-63, 1º set. 2017. Disponível em:<http://dx.doi.org/10.17507/tpls.0709.07.> Acesso em: 25 Out. 2019.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 11. ed. São Paulo: Atlas, 2012.

ZIEGENFUSS, D. H.; FURSE, C. Open ingup collaboration and part nership possibilities. **Digital Library Perspectives**, v. 32, n. 2, p.103-16, 9 maio 2016. Disponível em: http://dx.doi.org/10.1108/dlp-09-2015-0014. Acesso em: 25 out. 2019.

APÊNDICE A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE) - ALUNO MAIOR

I – DADOS DE IDENTIFICAÇÃO

Nome do Aluno: _____

Sexo: F ( ) M ( ) Idade: _____

II – EXPLICAÇÕES SOBRE A PARTICIPAÇÃO NA PESQUISA

O senhor(a) está sendo convidado a participar de uma pesquisa que tem como objetivo elaborar uma proposta de formação on-line sobre segurança da informação, aqui em salgueiro. Esta pesquisa sobre minha responsabilidade, William da Silva Melo, faz parte do curso de mestrado que estou realizando no Instituto Federal do Sertão Pernambucano, campus Salgueiro. Um dos resultados esperados nessa pesquisa é promover uma conscientização a respeito do uso seguro do meio digital, considerando os impactos que o vazamento de informações sigilosas pode causar.

Essa participação no referido estudo será no sentido de responder a questionários de opinião, entrevista a respeito dos temas, realizar capacitação on-line e participar de testes e fóruns de discussão on-line. É importante alertar de que podem esperar alguns benefícios dessa pesquisa, tais como: Melhoria do conhecimento acerca da segurança da informação, do uso seguro do meio digital e possibilidade de capacitação na temática. Um risco envolvido é a sua recusa em participar em algum momento, por se sentir exposto durante a coleta de dados. Porém, existe a garantia que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, identificar será mantido em sigilo.

A participação na pesquisa é voluntária e você poderá se recusar a participar do estudo, ou retirar seu consentimento a qualquer momento, sem precisar justificar o porquê deseja sair. Será assegurada a assistência durante toda pesquisa, bem como garantido o livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo e suas consequências, enfim, sobre tudo o que queira saber antes, durante e depois da sua participação. De igual maneira, caso ocorra algum dano decorrente a participação no estudo, será devidamente indenizado, conforme determina a lei.

III – IDENTIFICAÇÃO DOS RESPONSÁVEIS PELA PESQUISA

Os pesquisadores responsáveis pelo estudo são: William da Silva Melo, e-mail: williamdasilvamelo@gmail.com, telefone: (89) 99946-5063 e seu orientador Francisco Kelsen de Oliveira, e-mail: francisco.oliveira@ifsertao-pe.edu.br, telefone: (87) 9944-9397.

Comitê de Ética em Pesquisa Envolvendo Seres Humanos do IF SERTÃO-PE - Rua Aristarco Lopes, 240, Centro, CEP 56.302-100, Petrolina-PE, Telefone: (87) 2101-2359 / Ramal 103, http://www.ifsertao-pe.edu.br/index.php /comite-de-etica-em-pesquisa, cep@ifsertao-pe.edu.br; ou poderá consultar a Comissão nacional de Ética em Pesquisa, Telefone (61)3315-5877, conep.cep@saude.gov.br.

IV – CONSENTIMENTO PÓS-ESCLARECIDO

Declaro que após ter sido devidamente esclarecido pelo pesquisador sobre os objetivos, benefícios e riscos de minha participação na pesquisa e compreendido a natureza deste estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

Salgueiro ____ de_____ de 2019.

_____

Assinatura do Aluno

_____

Assinatura de pesquisador responsável

APÊNDICE B - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE) – PAIS/RESPONSÁVEIS

I – DADOS DE IDENTIFICAÇÃO

Nome do Aluno: _____

Sexo: F ( ) M ( ) Idade: _____

Nome do Responsável (Pai, Mãe ou Responsável):

_____

II – EXPLICAÇÕES SOBRE A PARTICIPAÇÃO NA PESQUISA

Seu filho (ou menor sob sua responsabilidade) está sendo convidado a participar de uma pesquisa que tem como objetivo elaborar uma proposta de formação on-line sobre segurança da informação, aqui em salgueiro. Esta pesquisa sobre minha responsabilidade, William da Silva Melo, faz parte do curso de mestrado que estou realizando no Instituto Federal do Sertão Pernambucano, campus Salgueiro. Um dos resultados esperados nessa pesquisa é promover uma conscientização a respeito do uso seguro do meio digital, considerando os impactos que o vazamento de informações sigilosas pode causar.

Essa participação no referido estudo será no sentido de responder a questionários de opinião, entrevista a respeito dos temas, realizar capacitação on-line e participar de testes e fóruns de discussão on-line. É importante alertar de que podem esperar alguns benefícios dessa pesquisa, tais como: Melhoria do conhecimento acerca da segurança da informação, do uso seguro do meio digital e possibilidade de capacitação na temática. Um risco envolvido é a sua recusa em participar em algum momento, por se sentir exposto durante a coleta de dados. Porém, existe a garantia que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, identificar será mantido em sigilo.

A participação na pesquisa é voluntária e você poderá se recusar a participar do estudo, ou retirar seu consentimento a qualquer momento, sem precisar justificar o porquê deseja sair. Será assegurada a assistência durante toda pesquisa, bem como garantido o livre acesso a todas as informações e esclarecimentos adicionais sobre o estudo e suas consequências, enfim, sobre tudo o que queira saber antes, durante e depois da sua participação. De igual maneira, caso ocorra algum dano

decorrente a participação no estudo, será devidamente indenizado, conforme determina a lei.

III – IDENTIFICAÇÃO DOS RESPONSÁVEIS PELA PESQUISA

Os pesquisadores responsáveis pelo estudo são: William da Silva Melo, e-mail: williamdasilvamelo@gmail.com, telefone: (89) 99946-5063 e seu orientador Francisco Kelsen de Oliveira, e-mail: francisco.oliveira@ifsertao-pe.edu.br, telefone: (87) 9944-9397. Comitê de Ética em Pesquisa Envolvendo Seres Humanos do IF SERTÃO-PE - Rua Aristarco Lopes, 240, Centro, CEP 56.302-100, Petrolina-PE, Telefone: (87) 2101-2359 / Ramal 103, http://www.ifsertao-pe.edu.br/index.php /comite-de -etica-em-pesquisa, cep@ifsertao-pe.edu.br; ou poderá consultar a Comissão nacional de Ética em Pesquisa, Telefone (61)3315-5877, conep.cep@saude.gov.br.

IV – CONSENTIMENTO PÓS-ESCLARECIDO

Declaro que após ter sido devidamente esclarecido pelo pesquisador sobre os objetivos, benefícios e riscos de minha participação na pesquisa e compreendido a natureza deste estudo, manifesto meu livre consentimento em participar, estando totalmente ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

Salgueiro ____ de_____ de 2019.

_____

Assinatura do Pai/Mãe/Responsável

_____

Assinatura de pesquisador responsável

APÊNDICE C - TERMO DE ASSENTIMENTO LIVRE E ESCLARECIDO – ALUNO MENOR

Você está sendo convidado a participar da pesquisa: Uma proposta de formação on-line sobre segurança da informação, sob responsabilidade dos pesquisadores Francisco Kelsen de Oliveira, professor do IF Sertão-PE, e William da Silva Melo, professor do IFBAIANO. Seus pais ou responsáveis sabem de tudo o que vai acontecer na pesquisa (riscos e benefícios) e permitiram que você participe. Esta pesquisa será realizada para propor um modelo de formação on-line, aberta e massiva, capaz de aliar teoria e prática na temática da segurança da informação. Você não é obrigado(a) a participar e poderá desistir sem problema nenhum. Você só participa se quiser. A pesquisa será feita no Instituto Federal do Sertão Pernambucano campus Salgueiro, onde vocês estudam. Para isso, será realizado aplicação questionários de opinião, entrevista a respeito dos temas, capacitação on-line e participação de testes e fóruns de discussão on-line. Esta pesquisa será realizada para promover conhecimento acerca da segurança da informação e do uso seguro do meio digital além de possibilidade de capacitação complementar na temática da segurança da informação. Um risco seria em algum momento você se sentir exposto durante a coleta de dados. Porém, existe a garantia que sua privacidade será respeitada, ou seja, seu nome ou qualquer outro dado ou elemento que possa, de qualquer forma, identificar será mantido em segredo. Os resultados da pesquisa vão ser publicados, mas sem identificar as pessoas que participaram.

Caso aconteça algo errado, nos procure pelos telefones (89) 99946-5063, (87) 9944- 9397 ou pelos e-mails: williamdasilvamelo@gmail.com, francisco.oliveira@ifsertao-pe.edu.br. Comitê de Ética em Pesquisa Envolvendo Seres Humanos do IF SERTÃO-PE - Rua Aristarco Lopes, 240, Centro, CEP 56.302-100, Petrolina-PE, Telefone: (87) 2101-2359 / Ramal 103, http://www.ifsertao-pe.edu.br/index.php /comite-de -etica-em-pesquisa, cep@ifsertao-pe.edu.br; ou poderá consultar a Comissão nacional de Ética em Pesquisa, Telefone (61)3315-5877, conep.cep@saude.gov.br.

_____ _____

Assinatura do Menor Assinatura do pesquisador

APÊNDICE D - QUESTIONÁRIO PERFIL DOS ALUNOS

Se você é aluno no Instituto federal do Sertão Pernambucano favor, responda esse questionário para que possamos conhecer e identificar suas opiniões sobre o ensino a distância e sobre a segurança da informação. Salientamos, que você não será identificado e será garantido total sigilo e anonimato das informações.

1 - Qual sua idade?

2 - Qual seu sexo?

