

CAPÍTULO 2

AGILE CYBER TRAINING SYSTEM: MULTIMODALIDADE NA INTERAÇÃO PARA CAPACITAÇÃO EM SEGURANÇA CIBERNÉTICA

Joni A. Amorim, Doutor, Universidade Estadual de Campinas


RESUMO

Ao se considerar a dependência crescente da infraestrutura de tecnologia de informação e de comunicação, é cada vez mais relevante alinhar estrategicamente os investimentos em software, em hardware e, em especial, em recursos humanos. Para que as equipes responsáveis pela defesa cibernética estejam em condições de realizar apropriadamente seu trabalho, são cada vez mais relevantes os treinamentos focados nos mais recentes avanços percebidos e nos novos tipos de ameaças que surgem em paralelo. Em se tratando da Educação a Distância no mundo cibernético, as equipes responsáveis pela defesa cibernética são as equipes técnicas de suporte, destacando-se neste caso os profissionais de informática responsáveis por toda a infraestrutura a ser utilizada em um determinado curso a distância. Os treinamentos destas equipes devem incluir as áreas de competência em segurança identificadas como essenciais. Estes treinamentos podem ser entendidos como projetos com início, meio e fim. Tais projetos, desta forma, precisam ser apropriadamente gerenciados para que se atinjam os objetivos almejados com qualidade e custo aceitáveis. Nesta perspectiva, este trabalho apresenta e discute diferentes elementos afins ao gerenciamento de projetos de treinamento em defesa cibernética. Ainda assim, a discussão aqui iniciada pode também interessar a todos aqueles envolvidos tanto no oferecimento como na realização de pesquisas sobre treinamentos, deste modo indo além da defesa cibernética. O texto apresenta áreas de competência em defesa cibernética e discute os projetos de treinamento, com foco em abordagens que busquem melhorar o gerenciamento de projetos educacionais pela criação de escritórios de gerenciamento que funcionariam com base em processos bem definidos que apresentem suas respectivas ferramentas e técnicas. Partindo-se dos resultados relacionados às pesquisas discutidas, é apresentada em uma seção específica uma proposta de um novo sistema de treinamento útil à defesa cibernética.

Palavras-chave: Ciberespaço, Informática na Educação, Multimídia, Segurança.

INTRODUÇÃO

A defesa cibernética se torna essencial com a informatização da sociedade e com a utilização de diferentes tipos de equipamentos pelos mais diversos setores. A demonstração desta importância se percebe de diferentes formas como, por exemplo, pela criação em 2009 do Centro de Comunicações e Guerra Eletrônica do Exército (<http://www.ccomgex.eb.mil.br>)




e pela criação em 2012 do Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal (<http://www.dpf.gov.br/>). Diferentes pesquisadores, como Jorge et al. (2011), salientam a importância do treinamento de recursos humanos para que os mesmos estejam preparados para contra-atacar eventuais ameaças e/ou para evitá-las através da prevenção.

Os treinamentos podem ser entendidos como projetos com início, meio e fim. Tais projetos, desta forma, precisam ser apropriadamente gerenciados para que se atinjam os objetivos almejados com qualidade e custo aceitáveis, considerando-se também as áreas de competência em defesa cibernética. Inicialmente, como parte da fundamentação teórica deste trabalho investigativo, são apresentadas as quatorze áreas de competência em defesa cibernética segundo o “framework” “Information Technology Security Essential Body of Knowledge”, o que permite compreender melhor as necessidades de treinamento contínuo com foco nas competências a serem desenvolvidas e aprimoradas. Na sequência, apresentam-se os elementos essenciais afins aos conceitos de planejamento estratégico, destacando tanto sua importância em uma organização como também as especificidades da abordagem gerencial conhecida como “Balanced Scorecard” (BSC).

Uma seção específica sobre projetos de treinamento destaca o “framework” EduPMO, uma abreviação de “Educational Project Management Office”, uma abordagem que busca melhorar o gerenciamento de projetos educacionais pela criação de um escritório de gerenciamento que funcionaria com base em processos bem definidos que apresentem suas respectivas ferramentas e técnicas. Partindo-se dos resultados relacionados às pesquisas envolvendo o “framework” EduPMO, é apresentada em uma seção específica uma proposta de um novo sistema de treinamento útil à defesa cibernética, seção esta que precede a conclusão do trabalho, na qual potenciais trabalhos futuros são brevemente expostos.

ÁREAS DE COMPETÊNCIA EM DEFESA CIBERNÉTICA

Nesta seção são apresentadas as quatorze áreas de competência em defesa cibernética segundo o “framework” “Information Technology Security Essential Body of Knowledge” (<http://www.us-cert.gov/ITSecurityEBK/>). O “framework” EBK (SHOEMAKER e CONKLIN, 2011) é um produto que busca fornecer uma referência que indique o conhecimento essencial e as habilidades que os profissionais de segurança de tecnologia de



informação e de comunicação devem ter para desempenhar papéis e responsabilidades específicas.


A primeira competência seria “Data Security”, ou Segurança de Dados. Tal competência se refere à garantia de que os dados de interesse estejam tanto acessíveis como seguros. Isso envolve, inclusive, garantir a classificação dos dados e definir orientações aos envolvidos, inclusive no que se refere à definição de políticas específicas sobre o tema.

A segunda competência seria “Digital Forensics”, ou Perícia Forense Digital. Tal competência se refere às técnicas voltadas à coleta de evidências, após a ocorrência de eventos adversos. Como é evidente, uma grande quantidade de evidências forenses existem na forma informações “binárias” em sistemas computacionais, sendo essencial que uma organização não viole de maneira inapropriada a integridade dos dados durante uma perícia forense.

A terceira competência seria “Enterprise Continuity”, ou Continuidade Organizacional. Tal competência se refere às técnicas voltadas à garantia de funcionamento ininterrupto de uma organização após a ocorrência de eventos adversos. Ou seja, pretende-se que os sistemas e os dados voltem a estar disponíveis, o mais prontamente possível no caso de um evento inesperado, algo que pode ser feito pela identificação de riscos e de seus impactos, pela definição de um conjunto de ações associadas a tais riscos e, inclusive, pelo planejamento focado em “desastres” mais específicos.

A quarta competência seria “Incident Management”, ou Gerenciamento de Incidentes. Tal competência se refere a técnicas especificamente voltadas a responder a incidentes, caso estes ocorram, deste modo mantendo uma capacidade de resposta a incidentes através de um conjunto lógico de atividades relacionadas ao monitoramento, à análise e à resposta. No caso de incidentes nunca previstos, não existirá uma estratégia específica planejada, mas deverá ser possível ao menos compreender rapidamente qual a natureza do evento para que então sejam investigadas alternativas para se resolver o problema.

