ESCOLA NAVAL

talanto bien faire

Salomé de Jesus Vieira

Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Engenheiros Navais – Ramo de Armas e Eletrónica

Alfeite

2016

Salomé de Jesus Vieira

Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Engenheiros Navais – Ramo de Armas e Eletrónica

Orientação de: CFR EN-AEL Fernando Jorge Ribeiro Correia
Coorientação de: CTEN EN-MEC Gonçalo Nuno Baptista de Sousa

O Aluno Mestrando _____

O Orientador _____

Alfeite

2016

Epígrafe

"Todo o nosso progresso tecnológico, que tanto se louva, o próprio cerne da nossa civilização, é como um machado na mão de um criminoso".

(Einstein)

Dedicatória

Aos meus pais, pela compreensão, generosidade e amor incondicional. Porque esta dissertação não só culmina na minha realização pessoal, mas também está alicerçada no apoio que me concederam durante todo o meu percurso. Gostaria que existissem mais e melhores palavras para vos agradecer. Obrigada.

Agradecimentos

Gostaria de expressar o meu agradecimento a todos os que me ajudaram, encorajaram e contribuíram para a realização da minha dissertação de mestrado:

ao meu orientador, Senhor Engenheiro Fernando Jorge Ribeiro Correia pelo tempo que disponibilizou para me ajudar e por partilhar comigo o seu conhecimento.

ao meu coorientador Senhor Engenheiro Gonçalo Nuno Baptista de Sousa por ter aceite, desde o início, coorientar a minha tese, pelos conhecimentos e contatos disponibilizados que me possibilitaram o acesso a informação bastante proveitosa.

ao Senhor Engenheiro Rui Daniel Martins Costa, Chefe de Departamento de Armas e Eletrónica, e à Senhora Engenheira Catarina Neto Ribeiro, Chefe de Serviço de Armas e Eletrónica do NRP *Álvares Cabral*, pelo conhecimento e experiência que me transmitiram durante o meu estágio de embarque.

à Sara Pereira, Cristiana Carreira e Raísa Furfuro, amigas de longa data, porque, apesar da distância, sempre acreditaram em mim. Vocês mostraram-me o verdadeiro significado da amizade.

à Vanessa Martins e à Rita Cotrim, por nunca me deixarem cruzar os braços e me incentivarem a continuar, porque mais do que camaradas e amigas vocês me mostraram que, para ser irmãs, não é preciso ser de sangue.

aos meus pais, Agostinho Pereira Vieira e Maria Goreti de Jesus Roda, simplesmente por serem quem são, porque nunca colocaram limites nos meus sonhos e me apoiaram em todas as decisões que tomei.

Resumo

O papel das Tecnologias de Informação (TI) nas sociedades atuais é preponderante. O aparecimento da Internet e a vulgarização do seu uso veio alterar o paradigma do modo de funcionamento das sociedades.

As sociedades industriais transformaram-se em sociedades da informação, onde o conhecimento e a informação são valorizados e têm um papel fulcral. A internet, primeiramente considerada como um espaço de liberdade absoluta e que possibilitava o acesso e compartilhamento de dados instantaneamente e a partir de qualquer ponto do globo, é hoje vista como um fator de insegurança.

O ciberespaço está suscetível a novas formas de ameaça sobre a forma de crime no mundo virtual. Os ciberataques colocam em risco a privacidade e liberdade dos cidadãos, põem em causa a soberania do Estado e podem, ainda, divulgar informação que ameace a segurança nacional.

O presente trabalho discute os desafios que o ciberespaço nos coloca e analisa a componente legal que contribui para a cultura de segurança no ciberespaço, por forma a utilizá-lo de forma mais livre e fiável.

E não só, também propõe formas de mitigar os resultados de um ciberataque através de mecanismos de formação, onde cada um tem conhecimento dos problemas atuais da internet e quais as eventuais soluções para se protegerem.

Palavras-chave: ciberespaço, cibersegurança, componente legal, modelo de formação, Portugal.

Abstract

The role of Information Technology (IT) in contemporary societies is predominant. The emergence of the Internet and the popularization of its use has changed the paradigm of corporate operation.

Industrial societies have turned into information societies, where knowledge and information are valued and have a key role. The Internet, primarily regarded as an absolute space of freedom that allowed access and sharing data instantly from anywhere in the world, is now seen as a factor of insecurity.

Cyberspace is susceptible to new forms of threat as crime in the virtual world. Cyber-attacks threaten citizens' privacy and freedom, undermine state sovereignty and may also disclose information that threatens national security.

This master's thesis discusses the challenges that cyberspace sets and analyzes the legal component that contributes to the safety culture in cyberspace in order to use it more freely and reliably.

Not only that, also proposes methods to mitigate the results of a cyberattack through an educational programme, where everyone is aware of the current problems of internet and possible solutions to protect themselves.

Key-words: cyberspace, cybersecurity, legal component, training model, Portugal.

Índice

Lista de siglas e acrónimos

ACCS	*Air Command and Control System*
ADU	Administrador do Domínio do Utilizador
ALTBMD	*Active Layered Theatre Ballistic Missile Defence*
AM	Academia Militar
ANACOM	Autoridade Nacional de Comunicações
ANS	Autoridade Nacional de Segurança
C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*
CCDCoE	*Cooperative Cyber Defence Centre of Excellence*
CERT	*Computer Emergency Response Team*
CFR	Capitão-de-fragata
CIJIC	Centro de Investigação Jurídica do Ciberespaço
CIS	*Communications and Information Systems*
CNCS	Centro Nacional de Cibersegurança
CNPDPI	Comissão Nacional de Proteção de Dados Pessoais Informatizados
CRIE	Computadores, Redes e Internet na Escola
CRISI	Capacidade de Resposta a Incidentes de Segurança Informática
CRISI-FA	Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas
CRP	Constituição da República Portuguesa
CS	*Cyber Security*
CSAE	Chefe Serviço de Armas e Eletrónica
CSDP	*Common Security Defence Policy*
CSIRT	*Computer Security Incident Response Team*
CTEN	Capitão-tenente
DDoS	*Distributed Denial of Service*
DITIC	Direção das Tecnologias de Informação e Comunicação
EC3	*European Cybercrime Centre*
ECEE	Entidade de Certificação Eletrónica do Estado
EDA	*European Defence Agency*
EMGFA	Estado-Maior General das Forças Armadas

EN	Escola Naval
EN-AEL	Engenheiros Navais - Ramo de Armas e Eletrónica
ENISA	*European Union Agency for Network and Information Security*
ENSI	Estrutura Nacional de Segurança da Informação
ETNA	Escola de Tecnologias Navais
EU	*European Union*
EUA	Estados Unidos da América
EUROPOL	*European Police Office*
FCCN	Fundação para a Computação Científica Nacional
FCT	Fundação para a Ciência e Tecnologia
FFAA	Forças Armadas
GNS	Gabinete Nacional de Segurança
GODU	Gestor Operacional do Domínio do Utilizador
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação
GRISI	Grupo de Resposta a Incidentes de Segurança Informática
HQ ICTM	*Headquarters Information Communications and Technology Management*
IDN	Instituto da Defesa Nacional
INESC	Instituto de Engenharia de Sistemas e Computadores
INFOSEC	Segurança de Sistemas de Informação e Comunicação
ISEG	Instituto Superior de Economia e Gestão
IST	Instituto Superior Técnico
IT	*Information Technology*
MDN	Ministério da Defesa Nacional
MNCDET	*Multinational Cyber Defence Education & Training*
MoU	*Memorandum of Understanding*
NACMA	NATO ACCS *Management Agency*
NATO	*North Atlantic Treaty Organisation*
NC3A	NATO *Consultation, Command and Control Agency*
NCI	NATO *Communications and Information*
NCIRC	NATO *Computer Incident Response Capability*
NCSA	NATO *Communication and Information Systems Services Agency*
NNEC	NATO *Network Enabled Capability*

NREN	*National Research and Education Network*
OCDE	Organização para a Cooperação e Desenvolvimento Económico
OECD	*Organisation for Economic Co-operation and Development*
OEEC	*Organisation for European Economic Cooperation*
OSI	*Open Systems Interconnection*
OTAN	Organização do Tratado do Atlântico Norte
PCA	Publicações de Comunicações da Armada
PCSD	Política Comum de Segurança e Defesa
PRACE	Programa de Reestruturação da Administração Central do Estado
RCTS	Rede Ciência, Tecnologia e Sociedade
SCEE	Sistema de Certificação Eletrónica do Estado
SI	Segurança da Informação
SICA	Sistemas de Informação e Comunicação Automatizados
SL	*Service Line*
TCOR	Tenente-Coronel
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
UC	Unidade Curricular
UE	União Europeia
UEO	Unidades, Estabelecimentos e Órgãos
UMIC	Agência para a Sociedade do Conhecimento
USA	*United States of America*

Lista de Tabelas

Lista de Imagens

Capítulo 1

Introdução

1.1 Enquadramento

1.2 Justificação do Tema

1.3 Objetivos

1.4 Metodologia de Investigação

1.5 Organização do Documento

1 Capítulo 1: Introdução

1.1 Enquadramento

O conhecimento humano surge da necessidade permanente de entender o mundo que nos rodeia. Trata-se de uma ferramenta fundamental que o Homem utiliza não só para a sua sobrevivência, mas também para se relacionar com o seu semelhante.

A necessidade e a dúvida são os fatores impulsionadores do desenvolvimento das capacidades do ser humano e "as inovações tecnológicas sempre acompanharam a evolução humana e foram desenvolvidas com o objetivo de facilitar e aprimorar as atividades necessárias para a subsistência do homem." (Efing, 2012, p. 23).

Atualmente vivemos na "Era da Informação", e qualquer tentativa de definição da sociedade da informação[1] em que nos inserimos mostra-se redutora. A sua complexidade e amplitude é tal que podemos definir caraterísticas, mas não dar uma definição concreta de sociedade da informação.

A expressão "sociedade da informação" realça o papel da informação na sociedade, por vezes também designada por "sociedade do conhecimento", na medida em que o conhecimento é gerado a partir da informação. Esta inversão de paradigma veio relativizar o espaço e o tempo, uma vez que as novas tecnologias, como a internet, permitem o acesso e compartilhamento de dados a partir de casa e instantaneamente.

Cada vez mais a nossa vida profissional, pessoal e social depende da tecnologia, já não há uma distinção clara entre a casa e o local de trabalho. As diferentes dimensões da nossa vida estão correlacionadas.

A internet assume-se como "uma dimensão de comunicação livre", é "um símbolo de liberdade e de capacidade para dominar o tempo e o espaço" (Wolton, 1999, p. 92), pela sua acessibilidade, universalidade e por conduzir o processo de globalização.

Contudo, apesar do seu papel fundamental, a internet também compreende riscos, nomeadamente para a segurança e defesa nacionais, pois "apesar de numa primeira análise se considerar a internet como um espaço por excelência de liberdade absoluta e

[1] Um dos primeiros autores a referir o conceito de Sociedade da Informação foi o economista Fritz Machlup, no seu livro publicado em 1962, *The Production and Distribution of Knowledge in the United States*. Contudo, o desenvolvimento do conceito deve-se a Peter Drucker que, em 1966, no seu livro *The Age of Discontinuity*, fala pela primeira vez numa sociedade pós industrial em que o poder da economia assenta num novo bem precioso: a informação. (Crawford, 1983, pp. 380-385)

sem fronteiras, a realidade porém, leva-nos a observar o ciberespaço como um local não somente virtual e físico mas isento de regulamentação jurídica, onde os mais diversos crimes se podem manifestar" (Martins, 2012).

Assim, constata-se que temos uma necessidade emergente de educar os cidadãos para uma melhor utilização das novas tecnologias, uma vez que "a chave para a prosperidade futura e para os modos de vida qualitativamente diferentes está na aprendizagem dos processos de manipulação, transmissão, armazenamento e obtenção de informação" (Lyon, 1992, p. 1).

O ciberespaço é um assunto cada vez mais relevante, tanto a nível nacional como internacional. Somos confrontados com todas as suas capacidades, assim como com os aspetos positivos e negativos que resultam da sua utilização. Contudo, o conhecimento sobre o seu real funcionamento, bem como as suas vulnerabilidades e sujeições, dificilmente serão mapeadas por completo.

É necessário confrontar os desafios que o ciberespaço nos coloca com a capacidade de resposta desenvolvida, uma vez que a necessidade de cibersegurança é hoje mais importante que uma defesa bélica eficaz.

Novas formas de ameaça surgiram com a evolução tecnológica, "provocando a deslocação do campo de batalha para o ciberespaço", onde nos confrontamos com um "inimigo que se tornou invisível perante os nossos olhos" (Martins, 2012).

Os ciberataques põem em risco a privacidade e liberdade dos cidadãos, ameaçam a segurança nacional e até mesmo a soberania do Estado. Torna-se cada vez mais imperativa a necessidade de proteger a informação, uma vez que esta já não se encontra armazenada num espaço singular e preciso, mas sim no ciberespaço.

No ciberespaço, o controlo do acesso à informação torna-se mais difícil, podendo esta ser utilizada de forma abusiva, por indivíduos mal-intencionados, para servir interesses ilegítimos e afrontar os direitos, liberdade e segurança dos cidadãos.

De acordo com o *Special Eurobarometer 404 – Cyber Security Report*[2], as perdas devido a cibercrimes representam biliões de euros por ano, e estima-se que existem mais de 150.000 vírus e outros tipos de *malware* em circulação e aproximadamente um milhão de pessoas vítimas de cibercrime por dia. Os resultados apresentados no relatório indicam

[2] Relatório elaborado por *TNS Opinion & Social*, a pedido *da European Commission, Directorate-General Home Affairs*, composto pelos resultados de uma pesquisa feita aos 27 países que constituem a UE e à Croácia, entre maio e junho de 2013. Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf (consultado a 09/11/15).

que 28% dos utilizadores da Internet na União Europeia (UE) não está confiante da sua capacidade para usar serviços como *online banking* ou comprar bens *online*. Contudo, 70% afirmam estar razoavelmente ou muito confiantes, valores estes muito semelhantes aos obtidos no *Special Eurobarometer 390*[3], pesquisa efetuada em 2012.

Foi ainda apurado que 10% dos utilizadores sofreu fraude *online*, 6% experienciaram roubo de identidade, 12% não conseguiram aceder a serviços *online* devido a ciberataques, 12% dos utilizadores tiveram a sua conta pessoal acedida de forma indevida (*hacker*), 7% foi vítima de fraude bancária *online* e 14% afirma ter encontrado, acidentalmente, material que promove o ódio racial e extremismo religioso.

Posto isto, e tendo como ponto de partida este panorama, considera-se essencial colaborar para a consciencialização e ação política no que respeita à cibersegurança. Ao Estado reconhece-se a capacidade última de proteger os seus cidadãos, e para isso é necessário fazer frente a estas ameaças que são uma constante diária.

1.2 Justificação do Tema

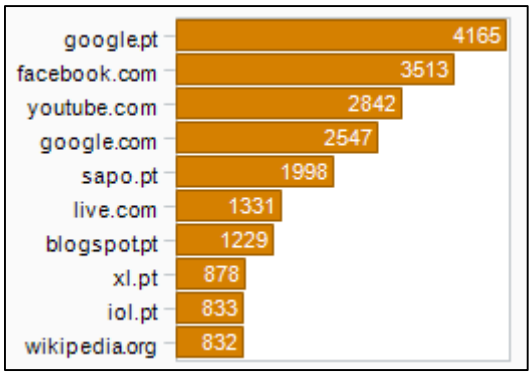
A utilização massiva das TI tem transformado a sociedade. Atualmente, a Internet é uma ferramenta que permite ao utilizador efetuar múltiplas tarefas. Não só é uma ferramenta de trabalho, mas também de diversão, indispensável a qualquer indivíduo.

Existem riscos associados à utilização da Internet, nomeadamente das redes sociais, dos quais é necessário ter conhecimento, estar alerta, agir em conformidade e, sobretudo, segurança.

Segundo uma notícia do Público, publicada em novembro de 2014, os Portugueses usam mais as redes sociais do que a média europeia.[4] Cerca de "70% dos utilizadores de Internet em Portugal usavam no ano passado [2013] redes sociais, significativamente acima dos 57% que eram a média dos 28 Estados-membros".

Em adição, conforme dados obtidos em 2015 e mostrados na figura 1, é possível constatar que o *Facebook* é a rede social eleita pelos utilizadores, estando em segundo lugar no Top 10 dos Domínios utilizados.

[3] Disponível em: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (consultado a 09/11/15).
[4] Disponível em: http://www.publico.pt/tecnologia/noticia/portugal-acima-da-media-da-ue-no-acesso-a-redes-sociais-online-1675356 Consultado a: 19/11/2015.



Fonte: Marktest, Netpanel *meter*

Figura 1 Top 10 Domínios em milhares de utilizadores únicos de 9 a 15 de novembro de 2015

A navegação dos Portugueses na Internet é distribuída, essencialmente, em torno do *Google, Facebook e YouTube*. O *Facebook*, que é hoje a rede social com mais adesão, em 2009 era notícia por ter ultrapassado o número de utilizadores do Hi5, que chegou a atingir os 3,2 milhões em Portugal.

A questão que se coloca, e que se tem vindo a tornar cada vez mais imperativa é de que forma se pode proteger os utilizadores dos perigos associados à utilização das redes sociais, e dos restantes domínios da Internet, quando estes, que reivindicaram pela criação de leis de proteção de dados pessoais estão hoje a publicar de livre e espontânea vontade os seus próprios dados nos perfis das redes sociais.

Os dados publicados voluntariamente pelos utilizadores das redes sociais vão deixando um rasto e são passíveis de se criar uma identidade digital acessível a qualquer outro utilizador. Há uma inconsciência generalizada, e uma despreocupação global com este assunto.

Os utilizadores expõem-se demasiado, revelando informações privadas e dados pessoais verdadeiros, o que pode acarretar consequências como roubos de identidade, assédios por parte de desconhecidos, raptos e violações.

Não há um conhecimento dos riscos associados e muito menos uma noção, ainda que básica, do que implica navegar na Internet. Os riscos atuais são bastantes e se não se educar os utilizadores para a cibersegurança estes não serão minimizados.

É nesta sequência que se compreende a necessidade emergente da cibereducação, isto é, consciencializar e educar os cidadãos para a importância da cibersegurança. Saber utilizar um computador não finda com o saber manuseá-lo e utilizar Internet não é tão simples como apenas aceder e navegar em *sites*. A gestão da informação, pessoal ou da organização, é um tema emergente que todas as entidades que manuseiam informação devem saber como fazer. Conhecer os mecanismos, políticas e procedimentos de

segurança pode não ser suficiente. É necessário também ter conhecimento sobre como a tecnologia funciona.

1.3 Objetivos

O principal objetivo do trabalho é propor um conjunto de Unidades Curriculares (UC) que permitam complementar, nos cincos anos de formação académica ministrada pela Escola Naval, matérias relacionadas com a utilização de Tecnologias de Informação e Comunicação (TIC) e Segurança da Informação (SI) e, por conseguinte, permitir aos oficiais da Marinha Portuguesa desempenhar as funções, relacionadas com a gestão da informação no ciberespaço.

Contudo, para atingir o objetivo proposto é necessário analisar a doutrina existente, e a que está a ser desenvolvida, em Portugal e restantes membros da UE e da Organização do Tratado do Atlântico Norte (OTAN), quer a nível público quer no privado. Assim, os objetivos estabelecidos para o presente trabalho foram os seguintes:

- Analisar as ações tomadas e organismos intervenientes na produção de política pública de cibersegurança em Portugal, na UE e na OTAN;
- Verificar a necessidade e pertinência da implementação de uma autoridade competente na área, o Centro Nacional de Cibersegurança, assim como do valor acrescido que traz para o desenvolvimento da política pública de cibersegurança em Portugal;
- Averiguar a necessidade de implementação de uma ou mais unidades curriculares, sobre a matéria em questão, no ciclo de estudos da Escola Naval;
- Efetuar entrevistas a oficiais da Marinha Portuguesa para verificar a necessidade de formação existente e aferir quais os conhecimentos e competências a desenvolver;
- Analisar unidades curriculares que sejam ministradas em outras Universidades, Institutos Superiores e Academias e com possível adaptação à organização Marinha Portuguesa;
- Propor uma ou mais unidades curriculares, devidamente justificadas, exequíveis e convenientes para a formação dos futuros oficiais da Marinha Portuguesa.

1.4 Metodologia de Investigação

Para realizar o presente trabalho, a metodologia de investigação utilizada foi baseada no método de investigação desenvolvido por Quivy e Campenhoudt, para as ciências sociais e humanas. A metodologia de Quivy e Campenhoudt é composta por três fases: rutura, construção e verificação, subdivididas em sete etapas, conforme Anexo A.

Assim, partindo da questão principal "Qual tem sido o papel da Escola Naval na formação dos oficiais da Marinha em matéria de cibersegurança?", e subsequente questão derivada "Qual a necessidade, em termos de formação, que os oficiais da Marinha têm para desempenhar funções relacionadas com a segurança da informação?", procedeu-se à pesquisa de informação e análise documental da literatura, livros, legislação, documentos e artigos científicos de autores reconhecidos, concluindo, assim, a primeira fase da metodologia de investigação: rutura.

Na segunda fase, a construção, foi efetuada uma análise e definição de conceitos, assim como um enquadramento teórico da temática abordada.

Seguidamente, foram conduzidas seis entrevistas, utilizando as respostas obtidas para análise e recolha de informação no terreno, por forma a validar a proposta a efetuar. As entrevistas enquadram-se na última fase, a verificação, e vêm validar a proposta efetuada com base na pesquisa anterior e respostas obtidas por oficiais da Marinha.

Para terminar, são apresentadas as conclusões do trabalho, concluindo a terceira fase da metodologia de Quivy e Campenhoudt.

1.5 Organização do Documento

O presente trabalho encontra-se dividido em cinco capítulos: capítulo 1 "Introdução", capítulo 2 "Revisão da Literatura", capítulo 3 "Proposta de Formação", capítulo 4 "Casos de Estudo" e, capítulo 5 "Conclusões".

No capítulo 1 é apresentado o impacto do desenvolvimento tecnológico, a pertinência e a razão de escolha deste tema, assim como a metodologia de investigação utilizada na realização do trabalho.