( )Masculino ( )Feminino

3 - Qual ano você cursa?
( ) 1º ( ) 2º ( ) 3º ( ) 4º

4 - Informe o nível de dedicação que você considera ter nos estudos, de acordo com a escala abaixo?
0 1 2 3 4 5 6 7 8 9 10

5 - Informe o nível de disciplina que você considera ter com os horários de estudos, de acordo com a escala abaixo?
0 1 2 3 4 5 6 7 8 9 10

6 - Considerando sua rotina atual, informe quanto tempo você teria disponível diariamente para fazer um curso on-line de segurança da informação.
0 1 2 3 4 5 6 7 8 9 10

7 - Você possui de recursos tecnológicos como computador e internet em casa disponíveis para estudar?
( )Sim ( ) Não

8 - Considerando todo o tempo que você passa utilizando o computador, tablet, Smartfone ou outros recursos tecnológicos de acordo com a escala abaixo, informe a porcentagem de tempo que você usa essas ferramentas para estudar?

a) Menos de 10 %
b) Entre 10 e 20 %
c) Entre 20 e 30 %
d) Entre 30 e 40 %

e) Entre 40 e 50 %
f) Entre 50 e 60 %
g) Entre 60 e 70 %
h) Entre 70 e 80 %
i) Entre 80 e 90 %
j) Mais de 90 %

9 - Informe com que frequência você utiliza aplicativos, fóruns, chats ou outros recursos de comunicação em grupo para tratar de assuntos relacionados a educação?

Fórum de discussão – ( ) Desconheço ( )Nunca ( )Quase nunca ( )Às vezes ( )Quase sempre ( )Sempre.
Chat – ( ) Desconheço ( )Nunca ( )Quase nunca ( )Às vezes ( )Quase sempre ( )Sempre.
Grupos de Whatsapp/ telegram/ facebook – ( ) Desconheço ( )Nunca ( )Quase nunca ( )Às vezes ( )Quase sempre ( )Sempre.

10 - Você costuma se preocupar com segurança quando utiliza serviços (site, aplicativo, e-mail, rede social, etc.) localizados na Internet?

() Sim ( ) Não

11 - Você já forneceu dados pessoais como endereço, telefone ou CPF através de sites, e-mails, aplicativos, ou qualquer outro meio de comunicação?
( ) Sim ( ) Não

12 - Você sabe identificar quando um serviço (site, aplicativo, e-mail, rede social, etc.) possui a segurança adequada?
( ) Sim ( ) Não

13 - O furto de identidade é o ato pelo qual uma pessoa tenta se passar por outra, assumindo uma falsa identidade com o objetivo de obter vantagens indevidas. Phishing, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário. Considerando esses e outros riscos que enfrentamos na internet, informe na escala abaixo sua capacidade para se proteger desses riscos.

Nível de capacidade para me proteger desses riscos - 0 1 2 3 4 5 6 7 8 9 10

14 - Qual o nível de conhecimento que você considera ter no tema segurança da informação?
Nível de conhecimento no tema segurança da informação - 0 1 2 3 4 5 6 7 8 9 10

15 - Considerando a escala abaixo, informe o grau de interesse que você tem no tema segurança da informação?
Nível de interesse no tema segurança da informação 0 1 2 3 4 5 6 7 8 9 10

16 - Você já fez algum curso a distância?
( ) Sim ( ) Não

17 - Se você fizesse um curso on-line de segurança da informação quais conteúdos considera serem importante abordar?
Exemplos de conteúdo: 1 - Conceitos básicos de segurança 2 - Tipos de malwares (vírus, worms...) 3 - Criptografia e etc...

18 - Como você acha que deveria ser um curso on-line de segurança da informação ?
( ) Totalmente on-line, sem tutor/professor
( )On-line com tutor/professor on-line especializado
( ) Semi presencial, on-line e com encontros presenciais com o tutor/professor

19 - Considerando os aspectos teóricos e práticos do curso, como deve ser ofertado o curso?
Abordagem teórica ( ) 0% ( ) 10% ( ) 20% ( ) 30% ( ) 40% ( ) 50% ( ) 60% ( ) 70% ( ) 80% ( ) 90% ( ) 100%
Abordagem prática ( ) 0% ( ) 10% ( ) 20% ( ) 30% ( ) 40% ( ) 50% ( ) 60% ( ) 70% ( ) 80% ( ) 90% ( ) 100%

20 - Qual a sua opinião sobre a segurança da informação no meio digital?

APÊNDICE E – PRÉ-TESTE E PÓS-TESTE

01 - Qual o seu nome?

02 - Qual ano você cursa?
( ) 1º ( ) 2º ( ) 3º ( ) 4º

03 - Qual seu telefone (Preferencialmente Zap)?

04 - Considerando seus conhecimentos sobre segurança da informação e o texto a seguir: “É uma falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema”. Essa definição de se refere a:

a) Risco
b) Fragilidade
c) Ameaça
d) Impacto
e) Vulnerabilidade

05 - A figura acima apresenta um cenário no qual uma pessoa usa uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B. Com base na figura e nos seus conceitos sobre segurança da informação, julgue os itens subsequentes**.**

a) A representante uma vulnerabilidade
b) A representante uma ameaça
c) A representante um risco
d) A representante um impacto
e) A representa um ativo

06 - A figura abaixo apresenta um cenário no qual uma pessoa usa uma vara e uma corda C para atravessar o ponto 1 para o ponto 2, na presença de A e B. Com base na figura e nos seus conceitos sobre segurança da informação, julgue os itens subsequentes.

a) C representa uma ameaça
b) C representa um risco
c) C representa uma vulnerabilidade
d) C representa um ataque
e) C representa um ativo

07 - A Segurança da Informação (SI) é especializada na proteção de um conjunto de informações com fim de preservação ou valor que possui para um indivíduo ou

organização. Sobre como propriedades básicas de segurança da informação, marque uma alternativa correta.
( ) Disponibilidade, rastreabilidade e simplicidade
( ) Rastreabilidade, usabilidade e notoriedade
( ) Confidencialidade, integridade e disponibilidade
( ) Integridade, usabilidade e simplicidade
( ) Confidencialidade, autenticação e disponibilidade

08 - Um técnico de informática está analisando como recursos de diversas pragas virtuais (malwares), para executar a instalação do antivírus adequado. Dentre as características específicas por ele analisadas, estão:
I. Programa que, além de executar as funções para as quais foram executadas, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário. Um exemplo é um programa que recebe ou obtém sites na Internet e que parece ser inofensivo. Esse programa geralmente consiste em um único arquivo e é explicitamente executado para que seja instalado no computador. II. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído na ação de outros códigos maliciosos, que podem afetar o computador ou atacantes que exploram vulnerabilidades existentes nos programas utilizados no computador. Após incluído, ele é usado para garantir o acesso futuro ao computador comprometido, permitir que ele seja acessado remotamente, caso haja necessidade de executar novamente os métodos de execução de invasão ou infecção e, na maioria dos casos, sem que seja notado. III. Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário. As descrições acima são, corretas e respectivamente, correspondentes a:

( ) Cavalo de Troia (trojan), backdoor e Ransomware
( ) Worm, backdoor e vírus
( ) Vírus, spyware e rootkit
( )Spyware, cavalo de Troia (trojan) e Ransomware
( )Bot, Rootkit e cavalo de Tróia (Trojan)

09 - Existem diversos tipos de códigos maliciosos, entre eles o spyware. Acerca desse assunto, é correto afirmar que Spyware consiste em:
( ) Programa ou parte de um programa de computador, normalmente malicioso, que se propaga, inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.
( ) Programa que além de projetar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário.

( ) Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.
( ) Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
( ) Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

10 - O _____ é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. É notadamente responsável por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho da rede e a utilização do computador. Assinale a alternativa que CORRETAMENTE preenche a lacuna do texto acima.
( ) Vírus
( ) Trojan
( )Spyware
( )Keylogger
( ) Worm

11 - E-mail spoofing é uma técnica que pode ser utilizada para propagação de códigos maliciosos, envio de spam e golpes de phishing. Esta técnica consiste em:
( ) Alterar as configurações de um servidor de e-mail para que dispare uma infinidade de e-mails falsos até encher a caixa de correio de um ou muitos usuários
( ) Falsificar o protocolo SMTP para inspecionar os dados trafegados na caixa de e-mail do usuário, por meio do uso de programas específicos.
( ) Alterar os campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.
( ) Efetuar buscas minuciosas no computador do usuário, com o objetivo de identificar informações sigilosas.
( ) Alterar os campos do protocolo SMTP, de forma que os e-mails do usuário sejam direcionados para outra sem que ele saiba.

12 - Das alternativas a seguir, assinale a única que contém eventos que caracterizam uma tentativa de ataque do tipo força bruta.
( ) Brechas resultantes de bugs no sistema
( ) Sobrecarga de servidores, alcançada por meio de ataques simultâneos e descentralizados
( ) A operação local e não autorizada de estações ou servidores
( ) A repetição automática de tentativas de acesso a um recurso protegido, com senhas criadas a partir de combinações aleatórias ou extraídas de listas pré-definidas.
( ) A captura de dados sensíveis a partir de um programa espião instalado no computador do usuário.

13 - A técnica de Sniffing

( ) Utiliza um ou mais computadores para tornar indisponível um serviço provido
( ) Tenta adivinhar por tentativa e erro a senha de um usuário.
( ) Captura e inspeciona dados que trafegam em uma rede
( ) Altera campos do cabeçalho de mensagens de e-mail para falsificar a origem da mensagem
( ) Altera o conteúdo de páginas web de forma maliciosa e publica informações contra a instituição mantenedora da página web.

14 - Spam e Spyware são basicamente:
( ) Dois softwares do typo player de vídeo
( ) Dois tipos de vírus fatais que podem danificar um computador.
( ) Respectivamente, um e-mail não solicitado e um programa espião
( ) Respectivamente, um programa espião e um e-mail não solicitado
( ) Respectivamente, um e-mail espião e um vírus de computador.

15 - Vários computadores de uma rede estão gerando spam, disseminando vírus, atacando computadores e servidores de forma não prevista pelos administradores. Foi identificado um malware que é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados nos computadores infectados, tornando-os zumbis. Tal comportamento é tipicamente ocasionado por uma ação de
( )Keylogger
( )Botnet
( ) Adware
( )Phishing
( )Spyware

16 - Na quinta-feira de manhã, John, um empregado da universidade XYZ, notou uma mensagem de aviso em seu computador dizendo que o sistema foi atacado por um Win32.VB worm. Mesmo que o software antivírus estava presente no sistema, o software não conseguiu detectar o novo worm porque não foi atualizado para a versão mais recente. Quando John tentou abrir seu e-mail, ele experimentou uma conexão de internet lenta. Ele percebeu que havia alguns nomes de arquivo incomuns no disco. John imediatamente informou seu amigo Bob, que também era um empregado XYZ, do problema. Bob checou seu computador em seu escritório e experimentou o mesmo problema que John. John e Bob verificado vários computadores nos laboratórios, e descobriu que Win32.VB verme havia infectado muitos outros computadores no laboratório. Eles contataram o setor de TI da Universidade XYZ. O administrador do sistema verificou os computadores constatando o incidente de segurança da informação. Como um resultado do ataque verme as atividades no laboratório da Universidade XYZ foram suspensas, o que causou um grande inconveniente. Na sua opinião, qual foi a vulnerabilidade explorada? Quais medidas devem ser adotadas para conter e se recuperar do incidente de segurança da informação relatado no estudo de caso acima?