A quinta competência seria “IT Security Training and Awareness”, ou Treinamento em Segurança de TI e Vigilância. Tal competência se refere às técnicas voltadas a garantir que os membros da organização tenham as competências necessárias às suas funções. Os treinamentos são essenciais para que todas as partes interessadas compreendam seus deveres e



obrigações relativamente à segurança, o que por sua vez induzirá um comportamento disciplinado e motivado, com práticas consistentes atreladas à responsabilidade de cada um.


A sexta competência seria “IT Systems Operations and Maintenance”, ou Manutenção e Operações de Sistemas de TI. Tal competência se refere às técnicas que garantem o funcionamento seguro da organização, inclusive com processos de coordenação afins à governança.

A sétima competência seria “Network and Telecommunications Security”, ou Segurança de Rede e de Telecomunicações. Tal competência se refere às técnicas voltadas à garantia do funcionamento seguro e sem interrupções da infraestrutura de informação e de comunicação, o que se reflete na criação de um conjunto coerente de políticas de uso de redes, de acesso remoto, de controle de segurança de redes, dentre outros aspectos relacionados.

A oitava competência seria “Personnel Security”, ou Segurança Pessoal. Tal competência se refere às técnicas que garantam uma prática segura pelos funcionários da organização em diferentes contextos. Os elementos envolvidos são muitos e precisam ser identificados pela organização com base em critérios como risco. A rotatividade de pessoal e a utilização de serviços terceirizados contribuem para o aumento da complexidade neste caso, em especial pela necessidade de uma apropriada definição de privilégios de acesso.

A nona competência seria “Physical and Environmental Security”, ou Segurança Física e Ambiental. Tal competência se refere às técnicas que garantem que o espaço físico seja seguro e apropriado. Uma dificuldade adicional neste caso se refere à divisão causada pelo fato da proteção física envolver bens materiais enquanto os ativos afins aos dados e às informações são intangíveis.

A décima competência seria “Procurement”, ou Aquisições. Tal competência se refere às técnicas voltadas à compra segura de produtos e serviços que, de maneira complementar, devem ser entregues de maneira também segura. Neste caso, um cuidado extra se refere aos documentos que devem encorajar maior cuidado por parte dos fornecedores com relação à segurança, como por exemplo, “Request for Proposals” (RFP) utilizados para encaminhamento de propostas de fornecimento.



A décima primeira competência seria “Regulatory and Standards Compliance”, ou Conformidade com Regulamentos e Padrões. Tal competência se refere às técnicas que garantam que a organização não viole regulamentos, padrões ou leis relacionadas à segurança.


A décima segunda competência seria “Security Risk Management”, ou Gerenciamento de Riscos de Segurança. Tal competência se refere às técnicas que permitam uma identificação dos riscos e seu contínuo acompanhamento. Entre outros aspectos, incluem-se a aceitação de certos riscos, a mitigação, a transferência e estratégias afins a evitar os riscos.

A décima terceira competência seria “Strategic Security Management”, ou Gestão Estratégica de Segurança. Tal competência se refere a diferentes questões estratégicas focadas em segurança e afins ao funcionamento da organização, o que inclui considerações sobre o alinhamento das iniciativas.

A décima quarta competência seria “System and Application Security”, ou Segurança de Sistemas e de Aplicativos. Tal competência se refere às técnicas que pretendem garantir que as máquinas e os respectivos softwares funcionem de maneira segura. Considerações sobre a etapa de programação no desenvolvimento de softwares, por exemplo, podem ser relevantes.

As diferentes áreas de competência supracitadas deixam evidente a complexidade e a abrangência da defesa cibernética, fato que por sua vez se reflete na constante necessidade de realização de treinamentos diversos. Tais treinamentos devem ainda ser direcionados a cada perfil profissional (SHOEMAKER e CONKLIN, 2011), como na função executiva de “Chief Information Officer” (CIO), na função de engenheiro de segurança, na função de profissional de compras, dentre outras funções impactadas pelas questões afins à defesa cibernética.

A defesa cibernética depende de planejamento operacional, tático e, em especial, estratégico. O planejamento é como um mapa a ser seguido pelas pessoas em suas atividades futuras para que consigam atingir os objetivos da organização, seja pública ou privada. Temos no mínimo três níveis de planejamento: (1) alto nível, com gerentes de alto nível, ou gerentes estratégicos; (2) nível médio, com gerentes de nível intermediário, ou gerentes táticos; e (3) baixo nível, com gerentes da linha de frente, ou gerentes operacionais. O planejamento estratégico considera a tomada de decisões sobre os objetivos e as estratégias de longo prazo, como planejar uma expansão nos setores de atuação. O planejamento tático traduz o




planejamento estratégico que é muito amplo e genérico em metas e planos específicos para uma parte da organização como, por exemplo, planos de aquisições, planos de recursos, etc. O planejamento operacional considera períodos de tempo bastante curtos, com foco em atividades rotineiras, como realização de entregas e/ou de recebimento de produtos, a interação com os clientes e/ou com os cidadãos, etc.

Supondo que a organização e/ou que uma unidade desta organização já formulou sua estratégia, é possível implementar tal estratégia através do BSC, uma proposta de sistema gerencial muito usada. Tal sistema foi originalmente desenvolvido pelo engenheiro com doutorado em pesquisa operacional e professor da Harvard Business School, Robert S. Kaplan, em conjunto com David P. Norton, também engenheiro com pós-graduação em pesquisa operacional e doutorado em administração. Kaplan e Norton (1997) sugerem que cada objetivo estratégico será associado a uma das quatro perspectivas do BSC: (1) Perspectiva Financeira; (2) Perspectiva dos Clientes; (3) Perspectiva dos Processos Internos; e (4) Perspectiva de Aprendizagem e Crescimento. Os indicadores estratégicos são associados aos objetivos estratégicos definidos originalmente.

GERENCIAMENTO DE PROJETOS DE TREINAMENTO

Nesta perspectiva, esta seção apresenta um modelo para o gerenciamento de projetos de produção e utilização de conteúdo digital útil a treinamentos (AMORIM, 2010). Tanto o modelo como a metodologia e a implementação recebem a denominação de EduPMO, uma abreviação de “Educational Project Management Office”, o que poderia ser traduzido como “Escritório de Gerenciamento de Projetos Educacionais”. Desta feita, o modelo, a metodologia e a implementação devem ser compreendidos como relacionados; mas, ainda assim, distintos.

Assim sendo, no contexto desta pesquisa, entende-se por “framework” um conjunto de premissas, conceitos, valores, métodos e práticas que constitui uma maneira de se perceber a realidade. As dimensões do modelo EduPMO (AMORIM, 2010) constituem uma referência que permite a uma organização interessada no gerenciamento de projetos de produção e/ou de utilização de conteúdo digital em educação verificar se todos os fatores relevantes foram considerados. Para tanto, parte-se de uma perspectiva de melhoria contínua dos




procedimentos sistemáticos envolvidos que também considere aspectos de gestão do conhecimento, gestão de transições e propriedade intelectual.