No capítulo 2 é feita uma breve apresentação das iniciativas na área da cibersegurança quer a nível nacional quer a nível europeu, a componente legal associada e atores intervenientes.

No capítulo 3 são analisadas as respostas obtidas através das entrevistas realizadas e, seguidamente, é apresentado um esquema de formação tendo em vista uma reestruturação das unidades curriculares da Escola Naval (EN), e adaptando a proposta às necessidades enunciadas.

No capítulo 4 são apresentados os casos de estudo que se consideram bons pontos de partida para a consciencialização da necessidade de cibereducação e que vêm colmatar o problema da falta de ensino na área da cibersegurança.

Por fim, no capítulo 5 é apresentada uma síntese do trabalho desenvolvido até então e deixadas algumas sugestões para continuidade de trabalhos futuros.

Capítulo 2

Revisão da Literatura

2.1 Mapa de Conceitos

2.1.1 Segurança

2.1.2 Segurança do Indivíduo

2.1.3 Segurança Nacional vs. Defesa Nacional

2.1.4 Ciberespaço

2.1.5 Ciberameaças

2.1.6 Ciberdefesa vs. Cibersegurança

2.1.7 Ciberguerra vs. Cibercrime

2.2 Cibersegurança na União Europeia

2.2.1 Casos dos ciberataques à Estónia e Geórgia

2.2.2 *European Union Agency for Network and Information Security*

2.2.3 Organização para a Cooperação e Desenvolvimento Económico

2.2.4 *European Defence Agency*

2.2.5 *European Cybercrime Centre*

2.3 Cibersegurança na Organização do Tratado do Atlântico Norte

2.3.1 *Cooperative Cyber Defence Centre of Excellence*

2.3.2 *Multinational Cyber Defence Education & Training*

2.3.3 NATO *Communications and Information* Agency

2.4 Cibersegurança em Portugal

2.4.1 CERT.PT

2.4.2 Gabinete Nacional de Segurança

2.4.3 Centro Nacional de Cibersegurança

2.4.4 IT4legal

2.4.5 Centro de Investigação Jurídica do Ciberespaço

2.5 Considerações Finais

2 Capítulo 2: Revisão da Literatura

2.1 Mapa de Conceitos

2.1.1 Segurança

O termo segurança abrange diversas aceções. Em linhas gerais, pode-se afirmar que este conceito deriva do latim *securitas*, que se refere à qualidade daquilo que é seguro, ou seja, aquilo que está protegido de quaisquer perigos, danos ou riscos. Quando se diz que algo é seguro, significa que é algo estável e indubitável. A segurança é uma certeza, mas também uma necessidade.

2.1.2 Segurança do Indivíduo

Segundo o artigo 27.º n.º1 da Constituição da República Portuguesa (CRP): "Todos têm direito à liberdade e à segurança". Contudo, só é possível beneficiar de liberdade e segurança num ambiente de justiça, como previsto no artigo 28.º da Declaração Universal dos Direitos do Homem, de 10 de dezembro de 1948: "Toda a pessoa tem direito a que reine, no plano social e no plano internacional, uma ordem capaz de tornar plenamente efetivos os direitos e as liberdades enunciados na presente Declaração".

O conceito de "segurança humana" ou segurança do indivíduo surgiu nos anos 1990 e veio alargar a noção tradicional de segurança, antes centrada na segurança dos Estados. Passou-se a atribuir mais valor ao próprio indivíduo.

A segurança do indivíduo visa proteger os indivíduos contra ameaças, criminalidade, violações dos direitos humanos, invasão de privacidade e ameaça à reserva de intimidade. Aponta ainda para ameaças como a fome, doença, pobreza, violação sexual, imigração, desemprego e tráfico de pessoas.

Em suma, todos têm direito à segurança, ao reconhecimento dos direitos fundamentais e de viver em liberdade e com dignidade.

2.1.3 Segurança Nacional vs. Defesa Nacional

A Segurança Nacional define-se como a condição da Nação que se traduz pela permanente garantia da sua sobrevivência em paz e liberdade; assegurando a soberania, independência e integridade do território, a salvaguarda coletiva de pessoas, bem como a

proteção dos seus bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas.[5]

O conceito de Segurança Nacional incorpora duas noções básicas: a Segurança Interna e a Segurança Externa ou Defesa Nacional.

Segurança Interna, de acordo com o artigo 1.º, n.º1 da Lei n.º 53/2008, de 29 de agosto, ou Lei de Segurança Interna, é definida como: "a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática", sendo que é exercida "em todo o espaço sujeito a poderes de jurisdição do Estado Português", segundo o artigo 4.º n.º1 do mesmo diploma.

Segurança Externa ou Defesa Nacional é assegurada pelo Estado, como consta no artigo 273.º n.º1 da CRP: "É obrigação do Estado assegurar a Defesa Nacional", e está definida no artigo 1.º da Lei n.º 29/82, de 11 de dezembro, ou Lei de Defesa Nacional e das Forças Armadas, como: "a atividade desenvolvida pelo Estado e pelos cidadãos no sentido de garantir, no respeito das instituições democráticas, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas".

2.1.4 Ciberespaço

Ciberespaço pode ser definido como um "ambiente virtual onde se agrupam e relacionam utilizadores, linhas de comunicação, *sites*, fóruns, serviços de internet e outras redes" (Gobierno de España, 2011, p. 43).

De acordo com o Dicionário Editora da Língua Portuguesa, ciberespaço é definido como um "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações".

No atual mundo globalizado, o ciberespaço é visto como um espaço virtual, "que a par dos tradicionais domínios da interação humana como a terra, o mar, o ar e o espaço, é o meio onde se desenvolvem as atividades económicas, produtivas e sociais das nações mais desenvolvidas" (Instituto da Defesa Nacional, 2013, p. 9)

[5] Ver Lei de Defesa Nacional e das Forças Armadas – Lei n.º 29/82, de 11 de dezembro.

"O ciberespaço é assim um ambiente em si mesmo, onde se deve ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-los, como os fatores humanos, uma vez que são estes que caraterizam os utilizadores deste ambiente" (Instituto da Defesa Nacional, 2013, pp. 9-10).

2.1.5 Ciberameaças

Ameaças que surgem na sequência da utilização massiva das TI ligadas em rede e que podem afetar infraestruturas críticas para o equilíbrio funcional da sociedade, assim como o sistema político internacional. Como exemplos de ciberameaças existe o *hacking*, o *hacktivismo*, o ciberterrorismo e a ciberespionagem.

O termo *hacking* refere-se a ações realizadas com recurso a ferramentas de *software* e *hardware* para exploração de vulnerabilidades dos sistemas informáticos com o objetivo de aumentar o nível de acesso ou controlo sobre os mesmos.

Hacktivismo é a ação conduzida por indivíduos ou grupos que utilizam meios informáticos e "vêem a Internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem" (Santos, 2011, p. 27). A ideologia defendida pode ter motivações distintas, desde políticas a religiosas, mas o objetivo final é comum: chamar a atenção da opinião pública para determinado assunto.

O ciberterrorismo consiste no uso das TI para ameaçar e realizar ataques políticos deliberados com grande impacto nos sistemas de redes de computadores e infraestruturas críticas. Promove o medo e o terror, "é um novo tipo de atividade criminal, (…) que materializa a convergência do ciberespaço com o terrorismo" (Santos & Bessa, 2008) que desencadeia determinadas ações políticas.

Ciberespionagem é caraterizada pela exploração de vulnerabilidades encontradas em *sites* para ter acesso a informação sensível. "É perpetrada por estados que procuram adquirir conhecimento e recolher informações, que lhe podem conceder uma vantagem estratégica sobre terceiros" (Pereira, 2012). A ciberespionagem é motivada pela vantagem competitiva sobre Estados ou ainda por benefícios financeiros provenientes da venda de informação roubada.

2.1.6 Ciberdefesa vs. Cibersegurança

Estes dois conceitos, apesar de pertencerem a domínios diferentes são complementares.

> "Por ciberdefesa entendem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco a soberania e segurança nacional, e cuja responsabilidade de resposta recai sobre as Forças Armadas (FFAA). Na cibersegurança incluem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco o espaço de liberdade individual/coletiva e de prosperidade que ele constitui e cuja responsabilidade de policiamento deve caber às Forças de Segurança e aos Serviços de Informações. A diferença entre a ciberdefesa e a cibersegurança é, por vezes, muito ténue e, devido à natureza de algumas ameaças, acabam por se sobrepor numa larga percentagem" (TCOR Ralo, 2013).

Assim, sucintamente, pode definir-se cibersegurança como a garantia de vigilância do ciberespaço para assegurar uma reação eficiente à prática criminosa no mesmo e, por sua vez a ciberdefesa "tem a função de garantir a realização de missões de segurança e defesa nacional, ou seja de garantir uma soberania do estado no ciberespaço global" (Nunes, 2012).

2.1.7 Ciberguerra vs. Cibercrime

Ciberguerra é "a materialização de ação de defesa ou de ataque contra todo o género de estruturas da informação e redes de computador, em que o campo de batalha é conduzido numa dimensão digital" (Santos & Bessa, 2008).

Cibercrime define-se como "toda e qualquer prática criminosa que tenha associadas à sua realização, ou como meio um aspeto *cyber* ou o recurso à utilização de computadores. Existem diversas tipologias e métodos de praticar o cibercrime, sendo um sistema o meio do ataque ou o alvo do mesmo"[6].

Desta forma, e tendo em conta os conceitos previamente definidos, faz sentido que as "Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às

[6] "What is Cybercrime?", Norton, Symantec. Disponível em: http://us.norton.com/cybercrime-definition (consultado a 11/11/15).

atividades relacionadas com o cibercrime e o *hacktivismo*, que os Serviços de Informação da República atuem em casos de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham de intervir para fazer face a ações de ciberguerra" (Nunes, 2012, p. 115), conforme se esquematiza na figura 2.

Figura 2 Cibersegurança Nacional - um edifício, vários pilares.[7]

2.2 Cibersegurança na União Europeia

Devido à emergência, necessidade e importância da cibersegurança, a UE publicou, em 2013, a "Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido"[8], que define cinco prioridades para a ação nesta área: a garantia de resiliência do ciberespaço; a redução drástica da cibercriminalidade; o desenvolvimento das políticas e das capacidades no domínio da ciberdefesa, no quadro da *Common Security Defence Policy* (CSDP) ou Política Comum de Segurança e Defesa (PCSD); o desenvolvimento de recursos industriais e tecnológicos para a cibersegurança; o estabelecimento de uma política internacional coerente em matéria de ciberespaço para a UE, que promova os valores fundamentais da mesma. (JOIN(2013) 1 final, pp. 4-5)

[7] Fonte: Nunes, Paulo Viegas (2012), A Definição de uma Estratégia Nacional de Cibersegurança, Cibersegurança, N.º133, IDN.

[8] Disponível em: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf Consultado a 16/12/2015.

A nível europeu existem diversas entidades com responsabilidades em matéria de cibersegurança e ciberdefesa, que muito têm contribuído para o desenvolvimento do conhecimento e doutrina nesta área e que se apresentam neste capítulo.

2.2.1 Casos dos ciberataques à Estónia e Geórgia

Entre abril e maio de 2007, a Estónia, um país na vanguarda da tecnologia, apelidado de *e*Stonia, onde a *Internet* é usada para realizar muitas das atividades quotidianas, foi alvo de uma sequência de ciberataques, maioritariamente do tipo *Distributed Denial of Service*[9] (DDoS).

Os ciberataques surgiram na sequência da decisão do governo da Estónia de mover, do centro da cidade para um cemitério na periferia da capital, Tallin, uma estátua de bronze de um soldado soviético da Segunda Guerra Mundial, a 27 de abril de 2007.

Houve vários protestos, tanto na Rússia como na Estónia, que foi ocupada pela União Soviética durante uma grande parte da Guerra Fria e, onde vive uma minoria russa. Segundo as autoridades Estónias, os ciberataques teriam sido ordenados pela Rússia, em retaliação pela remoção da estátua. Contudo, apesar de ter mostrado descontentamento e ter classificado a ação como "desumana", o governo russo negou qualquer envolvimento com os ataques.

Depois de concretizados, estes ciberataques não causaram danos a longo prazo. Contudo, o facto de terem posto abaixo diversos servidores governamentais, páginas de empresas e redes de pagamentos eletrónicos durante um certo período de tempo, tornou estes eventos caros, demorados e veio realçar os pontos fracos e vulnerabilidades da cibersegurança na Estónia.

Em agosto de 2008, durante a invasão russa da Geórgia, foram lançados ciberataques para derrubar sistemas bancários e *sites* que noticiassem a invasão. Estes foram maioritariamente do tipo *Web Defacement*[10] e DDoS, tal como tinha ocorrido um ano antes na Estónia.

Na origem dos ciberataques está o conflito armado que opôs a Federação Russa à Geórgia, devido ao território da Ossétia do Sul[11], reconhecido como parte integrante da

[9] Ataque informático que consiste em fazer com que um computador receba tantas solicitações por segundo ao ponto de ficar sobrecarregado e passe a recusar novos pedidos do utilizador. Desta forma o computador tem dificuldade ou é mesmo impedido de realizar as suas tarefas.
[10] Ataque cuja finalidade é mudar a aparência dos *sites* alvo, alterar o conteúdo e desfigurar o *site* original.
[11] Região separatista da Geórgia. Situa-se na zona montanhosa do Cáucaso, onde faz fronteira com a Ossétia do Norte.

Geórgia. Este território declarou independência no início da década de 1990 e pretendia unir-se à Ossétia do Norte, uma república autónoma dentro da Federação Russa. Estes foram controlados por *hackers* russos, com os quais o governo russo nunca admitiu qualquer envolvimento.

Os ciberataques duraram até ao final do mês de agosto, e a 26 de agosto de 2008, o presidente russo Dmitri Medvedev[12], anunciou que a Rússia reconhecia a independência da região separatista da Ossétia do Sul.

A novidade reside nesta nova frente de combate, o ciberespaço, pois tendo em conta o perfil dos tipos de ciberataques, estes não mostram qualquer inovação técnica. Os ataques tipo DDoS são conhecidos desde 1988, e as técnicas de *Web Defacement* utilizadas desde 1990, o que surpreendeu foi a proporção do ataque.

Estes eventos foram mais sentidos na Estónia, onde a população em geral estava habituada a uma utilização geral da Internet para acesso a diversos tipos de serviços. Na Geórgia os efeitos também foram sentidos, mas causaram menos transtorno à população, pois o nível de desenvolvimento da Sociedade da Informação era menor.

Com o desenrolar dos acontecimentos, e a proporção que estavam a tomar, foi captada a atenção da comunidade internacional, o que levou a OTAN a enviar especialistas para acompanhar de perto o desenvolvimento dos ataques e avaliar o enquadramento na sua política de defesa comum. Estes eventos em muito contribuíram para o planeamento de um centro de excelência para a ciberdefesa em Tallin, capital da Estónia.

2.2.2 *European Union Agency for Network and Information Security*

A *European Union Agency for Network and Information Security* (ENISA), em Portugal designada por Agência da União Europeia para a Segurança das Redes e da Informação foi criada em 2004, conforme o Regulamento (CE) n.º460/2004[13], e iniciou a sua atividade em 2005.

A sua missão consiste em contribuir para um elevado nível de segurança das redes e da informação na UE; promover a sensibilização para as questões envolvidas e

[12] 3.º Presidente da Rússia de maio de 2008 a maio de 2012, altura em que assumiu o cargo de 12.º Primeiro-Ministro da Rússia, que ocupa até à atualidade.
[13] Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:PT:PDF

desenvolver e promover uma cultura de segurança em benefício dos cidadãos, dos consumidores, das empresas e dos organismos do setor público.

O Regulamento (UE) n.º526/2013[14] do Parlamento Europeu e do Conselho relativo à ENISA revoga o Regulamento (CE) n.º460/2004, prorroga o seu mandato até 2020 e reforça a sua capacidade de fazer face a ciberataques e a outros desafios no domínio da segurança da informação.

O novo regulamento revigora as atribuições da ENISA, na medida que vem apoiar a elaboração da política e do direito da UE, promovendo a publicação das estratégias de segurança; apoiar o reforço da capacidade, prestando assistência aos Estados-membros e, neste âmbito inclui-se o apoio à Equipa de Resposta a Incidentes de Segurança Informática (CERT.PT); apoiar a cooperação voluntária e promover a sensibilização; apoiar a investigação, o desenvolvimento e a normalização e cooperar com as instituições e órgãos da UE que se ocupam da cibercriminalidade e da proteção da vida privada e dos dados pessoais, a fim de criar sinergias e abordar questões de interesse comum.

2.2.3 Organização para a Cooperação e Desenvolvimento Económico

A Organização para a Cooperação e Desenvolvimento Económico (OCDE), também designada por *Organisation for Economic Co-operation and Development* (OECD) foi oficialmente fundada a 30 de setembro de 1961, sediada em Château de la Muette em Paris, França.

Depois da criação da *Organisation for European Economic Cooperation* (OEEC) em 1948, desenvolvida para executar o Plano de Marshall[15], os governos individuais reconheceram a interdependência das suas economias e, por conseguinte, abriu-se o caminho para uma nova era de cooperação que veio mudar a Europa.

Posteriormente, o Canadá e os Estados Unidos da América (EUA) juntaram-se aos membros da OEEC e assinaram a Convenção da OECD a 14 de dezembro de 1960.

À data da assinatura da Convenção apenas 18 países europeus, o Canadá e os EUA uniram forças para criar uma organização dedicada ao desenvolvimento económico.

Contudo, atualmente são 34 os países que fazem parte desta organização e abrangem todo globo. Desde a América, do Norte e Sul, à Europa e Ásia-Pacífico, esta

[14] Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:PT:PDF

[15] Programa de recuperação empreendido pelos EUA, após a Segunda Guerra Mundial, para a reconstrução da Europa, um continente devastado pela guerra. Recebeu este nome devido ao Secretário de Estado dos EUA, George Marshall, o idealizador.

organização inclui vários países dos mais avançados, como também países emergentes de que são exemplo o México, Chile e Turquia.

A missão da OECD é promover políticas que melhorem a economia e o bem-estar social no mundo inteiro. Os governos dos diversos membros trabalham juntos, compartilham experiências e procuram soluções para problemas comuns e a OECD trabalha em conjunto com os governos para entender os fatores que impulsionam a mudança económica, social e ambiental.

A OECD mede a produtividade e o fluxo global do comércio e investimento, assim como analisa e compara os dados obtidos de forma a prever tendências futuras.

Em 2002 foram publicadas as OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*[16] adotadas pelo Conselho da OECD na 1037.º sessão, de 25 de julho de 2002.

Estas linhas orientadoras vêm dar resposta a um ambiente de segurança em constante mudança, promovendo o desenvolvimento de uma cultura de segurança; aumentando a consciencialização do risco, políticas, práticas, medidas e procedimentos; fomentando uma maior confiança entre os participantes; promovendo a cooperação e partilha de informação entre os intervenientes no desenvolvimento e implementação de políticas e práticas de segurança e, promovendo a consideração da segurança como um objetivo importante no desenvolvimento e aplicação de normas.

Foram definidos nove princípios orientadores:

- Consciência – os participantes devem estar cientes da necessidade de segurança dos sistemas de informação e redes, assim como do que podem fazer para a melhorar;
- Responsabilidade – todos os participantes são responsáveis pela segurança dos sistemas de informação e redes;
- Resposta – os participantes devem agir atempadamente e de forma cooperativa para prevenir, detetar e reagir a incidentes de segurança;
- Ética – os participantes devem respeitar os interesses legítimos de terceiros;
- Democracia – a segurança dos sistemas de informação e redes deve ser compatível com os valores de uma sociedade democrática;

[16] Linhas diretrizes para a Segurança da Informação, Sistemas e Redes: Para uma Cultura de Segurança. Ver: http://www.oecd.org/sti/ieconomy/15582260.pdf Consultado a 13/12/2015.

- Avaliações do Risco – os participantes devem realizar avaliações de risco;
- Modelo de Segurança e Implementação – os participantes devem incorporar a segurança como um elemento essencial dos sistemas de informação e redes;
- Gestão de Segurança – os participantes devem adotar uma abordagem global da gestão de segurança;
- Reavaliação – os participantes devem rever e reavaliar a segurança dos sistemas de informação e redes, e fazer as modificações necessárias das políticas de segurança, práticas, medidas e procedimentos.

2.2.4 *European Defence Agency*

A *European Defence Agency* (EDA) foi criada na dependência da Ação Conjunta do Conselho de Ministros a 12 de julho de 2004, para apoiar os Estados-membros e o Conselho nos seus esforços para melhorar as capacidades de defesa europeias no domínio da gestão de crises e apoiar a segurança europeia e a política de defesa.

A 12 de julho de 2011, o Conselho de Ministros definiu o estatuto, a sede e as regras de funcionamento da EDA, que substituiu a Ação Conjunta do Conselho de Ministros.

No âmbito da missão geral, foram atribuídas quatro funções à EDA: desenvolver as capacidades de defesa; promover a defesa, investigação e tecnologia; promover a cooperação de armamento e criar um Mercado Europeu de Equipamento de Defesa competitivo.

No âmbito do ciberespaço, a Estratégia de Cibersegurança da UE foi proposta em fevereiro de 2013 e aprovada pelo Conselho em junho desse mesmo ano, e sublinha que os esforços da UE, no que respeita à cibersegurança, envolvem também a dimensão da ciberdefesa. A cibersegurança é também uma das prioridades da EDA, realçada pelo Plano de Desenvolvimento de Capacidades da EDA.

O Conselho Europeu aprovou o *Cyber Defense Policy Framework*, o quadro político da ciberdefesa, em novembro de 2014, onde destacou cinco prioridades: apoiar o desenvolvimento das capacidades de ciberdefesa, relacionada com a CSDP, dos Estados-membros; melhorar a proteção das redes de comunicação CSDP utilizadas por entidades da UE; promover a cooperação civil-militar e sinergias com instituições relevantes da UE e agências de ciberdefesa, bem como do setor privado; melhorar as oportunidades de

formação, treino e educação e reforçar a cooperação com parceiros internacionais relevantes.