17 - Você está acessando uma rede social logado em sua conta pessoal e de repente visualiza um anúncio do site americanas contendo uma promoção imperdível de máquina de lavar. Como tinha feito recentemente uma pesquisa, comparando preços e marcas desse produto, percebe que o valor do anúncio se encontra muito abaixo do praticado no mercado. Ao clicar é redirecionado para uma página muito semelhante a da americanas, que detalha melhor a promoção, explica que você deve aproveitar a oportunidade relâmpago, que é possível comprar com apenas um clique (não é necessário cadastro) e afirma que a única modalidade de pagamento é por meio de boleto bancário. Sendo assim, salienta que a promoção está acabando naquele mesmo dia e que restam apenas poucas unidades do produto em estoque. Após gerar o boleto bancário e efetuar o pagamento da compra você tenta acompanhar o envio do produto pelo número do pedido descrito no boleto. Porém, não consegue visualizar o pedido cadastrado para sua compra no site, entra em contato telefônico pelo canal de atendimento ao cliente e percebe que foi vítima de um golpe. De acordo com os conhecimentos adquiridos no curso identifique quais vulnerabilidades podem ter sido exploradas para enganar o usuário? Identifique quais estratégias de golpe foram utilizadas? Explique quais ações o usuário deveria ter adotado para identificar a fralde? O que deve ser feito caso o usuário efetue o pagamento do boleto fraudulento?

18 - Crie um arquivo de "vírus" com o nome "DOCUMENTO" que seja capaz de desligar a máquina do usuário quando ele executar o arquivo.

19 - Considerando as estratégias de golpe e ataques que ocorrem na internet, faça a cópia de uma página que contenha uma oferta real em um site de vendas conhecido como: magazine Luíza, Americanas, Ricardo eletro ou outro...

APÊNDICE F - JOGO MOOCSEG

Material necessário

- 2 baralhos MOOCSEG
- 2 fitas adesivas
- Cronômetro
- Brinde (Prêmio)

Regras

- O professor ou mediador deve dividir a turma em dois grupos
- O baralho deve ser misturado, cada grupo receberá 15 pares de cartas contendo conceito – definição, esses conceitos estão relacionados aos princípios da segurança da informação e aos códigos maliciosos conforme ilustra a sessão baralho MOOCSEG.
- Não é permitida consulta
- Os grupos tem quinze minutos para discutir entre si o que consideravam ser os pares de cartas corretos
- Os grupos devem colar as cartas no quadro entregando suas respostas
- Cada par de cartas correto equivale a um ponto.
- Depois que o tempo acaba os grupos não podem entregar as respostas
- É feita a conferência da pontuação de cada grupo
- Enquanto é feita a conferência o professor ou mediador pode discorrer sobre os pares de cartas dando exemplos e relacionando os conceitos com situações reais amplamente divulgadas pela mídia.
- O grupo que que fez mais pontos vence o desafio e ganha o brinde.

Baralho MOOCSEG

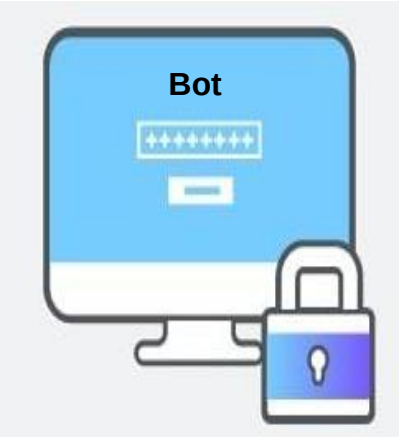
Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque

Possível evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso

Possível evento potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante

Programa ou parte de um programa de computador, normalmente malicioso, que permite inserir as seguintes cópias e se tornar parte de outros programas e arquivos.

Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.



Programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente

Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros

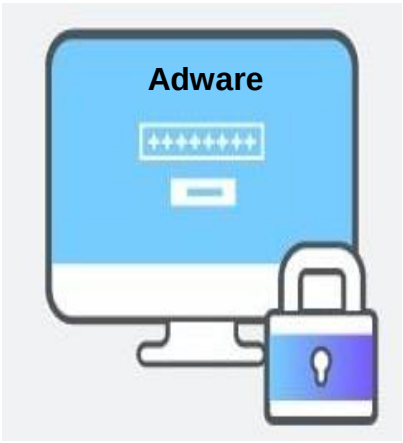
Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim

Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Código malicioso que exige o pagamento de um resgate para recuperar a informação do usuário

Golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social

Inspeciona os dados trafegados em redes de computadores



Spyware projetado especificamente para apresentar propagandas

Spyware capaz de armazenar a posição do cursor e a tela apresentada no monitor

Spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador

APÊNDICE G – ENTREVISTA COM OS ALUNOS

Pesquisador – Estão aqui os alunos do ensino médio integrado do curso informática eu quero esclarecer que essa pesquisa a participação é voluntária tá então se algum momento você se sentirem constrangidos ou quiserem sair da gravação da entrevista sintam-se à vontade. Eu preciso esclarecer também e todos os dados que forem colhidos aqui vai ser garantido o sigilo é Anonimato Então, se precisar utilizar alguma dessas falas vai ser usado um pseudônimo, um apelido, a gente não vai identificar vocês. Para que vocês fiquem bem à vontade nas respostas. Então, como a gente já comentou aqui anteriormente a temática do curso é um curso on-line, voltado para área da segurança da informação. tá então eu vou pedir a opinião de vocês para alguns temas a gente vai começar a falando a respeito dos conteúdos. Então pra vocês quais seriam os conteúdos devem ser abordados num curso on-line nesse tema de segurança da informação ?

Aluno 14- Falar sobre a detecção de sites, principalmente de compras que você utiliza dados importantes. A detecção desses sites que são vulneráveis a invasão, você saber se aquele site tem total segurança

Aluno 10 - tema bem interessante pra colocar seria criptografia, é ensinar as pessoas sobre proteção utilizando criptografia no hd pessoal...

Aluno 7– Acredito que o tema que seria fundamental seria introdução a segurança da informação, pois, tem pessoas que entram aqui no curso técnico e não tem noção.

Aluno 13– Não vou opinar sobre um conteúdo específico, seria uma ideia sobre a grade geral ser mais voltada pra segurança na internet e explicar também como os dados trafegam na internet. Como é que as vezes você pode usar um ip falso pra se passar por outro ip e pegar dados que eram dados que deveriam ser mandados pra o ip verdadeiro mas são enviados pra o ip falso, que eu acho que dá mais vontade de entender sobre segurança da informação.

Aluno 11– O que eu penso é que deveria ter um dia assim, dedicado a segurança, explicando quais medidas você deve tomar na rede pra não ser infectado. Por exemplo, como fazer senhas fortes, essas coisas assim.

Pesquisador - Mais alguém quer falar sobre esse tema ?

Pesquisador - Podemos passar pra o próximo ?

Quais as mídias ou elementos que devem ser utilizados nesse curso? Elementos no sentido assim ... texto, vídeo, animação ?

ALUNO 13– Pra mim a gente deve pegar casos reais por exemplo, o vazamento dos perfis dos políticos brasileiros que teve. Tem um canal no Youtube que eu acompanho o nome dele é Gabriel pato e foi muito bom, muito interessante porque ele explicou tudo que o cara fez lá! Acho que você pegar exemplos reais de coisas que aconteceram ao longo da história e há! vamos falar sobre ataque! Como foi que aconteceu! Acho que dá uma boa visão pros alunos.

Aluno 14– acho que utilização de vídeo aulas, até misturada parte vídeo aula e parte ação, justamente pra tanto pra manter o interesse do aluno, pra ele conseguir ficar mais vidrado no vídeo aula quanto pra deixar mais simples possível alguma situação. Pegando esse exemplo agora do Aluno 13, deixar uma situação que pode ser complexa, tentar apresenta-la de uma forma simples até gerar problematização

Aluno 10 - Eu acredito também que seria importante texto, porque assim... Eu já pesquisei e o que eu sinto falta é de uma coisa palpável em termos de conteúdo. Por exemplo, como fazer um ataque tem muito vídeo sobre isso no Youtube . Mas, não tem nada que possa se dizer realmente poxa eu aprendi! Então, eu acho que é importante ter a junção desses dois, junto com o texto, deve se explicar tipo o que ele usou. O tutorial e o texto também de como manter a segurança uma coisa nesse intuito.

Pesquisador - Mais alguém quer falar sobre esse tema ?

Pesquisador - Podemos passar pra o próximo ?

Pesquisador - **A respeito dos métodos de avaliação, qual ou quais seriam adequados ?**

Aluno 14– acho que seria importante dois métodos um que seria parte teórica, pra ver se ele entendeu determinado conceito de todos os conteúdos e outra de alguma forma prática que fosse simplificada. Fazer uma detecção se o computador tem vírus, detectar se aquele site tem proteções ou não tem nenhuma vulnerabilidade coisas do tipo...

Pesquisador - Mais alguém quer falar sobre esse tema ?

Aluno 7– Eu acredito que como se trata de um curso a distância, teria que ter uma frequência muito boa das unidades, tipo toda semana ter uma atividade sem ser

muito pesado mais que fizesse o aluno ter essa vontade e também o compromisso com o curso.

Aluno 10 – Acredito que o que o Aluno 7quis dizer foi tipo... com desafios né, propõe desafios pros alunos, pois isso, é interessante pra manter a pessoa focada, nossa eu tenho uma atividade eu tenho um desafio pra fazer!

Pesquisador - Mais alguém quer falar sobre esse tema ?

Aluno 7– Quando eu tava falando nessas atividades com frequência seria atividades menos pesadas mais que quando for olhar o todo dá um conteúdo denso. Porque, se passar alguma coisa muito pesada logo de cara, o aluno ele nem vai tentar fazer kkk.