Em tal modelo, as dimensões são separadas em dois tipos (AMORIM, 2010): explícitas e implícitas. As dimensões denominadas explícitas são aquelas efetivamente explicitadas, seja parcialmente ou totalmente, aos integrantes das diferentes equipes dos projetos. As implícitas, por sua vez, ainda que afetem de algum modo o trabalho das diferentes equipes dos projetos, não são diretamente explicitadas a estas e fazem parte do repertório de estratégias utilizadas pelo escritório de gerenciamento de projetos educacionais e pelos gerentes de cada projeto durante sua atuação. Ainda que exista um evidente inter-relacionamento entre as diferentes dimensões, sejam explícitas ou implícitas, estas foram divididas em quatro no primeiro caso e cinco no segundo, conforme se explicita a seguir.

As quatro dimensões explícitas recebem as seguintes denominações (AMORIM, 2010): DC ou Dimensão Conteudística; DP ou Dimensão Pedagógica; DT ou Dimensão Tecnológica; e DG ou Dimensão Gerencial. As cinco dimensões implícitas, por sua vez, recebem as seguintes denominações: DIGE ou Dimensão Implícita para a Gestão Estratégica; DIGC ou Dimensão Implícita para a Gestão do Conhecimento; DIGM ou Dimensão Implícita para a Gestão da Mudança; DIMM ou Dimensão Implícita para o Modelo de Maturidade; e DIPI ou Dimensão Implícita para a Propriedade Intelectual.

Em primeiro lugar, a DC ou Dimensão Conteudística (AMORIM, 2010), refere-se ao correto entendimento dos requisitos fundamentais dos projetos, em especial no que se refere ao conteúdo envolvido. Em segundo lugar, a DP ou Dimensão Pedagógica (AMORIM, 2010), refere-se às considerações sobre os aspectos de ensino e de aprendizagem envolvidos. Em terceiro lugar, a DT ou Dimensão Tecnológica (AMORIM, 2010), refere-se principalmente aos processos de detalhamento dos requisitos técnicos relativos aos produtos a serem produzidos e/ou utilizados. Em quarto lugar, a DG ou Dimensão Gerencial (AMORIM, 2010), refere-se a aspectos diversos, incluindo-se aí áreas de conhecimento específicas como gerenciamento da integração do projeto, gerenciamento do escopo do projeto, gerenciamento do prazo do projeto, gerenciamento do custo do projeto, gerenciamento da qualidade do projeto, gerenciamento dos recursos do projeto, gerenciamento da comunicação e das partes interessadas do projeto, gerenciamento dos riscos do projeto e gerenciamento das aquisições do projeto.




Em quinto lugar, a DIGE ou Dimensão Implícita para a Gestão Estratégica (AMORIM, 2010), refere-se a alcançar objetivos estratégicos específicos através do gerenciamento centralizado de vários portfólios e programas, o que inclui identificação, priorização, autorização, gerenciamento e controle dos projetos destes portfólios e programas. Em sexto lugar, a DIGC ou Dimensão Implícita para a Gestão do Conhecimento (AMORIM, 2010), refere-se a aspectos essenciais para produzir um gerenciamento efetivo do conhecimento, como colheita, filtragem, configuração, disseminação e aplicação. Em sétimo lugar, a DIGM ou Dimensão Implícita para a Gestão da Mudança (AMORIM, 2010), refere-se à gestão de transições diversas no contexto do projeto ou a transições na forma de trabalho das equipes dado o contexto singular de um projeto em específico. Em oitavo lugar, a DIMM ou Dimensão Implícita para o Modelo de Maturidade (AMORIM, 2010), refere-se à busca pela melhoria de processos. Em nono lugar, a DIPI ou Dimensão Implícita para a Propriedade Intelectual (AMORIM, 2010), refere-se aos aspectos da gestão da inovação e dos direitos de propriedade.

Para cada dimensão podem ser explicitados processos, denominados aqui de macroprocessos, sendo que cada macroprocesso pode ser apresentado através de uma descrição e/ou de um diagrama salientando as atividades e/ou tarefas a serem realizadas, com indicações de entradas (“inputs”) e saídas (“outputs”) do macroprocesso assim como de ferramentas e técnicas (F. & T.) úteis à aplicação do macroprocesso. De modo a subsidiar a aplicação de cada macroprocesso no contexto de projetos de produção e/ou de utilização de multimídia, podem ainda ser apresentados modelos (“templates”) de documentos.

Assim, para cada dimensão, temos diferentes artefatos para os macroprocessos: descrição, diagrama, entradas, saídas, ferramentas e técnicas úteis à aplicação do macroprocesso e modelos de documentos. De modo geral, os macroprocessos tendem a ser genéricos, mas os modelos de documentos apresentados pelo EduPMO são específicos para os contextos dos projetos em consideração, neste caso produção e/ou utilização de multimídia educacional. Para as nove dimensões, temos um total de 199 macroprocessos de acordo com Amorim (2010), sendo 32 para DC, 6 para DP, 8 para DT, 42 para DG, 64 para DIGE, 5 para DIGC, 5 para DIGM, 31 para DIMM e 6 para DIPI.

Conforme indica Hill (2008), uma metodologia para o gerenciamento de projetos provê um procedimento padronizado e passível de ser repetido que permite guiar a




performance dos projetos da concepção ao encerramento, com indicações do que fazer e de como fazer. Tal autor explicita que, de início, a metodologia pode se focar em introduzir uma série de processos simples, o que em projetos de produção e/ou de uso de multimídia poderia significar a criação de cronogramas com software específico ou o estabelecimento de uma comunidade de prática na Web. O autor salienta, entretanto, que em um segundo momento, deve-se ir além do essencial e buscar desenvolver um procedimento completo que considere o ciclo de vida do início ao fim; incluindo, portanto, iniciação, planejamento, execução, monitoramento e controle, e encerramento.

Assim, uma metodologia deve ser desenvolvida para aplicar padrões como o BABOK/IIBA (www.theiiba.org/BABOK/) e o PMBOK/PMI (www.pmi.org), assim como para aplicar práticas de interesse, como aquelas afins a propriedade intelectual, fábrica de multimídia e manufatura celular. Tal aplicação de padrões e práticas na organização pode ocorrer de forma gradativa, também considerando eventuais “metodologias técnicas” em uso, tais como aquelas relativas às especificidades da produção de áudio e de vídeo ou aquelas dos setores de contabilidade da organização.