> "*Cyberspace today is considered the fifth domain of warfare, equally critical to military operations as land, sea, air and space. Success of military operations in the physical domain is increasingly dependent on the availability of, and access to, cyberspace. The armed forces are reliant on cyberspace both as a user and as a domain to achieve defence and security missions. In this regard, the European Defence Agency is at work to support the development of cyber defence capabilities among its Member States".*[17]

2.2.5 *European Cybercrime Centre*

A *European Cybercrime Centre* (EC3) começou a sua atividade em janeiro de 2013, para reforçar a resposta da aplicação da lei da criminalidade informática na UE, e para ajudar a proteger os cidadãos europeus, empresas e governos no que respeita ao cibercrime. A sua criação foi uma prioridade no âmbito da Estratégia de Segurança Interna da UE.

Ao colocar o EC3 na dependência do *European Police Office* (EUROPOL), o EC3 ficou não só com a capacidade de aplicação da lei existente na EUROPOL, mas também de expandir significativamente outras capacidades, em particular o apoio operacional e analítico às investigações dos Estados-membros.

Assim, o EC3 foi encarregado de se concentrar em três áreas: cibercrimes cometidos por grupos organizados, particularmente aqueles que geram grandes lucros criminosos, como fraudes *online*; cibercrimes que causem danos graves à vítima, como exploração sexual de crianças e cibercrimes (incluindo ciberataques) que afetem as infraestruturas e sistemas críticos e de informação da UE.

Recentemente a EC3 assinou um *Memorandum of Understanding* (MoU), ou seja, um memorandum de entendimento, em janeiro de 2015 com a AnubisNetworks, uma empresa Portuguesa de cibersegurança e *threat intelligence*, para combater a ameaça global do cibercrime. O memorandum cria a possibilidade de trabalhar em conjunto através da troca de conhecimentos, estatísticas e informação estratégica.

[17] Disponível em: http://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence Consultado a 16/12/2015.

2.3 Cibersegurança na Organização do Tratado do Atlântico Norte

Na Cimeira de Lisboa, em novembro de 2010, foi assinada pelos Chefes de Estado da OTAN uma declaração que exigia a plena capacidade operacional da *North Atlantic Treaty Organisation* (NATO) *Computer Incident Response Capability* (NCIRC).

Por conseguinte, a OTAN celebrou o seu maior contrato em cibersegurança até à data e os Estados-membros foram incentivados a aumentar as suas próprias capacidades de cibersegurança[18].

O NCIRC veio permitir à OTAN supervisionar redes de computadores a partir da sua sede em Bruxelas, a fim de detetar e responder a ameaças cibernéticas e a vulnerabilidades em cerca de 50 *sites* da OTAN em 28 países.

Mais tarde, na Cimeira do País de Gales, em setembro de 2014, uma das cinco prioridades da OTAN era combater novas ameaças, isto é proteger os seus membros e aliados de novos desafios, quer ameaças representadas por extremistas, conflitos regionais e ciberataques.

Assim, a OTAN, uma aliança sólida que contribui para a paz e um ambiente de segurança face à evolução da situação internacional, reforçou o plano de ação no domínio da cibersegurança, devido à volatilidade do cenário de ameaças, e alicerçada em organismos, projetos e escolas.

2.3.1 *Cooperative Cyber Defence Centre of Excellence*

"The need for a cyber-defence centre to be opened today is compelling. It will help NATO defy and successfully counter the threats in this area"[19]- General James Mattis[20], Bruxelas, 14 de maio de 2008.

O NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCoE) em Tallin, Estónia foi estabelecido a 14 de maio de 2008, depois de a Estónia propor o conceito de

[18] Ver http://www.pcguia.pt/2012/03/nato-celebra-o-maior-contrato-de-ciberseguranca-da-sua-historia/. Consultado a 25/01/2016.
[19] A necessidade de criação de um centro de ciberdefesa é irrevogável. Irá ajudar a NATO a desafiar e combater com sucesso as ameaças nesta área.
[20] General dos *United States Marine Corps* na reserva. Desempenhou funções de *Supreme Allied Commander Transformation* da NATO de novembro de 2007 a setembro de 2009.

um centro de ciberdefesa à OTAN em 2004, o qual foi aprovado pelo *Supreme Allied Commander Transformation* em 2006.

A missão do CCDCoE é aumentar a capacidade, cooperação e partilha de informação ente as nações OTAN e parceiros na ciberdefesa, em virtude da educação, investigação, desenvolvimento e consulta de lições aprendidas.

A visão adotada pelo CCDCoE é ser a principal fonte de sabedoria na área da ciberdefesa, acumulando, criando e disseminando conhecimento com as nações e parceiros da OTAN.

Os centros de excelência da OTAN são instituições nacionais ou multinacionais que treinam e educam os líderes e especialistas dos membros e parceiros da OTAN, auxiliam no desenvolvimento de doutrina, identificam lições aprendidas, melhoram a interoperabilidade e capacidades, e testam e validam conceitos através da experimentação, oferecem conhecimento e experiência reconhecidos.

Figura 3 Centros de Excelência da OTAN

2.3.2 *Multinational Cyber Defence Education & Training*

O *Multinational Cyber Defence Education & Training* (MNCDET) é um projeto cujo objetivo é criar uma Plataforma de Coordenação da Educação e Treino em Ciberdefesa (ponto de coordenação central para uma rede de atividades de Educação e Treino) e desenvolver e proporcionar novas iniciativas, destinadas a preencher as lacunas de Educação e Treino em Ciberdefesa existentes ao nível da OTAN e das Nações.

Este projeto contribuirá para melhorar o processo de desenvolvimento das Capacidades Nacionais de Ciberdefesa e de Cibersegurança e para melhorar a interoperabilidade entre especialistas no âmbito da OTAN. Numa perspetiva nacional, as Nações terão a possibilidade de disponibilizar atividades de Educação e Treino à OTAN e às Nações Aliadas, e obter também certificação OTAN para atividades de Educação e Treino em Ciberdefesa.

O Projeto MNCDET desenvolve-se em diversas fases, estando neste momento a decorrer as fases 1 e 2. A Fase 1 corresponde à Definição de Competência e *Skills* da Ciberdefesa e a fase 2 está relacionada com os Requisitos de Educação e Treino em Ciberdefesa, respetivamente.

O desenvolvimento destas fases está a ser sincronizado e coordenado com a vertente internacional do Projeto, garantindo assim a necessária coerência e articulação dos esforços nacionais a desenvolver neste âmbito.

Os participantes do Projeto são o Ministério da Defesa, o Centro de Ciberdefesa das Forças Armadas, o Centro Nacional de Cibersegurança, a Marinha com a presença de representante da Escola Naval e o Exército, sendo que já manifestaram formalmente interesse em associar-se à vertente Nacional do Projeto cerca de 86 Entidades/Organizações públicas e privadas.

2.3.3 NATO *Communications and Information Agency*

A NATO *Communications and Information* (NCI) *Agency* foi criada a 1 de julho de 2012 em Haia, Holanda, como resultado da fusão da NATO *Consultation, Command and Control Agency* (NC3A), da NATO *Air Command and Control System* (ACCS) *Management Agency* (NACMA), da NATO *Communication and Information Systems Services Agency* (NCSA) e da NATO *Active Layered Theatre Ballistic Missile Defence* (ALTBMD) *Programme Office* e elementos da NATO *Headquarters* (HQ) *Information Communications and Technology Management* (ICTM).

No domínio da cibersegurança, a NATO NCI *Agency Cyber Security* (CS) *Service Line* (SL) é responsável pelo planeamento e execução da gestão do ciclo de vida de todas as atividades para a cibersegurança.

A CS SL fornece serviços especializados relacionados com a cibersegurança, incluindo as áreas científica, técnica, aquisição, operações, manutenção e suporte sustentável durante todo o ciclo de vida da informação, comunicações e tecnologia da OTAN, permitindo a condução segura das operações e negócios da Aliança através da NATO *Network Enabled Capability* (NNEC) e no contexto da NATO's *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (C4ISR).

A CS é responsável por fornecer um amplo conjunto de serviços: *Communications and Information Systems* (CIS) *security*, ciberdefesa, segurança da informação e dos computadores.

No âmbito das suas responsabilidades, a CS SL fornece suporte para o desenvolvimento e implementação de estratégia e legislação relacionada com a cibersegurança, e fornece serviços de manutenção do ciclo de vida para todas as TIC da OTAN.

A CS lidera no desenvolvimento de novas capacidades e inovação na cibersegurança. Incorpora a NCIRC *Technical Centre*, oferecendo serviços especializados para prevenir, detetar, responder e recuperar de incidentes de cibersegurança.

2.4 Cibersegurança em Portugal

Atualmente a necessidade de garantir a segurança da informação dos cidadãos, das organizações e do Estado é imperativa. Contudo, proteger a informação alojada nos sistemas e nas redes informáticas nem sempre constituiu um problema para a sociedade.

De certa forma, não houve necessidade de investir na cibersegurança, nem por parte dos decisores políticos nem por parte dos cidadãos, que não solicitavam que fossem tomadas medidas nesse sentido. Contudo, na sequência do desenvolvimento tecnológico, "não só as novas tecnologias revolucionaram o mundo como também provocaram um sentimento negativo em torno do fator de segurança, nomeadamente em questões de privacidade e garantia dos sistemas de informação do Estado" (Martins, 2012).

Relativamente ao ciberespaço foi constatada a inexistência de legislação específica para evitar e colmatar as problemáticas que advêm da sua utilização e cujos problemas estão na base de uma possível suspensão do funcionamento das infraestruturas críticas nacionais.

Primeiramente foi publicada a SEGNAC 4, Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas (Resolução de Conselho de Ministros n.º5/90, de 28 de fevereiro), que definia instruções que tinham como objetivo garantir a segurança nos sistemas informáticos, no que respeita ao tratamento de matérias classificadas.

Contudo, havia consciência que as normas definidas não constituíam plena segurança das redes e, pouco depois, surgiu a Lei de Proteção de Dados Pessoais face à Informática (Lei n.º 10/91, de 29 de abril) cujo princípio geral, conforme o artigo 1.º diz: "O uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão".

Com esta Lei foi criada a Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPI) a quem foi atribuída a função de "controlar o processamento automatizado de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei"[21].

Posteriormente, a Lei da Criminalidade Informática (Lei n.º 109/91, de 17 de agosto) que foi revogada pela Lei n.º 109/2009, de 17 de setembro (Lei do Cibercrime).

Em 1996, foi publicada a Resolução do Conselho de Ministros n.º 16/96, de 21 de março. Esta Resolução reconhecia que nas sociedades modernas, a informação é crescentemente transversal e intersetorial e, ainda referia as necessidades presentes de dinamização estratégica das orientações do Governo adequadas ao desenvolvimento da Sociedade de Informação.

Em 1997 surge o Livro Verde para a Sociedade da Informação em Portugal, que foi aprovado pelo Conselho de Ministros no dia 17 de abril de 1997. O livro Verde para a Sociedade da Informação reconhece que as novas TI têm grandes potencialidades em diversas áreas mas, por outro lado, alerta para a importância do estudo do impacto dessas inovações no funcionamento das instituições e do próprio Estado. É um documento que contempla as questões de proteção, integridade e veracidade dos dados informáticos.

[21] Conforme o artigo 4.º n.º1 do referido diploma.

Em 2002, Portugal confrontava-se com um "grave descontrole das contas públicas, com um crescimento desenfreado das despesas do Estado e com uma perigosa ameaça de não cumprimento das nossas obrigações no quadro da União Europeia"[22].

Foi por ter consciência do estado vigente do país que o Governo voltou a introduzir a questão da cibersegurança na agenda política, antecipando a criação de um Plano de Segurança Digital Nacional e o desenvolvimento de uma Estratégia de *eGovernment*[23], pois como foi constatado: "no que concerne aos indicadores da Sociedade da Informação, é imperioso retirar Portugal da cauda da Europa"[24].

Destaca-se, ainda, a Fundação para a Computação Científica Nacional (FCCN) que é a unidade da Fundação para a Ciência e Tecnologia (FCT I.P) responsável pela gestão e operação da Rede Ciência, Tecnologia e Sociedade (RCTS), ou seja, *National Research and Education Network* (NREN), portuguesa. Os membros da FCCN verificaram um aumento do número de incidentes de segurança informática e constataram que Portugal não tinha nenhuma equipa de resposta a este tipo de incidentes.

Assim, teve génese, em 2002, a equipa de resposta a incidentes de segurança informática, *Computer Emergency Response Team* (CERT), com a criação do CERT.PT, que veio ocupar um papel de relevo na cibersegurança nacional.

> "No que toca ao ciberespaço nacional, o CERT.PT preencheu a lacuna de um CERT de âmbito nacional, fornecendo um serviço de coordenação de incidentes de segurança, sempre que solicitado e na medida das suas capacidades"[25].

Ainda segundo a FCT: "a constituição da Rede Nacional de *Computer Security Incident Response Team* (CSIRT) (serviços de resposta a incidentes de segurança informática), iniciativa do CERT.PT foi de particular importância na criação de mecanismos eficazes de resposta a ameaças e de colaboração entre equipas CSIRT em Portugal"[26].

---

[22] Fonte: Programa do XV Governo Constitucional. Disponível em: http://www.portugal.gov.pt/media/464051/GC15.pdf (p.5) Consultado a 18/11/2015.

[23] Consiste na utilização das TIC na Administração Pública com o intuito de oferecer os serviços públicos mais eficazes e de melhor qualidade, para reduzir os prazos de espera dos utentes e aumento da transparência e responsabilidade dos serviços. Ver http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=URISERV:l24226b&rid=9 Consultado a 06/11/2015.

[24] Idem (p.141).

[25] Fonte: http://www.cert.rcts.pt/ Consultado a 19/11/2015.

[26] Retirado de: http://www.computerworld.com.pt/2015/03/25/funcoes-do-cert-pt-passam-para-cncs/ Consultado a 19/11/2015.

Em 2005, é criada a Estrutura Nacional de Segurança da Informação (ENSI), grupo de trabalho composto pela Agência para a Sociedade do Conhecimento (UMIC), pela Autoridade Nacional de Comunicações (ANACOM), FCCN e pelo Gabinete Nacional de Segurança (GNS), de onde resultou a elaboração da Política Nacional de Segurança da Informação, em fevereiro de 2005.

Na sequência da publicação do PEMGFA/CSI/004, de 14 de fevereiro de 2005, que definia requisitos de segurança no âmbito da ciberdefesa, criou-se a Capacidade de Resposta a Incidentes de Segurança Informática das Forças Armadas (CRISI-FA), no campo de ação do Grupo de Resposta a Incidentes de Segurança Informática (GRISI), e recorrendo às estruturas existentes nos Ramos das FFAA e do Estado-Maior General das Forças Armadas (EMGFA) cuja incumbência seria "promover a implementação da política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA" (Freire & Nunes, 2013, p. 57).

A Equipa de Missão Computadores, Redes e Internet na Escola (CRIE) é criada a 1 de julho de 2005 com a missão de organizar uma ação integrada no plano do uso educativo das TIC, para proporcionar mais e melhor instrução nas escolas nacionais.

Pela Resolução do Conselho de Ministros n.º 171/2005, de 3 de novembro é aprovada a criação da Entidade de Certificação Eletrónica do Estado (ECEE).

Em 2006, a Resolução do Conselho de Ministros n.º 39/2006, de 21 de abril veio aprovar as orientações, gerais e especiais, para a reestruturação dos ministérios, prevista no Programa de Reestruturação da Administração Central do Estado (PRACE), aprovado pela Resolução do Conselho de Ministros n.º 124/2005.

Em 2009, a Resolução da Assembleia da República n.º 88/2009, de 15 de setembro aprova a Convenção sobre o Cibercrime, adotada em Budapeste a 23 de novembro de 2001.

Em 2011, a Resolução do Conselho de Ministros n.º 46/2011, de 14 de novembro, constituiu o Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC), que elaborou um plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública.

Em 2012, a Resolução do Conselho de Ministros n.º12/2012, de 7 de fevereiro veio aprovar as linhas gerais do plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública e, através da medida 4 (definição e implementação de uma estratégia nacional de segurança da informação), propôs-se

consolidar a ENSI, definindo objetivos nacionais, responsabilidade, organização, gestão e serviços para a segurança da informação.

Nesta medida é referido que a ENSI compreenderá: "A criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (CNCS)" e "o aprofundamento e melhoria das condições de operação do Sistema de Certificação Eletrónica do Estado (SCEE), com vista à sua adequação aos requisitos internacionais mais recentes"[27].

Na sequência da Resolução do Conselho de Ministros n.º12/2012, de 7 de fevereiro surge a Resolução do Conselho de Ministros n.º42/2012, de 13 de abril que "visa constituir a Comissão Instaladora do Centro Nacional de Cibersegurança, colocando-a, atenta a transversalidade dos seus objetivos, na dependência do Primeiro-Ministro"[28].

Com a instalação do CNCS, este ficou a assegurar desde 16 de março as funções nacionais de resposta a incidentes na segurança informática, assumindo o trabalho até aqui do CERT.PT.

Por fim, no presente ano, a Resolução do Conselho de Ministros n.º36/2015, de 12 de junho veio aprovar a Estratégia Nacional de Segurança do Ciberespaço, que representa um:

> " (…) esforço destinado a reduzir debilidades ao nível da segurança das redes e da informação, aumentando a resiliência das suas infraestruturas críticas, (…) fundamental, quer no quadro da União Europeia, ao nível da Estratégia da União Europeia para a Cibersegurança, quer das políticas de Ciberdefesa da Organização do Tratado do Atlântico Norte (OTAN)."

2.4.1 CERT.PT

O CERT.PT é um Serviço de Resposta a Incidentes de Segurança da RCTS. A FCT e o CNCS celebraram um protocolo que assegura e agiliza a transição das funções nacionais de resposta a incidentes. Este protocolo promove a cooperação bilateral em áreas como a consciencialização no domínio da utilização segura da internet, a partilha

[27] Fonte: Resolução do Conselho de Ministros n.º12/2012, de 7 de fevereiro. Disponível em: https://m6.ama.pt/docs/RCM12_2012.pdf Consultado a 19/11/2015.
[28] Fonte: Resolução do Conselho de Ministros n.º42/2012, de 13 de abril. Disponível em: https://dre.pt/application/dir/pdf1s/2012/04/07400/0192501926.pdf Consultado a 19/11/2015.

de conhecimento e de boas práticas em matéria de cibersegurança e a partilha de ferramentas para gestão de incidentes.

Enquanto coordenador nacional de resposta a incidentes de cibersegurança, com a assinatura deste protocolo, o CNCS assegurará os diversos serviços prestados anteriormente pelo CERT.PT, na sua vertente nacional. O inicialmente CERT da FCT prosseguirá a sua atividade como RCTS CERT, focado agora nas comunidades de investigação e de ensino ligadas à RCTS, sob tutela do Ministério da Educação e Ciência.

Por sua vez, a Rede Nacional CSIRT tem como objetivos estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança; criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contramedidas pró-ativas e reativas; criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão e promover uma cultura de segurança em Portugal.

2.4.2 Gabinete Nacional de Segurança

O Gabinete Nacional de Segurança é um serviço central da administração do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar.

O GNS tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exerce a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no do SCEE.

A Autoridade Nacional de Segurança (ANS) dirige o GNS e é a entidade que exerce, em exclusivo, a proteção e a salvaguarda das informações classificadas.

Em 1960 o Decreto-Lei n.º 42806, de 14 de janeiro cria a ANS NATO, como resultado de Portugal ter de cumprir com as suas obrigações para com a OTAN. Em 1982 a promulgação da Lei n.º 29/82 (Lei de Defesa Nacional e das Forças Armadas), de 11 de dezembro passa a tutela da ANS para o Ministro da Defesa Nacional, em 1993 o Decreto-Lei n.º 47/93, de 26 de fevereiro (Lei Orgânica do Ministério da Defesa Nacional) alarga as competências da ANS aos Tratados e Alianças Internacionais celebrados por Portugal, à Administração Pública e às Representações Oficiais de Portugal no estrangeiro. Em

1997, com o Decreto-Lei n.º 217/97, de 20 de agosto, é alterada a designação da ANS para GNS e alargada a esfera de influência da ANS, sendo aprovadas a orgânica, o quadro de pessoal e o regulamento do seu funcionamento. Em 2007, o Decreto-Lei n.º 170/2007, de 3 de maio aprova a orgânica do GNS, definindo-lhe a Missão e as atribuições e estabelece as competências da ANS. Em 2012, o Decreto-Lei n.º 3/2012, de 16 de janeiro procede à 1ª alteração à lei Orgânica do GNS, prorroga competências da ANS, Missão e atribuições do GNS, ou seja, altera o Decreto-Lei n.º 170/2007, de 3 de maio. Em 2014, o Decreto-Lei n.º 69/2014, de 9 de maio procede à 2ª alteração à lei Orgânica do GNS, prorroga competências da ANS, Missão e atribuições do GNS; estabelece o CNSC, que funciona no âmbito do GNS e revoga o Decreto-Lei n.º 170/2007, de 3 de maio.

2.4.3 Centro Nacional de Cibersegurança

Estabelecido através do Decreto-Lei n.º69/2014[29], de 9 de maio, o Centro Nacional de Cibersegurança entrou em funcionamento em outubro de 2014, tendo definido como objetivos iniciais: Implementar as medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento dos organismos do estado, das infraestruturas críticas e dos interesses nacionais; e apostar claramente numa estratégia de prevenção, sensibilização e educando as organizações em particular e a sociedade civil em geral para as questões da cibersegurança, contribuindo desta forma para a criação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança.

Este CNCS veio, assim, contribuir para que Portugal use o ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional.

Uma das formas que utiliza para atingir os seus objetivos é a sensibilização. O CNCS promove eventos no âmbito das iniciativas de divulgação, sensibilização e discussão aberta das temáticas relacionadas com a segurança e cidadania no ciberespaço e cibersegurança em geral.

[29] Disponível em https://dre.pt/application/dir/pdf1s/2014/05/08900/0271202719.pdf Consultado a 15/12/2015.

2.4.4 IT4legal

A IT4legal é um grupo informal dedicado à partilha e divulgação de informação acerca de sistemas de informação nas sociedades de advogados.

Este grupo nasceu da constatação de que há necessidades específicas desta atividade, necessidades que são comuns a todas as sociedades de advogados portuguesas e, simultaneamente, de que a informação acerca das soluções e métodos mais adequados para dar resposta a tais necessidades não se encontra facilmente disponível.