Aluno 13- kkkkk Eu acredito que o que Aluno 10 também quis dizer com desafio foi... Pois, tem professor que fala há o desafio pra próxima semana é por exemplo, pegar o primeiro ano da gente o professor 6 eu lembro até hoje ele colocou para descobrir que tipo de dados o cabo SATA transmite. Aí tipo, aquilo não é pesado mais só pelo fato dele colocar desafio já instiga o aluno. Então colocar algo simples mais que no final vai formar algo concreto.

Pesquisador - Mais alguém quer falar sobre esse tema?

Pesquisador - Podemos passar pra o próximo?

Pesquisador - **De que maneira pra vocês seria possível aliar teoria à prática?**

Aluno 14– Como o **Aluno 13** já tinha falado anteriormente, a sugestão é mostrar situações reais. Você ensina toda a teoria pro aluno e quer entender melhor como funciona essa teoria pega o exemplo de tal acontecimento. O professor traz o acontecimento de algo que utiliza todas aquelas teorias na prática. Então, assim você consegue ligar os dois e mostra que isso é possível de ser aplicado.

Aluno 10 – Acho que o que o **Aluno 14** falou é importante, mais acho que o aluno tem que fazer pois quando ele faz ele diz assim... Nossa eu fiz! consegui! é possível! Então, acho que além de demonstrar e fazer essa junção, colocar o aluno pra fazer também, pra praticar de uma forma segura, que ele não quebre nenhuma lei. Mas que ele possa dizer nossa eu fiz! sei lá o cara ter sei lá doutorado, manja mas eu também consegui. Pra instigar mais ainda ele a continuar focado no curso

Aluno 12 – Eu penso que como o **Aluno 14** falou, o professor vai trazer algo real assim e vai pedir pra o aluno fazer algo muito mais simplificado, só pra ele ter uma noção de como foi feito.

Aluno – **10** kkk alias **Aluno 10** Um bom exemplo kkkk. Um bom exemplo foi o que o professor 1 fez que ele deu um conteúdo sobre vírus pra gente e mandou agente fazer um arquivo .bat pra abrir a calculadora várias vezes, então foi algo simples mais interessante.

Aluno 13- Eu posso não exatamente falar sobre um exemplo mais tipo dá uma dica pra vocês vê ?kkkkkk Pois pronto, **Aluno 13** kkkkkk. Pelo menos na minha opinião os vídeos do Gabriel pato são um exemplo perfeito de como você alia teoria e prática, porque ele vai explicando e depois ele faz ele não só fala, ele fala e faz realmente todo o processo. Ele cria máquina virtual, ele usa o celular dele e cria um e-mail fake, ele até alugou um servidor mais tipo daqueles que é baratinho eu esqueci o nome agora. Um servidor lá pra usar, pra fazer a demonstração, ele faz as coisas num nível mais avançado, mas se dá pra fazer no nível avançado também dá pra fazer num nível mais simples. Aí seria mais ou menos isso, que no final é tudo que eles já falaram eu não adicionei nada kkkkkkkkkkkk.

Pesquisador - Mais alguém quer falar sobre esse tema?

Pesquisador - Podemos passar pra o próximo?

Pesquisador - Pra vocês qual deveria ser a duração desse curso ?

Aluno 10 – Acredito que deveria ser feito em módulos por exemplo, o primeiro ano, o módulo 2º ano, pra usar o conhecimento que nós já aprendemos no curso junto com o curso on-line. Por exemplo, no terceiro ano a gente tem redes né, é possível juntar segurança com redes, ia fazer com que os alunos pudessem aprender coisas dos dois conteúdos. Então acho que por módulo seria bem interessante

Aluno 14– Juntando a ideia de **Aluno 10** acho que três meses se encaixa bem, porque não é muito tempo, mas também não é pouco. E mais pra o final do ano pois, assim ele já juntou bastante conhecimento ao longo do ano e colocando no final ele consegue juntar o que ele já sabe com o que ele vai aprender nesses meses. Uma pergunta esse curso vai ficar disponível sempre disponível? Não! se for ficar sempre disponível concordo com **Aluno 10** por módulos seria o melhor jeito. Aí tipo se for fazer o cálculo, esse modulo aqui se for seguir o projeto do curso acho que ele vai demorar 3 meses pra terminar assim, estudando umas 3 horas por semana.

Aluno 7– Mas eu acredito que tem que colocar um limite aí, se não vai ficar postergando, postergando até chegar lá no final e não vai ter feito. Acho que seria melhor colocar prazos. E vou discordar um pouco de **Aluno 14** porque ele falou que seria melhor colocar mais pra o final do curso de cada ano letivo, se for pensar assim

até faz sentido porque o aluno já vai ter adquirido conhecimento pra nessa parte final do curso conseguir resolver os problemas as atividades que serão propostas. Mas o primeiro semestre é o período que o aluno está mais tranquilo ainda assim, é o período que ele mais tem tempo pra realizar outras atividades que não são da escola. Já no período final ele está mais preocupado com as coisas da escola ele pode acabar deixando até de lado as coisas do curso.

Aluno 11– Eu acho que se for falar do período os assuntos aprendidos nesse curso podem auxiliar ao longo do ano.

Aluno 10 – Interessante acho que o **Aluno 7** disse, acho que maioria aqui não vai conhecer mais eu sou um cara que gosto de estudar pra concurso, tem o alfacom uma grande empresa de concurso público brasileira. E eles colocam o tempo, você faz sua inscrição e tem acesso ao curso, só que sê tem um tempo pra usufruir daquele curso, passou aquele tempo aquele curso não é mais seu e se você quiser novamente vai ter que adquirir de novo. Então, o que o **Aluno 7** falou faz sentido porque se não vai ficar postergando, postergando e pode ser que outra pessoa poderia estar usufruindo daquele conteúdo e não está aproveitando.

Pesquisador - Mais alguém quer falar sobre esse tema?

Pesquisador - Podemos passar pra o próximo?

Pesquisador -**Qual seria o cronograma, acho que vocês já falaram um pouco, mais alguém quer acrescentar a respeito do tema ?**

Aluno 9 - Acho que uma alternativa seria colocar um curso de férias por exemplo kkkkk.

Aluno 10 – kkkkkkkkkk olha vamos ser sinceros, Pow! Só se... Não, não dá! kkkk. Acho que poucas pessoas vão abdicar de suas férias pra fazer um curso on-line. Acho que pouquíssimas, vamos ver só aqui quantos fariam isso nas suas férias ?kkkkkkkkkkkkk

Aluno 14– Cara eu não fiz nem o projeto kkkkkkkkkkkkkk quanto mais curso on-line

Aluno 10 – Então o que quero dizer acho que no primeiro semestre é interessante.

Aluno 14– Questão de prazo, prazo de entrega de atividade sempre bom colocar pro final da semana, sábado ou domingo. Pois, justamente porque se ele não

tiver tempo na semana ele tem esses dois dias pra fazer, colocar no meio da semana complica a situação do aluno.

Aluno 7– Eu acredito também que não seria bom passar projetos que dessem longo tempo de duração, porque acredito na teoria que o aluno vai relaxar também kkkkk. Então seria melhor colocar prazos semanais, naquela ideia que é melhor colocar algo que ao primeiro olhar é simples, mais que quando vai pra o todo tem alguma coisa bem densa e completa.

Aluno 10 – O que **aluno 7** disse me deu um estalo.

Aluno 10 – Som do estalar de dedos

Aluno 9 – Oxe o que foi?

Aluno 10 - Enfim, aleatório, coisa de gente doida, tenta entender não! Rotatividade também seria interessante, porque você passa o conteúdo sê passa uma atividade baseada num conteúdo pra uma semana, só que quem garante que ele não vai esquecer aquilo no final do curso? Então é bom ter uma rotatividade nas atividades, é muito comum isso aqui na programação, você não pode ir pro quarto bimestre se você não tiver o conhecimento do primeiro. Não dá pra trabalhar com *for* se eu não souber utilizar uma variável. Então, essa conexão seria sempre necessária que eu volte pro início pra ter aquele conhecimento de novo pra eu poder desenvolver e continuar essa rotatividade.

Aluno 14- Sempre reaproveitando os outros conteúdos ...

Aluno 9 - Tipo subindo níveis...

Tem mais alguma coisa que vocês queiram acrescentar pra falar a respeito. Pois, já encerrou os tópicos se vocês quiserem acrescentar, comentar?

Quero agradecer então a participação de todos. Obrigado!

APÊNDICE H – ENTREVISTA COM OS PROFESSORES

Pesquisador - Então pra vocês quais seriam os conteúdos devem ser abordados num curso on-line nesse tema de segurança da informação?

Professor 1 – A temática dá uma visão geral mais introdutória, ver os conceitos iniciais até seu uso na prática. Segurança criptografia, acesso... E que os alunos também consigam orientar outras pessoas em relação a segurança de forma geral. Mais a nível de usuário, não chegar num nível avançado, do básico para o intermediário

Professor 2 – O que eu sugiro seria começar com uma abordagem mais tranquila como engenharia social, que é um tópico mais tranquilo e após essa parte que os alunos se interessam bastante pois é fácil de entender e é mais fácil abrir os olhos pra outras coisas. Depois seria falar um pouco sobre criptografia que eu acho essencial, as técnicas de criptografia que existem como a cifra de césar, que é o algoritmo mais simples que tem, depois falar de outros algoritmos como RSA. Além disso, falar sobre alguns tipos de ataque como DOS, DDOS. Falar sobre algumas questões como o próprio professor falou, como comprar, como gerar uma senha forte, como ter um site confiável.

Professor 1 – Certificado digital

Professor 2 – Certificado digital, sites com https né... que vai ter criptografia dos dados, acho que todos esses são temas interessantes que eles têm que minimamente conhecer. Acho que esses são os tópicos básicos que devem ser abordados nessa disciplina.

Professor 1 – A parte de malware também. Porque a ideia da disciplina é que ele tenha uma visão geral de segurança, que saiba o tema o que é segurança da informação e saiba aplicar a nível básico e intermediário, então ele tem que ter a capacidade de orientar uma pessoa leiga sobre como fazer uma compra na internet, os cuidados que tem que se tomar e etc.

Professor 2 – Os tipos de ataque que tem é ... sou professor de redes, quer dizer ensino um monte de coisas mais minha área de atuação é mais em redes. Em redes fica mais fácil falar sobre os tipos de ataque DOS DDOS aí tem a parte de spam de filtros de firewall. São assuntos um pouco mais complexos mais que são interessantes de ser abordados. Tem aquela técnica que você finge ter um ip que você

não tem e é legal o pessoal entender essas técnicas para criar mecanismos de segurança. Mais assim não cheguei a ministrar esses assuntos porque sei que há uma dificuldade técnica até pela bagagem que eles têm. Então, são assuntos bem interessantes, sê tem os ataques reflexivos, ataques de negação de serviço, syflood.