Com isso, supondo-se, por exemplo, quatro ciclos em sequência, uma opção possível envolveria, no primeiro ciclo, o desenvolvimento progressivo da metodologia o qual poderia se iniciar por um macroprocesso específico como o de gerenciamento de tempo com cronogramas em todos os projetos de organização, passando no segundo ciclo por uma série de processos fundamentais como os que se referem ao conjunto de macroprocessos relativos à propriedade intelectual, atingindo-se em um terceiro ciclo a incorporação das metodologias técnicas aos macroprocessos em uso como os que se referem à integração dos cronogramas de desembolso à análise de valor agregado, e chegando-se a um quarto ciclo com o desenvolvimento completo da metodologia para todos os projetos, incluindo todos os macroprocessos relevantes e seus respectivos modelos de documentos, com detalhamento das ferramentas e técnicas.


Tal perspectiva sugere que se definam de início quais os componentes da metodologia, o que pode incluir até mesmo glossários com a terminologia relevante, para que então se defina qual será a plataforma a ser utilizada para a implementação desta metodologia. São cinco tipos fundamentais de plataforma (HILL, 2008): (1) plataforma baseada em papel, com uso eventual de softwares diversos pelas equipes e com a reimpressão de guias e manuais



conforme ocorrerem atualizações; (2) plataforma baseada na orquestração do uso de softwares, com um maior planejamento do uso de softwares diversos, mas sem que exista uma integração maior para o intercâmbio de dados entre os softwares; (3) plataforma baseada em alguma suíte de softwares para o gerenciamento de projetos, com o uso conjunto de vários softwares já integrados entre si, o que de modo geral implica na aquisição de soluções genéricas oferecidas por empresas especializadas; (4) plataforma baseada em alguma suíte de softwares para a gestão da empresa como um todo mas que também apresente funcionalidades para o gerenciamento de projetos, o que mais uma vez tende a implicar na aquisição de soluções genéricas oferecidas por empresas especializadas; e (5) plataforma baseada na construção de software específico para o contexto da organização, o que implica quase sempre em custos significativamente mais altos.

Em contextos como aqueles dos projetos de produção e/ou de utilização de multimídia, as vantagens da orquestração do uso de softwares sobressaem dada a necessidade de utilização de muitos softwares específicos tanto na parte de gerenciamento de custos e de cronogramas como na parte de produção de produtos como áudio e vídeo. Por outro lado, conforme indica Hill (2008), o menor investimento inicial de uma plataforma baseada em papel deve ser considerado por ser esta a maneira mais rápida e fácil de iniciar a implementação da metodologia, viabilizando-se uma introdução aos padrões e práticas do gerenciamento de projetos na organização. Tal autor salienta que uma plataforma baseada em papel também pode ser vista como útil ao desenvolvimento da estrutura e do conteúdo da metodologia, o que depois viabilizaria uma automação parcial ou total através do desenvolvimento de algum dos outros quatro tipos de plataforma.


Na maioria dos contextos, pode ser de interesse gerar um documento formal escrito detalhando a proposta relativa ao escritório de projetos, com objetivos, custos, escopo, cronograma, etc. Diversas estruturas podem ser consideradas para tal tipo de documento, tal como sugerem Kendall e Rollins (2003). Tais autores indicam como modelo geral um documento com seis seções a serem precedidas por um resumo executivo: (1) seção introdutória com uma visão geral da proposta, apresentando informações para contextualização, objetivos, alinhamento com a estratégia da organização e tipo de oportunidade, como diminuição de custos e de riscos ou aumento da probabilidade de sucesso dos projetos; (2) seção sobre o escopo da proposta, indicando requisitos, uso de tecnologia,



análise de impacto sobre as partes interessadas, fatores críticos de sucesso, etc.; (3) seção destacando a abordagem, com indicação de alternativas possíveis, premissas, obstáculos, expectativas das partes interessadas, planejamento de aquisições, planejamento da comunicação, planejamento do controle de mudanças (alterações), entre outros; (4) seção específica sobre gerenciamento de riscos, incluindo uma matriz de identificação de riscos identificando cada risco percebido assim como sua quantificação em termos de probabilidade e impacto e a possível resposta em caso de ocorrência; (5) seção detalhando aspectos financeiros, com custos por categoria em cada fase e análise custo/benefício, indicando-se formas de medição para se verificar se os benefícios estão ou não sendo atingidos, o que pode incluir métricas específicas da organização já em uso; e (6) seção detalhando os cronogramas das fases, as quais podem se referir a planejamento, execução e finalização, com diferentes etapas dentro de cada fase.

Com base nesta discussão (AMORIM, 2010), a Metodologia EduPMO, a qual se refere à metodologia para implementação do Modelo EduPMO, apresentará 3 fases por ciclo, com a abreviação D-I-A: (1) Desenhar, (2) Implementar e (3) Avaliar. A metodologia pode ser aplicada a um ou mais projetos da organização, sendo que a fase de desenho deve considerar o contexto atual para determinar o que é possível implementar a curto, médio e longo prazo; feito isso, a fase de implementação fará tal implementação de curto prazo para então realizar uma avaliação que fornecerá elementos para a próxima fase de desenho. Exemplificando para um curso que faça uso de multimídia, como um curso de graduação dividido em 8 semestres, poderíamos ter 8 ciclos, com uma avaliação ao final de cada semestre que permitiria uma melhoria contínua do gerenciamento.

A primeira fase (AMORIM, 2010), relativa a “Desenhar”, teria como atividades fundamentais as seguintes: (i) identificação pelo escritório de projetos dos componentes da metodologia passíveis de serem implementados na organização no contexto atual, o que pode incluir definir as dimensões relevantes e gerar componentes como glossários, guias, etc., definindo padrões e práticas de interesse; (ii) projetar os processos do ciclo de vida, o que neste caso implica em definir os macroprocessos relevantes para cada dimensão, com descrição, diagrama, entradas, saídas, ferramentas e técnicas úteis à aplicação do macroprocesso e modelos de documentos; (iii) selecionar a plataforma que viabilizará a implantação da metodologia; e (iv) se necessário, gerar um documento formal escrito




detalhando a proposta relativa ao funcionamento do escritório de projetos durante o ciclo em questão, com objetivos, custos, escopo, cronograma, etc.

A segunda fase(AMORIM, 2010), relativa a “Implementar”, teria como atividades fundamentais as seguintes: (i) capacitação do gerente do projeto pelo escritório de projetos; (ii) planejamento detalhado da transição (mudança) na forma de trabalhar para a melhoria no gerenciamento do projeto específico sob consideração; (iii) capacitação da equipe do projeto pelo gerente do projeto ou pelo escritório de projetos, desse modo viabilizando-se a realização da transição (mudança) na forma de trabalhar para a melhoria no gerenciamento do projeto específico sob consideração; e (iv) realização da implementação, o que pode incluir desde o início do uso de um novo software para a realização de algumas tarefas até a implementação de uma série de processos relativos a uma determinação dimensão.