Assim, surgiu a iniciativa de reunir regularmente os responsáveis pelos sistemas de informação de várias sociedades de advogados, com o objetivo de reunir e partilhar informação acerca de temas que revestem maior relevância para estas organizações, entre os quais se inclui a segurança da informação.

A participação neste grupo é restrita a profissionais das sociedades de advogados, não sendo permitidos potenciais fornecedores de tecnologia ou serviços, por forma a evitar a prevalência de interesses e comerciais e manter a discussão e partilha de informação o mais autêntica e aberta possível.

2.4.5 Centro de Investigação Jurídica do Ciberespaço

O Centro de Investigação Jurídica do Ciberespaço (CIJIC), da Faculdade de Direito de Lisboa, estuda, investiga, partilha e difunde conhecimento no âmbito do Ciberespaço. Possui uma visão multidisciplinar e uma abordagem integrada de várias áreas do conhecimento, tal como os imensos desafios do ciberespaço assim exigem.

Com o CIJIC é concretizada a ideia de agrupar um conjunto de professores de várias Escolas, fundindo as suas competências, com o suporte institucional das respetivas entidades de ensino a que estão ligados, para divulgar e ensinar as disciplinas jurídicas envolvidas na regulação normativa do ciberespaço. A forma de divulgar o esforço e trabalho desenvolvido é a revista científica: *Cyberlaw by* CIJIC.

Este centro veio cimentar o protocolo entre a EN, a Faculdade de Direito e o Instituto Superior Técnico (IST) para a realização do mestrado em Segurança da Informação e Direito da Cibersegurança; a colaboração com a Faculdade de Ciências da Universidade de Lisboa e o GNS, na criação de condições para o surgimento da CNCS e ainda veio firmar protocolos com as mais reputadas instituições de ensino e de investigação na área do ciberespaço.

2.5 Considerações Finais

No âmbito do trabalho de investigação realizado, existem múltiplas agências, organismos, escolas e projetos pertencentes à UE, à OTAN e a organizações nacionais que abordam o tema da cibersegurança. O seu propósito difere, passando pela investigação, monitorização, prevenção e também formação.

Na tabela 1 é possível resumir e clarificar as linhas de ação de cada agência, organismo, escola ou projeto abordado no presente capítulo.

Não obstante a importância do trabalho realizado por cada uma destas entidades, têm mais relevância, para o seguimento da presente tese de mestrado, as entidades que dão formação.

Desta forma, reduzimos a lista para apenas três entidades, uma escola, um projeto ao nível da OTAN e um centro a nível nacional.

O CCDCoE é a principal fonte de erudição da OTAN. Investiga, consulta lições aprendidas e dissemina o conhecimento adquirido com as nações e parceiros da OTAN. Por sua vez, o MNCDET é um projeto que veio colmatar as lacunas de educação e treino existente ao nível da OTAN.

A nível nacional o CNCS veio aumentar a cultura nacional de cibersegurança. Atua ao nível da sensibilização, promovendo eventos de discussão aberta de temáticas relacionadas com a segurança e cidadania no ciberespaço e cibersegurança em geral.

Ao longo do último ano foram realizadas diversas atividades de sensibilização abertas à comunidade em geral, alguns dos temas apresentados foram: "Mobilização e Ação Coletiva no Ciberespaço", "Quem sou eu na Internet", "A nossa informação está segura?" e "*Why we need CyberSkills*?". Paralelamente foram realizadas sessões de índole mais específico tais como: "Segurança na Internet" para alunos de Mestrado no Instituto Superior de Economia e Gestão (ISEG), "Internet Mais Segura 2015" uma sessão de esclarecimento para a comunidade escolar e "Desafios da Cibersegurança" para auditores de Justiça, futuros Magistrados Judiciais e do Ministério Público.

Em suma, as instituições governamentais preocupam-se com a monitorização e a prevenção. Contudo, uma forma de prevenir é oferecer formação, um aspeto que está a ser descurado.

Existe formação na área da cibersegurança, formação de qualidade e pertinente, mas ministrada por instituições que estão vocacionadas para áreas específicas de atuação.

Contudo, ao nível institucional existem poucas ações de formação e cursos, a formação oferecida não está adequada à organização Marinha. Pode auxiliar como complemento, mas não como um todo, uma vez que não está adaptada à população alvo e às funções específicas desempenhadas na nossa organização, a Marinha.

A formação, para trazer valor acrescido tem de estar adaptada a estes dois critérios, a população alvo, que vai frequentar a formação, e as funções que exercem. Assim, o trabalho desempenhado por estas três entidades formadoras vem corrigir algumas lacunas na nossa formação, mas não é suficiente porque não é adequada à especificidade dos nossos cargos.

Tabela 1 Quadro-Resumo

Entidade	Agência/Organismo/Escola	Investigação	Monitorização	Prevenção	Formação
UE	ENISA	✓	✓	✓	
	OECD	✓	✓	✓	
	EDA	✓		✓	
	EC3		✓	✓	
OTAN	CCDCoE	✓			✓
	MNCDET				✓
	NCI Agency	✓	✓	✓	
PT	CERT.PT	✓	✓	✓	
	GNS		✓	✓	
	CNCS		✓	✓	✓
	IT4legal		✓	✓	
	CIJIC	✓			

Capítulo 3

Proposta de Formação

3.1 Formação Necessária e Exequível

3.2 Lacunas Académicas

3.3 Proposta Fundamentada

3 Capítulo 3: Proposta de Formação

3.1 Formação Necessária e Exequível

A Escola Naval é um estabelecimento de Ensino Superior Público Universitário Militar destinado a formar os oficiais dos quadros permanentes da Marinha Portuguesa. A instituição conta um corpo docente constituído por professores militares e civis, que associam à sua função de docência uma vasta experiência profissional.

Não obstante a integrante profissional ministrada, assim como a formação militar-naval numa componente mais prática oferecida aos cadetes da EN, a formação académica é o ponto fulcral, havendo um conjunto de mestrados integrados em diversas especialidades.

Uma vez que, na área da cibersegurança, a formação oferecida pelos diversos organismos, agências, escolas e projetos são endereçados apenas a alguns elementos da Marinha, em que a sua atividade profissional está diretamente relacionada com TIC e SI, torna-se imperativo perceber o que é producente e adequado à especificidade dos nossos cargos, e lecionar, como formação base, a todos os futuros oficiais da Marinha matérias relacionadas com a cibersegurança.

É previsível que, para falar de cibersegurança, se pressuponham conhecimentos em determinadas áreas que também não estejam a ser abordados com a devida abrangência e de forma aprofundada.

Como referido, a formação tem de estar adaptada à população alvo e suas respetivas funções e, por conseguinte, faz sentido que os alunos da Escola Naval, de qualquer classe, tenham um conhecimento genérico da importância da cibersegurança, onde se inclui as causas, os efeitos e as consequências. Porém, conforme informação obtida junto de oficiais da classe de Engenheiros Navais – ramo Armas e Eletrónica (EN-AEL), verifica-se que nas suas funções a bordo das unidades navais e unidades em terra, os oficiais desta classe carecem de formação específica nas componentes de Cibersegurança, Segurança da Informação e Gestão da Segurança da Informação.

Neste contexto, são sugeridas duas unidades curriculares distintas: uma primeira, transversal a todas as classes, fundamentos de cibersegurança, cujo objetivo será ministrar as ferramentas e conhecimentos que importa reter de segurança informática em

computação, como os conceitos básicos de segurança, os estados da informação, as políticas de segurança e a gestão da mesma. Posteriormente, será sugerida uma segunda unidade curricular, mais específica, mas destinada apenas a alunos da classe EN-AEL, onde serão aprofundados aspetos operacionais como políticas e procedimentos, mecanismos de ataque e defesa e análise de risco.

Neste sentido, foram efetuadas entrevistas (ver Anexo B) com esse propósito, perceber, através de quem já desempenha funções, quer seja a bordo, quer seja na Direção das Tecnologias de Informação e Comunicação (DITIC), se se considera necessário aprofundar determinadas temáticas.

As entrevistas foram conduzidas pelo autor e feitas a vários oficiais da classe de EN-AEL. Os resultados serão utilizados para fundamentar os conteúdos programáticos da unidade curricular específica para mestrandos desta classe, uma vez que a primeira unidade curricular, comum a todas as classes, será genérica e facultará as ferramentas básicas para assimilar a importância e pertinência do tema.

Desta forma, considera-se necessário e, sobretudo, exequível uma unidade curricular, de caráter académico, pois essa é de facto a missão da Escola Naval.

Não descorando das lacunas profissionais, pois elas existem, todavia, há unidades incumbidas de administrar formação profissional e há uma lista de cursos a frequentar antes de destacar quer para unidades navais, quer para a DITIC. São esses cursos que vão fornecer ferramentas práticas, que aliadas à teoria que os oficiais da marinha já são portadores fará todo o sentido e ajudá-los-á no desempenhar das funções que lhes são atribuídas.

As entrevistas efetuadas foram constituídas por quatro questões gerais e duas questões particulares. As questões particulares foram colocadas exclusivamente para os oficiais entrevistados que desempenham funções na DITIC.

O objetivo passou por compreender que disciplinas poderiam ter sido mais aprofundadas, ou, matérias que não foram de todo lecionadas e, efetivamente foram necessárias ao longo dos seus percursos profissionais.

Em suma, ao inferir, através das entrevistas, é proposto um conjunto de temas fundamentais a contemplar na UC específica do ciclo de estudos de EN-AEL.

3.2 Lacunas Académicas

As entrevistas realizadas no âmbito da presente dissertação de mestrado foram conduzidas do geral para o particular, de forma a criar um encadeamento lógico que permitisse perceber, claramente, as necessidades sentidas por cada um dos entrevistados. Findas as entrevistas é possível afirmar que há uma certa uniformidade nas respostas, sendo que as maiores discrepâncias se devem ao facto de existir uma diferença no período em que cada entrevistado passou pela Escola Naval.

Em primeiro, foi questionada a opinião individual sobre os conhecimentos necessários à saída da EN, isto é, depois de cinco anos de formação superior universitária militar, quais as unidades curriculares que melhor preparam os recentes Engenheiros Navais – ramo Armas e Eletrónica a desempenhar as funções para as quais foram preparados.

As respostas dadas à primeira questão, por todos os entrevistados, foram idênticas, uma vez que para desempenhar o cargo de Chefe de Serviço de Armas e Eletrónica (CSAE), em que, dependendo do navio, também faz quartos à ponte, as UCs mais necessárias são as comuns a todas as classes - Navegação e Comunicações. Quanto às disciplinas específicas da classe de EN-AEL, as respostas também permitiram chegar a um consenso, tendo sido apontadas UCs como Sistemas de Armas, Sistemas de Radar e Radioajudas, Antenas e Radiopropagação e Sistemas de Telecomunicações. Estas UCs permitiram adquirir os conceitos principais para perceber o funcionamento das armas e sensores que equipam um navio.

Porém, existe um conjunto de UCs específicas dos EN-AEL, que é de opinião geral que devem ser restruturadas e aprofundadas. Estas UCs foram consideradas necessárias para que os EN-AEL possam desempenhar as suas funções que lhes são exigidas no decorrer da sua atividade profissional. As matérias em questão estão relacionadas com a segurança da informação e com o funcionamento das redes de comunicação automática de dados.

Ainda no seguimento da resposta à segunda pergunta, um dos inquiridos mencionou a pertinência dos cursos DKI 35 e DKI 36, ministrados pela Escola de Tecnologias Navais (ETNA).

O Curso de Adaptação Conceitos de Redes de Comunicação de Dados (DKI 35) é um curso de índole profissional que visa a aquisição de conhecimentos no âmbito das

redes de comunicações. Confere competências elementares necessárias à utilização de redes locais e equipamentos associados (ver Anexo C) e é destinado a oficiais, sargentos, praças, militarizados e civis equiparados, tendo a duração aproximada de três dias úteis, cerca de 18 horas e não pressupõe a obtenção de nenhum curso previamente.

Relativamente ao Curso de Adaptação em Administração Windows NT[30] (DKI 36), este permite adquirir conhecimentos no âmbito da administração de um servidor. Pressupõe a conclusão, com êxito, do curso DKI 35 e, sugere a obtenção do Curso de Aperfeiçoamento em Segurança de Sistemas de Informação e Comunicação (INFOSEC), com o código AKS08, *a posteriori*.

Este curso é destinado ao mesmo público-alvo que o anterior, uma vez que vem no seguimento do primeiro, e tem a duração estimada de cinco dias úteis, cerca de 30 horas. Analisando os seus conteúdos programáticos (ver Anexo D) depreende-se que fornece as ferramentas práticas necessárias para administrar um servidor, o que vai de encontro à opinião geral dos inquiridos: a falta de componente prática para desempenhar funções.

Não obstante, por se tratarem de cursos técnicos, não são adequados à proposta que se pretende fazer, uma vez que, como já fora referido anteriormente, há unidades incumbidas de administrar formação técnica e há uma lista de cursos a frequentar antes de destacar quer para unidades navais, quer para a DITIC, onde constam estes dois cursos mencionados.

Para terminar a entrevista foi questionado mais especificamente, no que respeita à segurança dos sistemas de informação e redes de computadores o que importava abordar e não foi feito durante o percurso escolar na EN. As respostas foram, de certa forma, de encontro às da pergunta anterior, uma vez que sabendo a motivação da entrevista realizada, todos os inquiridos se focaram no tema geral.

Ainda assim, surgiu uma resposta que foi tida em conta para o presente trabalho, sendo ela a pertinência da consulta e conhecimento das Publicações de Comunicações da Armada (PCA).

O objetivo das PCA é "estabelecer os conceitos e as políticas associadas aos Sistemas de Informação e Comunicação da Marinha, bem como o estabelecimento dos

[30] *New Technology*. Nome da família de sistemas operativos do *Windows* até ao *Windows NT* 5.0 que passou a ter a designação comercial de *Windows* 2000.

requisitos mínimos de Sistemas de Informação e Comunicação a dotar os Órgãos, Comandos e Unidades da Marinha."[31]

A PCA 2 (B) é a Doutrina para os Sistemas de Informação e Comunicação Automatizados (SICA) na Marinha e tem como finalidade estabelecer o conceito, definir requisitos e adotar a estrutura organizacional para acompanhar a rápida evolução tecnológica dos SICA.

Os SICA são, portanto, um conjunto de equipamentos e respetivos procedimentos organizados com o propósito de armazenar, transferir e processar informação para apoiar o comando, controlo, comunicações e a gestão de uma organização. Mais concretamente os SICA da Marinha apoiam no cumprimento da missão de uma unidade da Marinha, uma vez que a capacidade de comando e controlo é sustentada pelos mesmos, contribuindo para disponibilizar, trocar e preservar a informação.

A PCA 3, designada por Política de Segurança para Interligação de Redes e Sistemas de Informação e Comunicação Automatizados, vem definir o risco de segurança como a "probabilidade da exploração das vulnerabilidades através das ameaças a uma rede ou SICA, afetando a informação aí residente"[32].

No processo de gestão do risco, "uma ameaça só tem significado se existir uma vulnerabilidade que pode ser explorada através de um ataque, e que uma vulnerabilidade só se torna efetiva se existir uma ameaça para a explorar"[33].

Na PCA 10 trata-se do Conceito de Implementação dos SICA no Domínio do Utilizador, onde é referido que ao nível de Administrador, o Gestor Operacional do Domínio do Utilizador (GODU) deverá ter conhecimento dos serviços básicos e funcionais disponibilizados, saber quais os requisitos funcionais a implementar e manter no seu Domínio da Unidade, conhecer os requisitos de segurança e das entidades exteriores ao Domínio da Unidade responsáveis pela sua gestão.

Por sua vez, o Administrador do Domínio do Utilizador (ADU) deve possuir "capacidades globais dos serviços básicos e funcionais disponibilizados, das arquiteturas lógica e física, dos requisitos de segurança e das entidades responsáveis pela sua gestão de modo a habilitá-lo a assessorar o GODU"[34]. "O ADU deverá possuir formação na área

[31] Fonte: PCA1 (Publicações de Comunicações da Armada), p. 1.1.
[32] Fonte: PCA3 (Política de Segurança para Interligação de Redes e Sistemas de Informação e Comunicação Automatizados), p. 2.1.
[33] Idem, p. 2.3.
[34] PCA 10 (Conceito de Implementação dos Sistemas de Informação e Comunicação Automatizados (SICA) no Domínio do Utilizador), pp. 4.3-4.4.

de administração de redes das plataformas e sistema operativo de rede e de utilizador que se encontrem instaladas"[35].

Segue-se o conceito de implementação dos Sistemas de Informação e Comunicação Automatizados, ao nível do Domínio da Rede na Marinha (PCA 12 (A)) que pretende harmonizar e controlar a configuração dos serviços e dos normativos de segurança a aplicar.

A PCA 15 vem abordar a Intranet e Internet na Marinha. A Intranet na Marinha sustenta o conjunto de tecnologias para recolha, disseminação, processamento, armazenamento e transmissão da informação que é tanto mais valiosa quanto a sua relevância, confiança e disponibilidade em tempo útil.

Quanto à Internet, este é um serviço que permite a interligação da Intranet da Marinha a redes externas, mas com isto aparece o problema ao nível das considerações de segurança da respetiva interligação, uma vez que os padrões de utilização e mesmo os próprios utilizadores são muito diferentes. Por questões de segurança o acesso à Internet só é permitido após a autenticação do utilizador, o que pressupõe a sua identificação e uma palavra-chave.

Por fim, a PCA 16, o Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha aborda a proteção dos SICA, fala da necessidade de "implementação e gestão de políticas de segurança adequadas, mas também de uma estrutura que seja capaz de monitorizar, identificar, alertar, responder e recuperar, na eventualidade de um SICA sofrer uma quebra de segurança relacionada com a confidencialidade, integridade, disponibilidade, autenticação e não-repúdio da informação"[36].

"Para este fim, é necessário implementar uma Capacidade de Resposta a Incidentes de Segurança da Informação (CRISI), que permitirá responder de forma concertada a incidentes de segurança da informação, relacionados com atividades de software malicioso, atividades maliciosas, negação de serviços, ou outras ameaças/ vulnerabilidade inerentes aos SICA. A CRISI recorre às valências dos vários setores, utilizando assim, de forma coordenada, as capacidades funcionais disponíveis necessárias"[37].

[35] Idem, pp. 4.4.
[36] PCA 16 (Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha), p. 1.1.
[37] Idem.

"Admitindo-se que mesmo a melhor infraestrutura de segurança da informação não consegue evitar eventuais intrusões ou outras ações maliciosas aos seus sistemas, importa que as organizações disponham de uma estrutura adequada, que de forma eficaz responda a um incidente de segurança da informação"[38].

Assim, sugere-se que seja considerada a integração da consulta e leitura das referidas publicações na disciplina Comunicações I, lecionada no primeiro semestre do 2ºano da Escola Naval, conforme Anexo G.

Sendo a Unidade Curricular de Comunicações I uma UC ministrada a todas as classes, é pertinente que todos os cadetes tenham oportunidade de consultar e analisar sumariamente o conteúdo das PCA. Uma vez que nesta UC é transmitida aos cadetes, entre outras competências, a de saber onde encontrar e como consultar determinada informação nas publicações existentes, fará sentido integrar, no conteúdo programático de Comunicações I, estas publicações, utilizadas como menos frequência mas de extrema importância, agora que a temática da cibersegurança tem vindo a obter mais relevância.

Em suma, com as entrevistas realizadas, foram tidas em conta diversas opiniões, todas elas importantes e com contributos vantajosos para o desenrolar do presente trabalho. Contudo, apesar de não se poderem considerar todas as necessidades sentidas e explicadas pelos inquiridos é possível, através do leque de opções sugerido, adaptar uma unidade curricular à maioria das temáticas de caráter académico apresentadas.

Quanto ao que não será possível incluir nas unidades curriculares propostas, e que permitirá aos Engenheiros Navais – ramo de Armas e Eletrónica chegar a bordo melhor preparados para as suas funções, deve ser frequentado em cursos profissionais lecionados na ETNA. Estes cursos devem fazer parte do pacote de formação necessária para o desempenho das funções a bordo das unidades navais.

3.3 Proposta Fundamentada

Tendo em conta a formação necessária e exequível, para os cadetes da Escola Naval, e as lacunas académicas reportadas por oficias da Marinha entrevistados, concluiu-se que seria proficiente propor duas unidades curriculares. Estas UCs devem ir de encontro às necessidades sentidas e estar de acordo com as conclusões tiradas.

[38] Idem, p. 2.1.

A primeira unidade curricular proposta é designada de Fundamentos de Cibersegurança. Esta UC deve ser destinada a todos os alunos que frequentem o 1º ano da Escola Naval. Trata-se de uma UC de caráter geral que visa esclarecer os conceitos básicos inerentes e despertar interesse para esta temática, assim como fazer compreender a necessidade e atualidade da cibersegurança.

Esta UC foi sugerida como uma cadeira semestral, composta por quatro horas semanais de aulas exclusivamente teóricas. Os conteúdos programáticos serão avaliados em dois testes escritos e, caso a média obtida não seja positiva, será realizado um exame final com toda a matéria lecionada.

O objetivo final é que os alunos do 1ºano fiquem com a noção da importância da cibersegurança e dos riscos que eles próprios correm ou podem fazer, por desconhecimento, a instituição correr. Ter uma noção das potencialidades do ciberespaço e dos problemas a que os utilizadores da internet estão sujeitos é o primeiro passo para criar uma cultura de boas práticas e segurança.

Como foi referido no subcapítulo 3.2 "Lacunas Académicas" sugere-se que no seguimento desta unidade curricular sejam abordadas as PCA na unidade curricular Comunicações I, lecionada no primeiro semestre do 2ºano da Escola Naval. A introdução das PCA na matéria lecionada visa complementar e cimentar os conhecimentos adquiridos em Fundamentos de Cibersegurança e, por conseguinte, não tornar esta mesma unidade curricular demasiado extensa.

Ainda assim, os oficiais EN-AEL entrevistados foram mais específicos nas necessidades sentidas quando lhes foram questionadas. Logo, tornou-se necessário propor uma segunda unidade curricular que viesse fornecer as competências mencionadas e que não fariam sentido lecionar a todos os alunos do 1ºano devido à sua especificidade e aprofundamento do tema.