Professor 1 – E como ele vai pra uma empresa depois do curso técnico ele tem que saber por exemplo: Orientar uma pessoa a criar senhas seguras; Orientar a empresa a questão de uso de sites. Então, assim ele também ele deve ser capaz de criar um plano de segurança da informação para a empresa.

Professor 3 - Como está se visando assim para jovens, um público de médio integrado o conteúdo que aproximasse da realidade deles. Então, visse a questão das ementas, considerando a bibliografia existente, aquelas políticas de utilização de equipamentos. Mas, contextualizasse com coisas que às vezes ainda não estão em livros que são consagrados como por exemplo, redes sociais que é algo presente que os jovens utilizam com bastante frequência. E o exemplo da rede social você pode trazer para conteúdos que são vamos dizer assim... Corporativos né! Para você apresentar segurança da informação dentro da empresa, aquele plano diretor de políticas da informação.

Acredito que pegar os conteúdos clássicos que encontramos nos livros e contextualizar com a realidade do jovem que ele não tem essa vivência Empresarial corporativa. Mas ele tem a vivência de utilizar a internet e as redes sociais não fazer esse, esse, vínculo nessa junção das duas coisas. Então, pegar os contos clássicos e contextualizar na vida cotidiana.

Pesquisador Quais as mídias ou elementos que devem ser utilizados nesse curso on-line com essa temática?

Professor 2 – Bom... é... Acho que hoje em dia essa é uma questão bem complicada, porque só texto não vai funcionar mesmo. Acho que teria que ter vídeo certamente, ou uma forma interativa só um exemplo senha, como o professor falou, como ter uma senha forte sê vê que muitos sites pedem pra tu colocar caracteres especiais, número maiúsculo aí pode ter uma página onde o cara interage e pode dizer se a senha é fraca ou se é forte dinamicamente.

Se for algo muito texto teórico a gente sabe que hoje em dia não é atrativo principalmente, pra esses adolescentes que estão no Youtube o tempo todo.

Professor 1 – Nesse cenário hoje de rede social e da informação muito assim... então, se trouxer temas, estudos de caso ou realizar alguma atividade baseada em problema PBL trazer algo que se tenha baseado na mídia. Pois, só texto hoje com tanta multimídia que nós temos, só texto não atrai o aluno. Desafios, problemas reais, gamificação, algum processo que gere desafio pra o aluno! Pra que ele vá pra informação em todos os níveis né! Não só texto, texto... Então, vídeo, áudio, problema, ver algo que aconteceu real, acho que tudo isso agregado vai mais a atenção do aluno, vai gerar um conteúdo que seja melhor na questão da construção do conhecimento.

Professor 3 - Buscando utilizar o potencial da tecnologia eu acredito que o clássico que a gente vê nos cursos é ... no estilo MOOC é o vídeo né! mas nós temos um potencial da multimídia, que pode ser empregada, que pode enriquecer ainda mais esse, esse, curso!

A multimídia ela uma das características principais dela é a interação então, se for agregado elementos de interação dentro deste curso, aquele conteúdo teórico que ficou no vídeo e às vezes no material de leitura ele pode ser vivenciar uma prática, vamos dizer um pouco restritiva que não vai ser a não vai ser uma realidade, mas você tem um ambiente controlado ali multimídia que pode expor o aluno do curso. É uma situação dele vivenciar aquela teoria e ele viu no vídeo e que leu em algum material do texto então, acredito que a multimídia enriqueceria muito curso.

Pesquisador - Quais devem ser os métodos de avaliação utilizados?

Professor 2 – Na plataforma a distância é um pouco mais difícil

Professor 1 – É avaliar é sempre... Eu já fiz alguns cursos on-line que dão certificados por uma pontuação mínima. Mas pra área da segurança da informação acho que tem que ter atividades práticas, que ele possa desenvolver e ele vai ganhando uma pontuação. Tem que ter também perguntas pra quando o aluno acabe de ler ele responda, algum tipo de interação nesse sentido

Professor 2 – Algumas perguntas com um tempo pra ele responder, no final da unidade, Atividades práticas, pode ver também o nível de interação nos fóruns, isso é muito comum quando a gente pega AVA ou MOOC. O pessoal medir a interação dos alunos, bem isso aí é uma área de estudo em mestrado, doutorado. Como você medir o grau de interação do aluno, o tempo que ele fica conectado na mesma página, o número de vezes que ele falou no fórum tudo isso são métricas que podem ser

coletadas. Mais a mais simples é você colocar um questionário, ver o número de posts que ele fez, ou replace que ele deu no fórum e fazer essas atividades práticas, concordo inteiramente com o professor **Professor 1** acho que é essencial nessa disciplina.

Professor 1 – Acho que ter um certificado também... É uma coisa que o aluno concorreu tem que receber. Bem isso dá a ele dá uma motivação pois, ele pensa vou fazer o curso e no final vai ter certificado.

Professor 3 - A avaliação sempre é um instrumento complexo né! Para se avaliar o que que foi absorvido ali pelo aluno acredito que uma mescla de, de elementos. Eu poderia ter questões em um formulário on-line objetivo e ter questões-problema que o aluno ele fosse refletir. Então, às vezes não seria uma questão que tivesse uma resposta única, mas fossem questões subjetivas.

Se for uma avaliação automática né que dá para se fazer com formulário com questões objetivas, mas a questão subjetiva que fosse exposta a ele fosse mais uma questão reflexiva, para que eles se colocassem naquela situação e conseguisse avaliar. E dá até para fazer a mescla disso né! Dá para fazer uma mescla de forma que a respostas objetivas elas estejam vinculadas a este cenário de reflexão. Eu acredito se fosse um curso totalmente on-line esse instrumento! Agora se for pensar no curso que tivesse uma parte presenciar aí até daria para utilizar outros instrumentos de avaliação entre os participantes, até que eles pudessem trabalhar de forma colaborativa, para que eles desenvolvessem soluções para problemas de fossem expostos, para as situações que fossem apresentadas, que apresentassem risco de segurança da informação, então, coisas do cotidiano coisas que pudessem ter um contexto corporativo.

Pesquisador - De que maneira pra vcs seria possível aliar teoria à prática?

Professor 1 – Como o professor**Professor 2** falou, criar ambientes, problemas reais que ele tenha que resolver, definir um servidor virtual, uma invasão um site de segurança em uma compra E-comerce, interagir, perguntar como ele iria resolver, como são os procedimentos, trazer meio que uma realidade que ele vai encontrar no mercado de trabalho

Professor 2 – Exatamente.

Pesquisador - Pra vocês qual deveria ser a duração desse curso?

Professor 1 - Difícil definir o tempo pois depende da quantidade de conteúdo, é o aluno em geral hoje ele faz dez coisas ao mesmo tempo. Então, ele também ter foco é... Talvez seria interessante definir um tempo de início, data tal e tem até data tal pra finalizar. Mas, definir um tempo específico depende do conteúdo a duração vai depender da quantidade de conteúdo.

Pesquisador – Tem uma pergunta que vai ser feita pra os alunos e talvez vocês como professores possam contribuir. Por dia quanto tempo vocês acham que eles teriam disponível pra se dedicar a um curso on-line, nessa temática de segurança, considerando já a quantidade de atividades que ele já tem.

Professor 2 - Contando 5 dias da semana?

Pesquisador - Sim contando 5 dias da semana?

Professor 2 - 30 mim

Professor 1 - É acho que está um bom tempo 30 min, porque se ele se interessar pelo curso ele faz em um dia, depende muito do interesse do aluno também

Professor 3 - Vai depender muito também da ementa que vai ser abordada, as vezes se for uma ementa muito densa aí é claro que tem que estender um pouco curso, mas imaginando se que seja algo introdutório para que o aluno ele tenha é... O mínimo de informações ali para compreender riscos e possíveis soluções, eu acredito que algo em torno de umas 40 horas seria interessante né! É ... seria um curso aí de... se fosse intensivo de uma duas semanas, que daria essas 40 horas e que o conteúdo fosse de uma forma é ... trouxesse a questão com a multimídia você poderia trazer algo mais interativo e lúdico, que tornasse o conteúdo mais receptivo né, pelo, pelo público.

Agente sabe que o público do médio integrado entre 13 e 14 anos então, como sua abordagem visa pegar os alunos de todos os anos não vai ter aquele mais imaturo e aquele que já está chegando ali adulto que vai ter um pouco mais de maturidade, então para tornar-se um clima mais suave aos conteúdos divide-se essa, essa carga horária de umas 40 horas entre conteúdos interativos conteúdos de leitura e de reflexão.

Pesquisador – Qual o cronograma que o curso deveria seguir, considerando o período letivo?

Professor 2 – Poderia ser um curso de férias acho que seria um ótimo momento pois os alunos estariam sem outra atividade e teriam tempo de se dedicar integralmente, só uma sugestão.

Professor 1 – É concordo

Professor 2 – Seria um curso mais intensivo.

Professor 3 - Se for pensar no aluno do ensino médio que está entrando o primeiro ano acredito que talvez fosse no segundo semestre do ano. Porque, o aluno quando ele entra, ele vai ter o primeiro impacto ainda não vai estar adaptado a instituição e depois que ele fazer as primeiras aulas de informática básica de conceitos fundamentais. Eu acredito que ele conseguiria absorver melhor as informações do curso.

Se fosse para o primeiro Ano no primeiro semestre ele não iria aproveitar tanto o conteúdo que fosse apresentado. Já, para os alunos do último anos lá na tua instituição tiver o quarto né... O quarto ano é ... eu acredito que tem que ser no iniciozinho. Porque, eles vão tá muito alvoroçados no final com a questão do Enem, questão de SISU, vão estar preocupados entrar em uma instituição de ensino superior. Então, se trouxesse curso para o início ou até não fosse ofertado para último ano. Porque pelo menos a realidade que a gente tem aqui no IF SERTÃO-PE é que os alunos do último ano do ensino médio eles, eles, não se concentram tanto para esse tipo de atividade, porque a cabeça deles está voltada muito para finalizar o curso e ingressar na universidade. Então, mais ou menos o que eles pensam a estratégia que eles traçam então acredito que do primeiro ao terceiro ano no caso seria mais interessante.