A terceira fase(AMORIM, 2010), relativa a “Avaliar”, teria como atividades fundamentais as seguintes: (i) avaliar a implementação realizada com base no planejamento detalhado da transição (mudança) na forma de trabalhar para a melhoria no gerenciamento do projeto específico sob consideração; (ii) indicar possíveis ações para o próximo ciclo D-I-A relativo ao projeto específico sob consideração; (iii) buscar por oportunidades de melhoria na metodologia com base na avaliação da implementação; e (iv) indicar possíveis revisões dos processos do ciclo de vida, o que neste caso implica em eventualmente rever os macroprocessos relevantes para cada dimensão e os seus artefatos, o que inclui descrição, diagrama, entradas, saídas e F. & T. úteis à aplicação do macroprocesso e modelos de documentos.

Assim, a Metodologia EduPMO (AMORIM, 2010), a qual se refere à metodologia para implementação do Modelo EduPMO, fará uso do ciclo D-I-A continuamente, deste modo permitindo que tanto a metodologia seja melhorada com base nas avaliações relativas aos projetos que a utilizam, como também que um projeto de maior duração possa passar por melhorias em seu gerenciamento durante a sua execução. Com isso, não apenas se garante que as melhorias ocorram, mas também se pretende que isso ocorra de forma organizada em períodos pré-estabelecidos, o que permite que tanto as equipes como os gerentes de cada projeto contribuam com propostas e sugestões que podem vir a afetar a organização como um todo.




Nesse cenário, tendo-se o escritório de projetos estruturado para cada dimensão, com modelos, diagrama, descrição, entradas, saídas e F. & T. para cada macroprocesso de cada dimensão, torna-se possível a tal escritório auxiliar o gerente na seleção de quais macroprocessos são relevantes e/ou apropriados para seu projeto específico em um dado momento. Isso permite que se desenvolva, dentre outras ações possíveis, um “guia do gerente do projeto”, o qual seria um documento com 9 seções, sendo, portanto, uma seção por dimensão, onde para cada dimensão se explicitariam os macroprocessos de interesse para que em um segundo momento se detalhem os microprocessos que serão seguidos pelas equipes. Neste caso, entende-se por microprocesso um procedimento específico que pode não estar previsto no escritório de projetos mas que pode ser de interesse para o projeto, com base na perspectiva do gerente do projeto que define como a equipe deve trabalhar.

Através do uso do “guia do gerente do projeto”(AMORIM, 2010), elaborado com o acompanhamento do escritório de projetos, o gerente vai usar diferentes ferramentas e técnicas para gerar o “manual da equipe do projeto”, que explicita quais são os macroprocessos e os microprocessos a serem seguidos por esta equipe durante o decorrer do projeto, inclusive com modelos de documentos, etc.

O “manual da equipe do projeto” (AMORIM, 2010) refletirá a metodologia a ser utilizada pelo gerente em cada projeto específico, com a indicação de fases e de atividades, assim como de cronograma a ser seguido pela equipe. Em projetos maiores, pode ser de interesse dividir tais manuais em vários documentos distintos, sendo um para cada tipo de profissional envolvido. Exemplificando, pode ser de interesse separar as instruções do pessoal da parte financeira do pessoal da parte de produção, sendo que neste último caso poderiam existir seções distintas relativas à produção de cada mídia específica, evitando-se assim que os profissionais envolvidos sejam sobrecarregados com informações que não são necessárias à sua atuação específica.

Deve-se notar que, caso não exista na organização uma estrutura específica para o escritório de projetos que possa prestar suporte aos gerentes de cada projeto, ainda se entende como possível o uso do “framework” EduPMO. Para tanto, o modelo, a metodologia e a implementação podem ser desenvolvidos de modo mais simplificado pelo gerente de projeto para uso no contexto específico dos projetos sob sua gerencia. Ainda assim, o ideal é que se tenha o suporte de um escritório de projetos, pois isso possibilita benefícios diversos, o que




inclui a viabilização de diferentes formas de suporte aos gerentes, o que pode incluir até mesmo as comunidades de prática. Sem a existência de um escritório, tende a ser improvável que muitos dos 199 macroprocessos apresentados na literatura (AMORIM, 2010) sejam implementados pelos gerentes e/ou por suas equipes, o que tende a dificultar ações relativas à melhoria de processos e à gestão do conhecimento, dentre outras.

Maiores detalhes sobre o “framework” EduPMO podem ser encontrados na literatura (AMORIM, 2010).

PROPOSTA DE UM NOVO SISTEMA DE TREINAMENTO

Partindo-se dos resultados relacionados às pesquisas envolvendo o “framework” EduPMO (AMORIM, 2010) descrito na seção anterior, encontra-se em desenvolvimento uma proposta de um novo sistema de treinamento que inclui como relevantes os quatro objetivos seguintes: (1) identificar as principais ameaças em infraestruturas de tecnologia de informação e de comunicação e relacionar essas ameaças às necessidades de treinamento em segurança cibernética; (2) criar medidas que digam o que fazer para se aumentar drasticamente o desempenho de projetos de treinamento em segurança cibernética através do uso do conceito de indicador chave de desempenho; (3) propor um “framework” com os melhores métodos e práticas para a gestão de projetos de treinamento em segurança cibernética; (4) construir uma prova de conceitos de um novo sistema de treinamento em segurança cibernética.

O primeiro e principal resultado seria um “framework” com os melhores métodos e práticas para a gestão de projetos de treinamento, destacando-se aqueles afins à segurança cibernética; este “framework” seria útil tanto para o planejamento como para a execução de projetos de treinamento. Tradicionalmente, tais treinamentos fazem uso de multimídia e de diferentes tipos de simulações. Um segundo resultado envolve identificar os principais requisitos de um novo software para ser usado como um sistema de treinamento. Um terceiro resultado envolveria identificar e disseminar o corpo de conhecimento que abrange os melhores métodos e práticas para a gestão de projetos de treinamento em segurança cibernética. Neste sentido, é esperada a publicação de trabalhos científicos originais em revistas indexadas nas principais plataformas de informação sobre investigações nas ciências, desse modo disseminando o trabalho empírico e teórico originado a partir desta pesquisa.