A segunda unidade curricular proposta, Segurança da Informação e Cibersegurança, é destinada apenas aos alunos do 4ºano da Escola Naval, da classe de EN-AEL. É uma UC composta por aulas teórico-práticas, e também aulas meramente práticas, cujo objetivo é capacitar os alunos para compreender o funcionamento, desenhar e construir uma rede de computadores.

Trata-se de uma disciplina de cariz mais prático, que visa fornecer ferramentas mais aprofundadas sobre as matérias de telecomunicações e de redes de computadores, indo de encontro com as necessidades e interesses manifestados durante as entrevistas realizadas.

Assim, conforme Anexos E e F é possível observar os objetivos e unidades de aprendizagem idealizados para cada uma das unidades curriculares propostas, respetivamente, assim como a carga horária semanal, métodos de avaliação e bibliografia aconselhada.

Capítulo 4

Casos de Estudo

4.1 Oferta Formativa de Universidades e Institutos Superiores Nacionais

4.2 Oferta Formativa na Academia Militar

4 Capítulo 4: Casos de Estudo

4.1 Oferta Formativa de Universidades e Institutos Superiores Nacionais

No Instituto Superior de Estatística e Gestão de Informação, unidade orgânica da Universidade Nova de Lisboa faz parte do plano de curso da Licenciatura em Sistemas e Tecnologias de Informação a unidade curricular "Segurança Informática"[39]. O objetivo desta unidade curricular é compreender, aplicar e gerir a segurança informática em computação, comunicação e sistemas organizacionais. No final, os discentes deverão estar aptos a providenciar aos utilizadores uma infraestrutura de segurança suficientemente boa para que esta seja considerada uma vantagem na organização. Aspetos operacionais como políticas e procedimentos, mecanismos de ataque e defesa, análises de risco, recuperação e segurança da informação são abordados nesta unidade curricular.

Por sua vez, a Universidade de Aveiro dispõe de quatro unidades curriculares dentro da temática, sendo elas: Segurança[40], Segurança e Gestão de Risco[41], Segurança Informática e nas Organizações[42] e Segurança Avançada em Redes[43].

A primeira tem como objetivo geral apresentar e descrever os principais conceitos fundamentais da segurança em sistemas computacionais. Nesta cadeira é também feita uma introdução à criptografia e à criptanálise. A segurança é abordada em diversos contextos, como a segurança dos programas, dos sistemas operativos, das máquinas virtuais e das bases de dados.

A segunda tem como objetivos aprender a projetar e orientar o desenvolvimento de uma política de segurança na organização, aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação, e ainda aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, vulnerabilidades, ameaças e aplicar garantias e controlos adequados.

[39] Disponível em: http://www.unl.pt/guia/2013/isegi/UNLGI_getUC?uc=82036.
[40] Disponível em: http://www.ua.pt/deti/uc/2834.
[41] Disponível em: http://www.ua.pt/deti/uc/6489.
[42] Disponível em: http://www.ua.pt/uc/4143.
[43] Disponível em: http://www.ua.pt/deti/uc/6248.

A terceira unidade curricular pretende oferecer uma visão geral na temática da Segurança Informática, com ênfase particular para os problemas de segurança que se colocam ao nível das organizações. Esta unidade curricular abrange os aspetos base da segurança informática, a definição de políticas de segurança e a sua implantação usando diversos mecanismos de segurança. Aditivamente, aborda questões éticas, legais e sociais da segurança nas organizações.

Por fim, a quarta unidade curricular, Segurança Avançada em Redes, apresenta e descreve diversas vulnerabilidades de segurança dos sistemas computacionais em rede. As vulnerabilidades enquadram-se nos problemas que podem levantar se forem conhecidas e exploradas, nas soluções teóricas que atualmente se conhecem para eliminar as vulnerabilidades e nas soluções técnicas que atualmente se usam (sistemas operativos, protocolos de comunicação, interligação de redes, *security appliances*).

Esta unidade curricular é lecionada pelo Professor André Zúquete, autor do livro de referência "Segurança em Redes Informáticas", que faz parte da bibliografia recomendada para as propostas elaboradas na presente tese de mestrado.

Na Universidade do Minho, faz parte do plano de curso do Mestrado em Engenharia Informática uma unidade curricular intitulada Criptografia e Segurança de Sistemas de Informação[44]. Esta UC tem como alvo a segurança da informação e a confiabilidade dos sistemas informáticos. Pretende-se, entre diversos objetivos, que os formandos conheçam e dominem as diversas vertentes da administração de sistemas informáticos como forma de assegurar segurança e correção e também conheçam, selecionem e apliquem técnicas de desenvolvimento de aplicações seguras.

Na Faculdade de Ciências da Universidade do Porto é possível frequentar o Mestrado em Segurança Informática, que visa a formação avançada e de qualidade de profissionais e investigadores na área da cibersegurança. Este curso procura melhorar os conhecimentos técnicos e práticos de segurança informática dos licenciados que pretendam seguir rapidamente uma carreira profissional de sucesso na área e, simultaneamente, cimentar os conceitos teóricos daqueles que queiram prosseguir uma formação académica.

No Instituto Superior Técnico, a Segurança de Informação é uma área ativa de ensino, investigação e cooperação internacional em Matemática e Engenharia, nomeadamente ligadas ao Instituto de Telecomunicações (IT) e ao seu Grupo de

[44] Disponível em: http://mei.di.uminho.pt/?q=pt-pt/1213/cssi.

Segurança e Informação Quântica, e ao Instituto de Engenharia de Sistemas e Computadores (INESC).

Conjuntamente, a sua atividade revela-se em dezenas de artigos científicos anuais, projetos científicos e de cooperação nacional e internacional, e serviços de consultadoria a empresas e organismos do estado, incluindo o Gabinete Nacional de Segurança, bem como na formação avançada de especialistas materializada pelo programa de Doutoramento em Segurança da Informação do IST.

Existe uma unidade curricular, ministrada no Mestrado Integrado de Engenharia Eletrotécnica e de Computadores, Segurança Informática em Redes e Sistemas, cujo objetivo é fornecer um conjunto de conceitos, metodologias e ferramentas de segurança informática que permita abordar o tema face a um conjunto de tecnologias alargado, tais como: redes locais, redes pessoais, redes globais, desenvolvimento de *software*, sistemas operativos, sistemas distribuídos, bases de dados, e sistemas de ficheiros.

A UC começa por definir um conjunto de conceitos de segurança informática, para depois identificar os componentes críticos da arquitetura de segurança de uma organização. Por fim para cada um destes componentes são identificadas as suas vulnerabilidades, e descritas algumas metodologias e ferramentas para as eliminar.

Apesar de ser uma área relativamente recente e simultaneamente por ter um caráter marcadamente multidisciplinar, a oferta de formação superior nas universidades nacionais é ainda escassa, estando, no entanto, em progresso.

Contudo, é de salientar que apesar de nas Universidades e Institutos Superiores existir consciencialização para os problemas da cibersegurança, estes direcionam a sua oferta formativa apenas para quem vai trabalhar exclusivamente na área, alunos do mestrado ou licenciatura em engenharia informática ou tecnologia informática, o que não é aplicável à Escola Naval, que não está a formar engenheiros informáticos, porém pretende-se que os oficiais da Marinha tenham noções sobre cibersegurança.

Assim, por forma a acompanhar o progresso das Universidades e Institutos Superiores, no que respeita à cibersegurança, gerando conhecimento e criando respostas aos desafios colocados pelo ciberespaço e consequente impacto de ciberataques, faz sentido que a Escola Naval crie também medidas para transmitir conhecimento nesta área, isto é, cibereducar os cadetes da Escola Naval.

4.2 Oferta Formativa na Academia Militar

Na sequência da realização da presente tese de mestrado foi efetuada uma reunião com o Tenente-Coronel (TCOR) de Infantaria (Engenheiro Informático) José Carlos Lourenço Martins, professor regente da UC de Segurança da Informação, dos Sistemas de Informação e Ciberdefesa na Academia Militar (AM).

A unidade curricular de Segurança da Informação, dos Sistemas de Informação e Ciberdefesa (conforme Anexo H e Anexo I) está orientada de acordo com a visão da AM relativamente à cibersegurança. É uma UC que pretende atuar a nível organizacional, devido à sua relevância.

Segundo a visão da AM, o fator humano é preponderante para que possa existir uma cultura de segurança em qualquer organização, como se pode observar pela seguinte citação, utilizada pelo TCOR Lourenço Martins e da autoria de Tu e Yuan[45]: "*An Organization's information security strategy should comprehensively address the human factors such as security awareness and security training"*.

Assim, esta UC visa sensibilizar e treinar os utilizadores, neste caso os cadetes da AM para a segurança da informação. Conforme a visão de formação em cibersegurança da AM que se materializa numa disciplina académica, são realizados com frequência exercícios académicos (*Capture the Flag*[46]), em parceria com a Universidade do Minho e a UBINET[47]. Este tipo de exercício visa explorar vulnerabilidades dos sistemas de informação, por forma a treinar o aluno na aplicação de ferramentas de análise de sistemas e identificar os processos e mecanismos de solução. Permitem o ensino do chamado *Ethical Hacking.*

Sucintamente a UC está estruturada da seguinte forma: começa-se por fazer uma análise estratégica/gestão, isto é, conhecer a organização, conhecer o adversário, conhecer e ter noção das nossas capacidades, saber identificar e avaliar o risco, ou seja, saber priorizar de forma qualitativa e, por fim são abordadas as políticas de segurança. Posto isto é efetuado o primeiro teste escrito aos alunos.

[45] Disponível em: Tu, Zhiling and Yuan, Yufei (2014). *Critical Success Factors Analysis on Effective Information Security Management: A Literature Review*. Twentieth Americas Conference on Information Systems, Savannah.

[46] Competição que envolve diversas competências dos estudantes para a resolução de desafios relacionados com a segurança da informação, com o objetivo de capturar a bandeira que normalmente se trata de um código, e pontuar.

[47] Ver: http://ubinet.ipbeja.pt/.

Por fim, é feita uma análise gestão/operacional, que consiste na abordagem à dimensão física e ambiental, a dimensão humana, teoria de redes e internet, criptográfica aplicada, segurança dos computadores e estudo da legislação e ciência forense computacional, sendo depois realizado o segundo teste escrito e o exercício prático.

Já numa perspetiva operacional/técnica, existe ainda uma outra unidade curricular opcional, apenas para cadetes do Mestrado Integrado em Engenharia Eletrotécnica Militar, na especialidade de Transmissões, onde se aprende, de forma significativamente mais aprofundada, a recolher informação, planear ataques de engenharia social, ataques às redes, às aplicações, às bases de dados e às aplicações Web.

Do ponto de vista da AM, nas organizações precisamos de pessoas altamente preparadas, é necessário apostar em pessoas com competência e não somente na tecnologia.

Esta é a visão que mais se adequa à Escola Naval, um modelo de formação com conteúdos que possam ser usados por qualquer elemento da organização, um modelo de cibersegurança para todos.

Em suma, utilizando outra citação do TCOR Lourenço Martins e da autoria de Peltier, que resume a visão e o propósito da unidade curricular lecionada na AM: *"Social engineering is the hardest form of attack to defend against because ir cannot be defended with hardware and software alone. A successful defence will require an effective information security architecture, starting with policies and standards and following through with a vulnerability assessment process"*[48].

[48] Disponível em: Peltier, Thomas R. (2006). *Social Engineering: Concepts and Solutions*, The EDP Audit, Control, and Security Newsletter, Vol. XXXIII, Nº 8.

Capítulo 5

Conclusões

5.1 Análise do trabalho realizado

5.2 Recomendações e trabalho futuro

5 Capítulo 5: Conclusões

5.1 Análise do trabalho realizado

Este trabalho teve como objetivo enquadrar os temas da cibersegurança e do ciberespaço, e apresentar uma plataforma que permita identificar necessidades que levem à implementação do conceito de cibereducação a todos os utilizadores da Internet no geral, e aos cadetes da Escola Naval em particular.

Focada no fim último do presente trabalho, foi feito um levantamento da doutrina relacionada com o campo de estudo, uma análise do estado da arte.

Primeiro, foram definidos os conceitos considerados indispensáveis para a compreensão do trabalho. Seguiu-se uma análise das ações efetuadas pelos Estados-membros da União Europeia, começando pelos ciberataques que a Estónia e a Geórgia sofreram, em 2007 e 2008, respetivamente, e que vieram acentuar a necessidade de tomar medidas eficazes de resposta a este tipo de ataques, impulsionando o desenvolvimento de conhecimento na área.

A cibersegurança é um tema que tem vindo a merecer uma atenção crescente na União Europeia, na Organização do Tratado do Atlântico Norte, da qual também foram apresentadas as ações tomadas por três entidades, e em Portugal, pelo que foi descrita a evolução da preocupação a nível nacional, assim como a componente legal que foi acompanhando este progresso.

Para terminar, foi elaborado um quadro-resumo que permitiu comparar os objetivos de cada agência, organismo e escola analisado, concluindo que, apesar da evolução positiva que a formação na área da cibersegurança está a ter, esta não é adaptada à Marinha.

Por conseguinte, a pesquisa realizada tornou necessário efetuar entrevistas a oficiais da Marinha, para que estes pudessem, através da sua opinião pessoal, transmitir a necessidade e conveniência da Escola Naval investir também na cibereducação.

Assim, foram realizadas seis entrevistas que permitiram compreender a perceção de quem já está a desempenhar funções e se depara, diariamente, com questões de segurança da informação. Estas entrevistas, juntamente com a visão da Escola Naval sobre o que deve ser ensino nesta instituição, permitiram apresentar duas unidades

curriculares que estivessem de acordo com a exequibilidade e necessidade de formação e, simultaneamente, fossem ao encontro do que foi apontado como necessário pelos entrevistados.

Para não cingir as unidades curriculares propostas à opinião fundamentada dos entrevistados e à visão da Escola Naval sobre o ensino, foram apresentados casos de estudo.

Foi feito um levantamento do que existe em Universidades e Institutos Superiores de referência nacionais em matéria de cibersegurança, concluindo que a oferta se apresenta cada vez mais vasta, estando o Portugal a investir no conhecimento sobre cibersegurança.

Para terminar, foi apresentada a visão da AM sobre a necessidade de ensino nesta área, assim como foi feita uma descrição sucinta da unidade curricular lecionada na Academia Militar.

Em suma, a segurança da informação é da responsabilidade de todos os utilizadores de sistemas de comunicação em rede, que são tanto menos vulneráveis quanto maior o seu nível de cibereducação.

5.2 Recomendações e trabalho futuro

A Segurança da Informação não depende apenas da tecnologia disponível, mas essencialmente, a forma como os utilizadores empregam essa mesma tecnologia para gerir a informação. O conhecimento sobre o funcionamento da tecnologia e como a informação é processada permite reduzir os riscos e aumentar o nível de Segurança da Informação, ou seja, são necessárias ações de cibereducação que conduzam a uma cultura de segurança.

Em Portugal, têm-se observado uma crescente preocupação sobre a segurança da informação na Internet. Este facto pode ser verificado pelo número de seminários e conferências que tem sido realizados nos últimos anos. Porém, esta capacidade de atuação deve ser considerada com um complemento e atualização de conhecimento adquirido.

A base para se efetuar uma partilha de informação com segurança deve ter origem em matérias lecionadas durante o percurso académico de qualquer utilizador, adaptadas aos diferentes níveis de ensino. No ensino básico e secundário temos os adolescentes e jovens, grandes consumidores de novas tecnologias, que devem conhecer as vulnerabilidades dos sistemas que eles usam e como se podem proteger.

As ações de formação do nível utilizador e do nível lógico devem estar direcionadas para a realidade que eles têm dos sistemas de informação e para a perceção que têm de segurança. Deve ser aplicado o conceito de política de utilização aceitável, ensinando quais os limites que podem ser alcançados garantindo a segurança da informação que partilham.

Uma política de utilização aceitável para acesso a serviços em rede permite minimizar os riscos de segurança da informação. Deve ser do conhecimento de todos os utilizadores. Cada utilizador deve conhecer os procedimentos e mecanismos de segurança que estão associados à política de utilização aceitável e compreender as consequências que o desrespeito por estas regras podem trazer para cada um e para a organização.

No ensino superior temos homens e mulheres que estão a adquirir conhecimentos para ingressar no grupo da população ativa. São formados com competências necessárias para entrarem no mercado de trabalho, de acordo com a vocação de cada um. Matérias como a Gestão da Informação, a Segurança da Informação e a Gestão da Segurança da Informação devem fazer parte de todos os cursos do ensino superior, independentemente de os cursos não terem uma vertente tecnológica ou de gestão. Em alguma fase da atividade profissional, qualquer utilizador vai ter que usar sistemas de informação e ser responsável pela gestão de conteúdos.

A profundidade das matérias deve estar adaptada a cada curso, ou seja, não se pretende que um oficial da classe de Marinha substitua um oficial EN-AEL, ou vice-versa, mas o oficial EN-AEL tem que ter conhecimento aprofundado sobre a utilização dos sistemas de comunicação e da informação, e o oficial da classe de Marinha deve compreender os processos de armazenamento e processamento da informação em rede e a necessidade de manter a disponibilidade, integridade e confidencialidade da informação.

A Escola Naval deve investir nesta área, por forma a acompanhar o desenvolvimento das universidades nacionais que estão a formar pessoas qualificadas na área de cibersegurança.

Propõe-se que sejam integradas, nos planos de estudos dos cadetes da EN, unidades curriculares na área da cibersegurança, uma vez que a cibereducação é uma matéria que deve estar presente no percurso académico de qualquer pessoa e deve ser continuada com ações de atualização durante a vida profissional de cada um.

Bibliografia

ASSOCIAÇÃO IT4LEGAL, Página Oficial da […], 2013, http://www.it4legal.org/, consultado a 10/12/2015.

AUTORIDADE NACIONAL DE COMUNICAÇÕES, Página Oficial da […], 2016, http://www.anacom.pt/, consultado a 15/12/2015.

CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO, Página Oficial do […], 2016, http://www.cijic.org/, consultado a 10/12/2015.

CENTRO NACIONAL DE CIBERSEGURANÇA, Página Oficial do […], 2015, http://www.cncs.gov.pt/pagina-inicial/index.html, consultado a 06/11/2015.

COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, Página Oficial do […], 2016, https://ccdcoe.org/, consultado a 08/12/2015.

COUNCIIL OF EUROPE, Página Oficial do […], 2015, http://www.coe.int/en/web/portal/home, consultado a 08/12/2015.

CRAWFORD, Susan (1983), *The origin and development of a concept: the information society, Bull, Med. Libr. Assoc. 71(4) October*, pp. 380-385. Disponível em: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC227258/pdf/mlab00068-0030.pdf, consultado a 19/10/2015.

EFING, António Carlos e FREITAS, Cinthia Obladen de Almendra (2012), *Direito e Questões Tecnológicas Aplicados no Desenvolvimento Social (Vol.2),* 1ª ed., Curitiba, Juruá Editora.

EUR-LEX, Página Oficial do […], 2016, http://eur-lex.europa.eu/homepage.html, consultado a 10/12/2015.

EUROPEAN DEFENCE AGENCY, Página Oficial da […], 2015, http://www.eda.europa.eu/, consultado a 10/12/2015.

EUROPEAN POLICE OFFICE, Página Oficial da […], 2016, https://www.europol.europa.eu/, consultado a 10/12/2015.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, Página Oficial da […], 2016, https://www.enisa.europa.eu/, consultado a 16/12/2015.

ESTADO-MAIOR DA ARMADA (2002), *Publicações de Comunicações da Armada – PCA 1*, Lisboa.

ESTADO-MAIOR DA ARMADA (2004), *Doutrina para os Sistemas de Informação e Comunicação Automatizados (SICA) – PCA 2 (B)*, Lisboa.

ESTADO-MAIOR DA ARMADA (2004), *Política de Segurança para Interligação de Redes e Sistemas de Informação e Comunicação Automatizados – PCA 3*, Lisboa.

ESTADO-MAIOR DA ARMADA (2005), *Conceito de Implementação dos Sistemas de Informação e Comunicação Automatizados (SICA) no Domínio de Utilizador – PCA 10*, Lisboa.

ESTADO-MAIOR DA ARMADA (2008), *A Intranet e Internet na Marinha – PCA 15*, Lisboa.

ESTADO-MAIOR DA ARMADA (2012), *Conceito de Implementação dos Sistemas de Informação e Comunicação Automatizados (SICA) no Domínio da Rede – PCA 12 (A)*, Lisboa.

ESTADO-MAIOR DA ARMADA (2012), *Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha – PCA 16*, Lisboa.

FUNDAÇÃO PARA A COMPUTAÇÃO CIENTÍFICA NACIONAL, Página Oficial da […], 2016, https://www.fccn.pt/pt/, consultado a 19/11/2015.

GABINETE NACIONAL DE SEGURANÇA, Página Oficial do […], 2016, https://www.gns.gov.pt/, consultado a 06/11/2015.

GOBIERNO DE ESPAÑA *(2011), Estrategia Española de Seguridad: Una responsabilidad de todos*, Madrid.

INSTITUTO DA DEFESA NACIONAL (2012), "Cibersegurança", N.º133, Instituto da Defesa Nacional. Disponível em: http://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf.

INSTITUTO DA DEFESA NACIONAL (2013), "Estratégia da Informação e Segurança no Ciberespaço", Caderno N.º12, Instituto da Defesa Nacional. Disponível em: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

INSTITUTO SUPERIOR TÉCNICO, Página Oficial do […], 2016, http://tecnico.ulisboa.pt/pt/, consultado a 03/02/2016.

LYON, David (1992), *A Sociedade da Informação. Questões e Ilusões*, Oeiras, Celta Editora.

MARTINS, Marco (2012), "Ciberespaço: Uma nova realidade para a Segurança Nacional", Cibersegurança. Caderno N.º133 IDN, Lisboa, pp.32-49.

MULTINATIONAL CYBER DEFENCE EDUCATION & TRAINING, Página Oficial do […], 2016, http://www.mncdet-pt.net/, consultado a 24/11/2015.