Pesquisador - Quero assegurar que vcs não serão identificados na pesquisa, caso seja necessário citar algumas das falas vai ser usado um pseudônimo.

Obrigado aí pela contribuição, tem mais alguma coisa que você queria sugerir?

Professor 2 - Por anda

Professor 3 - Acredito que o curso sempre é válido e esse tema de segurança da informação está cada vez mais em voga. À medida que a quantidade de acesso à internet e dispositivos na rede né estão, estão interligados aí e os jovens principalmente eles não tem uma noção das consequências dos atos que eles fazem. Então, às vezes uma foto de brincadeira de um colega, é ... o endereço da casa e informações no cartão de crédito que passou ali de forma despretensiosa pode causar sérios danos e isso na vida pessoal deles. E se eles não têm orientação básica eles

podem começar até estagiando em uma empresa muito antes dizer a disciplina segurança da informação no curso.

Então, ela começa ali no primeiro ano da estagiar, talvez ou no segundo aquele estágio não obrigatório e lá dentro da empresa por não ter noções mínimas ele pode até expor a empresa e os clientes dessa empresa a situações complicadas e até situações que podem levar a crimes virtuais e danos financeiros físicos ou psicológicos aos envolvidos né! Então, acredito que é muito válidos informações e que o curso ficasse. Sugestão né... Que ele ficasse on-line, para que a informação pudesse alcançar o maior número de pessoas possíveis, depois de concluída a pesquisa para não ficar restrito simplesmente é uma instituição essa participação

APÊNDICE I – TRANSCRIÇÃO GRUPO DE INTERAÇÃO

04/11/19 22:42 - As mensagens enviadas a este grupo agora estão protegidas com criptografia de ponta a ponta. Toque para obter mais informações.
04/11/19 22:42 - Você criou o grupo "Segurança Teoria/Prática"
04/11/19 22:43 - Você removeu Professor 4
04/11/19 22:47 - Você mudou a imagem deste grupo
04/11/19 23:01 - : Olá prezados, sejam bem-vindos ao grupo de discussão do curso Segurança da Informação – Aliando teoria e prática.
Iremos nos limitar a postagens relacionadas ao conteúdo do curso, ou seja, nada de correntes, evite postar mensagens com conteúdo de propaganda, brincadeiras, piadas, racismo, pornografia, ou ativismo político/religioso. Afinal, a intenção é que vocês possam tirar suas dúvidas sobre o conteúdo do curso.
Iniciaremos nossas discussões com a primeira unidade (conceitos e princípios da segurança da informação, uso seguro das redes sociais e criptografia)
07/11/19 08:39 - Aluno 1 entrou usando o link de convite deste grupo
07/11/19 09:35 - Aluno 26 entrou usando o link de convite deste grupo
07/11/19 16:52 - Aluno 27 entrou usando o link de convite deste grupo
07/11/19 16:53 - Aluno 3 entrou usando o link de convite deste grupo
07/11/19 17:03 - Aluno 19 entrou usando o link de convite deste grupo
07/11/19 17:36 - Aluno 4 entrou usando o link de convite deste grupo
07/11/19 18:59 - Aluno 28 entrou usando o link de convite deste grupo
07/11/19 19:15 - Aluno 3 : Professor, manda as fotos dos ganhadores
07/11/19 19:17 - :Eita, kkkk não tirei de todos
07/11/19 19:17 - :<Arquivo de mídia oculto>
07/11/19 19:17 - :<Arquivo de mídia oculto>
07/11/19 19:56 - Aluno 20 entrou usando o link de convite deste grupo
07/11/19 21:58 - Aluno 2 entrou usando o link de convite deste grupo
11/11/19 20:10 - Você adicionou Aluno 29, Aluno 30 , Aluno 31 , Aluno 32, Aluno 33 , Aluno 15 , Aluno 34 , Aluno 23 , Aluno 35 , Aluno 36, Aluno 38, Aluno 37, Aluno 21 , Aluno 39 , Aluno 40 , Aluno 41, Aluno 2 , Aluno 42 , Aluno 43 , Aluno 25 , Aluno 44, Aluno 45 , Aluno 24 , Aluno 22 , Aluno 46 , Aluno 25 , Aluno 47 , Aluno 48, Aluno 49, Aluno 50 , Aluno 51 , Aluno 52, Aluno 4 , Aluno 6 , Aluno 7 e Aluno 53
11/11/19 20:10 - : Olá Pessoal, sejam bem-vindos ao grupo de discussão do curso Segurança da Informação – Aliando teoria e prática https://mooc-seginfo.appspot.com/moocseg/course. Aqui você pode tirar suas dúvidas, fazer comentários, conversar com os colegas.
Espero que consigam iniciar logo os estudos!! Gostaria que nos limitássemos a postagens relacionadas ao conteúdo do curso, ou seja, nada de correntes, evite postar mensagens com conteúdo de propaganda, brincadeiras, piadas, racismo, pornografia, ou ativismo político/religioso. *Favor, não mandem áudios*
Iniciaremos nossas discussões perguntando o que acharam do jogo de cartas MoocSeg ?
11/11/19 20:11 - :<Arquivo de mídia oculto>
11/11/19 20:14 - Aluno 19: Gostei muito, mas fiquei surpreso de ter errado tantos. Alguns detalhes na descrição de cada carta confundiam um pouco, achei que acertaria mais, principalmente os que julgava conhecer bem. Foi divertido!

11/11/19 20:16 - : Que bom que gostou! Realmente, alguns detalhes fazem a gente se confundir. Interessante, que algumas daquelas definições caíram em provas de concurso então, vale a pena fixar...
11/11/19 20:33 - : E aí minha gente, mais alguém se manifesta ?
11/11/19 20:33 - Aluno 4: Tô com preguiça ;-;
11/11/19 20:36 - Aluno 25 : Concordo com o Aluno 19, achei que fosse acertar mais, mas acabei me deparando com umas palavras que nunca vi na vida. Foi bem legal!
11/11/19 20:44 - Aluno 30 saiu
11/11/19 20:49 - Aluno 21 : Foi bastante envolvente, e construtivo de alguma forma.
11/11/19 20:59 - Aluno 22 : Foi legal
11/11/19 21:00 - Você adicionou Professo 4
11/11/19 21:00 - Aluno 3 : Achei muito bom, ótimo jogo.
11/11/19 21:01 - Aluno 23 : Foi da hora
11/11/19 21:03 - Aluno 24 : Não vou mentir, eu só conhecia 30% dos cards ;-;
11/11/19 21:10 - Aluno 25 : Eu gostei do jogo de cartas
11/11/19 21:10 - Aluno 25 : e consegui acertar alguns porque jasobri esses ataques e foi bem difficil de resolver
11/11/19 21:14 - Aluno 4: Eu conhecia as palavras, mas esqueci os significados na hora ;-;
11/11/19 21:29 - Você removeu +55 87 9136-8768
11/11/19 21:30 - Você adicionou Aluno 54
11/11/19 22:10 - Aluno 32 saiu
12/11/19 08:28 - Aluno 41 saiu
13/11/19 16:07 - : Pessoal, Boa Tarde! Temos uma boa notícia!!! Conseguimos pontuação extra pra quem concluir integralmente o curso on-line de segurança até o dia 30/11 https://mooc-seginfo.appspot.com/moocseg/course. Até o momento Professor 4 e o Professor 2 já confirmaram e irão explicar pra vcs em sala
13/11/19 16:09 - : Essa semana tentem concluir ao menos a Unidade 1.
13/11/19 16:09 - Aluno 3 : Certo, estou quase lá.
13/11/19 16:09 - :
13/11/19 16:10 - : Vou mandar uma enquete aqui pra exercitarem conceitos da Unidade 1.
13/11/19 16:10 - :<Arquivo de mídia oculto>
13/11/19 16:10 - Aluno 3 : Ok
13/11/19 16:10 - : Considerando os conceitos sobre segurança da informação abordados na unidade 1, relacione 1 - Entrada, 2- Tiro e 3- Assaltante com os conceitos: Ameaça, Risco e Vulnerabilidade.
Ex: William 1-Ameaça, 2- Vulnerabilidade, 3-Risco
13/11/19 16:11 - : Copiem a resposta de vcs
13/11/19 18:13 - Aluno 25: É para mandarmos aqui mesmo?
13/11/19 18:25 - : Isso
13/11/19 18:29 - : Tipo assim☝
14/11/19 08:08 - : Galera, Bom Dia!
14/11/19 08:09 - : Estou achando vcs tão tímidos, tão inibidos no grupo ...
14/11/19 08:14 - : Retirei do curso o texto abaixo, vou postar aqui pra ver se ajuda na enquete. Não precisam ter medo de responder, aqui no grupo não temos nenhum tipo de avaliação.
14/11/19 08:14 - : A *vulnerabilidade* está intimamente ligada ao ponto fraco de um ativo, ou seja, pode ser entendida como uma fragilidade.