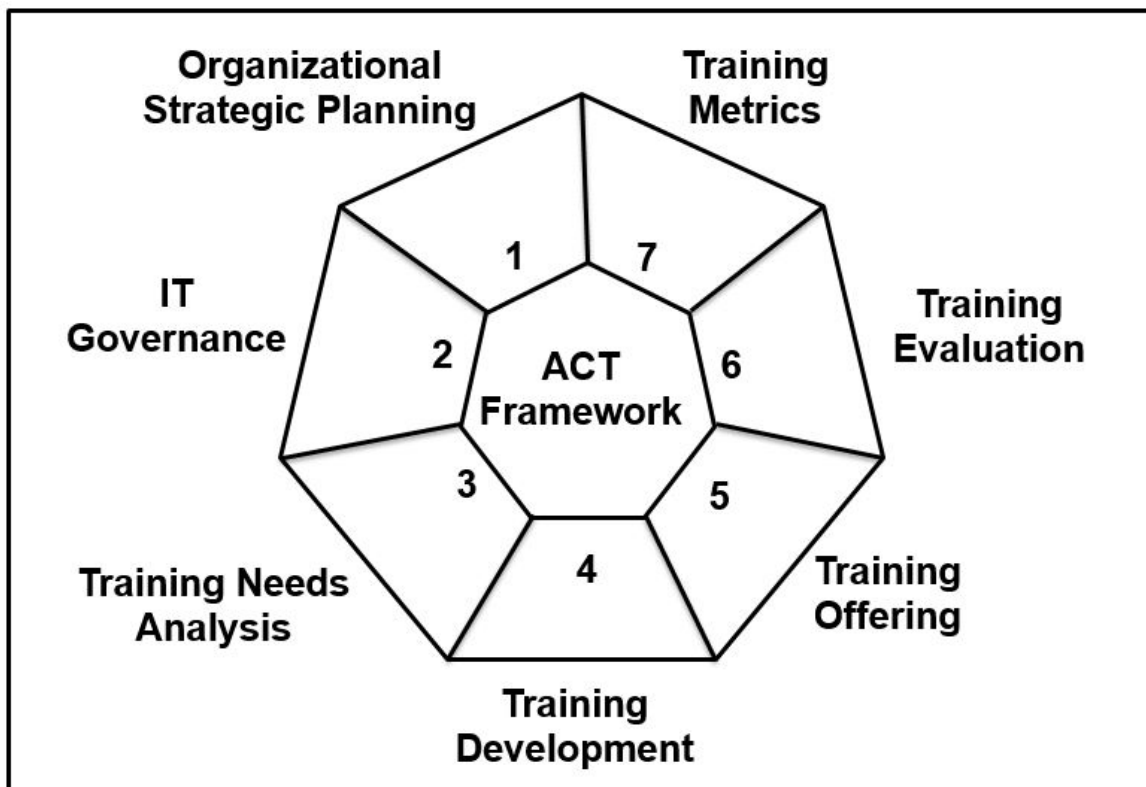


Vale destacar que o objetivo (1) será realizado por uma revisão da literatura sobre as ameaças em infraestruturas de tecnologias de informação e de comunicação. O objetivo (2) será realizado por uma revisão de literatura sobre indicadores chave de desempenho e por uma síntese dos estudos existentes sobre projetos de treinamento em segurança cibernética. O objetivo (3) será executado pelo desenvolvimento de um “framework” com os melhores métodos e práticas para a gestão de projetos de treinamento em segurança cibernética, deste modo explicitando um modelo de referência que apresente os principais processos e as principais ferramentas e técnicas de interesse. O objetivo (4) será realizado com base na análise de requisitos de um novo sistema de treinamento em segurança cibernética e com base em uma série de experimentos de demonstração. Dependendo da complexidade, a prova de conceitos vai exigir do pesquisador tanto a construção de um protótipo, ou “mock-up” com ferramentas de “wire-framing”, como também a modelagem de processos com diagramas tais como fluxogramas, deste modo permitindo que uma equipe de desenvolvimento possa eventualmente realizar as atividades de programação. Neste caso, o pesquisador gerenciaria o teste de aceitação do usuário, ou “User Acceptance Testing” (UAT), e/ou aplicaria procedimentos de garantia de qualidade.

A metodologia de investigação indicada deixa evidente a exequibilidade da proposta. Trata-se de uma proposta dotada de significativa originalidade na medida em que tem como foco temas de importância crescente, mas ainda pouco explorados na literatura acadêmica.

A investigação culminaria, assim, com o desenvolvimento de um “framework” para a gestão de treinamentos em segurança cibernética e com a identificação preliminar dos requisitos de um novo sistema voltado ao treinamento em segurança cibernética. As figuras seguintes resumem alguns aspectos afins ao “framework” ACT e ao sistema ACT, onde a abreviação se refere a “Agile Cyber Training”.

Figura 1 - Visão geral das sete fases do “framework” ACT, sendo que cada fase apresenta os seus respectivos processos, ferramentas e técnicas.



Fonte: O Autor.

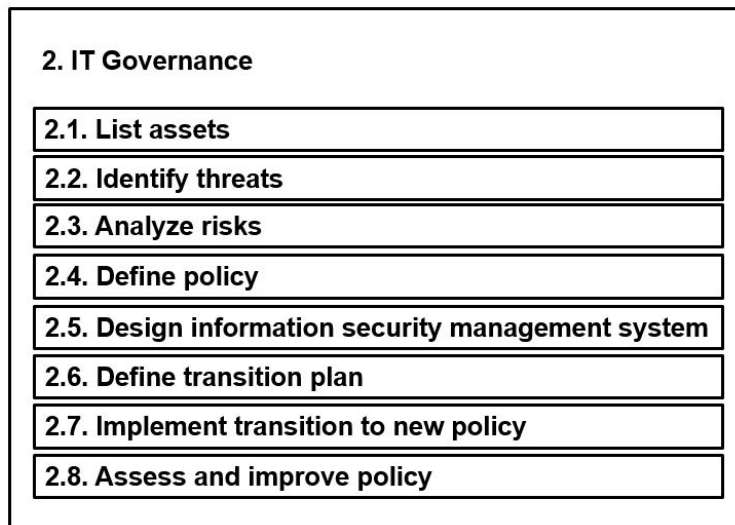
Figura 2- Apresentação dos processos da fase 1 do “framework” ACT, desenvolvida com foco no uso do Sistema Gerencial conhecido como “Balanced Scorecard” (BSC) e no conceito de “Office of Strategy Management” (OSM).

- | |
|---|
| 1. Organizational Strategic Planning |
| 1.1. Create strategy for organization |
| 1.2. Create balanced scorecard for organization |
| 1.3. Create scorecards for units of organization |
| 1.4. Create scorecards for teams of units |
| 1.5. Create scorecards for individuals |
| 1.6. Plan operations and projects |
| 1.7. Execute operations and projects |
| 1.8. Monitor performance measures |
| 1.9. Assess and improve strategy |

Fonte: O Autor.