NATO COMMUNICATIONS AND INFORMATION AGENCY, Página Oficial do […], 2014, https://www.ncia.nato.int/Pages/homepage.aspx, consultado a 11/11/2015.

NORTH ATLANTIC TREATY ORGANISATION, Página Oficial da […], 2016, http://www.nato.int/, consultado a 12/11/2015.

NUNES, Paulo Viegas (2012), "A Definição de uma Estratégia Nacional de Cibersegurança", Cibersegurança. Caderno N.º133 IDN, Lisboa, pp.113-126.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Página Oficial da […], 2016, http://www.oecd.org/, consultado a 24/11/2015.

PEREIRA, Júlio (2012), Cibersegurança – O Papel do Sistema de Informações da República Portuguesa, Lisboa, Diário de Bordo.

RALO, TCOR Jorge (2013), "Artigo de Opinião – CiberSegurança e CiberDefesa", Direção-Geral de Política de Defesa Nacional. Disponível em: http://dgpdn.blogspot.pt/2013/03/artigo-de-opiniao-ciberseguranca-e.html. Consultado a 09/11/2015.

SANTOS, Lino (2011), *Contributos para uma melhor governança da cibersegurança em Portugal*, Lisboa, Tese de Mestrado, Faculdade de Direito da Universidade Nova de Lisboa. Disponível em http://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF

SANTOS, Paulo e BESSA, Ricardo e PIMENTEL, Carlos (2008), *Cyberwar – O Fenómeno, as Tecnologias e os Atores*.

SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA RCTS, Página Oficial do […], 2016, http://www.cert.rcts.pt/, consultado a 06/11/2015.

UNIVERSIDADE DE AVEIRO, Página Oficial da […], 2016, http://www.ua.pt/, consultado a 30/06/2016.

UNIVERSIDADE DO PORTO, Página Oficial da […], 2015, https://sigarra.up.pt/up/pt/web_page.inicial, consultado a 30/06/2016.

UNIVERSIDADE NOVA DE LISBOA, Página Oficial da […], 2016, http://www.unl.pt/, consultado a 30/06/2016.

VEDOR, Luís (2012), "NATO celebra o maior contrato de Cibersegurança da sua história", Disponível em: http://www.pcguia.pt/2012/03/nato-celebra-o-maior-contrato-de-ciberseguranca-da-sua-historia/, consultado a 17/12/2015.

WOLTON, Dominique (1999), *E depois da Internet?*, Algés, Difel.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Decreto-Lei n.º 42806, Diário da República, I Série nº. 10/60, 14 de janeiro, p. 49.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 27º nº.1, *Constituição da República Portuguesa*, Título II, Capítulo I, 25 de abril de 1976, p. 8.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 273º nº.1, *Constituição da República Portuguesa*, Título X, Capítulo V, 25 de abril de 1976, p. 84.

REPÚBLICA PORTUGUESA, ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS, Artigo 28º, *Declaração Universal dos Direitos do Homem* de 10 de dezembro de 1948, Diário da República, I Série A nº. 57, de 9 de março de 1978, p. 491.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 1º, *Lei nº. 29/82 - Lei de Defesa Nacional e das Forças Armadas*, Diário da República, I Série nº. 285, Capítulo I, 11 de dezembro.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 5/90, Diário da República, I Série nº. 49, 28 de fevereiro, pp. 806 (2) - 806 (17).

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 1º, *Lei nº. 10/91 - Lei de Proteção de Dados Pessoais face à Informática*, Diário da República, I Série A n.º 98, Capítulo I, 29 de abril, p. 2366.

REPÚBLICA PORTUGUESA, MINISTÉRIO DA DEFESA NACIONAL, Decreto-Lei n.º 47/93, Diário da República, I Série A nº. 48, 26 de fevereiro, pp. 801 - 807.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 16/96, Diário da República, II Série nº. 69, 21 de março.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 124/2005, Diário da República, I Série B nº. 149, 4 de agosto, pp. 4502 - 4504.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 171/2005, Diário da República, I Série B nº. 211, 3 de novembro, pp. 6284 - 6285.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 39/2006, Diário da República, I Série B nº. 79, 21 de abril, pp. 2834 - 2866.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 1º nº.1, *Lei nº. 53/2008 - Lei de Segurança Interna*, Diário da República, I Série nº. 167, 29 de agosto, p. 6135.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Artigo 4º nº.1, *Lei nº. 53/2008 - Lei de Segurança Interna*, Diário da República, I Série nº. 167, 29 de agosto, p. 6135.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, *Lei nº. 109/2009 - Lei do Cibercrime*, Diário da República, I Série n.º 179, 15 de setembro, pp. 6319-6325.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA, Resolução da Assembleia da República n.º 88/2009, Diário da República, I Série nº. 179, 15 de setembro, pp. 6354 - 6378.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 46/2011, Diário da República, I Série nº. 218, 14 de novembro, p. 4848.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 12/2012, Diário da República, I Série nº. 27, 7 de fevereiro, pp. 596 - 605.

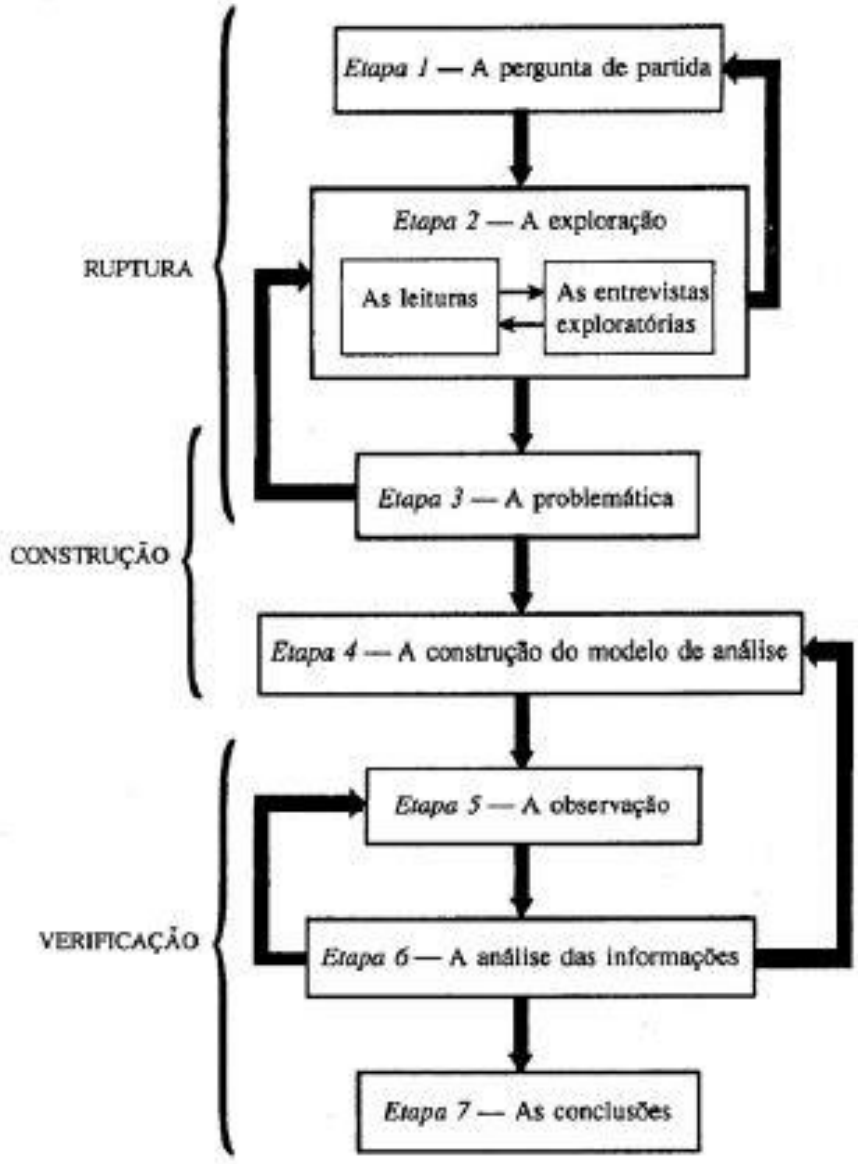
REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 42/2012, Diário da República, I Série nº. 74, 13 de abril, pp. 1925 - 1926.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Decreto-Lei n.º 69/2014, Diário da República, I Série nº. 89, 9 de maio, pp. 2712 - 2719.

REPÚBLICA PORTUGUESA, PRESIDENCIA DO CONSELHO DE MINISTROS, Resolução do Conselho de Ministros n.º 36/2015, Diário da República, I Série nº. 113, 12 de junho, pp. 3738 - 3742.

ANEXOS

Anexo A – Método de Investigação de Ciências Sociais e Humanas de Quivy e Campenhoudt



Anexo B – Guião de Entrevistas

No âmbito da realização da minha tese de mestrado, subordinada ao tema "Segurança da Informação no Ciberespaço – A Cibereducação no caminho da Cibersegurança" serão realizadas entrevistas a vários oficiais da classe de Engenharia Naval – ramo de Armas e Eletrónica.

O objetivo das entrevistas é perceber, através dos entrevistados, as lacunas existentes na formação académica ministrada na Escola Naval relativamente à segurança dos sistemas de informação e redes de computadores. Assim como, ficar com a noção dos conhecimentos necessários e que importam abordar para desempenhar funções a bordo e na DITIC, consoante o Engenheiro entrevistado.

Findas as entrevistas pressupõe-se que será possível propor uma unidade curricular, que comtemple os conteúdos programáticos sugeridos e essenciais para o bom desempenho de funções, uma proposta fundamentada nas necessidades sentidas por quem, atualmente, exerce funções.

Dados dos entrevistados:

1. CTEN EN-AEL Sobral Boavista, N.R.P Bartolomeu Dias (Anexo B1);
2. CTEN EN-AEL Martins Costa, N.R.P Álvares Cabral (Anexo B2);
3. 1TEN EN-AEL Catarina Neto Ribeiro, N.R.P Álvares Cabral (Anexo B3);
4. 1TEN EN-AEL Serrano dos Santos, N.R.P Bartolomeu Dias (Anexo B4);
5. 1TEN EN-AEL Gonçalves Capela, DITIC (Anexo B5);
6. 1TEN EN-AEL Roxo Felício, DITIC (Anexo B6).

Questões gerais:

1. O que considera conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções?
2. Que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico?
3. No que respeita a segurança dos sistemas de informação e redes de computadores, que temas importa abordar mais aprofundadamente para desempenhar funções a bordo?
4. Quem gere a informação do navio que está no portal da Marinha e Página de *Facebook* da Marinha Portuguesa?

Questões extraordinárias para os entrevistados que desempenham funções na DITIC:

5. Qual a função que desempenha na DITIC?
6. No seu percurso de EN teve disciplinas de redes?

Anexo B1 – Entrevista Engenheiro Sobral Boavista

O que consideram conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções?

Eng. Sobral Boavista: Na minha opinião seria essencial uniformizar, de certa forma, a formação ministrada aos oficiais, sargentos e praças, uma vez que, a bordo, temos de falar todos a mesma linguagem. Para desempenhar as funções a bordo convém perceber o que se pretende da rede de bordo e o que se pretende que cada pessoa execute. Com a MLU do navio, a rede de bordo vai ficar muito avançada e o conhecimento que temos sobre ela é *learning on job*, uma vez que quando andei na EN as cadeiras de redes que tive estavam a ser construídas e a matéria abordada não foi muito aprofundada.

Que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico?

Eng. Sobral Boavista: No que respeita à área das Telecomunicações acho que a formação da EN me deu apenas o básico, mas como já disse, na minha altura as cadeiras de redes e telecomunicações estavam nos seus primórdios. Como chefe de serviço é necessário aprofundar mais estas temáticas, posteriormente, como chefe de departamento a função é mais abrangente mas menos específica, fazemos uma gestão macro. Contudo, convém aprofundar mais as relações entre as camadas protocolares, com especial foco nas camadas 3, 4 e 7.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas importa abordar mais aprofundadamente para desempenhar funções a bordo?

Eng. Sobral Boavista: Interessa aprender o básico da gestão da rede. Seria importante aprofundar a formação base que há na EN, onde aprendemos os conceitos e os fundamentos e complementar essa formação com cursos complementares como os dados na ETNA, cursos práticos de aperfeiçoamento. Não cingir essa formação àqueles que, no futuro, serão os nossos subordinados, os executantes, para falarmos todos a mesma linguagem. Uma das minha incumbências é ser o GODU de bordo, e tenho pessoas dedicadas à rede informática, contudo a nossa formação prática é muito curta e seria de valor investir nesta área, para auxiliar os meus subordinados. É importante também perceber qual a função da DITIC e o que fazem por nós que estamos embarcados.

Quem gere a informação do navio que está no portal da Marinha e Página de *Facebook* da Marinha Portuguesa?

Ao navio apenas é pedido para facultar fotografias. Aqui fazemos uma seleção das que consideramos melhores, enviamos para o gabinete do CEMA e daí por diante, tudo o resto já não é da nossa responsabilidade.

Anexo B2 – Entrevista Engenheiro Martins Costa

O que consideram conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções?

Eng. Martins Costa: Acho que as cadeiras essenciais à saída da EN são aquelas que prepararam os Aspirantes para a vida a bordo, quer ligadas às incumbências da ponte, como navegação e comunicações, quer a parte da manutenção, como processar pedidos de reparação ou abate de material, a título de exemplo, ou também planeamentos trimestrais e estado do material certificado, a parte de gestão de material, que normalmente o primeiro contato que temos com isto é realmente quando vamos para o estágio de embarque no 5ºano.

Que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico?

Eng. Martins Costa: Na minha opinião seria importante oferecer aos aspirantes um estágio que desse a conhecer o funcionamento, interligação, as fases do processo e que permitisse lidar com as coordenações da Direção de Navios, Direção de Abastecimento, Arsenal do Alfeite e Esquadrilha de Superfície. Esta informação não é lecionada em nenhuma cadeira na EN, mas é uma função importante que temos de desempenhar, nomeadamente para o aprontamento de um navio e períodos de revisão intermédia, e seria interessante dar a conhecer este sistema aos Aspirantes antes do estágio de embarque.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas importa abordar mais aprofundadamente para desempenhar funções a bordo?

Eng. Martins Costa: Eu tirei um curso na ETNA, o MCSA, *Microsoft Certified Systems Administrator*, que me deu ferramentas práticas que não necessitei na sua totalidade para desempenhar funções de ADU, como Chefe de Serviço, e mais tarde como Chefe de Departamento. Para desempenhar funções a bordo é necessário um curso com informação útil para a execução de tarefas e não algo puramente teórico e demasiado complicado. O INFOSEC é também um bom curso mas, novamente, não é prático. Para desempenhar funções a bordo importa analisar as PCAs, que são a doutrina existente nesta área e saber quais são as boas práticas que se devem seguir, o que se deve verificar numa rede, como gerir a pública, o que o gestor da rede deve ter em atenção, essencialmente saber gerir da melhor forma o domínio do utilizador. Importa rever o normativo e o procedimento, pois

nem tudo o que está escrito está a ser implementado. Podemos estar a expor-nos, como é o exemplo das redes *wireless*. Quando fazemos o login de utilizador as nossas credenciais vão em claro, não vão encriptadas, logo é possível ter acesso às mesmas. No que respeita a segurança dos sistemas de informação e redes de computadores importa esclarecer concretamente o que se pode ou não fazer, aprender a administrar uma rede, aprender o básico da cibersegurança para desempenhar a função de administrador de uma rede de bordo.

Anexo B3 – Entrevista Engenheira Catarina Neto Ribeiro

O que consideram conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções?

Eng.ª Neto Ribeiro: Primeiramente, as cadeiras que necessitamos são as comuns a todas as classes, como comunicações, navegação e gestão da manutenção, que não existe como unidade curricular mas que seria vantajosa a sua introdução. Relativamente às cadeiras de departamento, não menos importante, as mais úteis terão sido Sistemas de Radar e Radioajudas, Antenas e Radiopropagação, Sistemas de Telecomunicações e Sistemas de Armas.

Que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico?

Engª Neto Ribeiro: Acho que seria útil ter uma introdução teórica ao que é, e em que consiste a gestão da manutenção. Assim como também seria interessante passar pela DITIC e conhecer o trabalho por eles desenvolvido. Talvez ter, posteriormente, uma formação mais especializada, como por exemplo um mestrado no IST também iria contribuir para um maior conhecimento e à vontade no desempenhar das funções.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas importa abordar mais aprofundadamente para desempenhar funções a bordo?

Engª Neto Ribeiro: Acho importante falar de rede de comunicações de dados e administração de servidores. A bordo das unidades navais o Chefe de Serviço de Armas e Eletrónica desempenha a função de ADU e sem abordar estes temas é difícil perceber o que está implementado a bordo. Explorar as camadas protocolares 3,4 e 7 do modelo OSI poderia ser útil na medida que nos fornecia mais ferramentas para compreender o funcionamento da rede de bordo.

Anexo B4 – Entrevista Engenheiro Serrano dos Santos

O que consideram conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções?

Eng. Serrano dos Santos: A minha função de bordo é ser o chefe de serviço de Armas, Eletrónica e Informática, sou o ADU (Administrador do Domínio da Unidade), funções que acumulo com a de OSDU (Oficial de Segurança do Domínio do Utilizador), ou seja, sou o responsável pela segurança da informação. Tenho dois subordinados que desempenham funções na secção de informática, a classe deles é indiferente, uma vez que para poder desempenhar essa função basta ter uma especialização em informática e é isso que é essencial a EN dar-nos. Aprofundar a teoria de redes e sistemas de telecomunicação e depois de termos bases sólidas complementar essa formação com a prática. Ter os cursos que os nossos subordinados também frequentaram para compreender na totalidade o que está a ser implementado, uma vez que quando vimos para bordo não temos base nenhuma do que é ser o ADU, ganhamos essas capacidades com a experiência.

Que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico?

Eng. Serrano dos Santos: Senti falta de aprofundar as cadeiras de redes e telecomunicações que tive na EN, cimentar melhor essa teoria. Contudo, também gostaria que, depois de analisar o plano de curso de cursos como DKI 35 e 36, proporcionados pela ETNA, fossem incorporados na EN alguns dos objetivos desses cursos, que são importantes tirar antes de destacar para um navio. Outra opção seria incluir esses cursos no plano de estágio dos aspirantes, para que quando fossem fazer o seu estágio de embarque já tivessem essas noções.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas importa abordar mais aprofundadamente para desempenhar funções a bordo?

Eng. Serrano dos Santos: Perceber a arquitetura e funcionamento de uma rede, aprofundar estes conhecimentos, mas sobretudo complementá-los com a prática inerente. Na realidade as nossas funções não implicam a execução, isso é tarefa para os nossos subordinados, mas implica a compreensão, e para tal a teoria não basta.

Anexo B5 – Entrevista Engenheiro Gonçalves Capela

Qual a função que desempenha na DITIC?

Eng. Gonçalves Capela: Na DITIC sou o Adjunto da Secção de Telecomunicações. Projeto, planeio e giro o sistema rádio em terra e apoio às unidades navais, o que engloba as comunicações VHF e MHF baseadas em terra e que servem unidades navais.

No seu percurso de EN teve disciplinas de redes?

Eng. Gonçalves Capela: Sim, as disciplinas que tive na EN sobre redes deram-me o conhecimento base. Contudo, posso dizer que posteriormente à EN tirei, voluntariamente, um Mestrado Integrado de Engenharia Eletrotécnica e de Computadores que me forneceu ferramentas mais aprofundadas e especializadas para as funções que fui desempenhando.

O que considera conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar primeiramente, funções a bordo e, atualmente, funções na DITIC?

Eng. Gonçalves Capela: Para desempenhar funções a bordo claramente as disciplinas como Sistemas de Radar e Radioajudas, Antenas e Radiopropagação e Sistemas de Telecomunicações são as mais úteis. Contudo, gestão da manutenção é um aspeto bastante importante e que não é lecionado na EN. Atualmente, na DITIC as minhas funções são mais técnicas e menos de liderança e, para isso é necessário uma unidade curricular mais abrangente, que nos forneça bases mais sólidas, como Segurança Informática em Redes e Sistemas, que tive no IST e que considero ter sido bastante útil.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico e importa abordar mais aprofundadamente?

Eng. Gonçalves Capela: O que aprendi no IST contribuiu muito para as funções que desempenho atualmente. Uma disciplina que tive no Mestrado Integrado de Engenharia Eletrotécnica e de Computadores, e que fazia sentido ter na EN foi Segurança Informática em Redes e Sistemas. Esta disciplina analisa os aspetos de segurança no modelo OSI, fala dos quatro níveis de segurança, faz uma análise da segurança em base de dados, da camada de transporte, análise VPN, tem um conteúdo programático interessante e útil. Outras sugestões seriam Sistemas de Telecomunicações de Fibra Ótica e Via Rádio, sendo esta segunda muito importante para as minhas funções na DITIC. Assim como Redes de Telecomunicações, uma cadeira que aprofunda os Sistemas de Telecomunicações, e explica o funcionamento de uma rede de telecomunicações de uma

rede muito grande e fala da Rede de Transporte PDH e SDH. Importaria também abordar, dentro das telecomunicações a componente militar, *networking* e radiodifusão.

Anexo B6 – Entrevista Engenheiro Roxo Felício

Qual a função que desempenha na DITIC?

Eng. Roxo Felício: Chefe de secção dos Sistemas de Gestão em Exploração. Como por exemplo o MMHS, cujo sistema sou administrador e POC.

No seu percurso de EN teve disciplinas de redes?

Eng. Roxo Felício: Sim, tive uma disciplina, Sistemas de Telecomunicações. Contudo, essa disciplina não nos dá conhecimentos práticos de como projetar, gerir e administrar uma rede, o domínio do utilizador.

O que considera conhecimentos necessários/disciplinas essenciais à saída da EN para desempenhar as suas funções na DITIC?

Eng. Roxo Felício: Na minha opinião, o plano de estágio dos Aspirantes deveria incluir cursos ministrados na ETNA como o DKI 35 e 36 (consultar planos de cursos na Intranet), pois há uma lacuna na parte da execução. Na EN temos disciplinas que trabalham as camadas, definimos as camadas mas não a sua aplicação. Falta-nos a parte prática, arrancar com servidores, pôr máquinas no domínio… Assim como, deveria também passar-se pela DITIC e ficar a conhecer as suas diversas áreas de trabalho. O que se constata é que quando surge um problema temos de ir investigar uma solução, pesquisamos, perguntamos ou foi informação que nos foi dada na passagem de serviço, porque componente prática não temos na EN, temos de adquirir com a experiência. Devia investir-se nesta componente.