Ameaça pode ser considerada como um agente que causa determinado evento ou atitude indesejável com potencial para remover, desabilitar ou destruir um recurso.
Um *risco* de segurança é um evento possível e potencialmente danoso a uma organização, isto é, um evento hipotético, que possui chance de ocorrência futura que não é nula e que apresenta impacto negativo significante.
Nesse sentido, percebemos que o risco está intimamente ligado ao impacto (dano real), a ameaça está muito mais relacionada com os agentes e as vulnerabilidades são as fraquezas que podem ser exploradas...
14/11/19 08:15 - :<Arquivo de mídia oculto>
14/11/19 08:15 - : Considerando os conceitos sobre segurança da informação abordados na unidade 1, relacione 1 - Entrada, 2- Tiro e 3- Assaltante com os conceitos: Ameaça, Risco e Vulnerabilidade.
14/11/19 08:16 - Aluno 21 saiu
14/11/19 08:54 - Aluno 25: Aluno 1-Vulnerabilidade; 2-Risco; 3-Ameaça.
14/11/19 08:59 - :
14/11/19 08:59 - : Alguém concorda, discorda?
14/11/19 09:31 - Aluno 6 :
14/11/19 09:32 - Aluno 3 :
16/11/19 19:57 - Aluno 29 saiu
18/11/19 16:10 - : Pessoal, Boa Tarde! temos outra boa notícia! Além dos Professor 4 e Professor 2, o Professor 5 (Física 1º ano) concordou em dar pontuação extra para aqueles que concluírem o curso até 30/11. https://mooc-seginfo.appspot.com/moocseg/course
18/11/19 16:11 - Aluno 2 :Uou
18/11/19 16:12 - Aluno 2 : É quanto tempo o curso ???
18/11/19 16:12 - Aluno 2 : Ele dura quanto tempo
18/11/19 16:12 - Aluno 2 : .?
18/11/19 16:13 - :vc faz ele de acordo com seu ritmo. vai ficar disponível até 30/11
18/11/19 16:13 - : Peço que tentem concluir a unidade 2 até 23/11 e a unidade 3 até 30/11.
18/11/19 16:13 - : qualquer dúvida postem aqui
18/11/19 16:15 - : sugiro que quando chegarem no jogo criptografia (última atividade da unidade 1 usem o chrome ou outro navegador que permita tradução)
18/11/19 16:15 - : https://studio.code.org/s/hoc-encryption/stage/1/puzzle/1
19/11/19 15:57 - Aluno 25 : Ainda é possivel realizar a inscrição para o curso?
19/11/19 16:40 - Aluno 22 :<Arquivo de mídia oculto>
19/11/19 17:03 - : Pode sim kkk
19/11/19 17:03 - : Pessoal, Boa Tarde! temos outra boa notícia! Além dos Professor 4 e Professor 2, o Professor 5 (Física 1º ano) concordou em dar pontuação extra para aqueles que concluírem o curso até 30/11. https://mooc-seginfo.appspot.com/moocseg/course
19/11/19 17:04 - : Nesse link
20/11/19 18:50 - Aluno 54 entrou usando o link de convite deste grupo
23/11/19 06:43 - : Pessoal, bom dia! Como estão evoluindo no curso? Ainda temos 8 dias para terminarmos as unidades. Vamos lá
23/11/19 07:38 - Aluno 3 : Estou terminando a 2 unidade.
23/11/19 07:48 - : Que bom, vai dar certo!
23/11/19 07:50 - : Quem mais começou o curso pode dar um joinha?
23/11/19 08:06 - :Vamo lá minha gente, é só um joinha, vai doer não kkkkk
23/11/19 08:09 - Aluno 3 :

23/11/19 09:03 - Aluno 25 :
23/11/19 10:00 - Aluno 4 :
23/11/19 15:13 – Aluno 27:
23/11/19 15:39 - Aluno 4:
23/11/19 15:51 - Aluno 43 saiu
25/11/19 15:45 - : Pessoal, Quero parabenizar os que já conseguiram concluir o curso. Aluno 4, Aluno 6 e Aluno 1 (tempo record em dois dias kkk).
25/11/19 15:46-: o curso ainda está disponível no link: https://mooc-seginfo.appspot.com/moocseg/course até o dia 30/11
25/11/19 15:47 - : lembrando que os Profs: 5, 2, 1 e 4 darão pontuação extra para aqueles que concluírem
25/11/19 15:51 - : Interessante lembrar também que o conteúdo abordado e muitas questões do curso foram retiradas de concursos da área
25/11/19 15:53 - : como por exemplo essa aqui:
25/11/19 15:53 - : 05 - Um Técnico de Informática está analisando como recursos de diversas pragas virtuais (malwares), para executar a instalação do antivírus adequado. Dentre as características específicas por ele analisadas, estão:
I. Programa que, além de executar as funções para as quais foram executadas, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário. Um exemplo é um programa que recebe ou obtém sites na Internet e que parece ser inofensivo. Esse programa geralmente consiste em um único arquivo e é explicitamente executado para que seja instalado no computador. II. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído na ação de outros códigos maliciosos, que podem afetar o computador ou atacantes que exploram vulnerabilidades existentes nos programas utilizados no computador. Após incluído, ele é usado para garantir o acesso futuro ao computador comprometido, permitir que ele seja acessado remotamente, caso haja necessidade de executar novamente os métodos de execução de invasão ou infecção e, na maioria dos casos, sem que seja notado. III. Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário. As descrições acima são, corretas e respectivamente, correspondentes a
25/11/19 15:55 - : a) Cavalo de Troia (trojan), backdoor e ransomware
25/11/19 15:55 - : b) Worm, backdoor e vírus
25/11/19 15:55 - : c) Vírus, spyware e rootkit
25/11/19 15:56 - : d) Spyware, cavalo de Troia (trojan) e ransomware
25/11/19 15:56 - : e) Spyware, cavalo de Troia (trojan) e ransomware
25/11/19 15:56 - : Vamos lá!!! qual alternativa vcs acham que é a correta ?
25/11/19 15:57 - Aluno 42 saiu
25/11/19 16:01 - Aluno 34 saiu
25/11/19 16:02 - Aluno 3 : .
25/11/19 16:19 - Aluno 1 : Obrigado
25/11/19 16:43 - Aluno 4: Eu fiz speedrunksks
25/11/19 16:43 - Aluno 1 : 2 cara kkkk
25/11/19 20:10 - Aluno 6 :<Arquivo de mídia oculto>
25/11/19 20:17 - Aluno 3 :Atah
25/11/19 20:31 - Aluno 48: Gente desculpa aí mas estou saindo
25/11/19 20:31 - Aluno 48 saiu

25/11/19 20:56 - Aluno 35 saiu
26/11/19 06:10 - : Muito bom, Aluno 3 está afiado. Acertou
26/11/19 06:10 - :
26/11/19 08:27 - Aluno 3 :
26/11/19 08:27 - Aluno 19: Grande Aluno 3!
26/11/19 08:27 - Aluno 3 :<Arquivo de mídia oculto>
26/11/19 08:28 - Aluno 3 :<Arquivo de mídia oculto>
28/11/19 15:30 - : Pessoal, Boa Tarde!
28/11/19 15:30 - Aluno 3 : Boa tarde
28/11/19 15:32 - : Teremos uma live ou videoconf ao vivo para demonstrar um *ataque DOS* (ataque de negação de serviço) amanhã, Iremos utilizar o S.O Kali Linux.
28/11/19 15:33 - : qual seria o melhor horário pra vcs ?
28/11/19 15:33 – Aluno 48: Pra mim aparte da noite
28/11/19 15:33 - Aluno 48: Tá bom
28/11/19 15:33 - Aluno 3 : Pra mim a parte da manhã.
28/11/19 15:33 – Aluno 49: Noite tbm
28/11/19 15:36 - Aluno 7 : Noite
28/11/19 16:06 - Aluno 1 : A noite
28/11/19 16:17 - Aluno 25: Noite.
28/11/19 16:49 - Aluno 4: Noite
28/11/19 18:36 - Aluno 4 : Noite
29/11/19 09:24 - : Bom Dia Pessoal?
29/11/19 09:24 - : Como estão evoluindo no curso ? Iremos prorrogar a data para finalizar até 07/12, é o ultimo prazo pois temos que repassar os nomes para os profs que prometeram ponto extra
29/11/19 13:11 - :Pesoal Teremos uma videoconf ao vivo para demonstrar um *ataque DOS* (ataque de negação de serviço) hj às 19:30, mando o link no grupo, Não percam
29/11/19 14:21 - Aluno 25: Ok
29/11/19 14:21 - Aluno 4: Okay
29/11/19 17:29 - Aluno 1 mudou seu número de telefone para um novo número. Toque para enviar uma mensagem ou para adicionar o novo número.
29/11/19 19:31 - : Fala pessoal, Boa Noite
29/11/19 19:31 - : Vou mandar o link do videoconf.
29/11/19 19:33 - : Para participar da videochamada, clique neste link: https://meet.google.com/urp-jdfn-tko
Para participar por telefone, disque +1 929-249-3884 e digite este PIN: 333 281 589#
29/11/19 19:33 - : Se utilizarem celular é possível que seja necessário baixar o app
29/11/19 19:34 - : A videoconf ao vivo para demonstrar um *ataque DOS* (ataque de negação de serviço)
29/11/19 19:36 - Aluno 19: Vai ficar gravado em algum lugar?
29/11/19 19:38 – Aluno 48: Bora entre aí Aluno 19
29/11/19 19:38 - Aluno 19: kkkk
29/11/19 19:38 - Aluno 19: Meu nome é Aluno 19, rapas!
29/11/19 19:38 - Aluno 19: rapaz*
29/11/19 19:38 - Aluno 4: Não era Aluno 19?
29/11/19 19:39 - Aluno 19: Confundem kkk
29/11/19 19:39 - Aluno 4: Ksksks
29/11/19 19:39 – Aluno 48: Bora logo meu povo
29/11/19 19:39 - Aluno 19: Bora lá, galera!
29/11/19 19:39 – Aluno 54: Joamerson

29/11/19 19:40 - Aluno 19: Vou entrar, espero vocês lá! Ou todo mundo já está?
29/11/19 19:41 - Aluno 4: Asahsuahsuhasuh
29/11/19 19:41 - Aluno 4: Só está o professor e o Aluno 48
29/11/19 19:41 - Aluno 4: <Arquivo de mídia oculto>
29/11/19 19:46 - : voltei
29/11/19 19:46 - Aluno 4: Percebi ksks
29/11/19 19:53 - Aluno 4: bora ;-;
29/11/19 19:54 - Aluno 24 : Indisponível ;-;
29/11/19 19:54 - Aluno 4: Putz ;-;
29/11/19 19:54 - Aluno 22 :Tbm
29/11/19 19:54 - Aluno 4: ;-;
29/11/19 20:09 - Aluno 25: <Arquivo de mídia oculto>
29/11/19 20:10 - Aluno 4: ;-;
29/11/19 20:10 - Aluno 4: Abre no navegador
29/11/19 20:10 - Aluno 25: Ele redireciona pra google play
29/11/19 20:10 - Aluno 4: Abre no modo anônimo
29/11/19 20:11 - Aluno 25: Vou tentar
29/11/19 20:11 - Aluno 4: Aok
29/11/19 20:11 - Aluno 25: Mesma coisa
29/11/19 20:12 - Aluno 4: Abriu pelo Chrome? :/
29/11/19 20:12 - Aluno 25: Opera
29/11/19 20:12 - Aluno 4: Ah
29/11/19 20:12 - Aluno 4: Tendi
29/11/19 20:13 - Aluno 4: Tenta desativar a opção de redirecionar app nas configurações do Android
29/11/19 20:13 - Aluno 25: Ok
29/11/19 20:14 - Aluno 27 : Pô eu baixe o app e tô tentando entrar
29/11/19 20:14 - Aluno 4: Blz
29/11/19 20:22 - Aluno 25: A videoconferência está sendo gravada?
29/11/19 20:22 - Aluno 4: Creio que sim
29/11/19 20:24 - Aluno 25: Ok, quero assistir dps
29/11/19 20:24 - Aluno 4: Okay
29/11/19 20:24 - Aluno 27 : Pô num conseguindo nem entrar
29/11/19 20:24 - Aluno 27 : Nessa pexte
29/11/19 20:24 - Aluno 3 :
29/11/19 20:29 - Aluno 3 : Essa mensagem foi apagada
29/11/19 20:29 - Aluno 3 :<Arquivo de mídia oculto>
29/11/19 20:31 - Aluno 3 :Aceitaaakkk
01/12/19 18:18 - Aluno 7 : O curso já está indisponível?
01/12/19 18:27 - Aluno 25 : .
01/12/19 19:08 - Aluno 4 : o site ta fora do ar
01/12/19 20:14 - : O site do curso? Ou a live
01/12/19 20:17 - Aluno 4 : Do curso
01/12/19 20:17 - Aluno 4 : .
01/12/19 20:17 - Aluno 4 : Estou tentando por esse link
01/12/19 20:21 - : faz login na conta do gmail ou google primeiro. Depois clica no link
01/12/19 20:22 - :ta disponível
01/12/19 20:22 - :<Arquivo de mídia oculto>
01/12/19 20:22 - : esse link mesmo: https://mooc-seginfo.appspot.com/moocseg/course