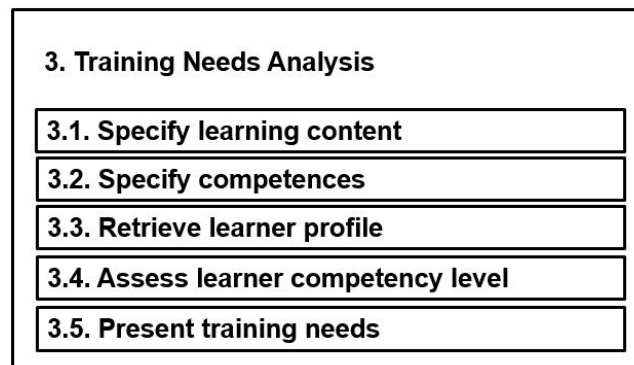


Figura 3 - Apresentação dos processos da fase 2 do “framework” ACT.



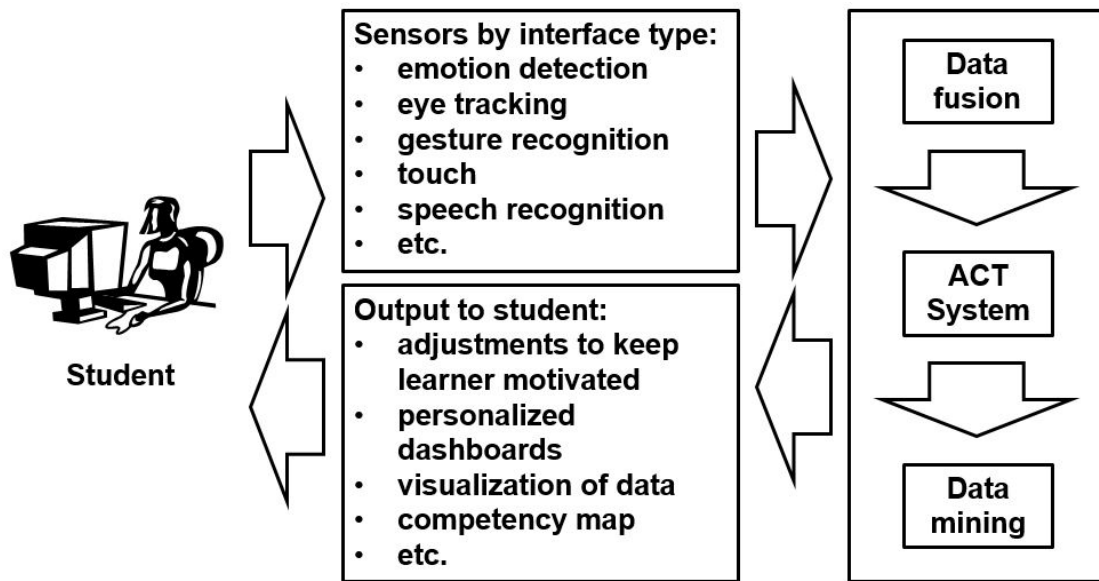
Fonte: O Autor.

Figura 4 - Apresentação dos processos da fase 3 do “framework” ACT.



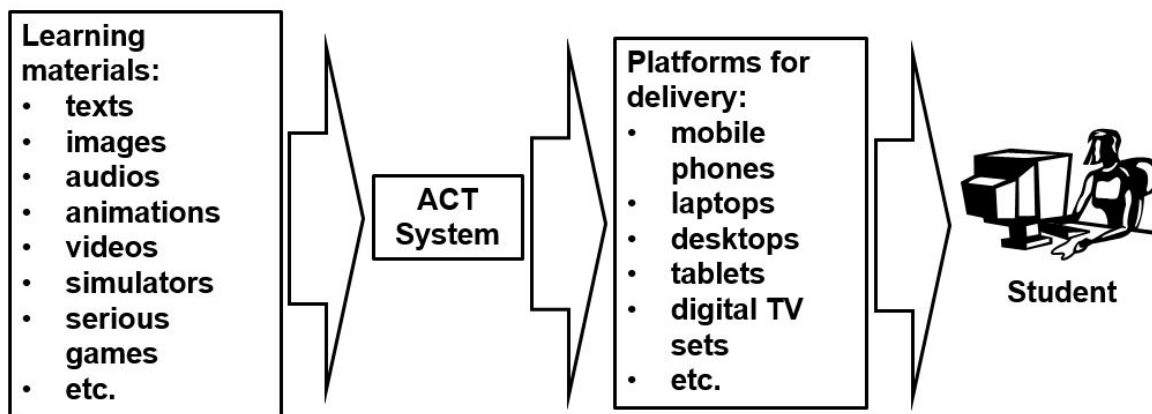
Fonte: O Autor.

Figura 5 - A multimodalidade na interação permite o uso de sensores diversos que geram dados relativos aos processos de ensino e de aprendizagem; com isso, após a fusão de dados e após a mineração de dados dentro do Sistema ACT, são apresentadas informações relevantes a cada um dos estudantes.



Fonte: O Autor.

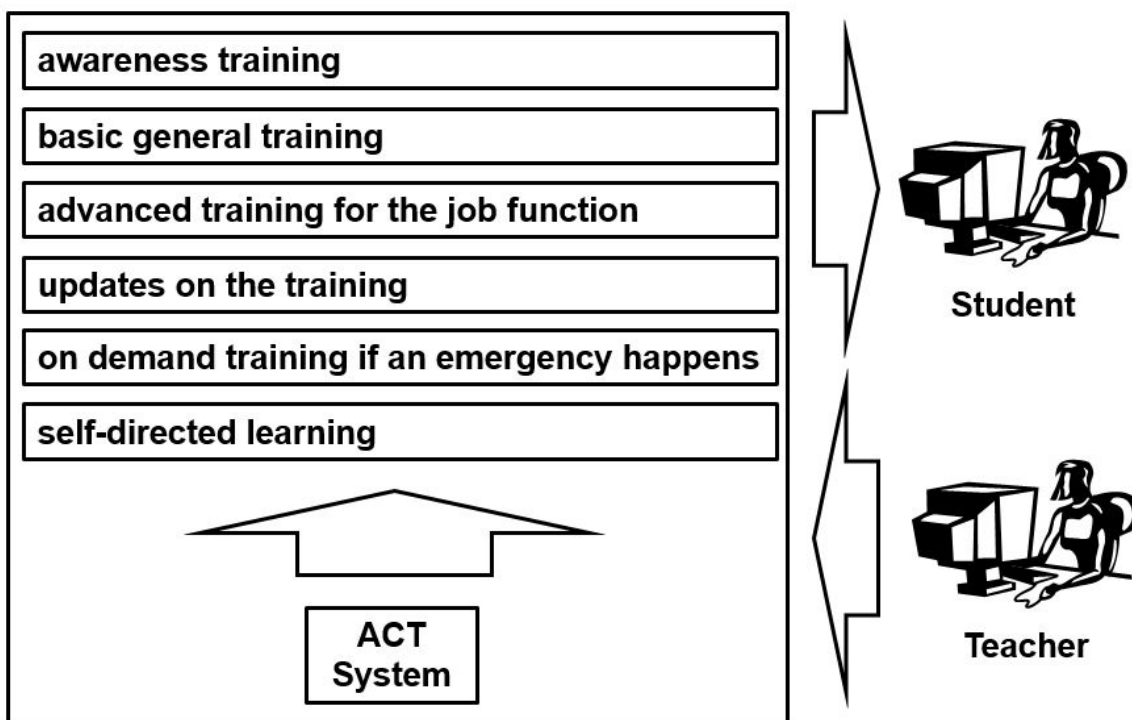
Figura 6 - Uma das principais características do Sistema ACT seria o uso de diferentes tipos de materiais instrucionais que seriam entregues através de plataformas diversas em um contexto de ubiquidade com considerações sobre mobilidade.