No que respeita a segurança dos sistemas de informação e redes de computadores, que temas/disciplinas sentiu falta ou achou que a EN apenas lhe facultou o conhecimento básico e importa abordar mais aprofundadamente?

Eng. Roxo Felício: Importa abordar as publicações relacionadas com o tema. São elas a PCA 2,3, 15 e 16, ficar a conhecer as boas práticas, os princípios pelos quais nos regemos, pois isto está tudo definido também nas STANAG's da NATO. A CRISI está a desenvolver trabalho para que todos os utilizadores da rede de Marinha tenham boas práticas. Portanto, seria interessante analisar estas publicações e dá-las a conhecer, para que se aja de acordo com o que está estabelecido, pois pode haver fuga de informação por desconhecimento dos utilizadores. Assim como, é importante saber a que tipo de ataques estamos sujeitos para saber como evitar ou solucionar o problema que daí advém.

Anexo C – Objetivos Curso DKI 35

DOC V: PLANOS DE FORMACAO	**FL 1 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1. OBJECTIVOS ESPECÍFICOS 1.1 Caracterizar o "Windows 2000" e a sua ligação em rede • Sistema operativo Windows 2000. • Funções do sistema operativo; • Características do "Windows 2000"; • Versões do "Windows 2000"; • Introdução às redes. • Vantagens de estar ligado em rede; • Papeis dos Computadores numa Rede; • Tipos de redes; • Sistemas operativos de rede; • Implementação de uma rede com o "Windows 2000". • Caraterísticas de um domínio; • Vantagens de um domínio; • Organização de um domínio; • Características da *Active Directory;* • Vantagens da Active *Directory;* • Acesso ao Windows 2000 através de uma rede. 1.2 Reconhecer mecanismos de administração de redes no "Windows 2000": • O *Help* no "Windows 2000". • Caraterísticas de procura; • Lista de "Favoritos". • Tarefas administrativas. • Tarefas de rotina administrativas; • Programação de Tarefas Administrativas. • Ferramentas administrativas. • Painel controlo; • Propriedades do sistema; • Informação do sistema;	Expositivo Demonstrativo Videoprojector Computador Manual

• Visualização de eventos; • Gestão de tarefas do "Windows"; • Desempenho; • Impressoras; • Partilha de pastas; • Gestão do disco; • *Backup;* • Gestão de segurança; • Ferramentas de rede; • Ferramentas adicionais; • Consola de gestão da “Microsoft” (MMC).	

DOC V: PLANOS DE FORMACAO	**FL 2 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1.3 Reconhecer a segurança na rede do "Windows 2000" • Contas de utilizador. • Contas de utilizador local; • Contas de utilizador de um domínio. • Grupos. • Direitos do utilizador. • Direitos comuns dos utilizadores; • Direitos designados na construção de grupos. • Permissões. • Introdução às permissões; • Permissões em ficheiros NTFS; • Permissões em pastas NTFS; • Permissões em pastas partilhadas; • Permissões de uma impressora. 1.4 Caraterizar a Rede "Windows 2000" • O alcance da Rede. • Componentes básicos de conectividade. • Adaptadores de rede; • Cabos de rede; • Modo de comunicação *Wireless*. • Tipologias de rede. • Bus; • Star, • Ring; • Malha (*Mesh*); • Hibrido. • Tecnologias de rede. • *Ethernet*; • *Token Ring;* • Modo de transferência assíncrona (ATM); • Interface de distribuição de dados por fibra (FDDI); • *Frame Relay.* • Expansão da Rede. • Repeaters e Hubs; • *Bridges;* • *Switches;* • *Routers;*	Expositivo Demonstrativo Videoprojector Computador Manual

• *Gateways*; •Tipos de conectividade para acesso remoto. •Telefone de rede publico comutado (PSTN); • Serviços integrados de Rede Digital (ISDN); • X.25; • Subscritor de linha digital assimétrica (ADSL).	

DOC V: PLANOS DE FORMACAO	**FL 3 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1.5 Reconhecer os protocolos de Rede • Introdução aos protocolos. • Tipos de protocolos; • Interligação de sistemas de abertura (OSI) Modelo de referencia; • Camadas do protocolo. • Transmissões de dados e protocolos. • Protocolos "Roteáveis" e "não Roteáveis"; • Tipos de transmissões de dados. • Protocolos comuns. • Protocolo de Controlo de Transmissão/Protocolo de Internet (TCP/IP); • *Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX);* • *NetBIOS Enhanced User Interface (NetBEUI);* • *AppleTalk.* • Outros protocolos de Comunicação. • Modo de Transferência assíncrono (ATM); • Associa9ao de Dados por infravermelho (lrDA). • Protocolos de Acesso remota. • *Dial-up;* • VPN. 1.6 Caraterizar o protocolo TCP/IP • Introdução ao TCP/IP. • O Processo de Comunicação; • Camadas TCP/IP; • Identificação de Aplicações. • Conjunto de protocolo TCP/IP. • Protocolo de Controlo de transmissão (TCP); • *User Datagram Protocol* (UDP); • Protocolo de Internet (IP); • Protocolo de Controlo de Mensagem na Internet (ICMP); • Protocolo de gestão de grupos na Internet (IGMP); • Protocolo de resolução de endereços (ARP); • Utilidades TCP/IP.	Expositivo Demonstrativo Videoprojector Computador Manual

• Resolução do Nome. • Tipos de Nomes: • Mapeamento IP estático; • Mapeamento IP Dinâmico; • Resolução de nomes no Windows 2000. • Exame dos Dados no processo de transferência. • Terminologia de pacote; • Componentes de *Frame*; • *Data Flow.*	

DOC V: PLANOS DE FORMACAO	**FL 4 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
• Encaminhamento de dados. • Encaminhamento IP; • *Routers* de ligação na transferência de dados. 1.7 Explorar o endereço IP • Classificação do endereço IP. • Endereço IP; • Classes do endereço IP. • O *Subnetting* numa Rede. • *Subnets;* • Máscara "*Subnet*"; • Determinação de "Hosts" locais e remotos; • Planeamento do endereço IP. • Diretrizes no endereçamento; • Designação de IDs de rede; • Designação do Host 10. • Designação do endereço TCP/IP. • Endereçamento estático IP; • Endereçamento automático IP; • Verificação da configuração TCP/IP; • Verificação da configuração TCP/IP utilizando o *Ipconfig.* 1.8 Usar o conceito de otimização na atribuição do endereço IP • Classless *Inter-Domain Routing* (CIDR). • Limitações no endereçamento de Classes IP; • Definição de CIDR. • Endereço IP Binário. • Conversão para o formate binário; • Conversão para o formato binário usando uma calculadora. • Máscara de *Subnet* Binária. • Máscara de *Subnet* em Bits; • Notação CIDR; • Cálculo do *Network 10;* • Determinação dos *Hosts* locais e remotos. • Atribuição do endereço IP usando o CIDR. • ID disponíveis para *Hosts*; • Otimizar a atribuição de endereços IP.	Expositivo Demonstrativo Videoprojector Computador Manual

DOC V: PLANOS DE FORMACAO	**FL 5 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1.9 Examinar os serviços "Web" • Conceitos de "Internet". • A Internet; • Serviços de Internet; • Intranets; • Nomeação de um domínio; • Tecnologias de Cliente. • Leitores de notícias (Newsreaders); • Web Browsers; • Protocolos de Internet; • Uniform Resource Locator (URL). • Ligação à Internet. • Tradutores de endereço de Rede (NATs); • Servidores Proxy; • *Firewalls*; • Servidor Microsoft Proxy. • Conceitos de identificação de um servidor Web. • Definição de Servidor Web; • *Microsoft Internet Information Services (liS).*	Expositivo Demonstrativo Videoprojector Computador Manual

DOC V: PLANOS DE FORMACAO	**FL 6 DE 6 FLS**
CURSO: Adaptação Conceito de Redes de Comunicações de Dados	**CODIGO:** DKI35
MODULO: ADAPTAÇÃO REDES DE COMUNICAÇAO DE DADOS	**DURACAO:** 18 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito dos conceitos elementares das redes de comunicações de dados sobre TCP/IP.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
2. AVALIAÇÃO **2.1 Teste n° 1** 2.1.1 Natureza: Normativa 2.1.2 Tipo: Sumativa 2.1.3 Objetivos a avaliar: 1.1 (2 Val); 1.2 (2 Val); 1.3 (2 Val); 1.4 (2 Val); 1.5 (2 Val); 1.6 (3 Val); 1.7 (3 Val); 1.8 (2 Val); 1.9 (2 Val). 2.1.4 Instrumentos: • Teste escrito misto • Teste prático processo • Duração: 3 horas • 0 a 20 valores.	Expositivo Demonstrativo Videoprojector Computador Manual

Anexo D – Objetivos Curso DKI 36

DOC V: PLANOS DE FORMACAO	**FL 1 DE 4 FLS**
CURSO: Adaptação em Administração Windows Server 200x	**CODIGO:** DKI36
MODULO: ADAPTAÇÃO EM ADMINISTRAÇÃO WINDOWS SERVER 200X	**DURACAO:** 30 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito da Administração do Windows Server 200x. Aplicar conhecimentos de administração do Windows Server.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1. OBJECTIVOS ESPECÍFICOS 1.1 Instalar um *upgrade* ao Windows 200x • Preparação da Instalação • Instalação do *Windows 200x Professional* a partir de um CD; • Instalação do *Windows 200x Advanced Server* a partir de um CD; • Upgrade ao *Windows 200x Professional*; • Upgrade ao *Windows 200x Advanced Server*; • Erros de Instalação; 1.2 Configurar o ambiente Windows 200x • Configuração e gestão do *hardware*; • Opções de visualização; • Configuração do sistema; • Configuração do ambiente de trabalho. • Opções de "Internet" para clientes; 1.3 Ligar clientes do *Windows 200x* em Redes • Conectividade do *Windows 200x*; • Ligação a uma Rede *Microsoft*; • Ligação a uma Rede *NetWare Novell*; 1.4 Criar e gerir contas de utilizador • Introdução as contas de utilizador; • Criação de contas de utilizador locais; • Criação e configuração de contas de utilizador num domínio; • Propriedades de uma conta de utilizador num domínio; • Otimização dos perfis de utilizador com suas definições. 1.5 Gerir os recursos de acesso utilizando grupos • Introdução aos grupos no *Windows 200x*; • Implementação de grupos num *Workgroup*; • Implementação de grupos num domínio.	Expositivo Demonstrativo Ativo Videoprojector Computador Manual

DOC V: PLANOS DE FORMACAO	FL 2 DE 4 FLS
CURSO: Adaptação em Administração Windows Server 200x	**CODIGO:** DKI36
MODULO: ADAPTAÇÃO EM ADMINISTRAÇÃO WINDOWS SERVER 200X	**DURACAO:** 30 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito da Administração do Windows Server 200x. Aplicar conhecimentos de administração do Windows Server.	

OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	METODOS, MEIOS E REF.
1.6 Administrar dados utilizando NTFS • Introdução as permissões NTFS; • Permissões NTFS; • Permissões especiais NTFS; • "Comprimir" Dados numa Partição NTFS; • Configuração de espaços de Disco em Partições NTFS; • Segurança de dados usando EFS. 1.7 Aceder a Rede para providenciar recursos de ficheiros • Introdução as pastas partilhadas; • Criação de pastas partilhadas; • Combinação de NTFS com permissões em pasta partilhadas; • Pastas administrativas partilhadas; • Pasta partilhada numa *Active Directory;* • Configuração de pastas partilhadas utilizando OF's. 1.8 Otimizar as "performances" no *Windows 200x* • Registos de eventos; • Gestor de tarefas para controlar recursos do sistema; • Monitor de sistema para controlar o seu desempenho; • Alertas; • Otimização das "performances". 1.9 Implementar a segurança no *Windows 200x:* • Segurança nos Desktops e Serviços usando politicas de Segurança; • Auditorias de acesso para os recursos do sistema; • introdução às auditorias; • Seleção de auditorias de eventos; • Planeamento de politicas de auditoria; • Seleção de politicas de auditoria; • Auditorias para recursos de acesso. 1.10 Configurar uma impressora • Introdução a impressão no Windows 200x; • Adição de uma impressora; • Configuração de uma impressora de rede; • Configuração de uma impressora de Internet.	Expositivo Demonstrativo Ativo Videoprojector Computador Manual

DOC V: PLANOS DE FORMACAO	**FL 3 DE 4 FLS**
CURSO: Adaptação em Administração Windows Server 200x	**CODIGO:** DKI36
MODULO: ADAPTAÇÃO EM ADMINISTRAÇÃO WINDOWS SERVER 200X	**DURACAO:** 30 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito da Administração do Windows Server 200x. Aplicar conhecimentos de administração do Windows Server.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1.11 Configurar *Windows 200x* para acessos portáteis • *Hardware* para acessos portáteis; • Opções de Gestão de alimentação para acessos portáteis • Disponibilidade dos ficheiros para utilizadores *off-line;* • Ligação a Redes e Computadores; • Soluções para problemas de acessos portáteis; 1.12 Configurar Discos • Tipos de Disco no *Windows 200x;* • Partições e discos básicos; • Volumes num disco dinâmico; • Volumes num disco dinâmico; • Tarefas Comuns na Gestão de Discos. • Gestão de Discos. 1.13 Implementar proteção em casa de desastre • Introdução à proteção de dados; • Configuração de uma *Uninterruptible Power Supply* (UPS); • Implementação de tolerância a falhas utilizando RAID; • Recuperação e restauro de dados; • Ferramentas e recuperação de dados. 1.14 Instalar serviços terminais • Introdução aos serviços terminais; • Planeamento da instalação; • Instalação de serviços terminais; • Estabelecimento de uma sessão terminal; • Configurações numa sessão; • Instalação de aplicações num servidor terminal; 1.15 Implementar clientes no *Windows 200x* • Instalação do *Windows 200x*; • Instalação de rede manual; • Adequação das necessidades de instalações usando *Switches*; • Instalação do *Windows 200x* utilizando o *Setup Manager Wizard*; • Duplicação de discos; • Instalação do *Windows 200x* utilizando RIS; • O *troubleshooting* no *Windows 200x*;	Expositivo Demonstrativo Ativo Videoprojector Computador Manual

DOC V: PLANOS DE FORMACAO	**FL 4 DE 4 FLS**
CURSO: Adaptação em Administração Windows Server 200x	**CODIGO:** DKI36
MODULO: ADAPTAÇÃO EM ADMINISTRAÇÃO WINDOWS SERVER 200X	**DURACAO:** 30 HORAS
SUB-MODULO:	**DURACAO:**
OBJETIVO GERAL: Demonstrar conhecimentos no âmbito da Administração do Windows Server 200x. Aplicar conhecimentos de administração do Windows Server.	
OBJ. ESPECÍFICOS, CONTEUDOS e AVALIACAO	**METODOS, MEIOS E REF.**
1.16 Implementar um servidor baseado no *Windows 200x* • Rotinas comuns • *File Server;* • *Print Server;* • *Application Server;* • *Web Server;* • Tarefas de rotina de administração.	Expositivo Demonstrativo Ativo Videoprojector Computador Manual

Anexo E – Ficha Unidade Curricular "Fundamentos de Cibersegurança"

Ficha de Unidade Curricular / *Curricular Unit File*

Ciclo de Estudos / *Study Cycle*

Mestrado Integrado em Ciências Militares Navais, na especialidade de Marinha Mestrado Integrado em Ciências Militares Navais, na especialidade de Administração Naval Mestrado Integrado em Ciências Miliares, na especialidade de Fuzileiro Mestrado Integrado em Ciências Militares Navais, na especialidade Engenharia Naval, Ramo de Armas e Eletrónica Mestrado Integrado em Ciências Militares Navais, na especialidade Engenharia Naval, Ramo de Mecânica

Unidade curricular / *Curricular Unit* (100 caracteres)

Fundamentos de Cibersegurança / *Cybersecurity Principles*

Docente responsável e respetiva carga letiva na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais)

Responsible academic staff member and lecturing load in the curricular unit (fill in the fullname and state the number of lecturing hours per week) (1000 caracteres)

A definir/ To define (4h/semana; 4h/*week*)

Outros docentes e respetivas cargas letivas na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais) (1000 caracteres)

-

Other academic staff and lecturing load in the curricular unit (fill in the fullname and state the number of lecturing hours per week) (1000 characters)

-

Objetivos de aprendizagem (OA) (enumerar os conhecimentos, aptidões e competências a desenvolver pelos estudantes, relativos a cada capítulo do conteúdo programático) → verbos/ações (1000 caracteres)

OA1 Conhecer os conceitos de sistema, dados, informação, conhecimento, sistemas de informação, infraestruturas críticas, ciberespaço, cibersegurança e ciberdefesa. OA2 Compreender o conceito de Segurança da Informação (SI) e o seu significado relativamente à operação de organizações públicas e privadas.

OA3 Analisar uma descrição de exemplos de desafios que têm surgido e que ameaçam os direitos das organizações públicas e privadas.

OA4 Caraterizar os principais vetores de ataque de um adversário.

OA5 Identificar os tipos de ataques a uma rede.

OA6 Identificar as caraterísticas da gestão efetiva da Segurança da Informação.

OA7 Identificar as métricas para quantificar o nível de segurança.

OA8 Descrever exemplos de regras de comportamento.

OA9 Compreender aspetos de segurança relacionados com utilizadores em geral.

OA10 Compreender a ameaça interna associada a utilizadores com privilégios.

OA11 Identificar os diferentes mecanismos e procedimentos, automáticos e manuais, que podem ser implementados numa organização.

OA12 Ser capazes de compreender a segurança em redes de dados ao nível do utilizador e ao nível do administrador da rede.

Learning outcomes (LO) of the curricular unit (enumerate knowledge, skills and competencies to be developed by students for each chapter of the syllabus) → verbs/actions (1000 characters)

LO1 Understand the concepts of system, data, information, knowledge, information systems, critical infrastructure, cyberspace, cybersecurity and cyberdefense.

LO2 Understand the concept of Information Security (IS) and its significance in relation to the operation of public and private organizations.

LO3 Analyze some examples of challenges that have arisen and threaten the rights of public and private organizations.

LO4 Characterize the main vectors of an opponent attack.

LO5 Identify the types of attacks on a network.

LO6 Identify the characteristics of an effective management of information security.

LO7 Identify metrics to quantify the level of security.

LO8 Describe examples of behavioral rules.

LO9 Understand security aspects related to general users.

LO10 Understanding the internal threat associated to users with privileges.

LO11 Identify the different mechanisms and procedures, automatic and manual, which can be implemented in an organization.

LO12 Be able to understand security at the user level data networks and the network administrator level.

Conteúdos programáticos (1000 caracteres)

A unidade curricular está organizada em onze Unidades de Aprendizagem (UA):

UA1 Aspetos fundamentais.

UA2 Conceitos básicos de segurança – princípios e estratégia.

UA3 Mecanismos de segurança – vulnerabilidade da rede.

UA4 Gestão da Segurança da Informação.

UA5 Tipos de ataques a rede de dados

UA6 Segurança em redes.

UA7 Ferramentas de segurança.

UA8 Políticas de Segurança.

UA9 Supervisão do cumprimento da política de segurança.

UA10 Controlo de Acesso.

UA11 Análise de Riscos.

Syllabus (1000 *characters*)

The curricular unit is organized in eleven Learning Units (LU):

LU1 Fundamental aspects.

LU2 Basic security concepts – principles and strategy.

LU3 Security mechanisms – network vulnerability.

LU4 Management of information security.

LU5 Types of attacks to the data networks.

LU6 Security networks.

LU7 Security tools.

LU8 Security policy.

LU9 Compliance supervision of the security policy.

LU10 Access Control.

LU11 Risk Analysis.

Demonstração da coerência dos conteúdos programáticos com os objetivos da unidade curricular (1000 caracteres)

As unidades de aprendizagem (UA) abrangem os objetivos de aprendizagem (OA) da seguinte forma:

- OA 1 é abordado nas UA1 e 2.

- OA 2 é abordada na UA2.

- OA 3 é abordada nas UA3 e 4.

- OA 4 é abordada nas UA3 e 5.

- OA 5 é abordada na UA5.

- OA 6 é abordada nas UA6 e 7.

- OA 7 é abordada nas UA7, 8 e 9.

- OA 8 é abordada nas UA8.

- OA 9 é abordada nas UA8 e 9.

- OA 10 é abordada nas UA8, 9 e 10.

- OA 11 é abordada nas UA8 e 9.

- OA 12 é abordada nas UA10 e 11.

Demonstration of the syllabus coherence with the curricular unit's objectives (1000 characters)

The learning units (LU) cover the learning outcomes (LO) as follows:

- LO 1 is addressed in LU1 and 2.

- LO 2 is addressed in LU2.

- LO 3 is addressed in LU3 and 4.

- LO 4 is addressed in LU3 and 5.

- LO 5 is addressed in LU5.

- LO 6 is addressed in LU6 and 7.

- LO 7 is addressed in LU7, 8 and 9.

- LO 8 is addressed in LU8.

- LO 9 is addressed in LU8 and 9.

- LO 10 is addressed in LU8, 9 and 10.

- LO 11 is addressed in LU8 and 9.

- LO 12 is addressed in LU10 and 11.

Metodologias de ensino (avaliação incluída) (1000 caracteres)

A unidade curricular é composta, exclusivamente, por aulas teóricas. As sessões incluem a exposição de conceitos e metodologias, e apresentação de casos de estudo. Tem como finalidade dar a conhecer a problemática vigente do ciberespaço e sua utilização. O objetivo final passa pela consciencialização e implementação do conceito de cibereducação a todos os utilizadores da Internet, ou seja, fornece as ferramentas necessárias de cibersegurança que conduzem a uma cultura de segurança.

Avaliação:

1ª Época: avaliação contínua composta por dois testes.

2ª Época: exame final (100%).