01/12/19 20:25 - Aluno 33 saiu
01/12/19 20:30 - Aluno 7 :<Arquivo de mídia oculto>
01/12/19 20:53 - : O meu tbm está assim
01/12/19 22:39 - Aluno 4: <Arquivo de mídia oculto>
01/12/19 22:42 - : Tem que fazer login
01/12/19 22:43 - : Observem se depois do login a urlesta completa com o course do final? https://mooc-seginfo.appspot.com/moocseg/course
01/12/19 22:45 - Aluno 4: O link está correto
01/12/19 22:46 - Aluno 4: Eu estou logado
01/12/19 22:46 - Aluno 4: Meu Google Chrome sempre faz auto-login
01/12/19 22:46 - Aluno 4: :/
01/12/19 22:47 - : Ah perai, acho que estava até 30
01/12/19 22:47 - : E esqueci de prorrogar no sistema. Vou fazer aqui rapidinho
01/12/19 22:46 - Aluno 4: Caraca, o site se auto-destruiu antes do tempo
01/12/19 22:47 - :Kkkkkk
01/12/19 22:53 - : Pronto, foi falha nostra. Agora deve liberar
01/12/19 22:56 - Aluno 4: Agora voltou!
01/12/19 22:57 - :
01/12/19 22:56 - Aluno 4: <Arquivo de mídia oculto>
03/12/19 10:00 - : Pessoal, Bom Dia! Esta correndo o último prazo do curso, até 07/12 somente. Vamos lá vai dar tempo ...
03/12/19 10:01 - : Aluno 3, Aluno 20 e Aluno 4 já terminaram a 1º Unidade
03/12/19 10:02 - : Aluno 2 já concluiu e Aluno 7 já concluíram 2º unidade, falta pouco
03/12/19 10:04 - Aluno 3 : Estou na 3 já.
03/12/19 10:04 - : Aluno 32 e Aluno 31 tbm terminaram a 1º Unidade
03/12/19 10:05 - : Bom demais, falta pouco
03/12/19 10:05 - : Parabéns a todos que iniciaram o curso, vamos que vamos
03/12/19 10:09 - Aluno 4: Pera, eu ou algum outro ?
03/12/19 10:11 - Aluno 2 :Pq em
03/12/19 10:11 - Aluno 2 : ??
03/12/19 10:11 - Aluno 2 :<Arquivo de mídia oculto>
03/12/19 10:11 - Aluno 2 : Não é até dia 7
03/12/19 10:11 - Aluno 4 : Acho q sou eu
03/12/19 10:12 - Aluno 4: Ah
03/12/19 10:13 - : Eu atualizei o prazo. Esse print é de hj?
03/12/19 10:17 - : Atualizei a data da prova tbm. Vê se liberou aí
03/12/19 11:11 - : respondam tbm a avaliação do curso, é muito importante
03/12/19 11:15 - Aluno 2 :Ss
03/12/19 13:31 - Aluno 2 saiu
04/12/19 22:10 - : Pessoal, boa noite! Faltam apenas 3 dias. Vamos lá falta muito pouco pra alguns
04/12/19 22:10 - : Aluno 2 já conseguiu concluir
04/12/19 22:13 - : Aluno 31, Aluno 15, Aluno 49, Aluno 35, Aluno 20 e Aluno 32 já estão na unidade 2
04/12/19 22:14 - : Aluno 7 falta só a prova final e a avaliação do curso
06/12/19 09:57 - : Pessoas, Bom Dia! Segue a relação dos alunos que já conseguiram concluir o curso
1º ano
Aluno 1
Aluno 2

2º ano
Aluno 3
Aluno 4
4º ano
Aluno 5
Aluno 6
06/12/19 09:58 - Aluno 3 :
06/12/19 09:58 - :<Arquivo de mídia oculto>
06/12/19 09:58 - : Parabéns a todos
06/12/19 09:59 - : ainda temos 2 dias, hj e amanhã para aqueles que ainda não concluíram
06/12/19 10:00 - : Aluno 4 do 2º ano e Aluno 6 4º poderiam me passar no pv seus nomes completos ?
06/12/19 10:25 - Aluno 4: <Arquivo de mídia oculto>
08/12/19 08:31 - : Pessoal, bom dia! Terminamos hj a meia noite o prazo para concluírem o curso Segurança da Informação: aliando teoria e prática. Vamos lá, ainda da tempo https://mooc-seginfo.appspot.com/moocseg/course
08/12/19 08:35 - Aluno 19: Acho que a prova final não pode mais ser feita.
08/12/19 08:39 - : Já livre eu, testa aí
08/12/19 08:39 - Aluno 19: Funcionou!
08/12/19 08:39 - Aluno 19: Obrigado!
08/12/19 08:39 - :
10/12/19 15:31 - : Pessoal, boa tarde! Já enviei os nomes dos alunos que concluíram o curso pra os profs que prometeram pontuação extra.
10/12/19 15:32 - : O curso ficará disponível na plataforma para aqueles que desejarem fazê-lo durante o período das férias. Porém, não contará mais como pontuação.
10/12/19 15:34 - : Agradeço a todos estou a disposição para o que precisarem.
10/12/19 15:35 - : Amanhã vou excluir os membros do grupo. Kquer coisa chamem no PV
10/12/19 15:41 - Aluno 3 : Boa tarde Pesquisador, conversei com o professor 1 (De programação e aplicativo gráficos), ele disse que também iria dar 1 ponto extra em uma das suas matérias (fica a escolha do aluno).
10/12/19 15:41 - :Blz, enviei a lista pra ele tbm
10/12/19 15:41 - Aluno 3 : Ah, certo.

APÊNDICE J –SATISFAÇÃO COM O CURSO

01 - De uma forma geral, considerando a escala abaixo informe seu grau de satisfação com o curso on-line de segurança da informação

0 1 2 3 4 5 6 7 8 9 10

02 - Seu grau de satisfação considerando o conteúdo do curso

0 1 2 3 4 5 6 7 8 9 10

03 - Seu grau de satisfação considerando a as mídias e elementos utilizados no curso

0 1 2 3 4 5 6 7 8 9 10

04 - Seu grau de satisfação considerando o material de leitura?

0 1 2 3 4 5 6 7 8 9 10

05 - Seu grau de satisfação considerando os desafios práticos?

0 1 2 3 4 5 6 7 8 9 10

06 - Seu grau de satisfação considerando os estudos de caso?

0 1 2 3 4 5 6 7 8 9 10

07 - Seu grau de satisfação considerando o jogo de criptografia?

0 1 2 3 4 5 6 7 8 9 10

08 - Seu grau de satisfação considerando as discussões no grupo do Whatsapp?

0 1 2 3 4 5 6 7 8 9 10

09 - Seu grau de satisfação considerando o material em vídeo?

0 1 2 3 4 5 6 7 8 9 10

10 - Seu grau de satisfação considerando a interatividade do curso?

0 1 2 3 4 5 6 7 8 9 10

11 - Seu grau de satisfação considerando a duração do curso?

0 1 2 3 4 5 6 7 8 9 10

12 - A forma de apresentar as informações utilizando material de leitura, vídeos, estudos de caso, jogos, trabalhos em grupo e desafios práticos permitiu aliar teoria e prática.
0 1 2 3 4 5 6 7 8 9 10

13 - O fórum de discussão foi uma ferramenta útil para tirar dúvidas, socializar ou discutir sobre os temas abordados no curso
0 1 2 3 4 5 6 7 8 9 10

14 - O que você achou do curso?

APÊNDICE K – PRODUTO EDUCACIONAL

O produto educacional fruto da pesquisa intitulada: Modelo de Formação para Educação Profissional e Tecnológica Baseada em pMOOC: Uma experiência com segurança da informação, apresentado pelo mestrando William da Silva Melo no programa de Pós Graduação em Educação Profissional e Tecnológica, ofertado pelo Instituto Federal de Educação, Ciências e Tecnologia do Sertão Pernambucano, campus Salgueiro se encaixa na modalidade de sequência didática.

Trata-se de um curso on-line aberto e massivo na área de segurança da informação, que tem a peculiaridade de trabalhar aspectos práticos e desenvolver habilidades e conhecimentos no público do EMITI. Sendo assim, o pMOOC Segurança da Informação: Aliando teoria e prática foi desenvolvido com base no modelo de formação construído nesta pesquisa, está disponível para acesso na plataforma *Course Builder* da Google (link: https://mooc-seginfo.appspot.com/moocseg/course).

Como produto educacional secundário foi desenvolvido um jogo de cartas denominado MOOCSEG, o mesmo está disponível no apêndice F desta pesquisa e compõe a sequência didática pMOOC Segurança da Informação: Aliando teoria e prática. O Jogo em questão foi concebido para inserir o elemento da gamificação no curso, foi aplicado presencialmente, em grupo e pelo seu formato pode ser adaptado para outras áreas do conhecimento. O produto educacional em questão está disponível no link: http://educapes.capes.gov.br/handle/capes/567384.