Fonte: O Autor.



Figura 7 - O Sistema ACT deve ser capaz de oferecer diferentes tipos de treinamentos conforme parâmetros diversos, sendo essencial que rastreie as ações dos alunos, deste modo gerando-se um histórico útil tanto para o próprio aluno como para a organização que precisa de indicadores de desempenho por tipo de treinamento, por programa de treinamento, por aluno, e assim por diante.



Fonte: O Autor.

A título de exemplo, um dos questionários desenvolvidos para a coleta de dados é apresentado a seguir.

Tabela 1 – Exemplo de questionário desenvolvido para a coleta de dados.

Dear Sir/Madam

We are researching cyber security training. In this phase of the research, we are collecting information about existing software useful for both training and research in cyber security.

This information will support decision on the use of existing software or on the development of new software for training. The software of interest would be used through a training system having other learning materials like videos, audios, animations, texts, etc. In this way, cost-effective training would be offered through different organizations, in special Brazilian Universities that have research on technical aspects of cyber security.

Documents like "A Role-Based Model for Federal Information Technology/Cyber Security Training" (October 2013, http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf), from NIST, suggest that all stakeholders in a certain organization should receive different kinds of training.

In the following questions, we are considering, in special, simulators and serious games for training on all aspects of cyber security.

In this way, we ask you to answer the following questions, which are divided into three parts: (1) interviewee data; (2) interviewee perspective on collaboration; (3) about the software. Thank you very much.

1. Interviewee Data

- 1.1. What is your full name?
- 1.2. How should we contact you?
- 1.3. What is the name of your organization?
- 1.4. Do you have a web page?
- 1.5. Is there any additional information about you that should be included here?

2. Interviewee perspective on collaboration

- 2.1. Do you participate on any collaboration with Brazil at the moment?
- 2.2. Would you like to collaborate in one or more of the following areas?
 - () Research on Cyber Security Technical Aspects
 - () Research on Cyber Security Training
 - () Other
- 2.3. Would you like to stay in Brazil as an invited researcher?
 - () Yes, for 1 year or more
 - () Yes, for a few months
 - () Yes, for a few weeks
 - () No
 - () Other
- 2.4. Would you like to teach Cyber Security in Brazil?
 - () Yes, in face-to-face courses
 - () Yes, in distance education courses
 - () No
 - () Other

3. About the software

- 3.1. What is the official name of the software?
- 3.2. Was the software developed mainly for research or for training?
- 3.3. What is the main purpose of the software?
- 3.4. Who owns the rights for the use of the software and/or who should be cited as author?

- 3.5. Who should be contacted in case we decide to use the software in Brazil for research and/or training purposes?
- 3.6. Is there any cost associated with the use of the software?
- 3.7. Are there papers, reports or other documents about the software that may be used as references?
- 3.8. Is there a web page about the software?
- 3.9. Is there a manual or a tutorial on how to install and use the software?
- 3.10. Does the software comply with any international standard like the IEEE P1278.2, the Standard for Distributed Interactive Simulation (DIS)?
- 3.11. How do you compare you software to others with similar purposes?
- 3.12. What is the future work planned for this software?


Fonte: O Autor.

CONCLUSÃO

Este texto evidenciou a relevância de um apropriado planejamento das iniciativas afins aos treinamentos em defesa cibernética, temática de interesse crescente em uma sociedade que a cada dia se encontra mais informatizada. O valor prático do trabalho envolve tanto apresentar o “framework” EduPMO, desenvolvido com foco na produção e na utilização de multimídia para a realização de educação presencial e a distância, como também envolve discutir as características mais específicas dos treinamentos em defesa cibernética, os quais podem ser entendidos como projetos que podem ser gerenciados com base em padrões internacionais e em consonância com o planejamento estratégico organizacional.

Espera-se, assim, que este trabalho contribua tanto para a investigação como para a discussão dos vários aspectos relevantes à defesa cibernética, com destaque para os projetos de treinamento. Como é evidente, o desenvolvimento de estratégias e soluções para treinamentos vai muito além da defesa cibernética, incluindo, portanto, quaisquer tipos de treinamentos a serem realizados na área de defesa.

Trabalhos futuros envolverão documentar os resultados da investigação sobre o novo sistema de treinamento proposto neste trabalho. A perspectiva é a de que ocorra tanto o desenvolvimento do novo sistema como também a transferência de tecnologia em um contexto de internacionalização, algo essencial quando se considera que certos aspectos da



defesa cibernética envolvem de maneira direta ou indireta a interação entre diferentes países via redes como a “World Wide Web”.

BIBLIOGRAFIA

AMORIM, J. A. **Engenharia Multimídia**. Tese (Doutorado) – Fac. Eng. Elétrica e de Computação, Universidade Estadual de Campinas, Campinas, Brasil, 2010. Disponível em: (<http://www.bibliotecadigital.unicamp.br/>). Acesso em: 10 ago. 2020.

HILL, G. M. **The Complete Project Management Office Handbook**. Boca Raton, USA: Auerbach Publications, 2008. ISBN 1420046802.

JORGE, C. A. F. et al. **Virtual Simulation for Training Personnel in Emergency and Security Preparedness and Counteraction**. In: Simp. Aplicações Operacionais em Áreas de Defesa – SIGE. Inst. Tec. Aeronáutica (ITA). 2011.

KAPLAN, R. S.; NORTON, D. P. **A Estratégia em Ação: Balanced Scorecard**. Campus Elsevier, 1997. ISBN 8535201491.

KENDALL, G. I.; ROLLINS, S. C. **Advanced Project Portfolio Management and the PMO: Multiplying ROI at Warp Speed**. J. Ross Publishing, 2003. ISBN 1932159029.

SHOEMAKER, D.; CONKLIN, W. A. **Cybersecurity: The Essential Body of Knowledge**. Boston, USA: Cengage Learning, 2011. ISBN 1435481690.