Teaching methodologies (including evaluation) (1000 characters)

The curricular unit is based, exclusively, on theoretical lessons. The theoretical sessions include presentation of concepts and methodologies, and presentation of study cases. The intention is to inform the current cyberspace problematic and their use. The ultimate goal goes through awareness and implementation of the concept of cibereducation to all Internet users, and so it provides the necessary cybersecurity tools leading to a culture of security.

Evaluation:

1st round: continuous assessment consists of two tests.

2nd round: final exam (100%).

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular (3000 caracteres)

A avaliação é composta por duas componentes: dois testes ou exame final individual.

A apresentação teórica de conceitos e metodologias vai ser objeto de avaliação nos testes escritos. Cada teste individual permite avaliar os OA enumerados ao nível teórico, divididos de forma equitativa, sendo que cada teste escrito avaliará metade dos AO propostos e terá o mesmo peso para a nota final.

Demonstration of the coherence between the teaching methodologies and the learning outcomes (3000 characters)

The elements of consists in two components: individual tests or final exam.

The presentation of theoretical concepts and methodologies will be subject to evaluation in the written tests. Each individual test allows to evaluate the LO enumerated, divided equally, each written test will assess half the proposed LO and will have the same weight for the final grade.

Bibliografia principal (1000 caracteres)

Kim, David e Solomon, Michael (2012). Fundamentals of Information Systems Security, 2ª Edição, Jones & Bartlett Learning, ISBN: 978-128-403-162-1

Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008). Cyberwar, FCA, ISBN: 978-972-722-597-2

Schou, Corey e Hernandez, Steven (2014). Information Assurance Handbook, 1ª Edição, McGraw-Hill Education, ISBN: 978-007-182-165-0

Main Bibliography (1000 *characters*)

Kim, David e Solomon, Michael (2010). Fundamentals of Information Systems Security, 1ª Edição, Jones & Bartlett Learning, ISBN: 978-076-379-025-7

Santos, Paulo, Bessa, Ricardo e Pimentel, Carlos (2008). Cyberwar, FCA, ISBN: 978-972-722-597-2

Schou, Corey e Hernandez, Steven (2014). Information Assurance Handbook, 1ª Edição, McGraw-Hill Education, ISBN: 978-007-182-165-0

Anexo F – Ficha Unidade Curricular "Segurança da Informação e Cibersegurança"

Ficha de Unidade Curricular / *Curricular Unit File*

Ciclo de Estudos / *Study Cycle*

Mestrado Integrado em Ciências Militares Navais, na especialidade de Engenharia Naval, Ramo de Armas e Eletrónica

Unidade curricular / *Curricular Unit* (100 caracteres)

Segurança da Informação e Cibersegurança / *Information Security and Cybersecurity*

Docente responsável e respetiva carga letiva na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais)

Responsible academic staff member and lecturing load in the curricular unit (*fill in the fullname and state the number of lecturing hours per week*) (1000 caracteres)

A definir/ To define (4h/semana; 4h/*week*)

Outros docentes e respetivas cargas letivas na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais) (1000 caracteres)

-

Other academic staff and lecturing load in the curricular unit (fill in the fullname and state the number of lecturing hours per week) (1000 *characters*)

-

Objetivos de aprendizagem (OA) (enumerar os conhecimentos, aptidões e competências a desenvolver pelos estudantes, relativos a cada capítulo do conteúdo programático) → verbos/ações (1000 caracteres)

OA1 Caraterizar o papel da segurança da informação e dos sistemas de informação para a obtenção da superioridade de informação no ambiente competitivo das organizações. OA2 Identificar e compreender os serviços de segurança primários, conceitos tradicionais e princípios que estão na base das decisões da Segurança da Informação. OA3 Compreender as políticas e procedimentos, mecanismos de ataque e defesa, análise do risco, recuperação e segurança da informação. OA4 Compreender, aplicar e gerir a segurança informática em computação, comunicação e sistemas organizacionais. OA5 Saber explicar o funcionamento geral da Internet e de uma rede de computadores local. OA6 Compreender o funcionamento das camadas Física, Ligação de Dados, Rede e Transporte do modelo OSI.

OA7 Conhecer a arquitetura protocolar TCP/IP e a Internet.

OA8 Abordar as questões da segurança das comunicações e a transferência eletrónica de dados.

OA9 Descrever os conceitos básicos da computação em nuvem.

OA10 Conhecer o funcionamento de diversas ferramentas de segurança e de análise de dados.

OA11 Dotar os alunos de conhecimentos na área das arquiteturas de rede padrão. Os conceitos de execução de ações são aplicados na resolução de situações reais relacionadas com o desenvolvimento e operação de sistemas de comunicações.

OA12 Efetuar em ambiente de laboratório de informática, exercícios de aplicação dos conhecimentos teóricos abordados.

Learning outcomes (LO) of the curricular unit (enumerate knowledge, skills and competencies to be developed by students for each chapter of the syllabus) → verbs/actions (1000 *characters*)

LO1 Characterize the role of information security and information systems for the attainment of information superiority in the competitive environment of organizations.

LO2 Identify and understand the primary security services, traditional concepts and principles that underlie the decisions of Information Security.

LO3 Understand the policies and procedures, mechanisms of attack and defense, risk analysis, recovery and information security.

LO4 Understand, implement and manage computer security in computing, communication and organizational systems.

LO5 Understand the general functioning of the Internet and a local computer network.

LO6 Understand the functioning of the layers Physical, Data Link, Network and Transport of the OSI model.

LO7 Knowing the architecture protocol TCP/IP and the Internet.

LO8 Addressing the issues of security of communications and electronic data transfer.

LO9 Describe the basics of cloud computing.

LO10 Know the functioning of various security tools and data analysis.

LO11 Provide students with knowledge in the area of standard network architectures. The actions implementing concepts are applied to solving real situations related to the development and communications systems operation.

LO12 Place in computer lab environment, application exercises approached theoretical knowledge.

Conteúdos programáticos (1000 caracteres)

A unidade curricular está organizada em dez Unidades de Aprendizagem (UA):

UA1. Introdução às redes de computadores.

UA2. Modelo OSI e TCP/IP.

UA3. Normas de redes e tecnologias WLAN.

UA4. Instalação de uma Ethernet.

UA5. Instalação de uma rede wireless.

UA6. Configuração de um router.

UA7. Tolerância a falhas de segurança.

UA8. Detetar problemas na rede.

UA9. Firewalls.

UA10. Scans de rede.

Syllabus (1000 characters)

The curricular unit is organized in ten Learning Units (LU):

LU1. Introduction to computer networks.

LU2. OSI and TCP/IP.

LU3. Standards networks and WLAN technologies.

LU4. Installing an Ethernet.

LU5. Installing a wireless network.

LU6. Configuring a router.

LU7. Tolerance to security breaches.

LU8. Detect network problems.

LU9. Firewalls.

LU10. Network scans.

Demonstração da coerência dos conteúdos programáticos com os objetivos da unidade curricular (1000 caracteres)

As unidades de aprendizagem (UA) abrangem os objetivos de aprendizagem (OA) da seguinte forma:

- OA 1 é abordado nas UA1.

- OA 2 é abordada na UA1 e 2.

- OA 3 é abordada nas UA2.

- OA 4 é abordada nas UA2 e 3.

- OA 5 é abordada nas UA2,3, 4 e 5.

- OA 6 é abordada nas UA2.

- OA 7 é abordada nas UA2.

- OA 8 é abordada nas UA7 e 8.

- OA 9 é abordada nas UA5 e 6.

- OA 10 é abordada nas UA8, 9 e 10.

- OA 11 é abordada nas UA4, 5 e 6.

- OA 12 é abordada nas UA4, 5 e 6.

Demonstration of the syllabus coherence with the curricular unit's objectives *(*1000 *characters)*

The learning units (LU) cover the learning outcomes (LO) as follows:

- LO 1 is addressed in LU1.

- LO 2 is addressed in LU1 and 2.

- LO 3 is addressed in LU2.

- LO 4 is addressed in LU2 e 3.

- LO 5 is addressed in LU2, 3, 4 and 5.

- LO 6 is addressed in LU2.

- LO 7 is addressed in LU2.

- LO 8 is addressed in LU7 and 8.

- LO 9 is addressed in LU5 and 6.

- LO 10 is addressed in LU8, 9 and 10.

- LO 11 is addressed in LU4, 5 and 6.

- LO 12 is addressed in LU4, 5 and 6.

Metodologias de ensino (avaliação incluída) (1000 caracteres)

A unidade curricular baseia-se principalmente em aulas teórico-práticas, havendo também um conjunto acentuado de aulas práticas. As sessões teórico-práticas incluem a exposição de conceitos e metodologias, e apresentação de casos de estudo.

As sessões práticas estão orientadas para a instalação de serviços em rede, e resolução de exercícios relacionados com esta ação.

Desenvolvimento de um projeto de grupo, no qual é pedido a elaboração dos requisitos funcionais e respetivo de desenho de uma rede de computadores. O projeto é elaborado em grupo.

Avaliação:

1ª Época: avaliação continua composta por testes e trabalhos práticos (projeto).

2ª Época: exame final (100%).

Teaching methodologies (including evaluation) (1000 *characters*)

The curricular unit is based primarily on theoretical and practical lessons, and also on a strong set of practical lessons. The theoretical-practical sessions include presentation of concepts and methodologies, and presentation of study cases.

The practice sessions are geared towards installation of network services, and resolution of a set of exercises related with the installation task.

Development of a project, in which is required to specify the network functional requirements and design the layout of a computer network. The project is drawn by a group of students.

Evaluation:

1st round: continuous assessment consists of tests and practical work (project).

2nd round: final exam (100%).

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular (3000 caracteres)

A avaliação é composta por duas componentes: testes ou exame final individual e um projeto.

A apresentação teórica de conceitos e metodologias está diretamente relacionada com os temas abordados nas aulas práticas. Esta interação irá proporcionar aos alunos os conhecimentos e competências enumerados como objetivos de aprendizagem (OA). Cada teste individual permite avaliar os OA enumerados, tanto ao nível teórico, como prático.

O projeto final da cadeira é um trabalho de investigação, que visa avaliar a capacidade dos alunos em aplicar os conceitos estudados no desenho de uma de rede de computadores de uma organização, e especificação dos requisitos funcionais que permitam a construção dessa mesma rede. O projeto final da cadeira, caso necessário, é um trabalho de investigação, que visa avaliar a capacidade dos alunos em aplicar os conceitos estudados. Apenas será realizado se os alunos não obtenham média positiva nos dois testes escritos.

Demonstration of the coherence between the teaching methodologies and the learning outcomes (3000 *characters*)

The elements of consists in two components: individual tests or final exam and a project.

The presentation of theoretical concepts and methodologies are directly related to the topics covered in practical lessons. This interaction will provide the students with the knowledge and skills listed as learning objectives (LO). Each individual test allows to evaluate the LO enumerated, at both theoretical and practical.

The project is a research topic that aims to assess students' ability to apply the concepts studied to design a computer network for an organization, and specify the functional requirements to be implemented in that network. The final project, if necessary, is a research investigation in which is assessed the capability of applying the learned subjects. It is needed only if the students do not obtain positive marks in both evaluation tests.

Bibliografia principal (1000 caracteres)

Boavida, Fernando e Bernardes, Mário (2012). TCP/IP Teoria e Prática, FCA, ISBN: 978-972-722-745-7

Zúquete, André (2013). Segurança em Redes Informáticas, 4º Edição Aumentada, FCA, ISBN:978-972-722-767-9

McClure, Stuart, Scambray, Joel e Kurtz, George (2012). Hacking Exposed, 7ª Edição, McGraw-Hill Education, ISBN: 978-007-178-028-5

Terpstra, John *et al* (2004). Hardening Linux, 1ª Edição, McGraw-Hill Education, ISBN: 978-007-225-497-6

Gouveia, José e Magalhães, Alberto (2013). Redes de Computadores Curso Completo, 10ª Edição Atualizada e Aumentada, FCA, ISBN: 978-972-722-781-5

Main Bibliography (1000 *characters*)

Boavida, Fernando e Bernardes, Mário (2012). TCP/IP Teoria e Prática, FCA, ISBN: 978-972-722-745-7

Zúquete, André (2013). Segurança em Redes Informáticas, 4º Edição Aumentada, FCA, ISBN:978-972-722-767-9

McClure, Stuart, Scambray, Joel e Kurtz, George (2012). Hacking Exposed, 7ª Edição, McGraw-Hill Education, ISBN: 978-007-178-028-5

Terpstra, John *et al* (2004). Hardening Linux, 1ª Edição, McGraw-Hill Education, ISBN: 978-007-225-497-6

Gouveia, José e Magalhães, Alberto (2013). Redes de Computadores Curso Completo, 10ª Edição Atualizada e Aumentada, FCA, ISBN: 978-972-722-781-5

Anexo G – Proposta de Alteração da Unidade Curricular "Comunicações I"

Proposta de Alteração de Unidade Curricular / *Amendment to Unit File*

Ciclo de Estudos / *Study Cycle*

Mestrado Integrado em Ciências Militares Navais, na especialidade de Marinha Mestrado Integrado em Ciências Militares Navais, na especialidade de Administração Naval Mestrado Integrado em Ciências Miliares, na especialidade de Fuzileiro Mestrado Integrado em Ciências Militares Navais, na especialidade Engenharia Naval, Ramo de Armas e Eletrónica Mestrado Integrado em Ciências Militares Navais, na especialidade Engenharia Naval, Ramo de Mecânica

Unidade curricular / *Curricular Unit* (100 caracteres)

Comunicações I / *Communications I*

Docente responsável e respetiva carga letiva na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais)

Responsible academic staff member and lecturing load in the curricular unit (fill in the fullname and state the number of lecturing hours per week) (1000 caracteres)

Conforme definido/ As defined (4h/semana; 4h/*week*)

Outros docentes e respetivas cargas letivas na unidade curricular (preencher o nome completo e indicar o número de horas letivas semanais) (1000 caracteres)

-

Other academic staff and lecturing load in the curricular unit (fill in the fullname and state the number of lecturing hours per week) (1000 characters)

-

Objetivos de aprendizagem (OA) (enumerar os conhecimentos, aptidões e competências a desenvolver pelos estudantes, relativos a cada capítulo do conteúdo programático) → verbos/ações (1000 caracteres)

OA1 Conhecer os requisitos mínimos de Sistemas de Informação e Comunicação a dotar os Órgãos, Comandos e Unidades da Marinha. OA2 Consultar a doutrina vigente na Marinha para as Tecnologias de Informação e Comunicação (TIC). OA3 Compreender os conceitos, políticas e procedimentos no que respeita às TIC.

Learning outcomes (LO) of the curricular unit (enumerate knowledge, skills and competencies to be developed by students for each chapter of the syllabus) → verbs/actions (1000 characters)

LO1 Understand the minimum requirements to provide the Organs, Command and Navy Units related to Information and Communication Systems. LO2 Analyze the current doctrine in the Navy for Information Technologies (IT). LO3 Understand the concepts, policies and procedures with regard to IT.

Conteúdos programáticos (1000 caracteres)

Propõe-se acrescentar as seguintes Unidades de Aprendizagem (UA): UA1 Objetivos das Publicações de Comunicações da Armada (PCA). UA2 Análise do conteúdo das seguintes publicações: PCA 2 (B), PCA 3, PCA 10, PCA 12 (A), PCA 15 e PCA 16.

Syllabus (1000 *characters*)

It is proposed to add the following Learning Units (LU): LU1 Objectives of the Navy Communications Publications. LU2 Analysis of the content of the following publications: PCA 2 (B), PCA 3, PCA 10, PCA 12 (A), PCA 15 e PCA 16.

Demonstração da coerência dos conteúdos programáticos com os objetivos da unidade curricular (1000 caracteres)

As unidades de aprendizagem (UA) abrangem os objetivos de aprendizagem (OA) da seguinte forma: - OA 1 é abordado nas UA1. - OA 2 é abordada na UA2. - OA 3 é abordada nas UA2.

Demonstration of the syllabus coherence with the curricular unit's objectives (1000 characters)

The learning units (LU) cover the learning outcomes (LO) as follows: - LO 1 is addressed in LU1. - LO 2 is addressed in LU2. - LO 3 is addressed in LU2.

Metodologias de ensino (avaliação incluída) (1000 caracteres)

Conforme definido na ficha da unidade curricular.

Teaching methodologies (including evaluation) (1000 characters)

As defined in the curricular unit file.

Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular (3000 caracteres)

Conforme definido na ficha da unidade curricular.

Demonstration of the coherence between the teaching methodologies and the learning outcomes (3000 characters)

As defined in the curricular unit file.

Bibliografia principal (1000 caracteres)

Conforme definido na ficha da unidade curricular.

Main Bibliography (1000 *characters*)

As defined in the curricular unit file.

Anexo H – UC lecionada na AM

ACADEMIA MILITAR

Ficha de Unidade Curricular [FUC]

Aprovado em _____

O COMANDANTE

_____

1. Unidade curricular / *Curricular Unit*

Código	Unidade Curricular	Regime de Frequência	Ano curricular	Semestre:
E361	Segurança da Informação, dos Sistemas de Informação e Ciberdefesa	Presencial	2º e 3º	2º

Localização na estrutura da Academia Militar:	
Departamento:	**Secção de Unidade Curricular:**
Ciências e Tecnologias de Engenharia	Engenharia Eletrotécnica

Área Cientifica	Créditos (ECTS)	Tempos Semanais	T	TP	PL	TC	S	E	OT
E3	4	3		45					

2. Designação do(s) Ciclo(s) de Estudos em que se insere a Unidade Curricular

Ciclo de Estudos a que a UC pertence / Study cicle to which the curricular unit belongs

Mestrado Integrado em Ciências Militares, na especialidade de Infantaria
Mestrado Integrado em Ciências Militares, na especialidade de Artilharia
Mestrado Integrado em Ciências Militares, na especialidade de Cavalaria
Mestrado Integrado em Administração Militar
Mestrado Integrado em Ciências Militares, na especialidade de Segurança (GNR)
Mestrado Integrado em Administração da Guarda Nacional Republicana
Mestrado Integrado em Engenharia Militar
Mestrado Integrado em Engenharia Eletrotécnica Militar, na especialidade de Transmissões
Mestrado Integrado em Engenharia Eletrotécnica Militar, na especialidade de Material
Mestrado Integrado em Engenharia Mecânica Militar

3. Docente responsável e respetiva carga letiva na unidade curricular *(nome completo)*

Responsible academic staff member and lecturing load in the curricular unit (fullname)

Nome do docente	Categoria	Grau	Horas Contacto	Regime de Tempo (%)
José Carlos Lourenço Martins	TCor	Doutor	45	Não aplicável (EMFAR)

4. Outros docentes e respetivas cargas letivas na unidade curricular

Other academic staff and lecturing load in the curricular unit

Nome do docente	Categoria	Grau	Horas Contacto	Regime de Tempo (%)
---	---	---	---	---

5. Requisitos prévios

Considerações sobre precedências relativas a conhecimentos ou aptidões a adquirir previamente à lecionação da UC

Ter conhecimentos de informática na ótica do utilizador.

6. Objetivos de aprendizagem

Conhecimentos, aptidões e competências a desenvolver pelos estudantes

Pretende-se que a unidade curricular possibilite ao discente:

1. Saber explicar os conceitos de Sistema, Dados/Informação/Conhecimento, Sistemas de Informação, Guerra de Informação, Operações de Informação, *Competitive Intelligence*, Infraestruturas Criticas, Ciberespaço, Cibersegurança e Ciberdefesa.
2. Saber explicar o funcionamento geral da Internet e de uma rede de computadores local a uma organização.
3. Saber explicar os principais conceitos de Segurança da Informação, dos Sistemas de Informação e de Ciberdefesa (SegInfoSICD).
4. Identificar alguns dos principais problemas típicos de SegInfoSICD.
5. Saber explicar as principais abordagens de SegInfoSICD ao nível organizacional.
6. Identificar as principais dimensões, categorias e controlos de SegInfoSICD.
7. Saber como fazer ao nível organizacional para resolver problemas de SegInfoSICD.
8. Saber como modelar cenários de incidentes de SegInfoSICD.
9. Saber explicar alguns dos principais métodos de ataque físicos e de engenharia social.
10. Saber explicar alguns dos principais métodos de ataque à infraestrutura tecnológica de uma organização.
11. Saber explicar as principais metodologias para realizar testes de penetração, no âmbito de uma auditoria.
12. Saber como realizar uma identificação e avaliação de riscos de SegInfoSICD.
13. Saber como realizar a construção de políticas de SegInfoSICD.
14. Saber como realizar um plano de auditorias de SegInfoSICD.
15. Saber como realizar um plano de SegInfoSICD.
16. Saber explicar os principais conceitos de criptografia e de estenografia.
17. Executar corretamente algumas das principais medidas de SegInfoSICD na ótica do utilizador.

Procura-se dar ênfase às seguintes competências gerais:
Tecnologias de Informação e Comunicação.
Análise e Conceção de Sistemas.
Raciocínio Analítico.

7. Conteúdos programáticos

Os conteúdos programáticos da unidade curricular estão definidos no Anexo à Ficha da Unidade Curricular.

8. Demonstração da coerência dos conteúdos programáticos com os objetivos da UC

Demonstration of the coherence between the syllabus and the curricular unit's objectives

Objetivos da UC	*Conteúdos Programáticos*
Objetivo 1	Sessão 1
Objetivo 2	Sessão 10
Objetivo 3	Sessão 4
Objetivo 4	Sessão 3, 4, 8, 9 e 10
Objetivo 5	Sessão 2
Objetivo 6	Sessão 3
Objetivo 7	Sessão 3, 4, 8, 9 e 10
Objetivo 8	Sessão 4
Objetivo 9	Sessão 8, 9
Objetivo 10	Sessão 10
Objetivo 11	Sessão 14 e 15
Objetivo 12	Sessão 5 e 7
Objetivo 13	Sessão 6
Objetivo 14	Sessão 6
Objetivo 15	Sessão 6
Objetivo 16	Sessão 11 e 12
Objetivo 17	Sessão 13

9. Metodologia de ensino:

Teaching methodologies

a. O ensino tem uma orientação essencialmente prática, com o recurso sempre que pertinente ao estudo de casos concretos e em cuja discussão será solicitada a participação dos discentes.

b. Exposição teórica complementada com a realização de trabalhos práticos, sempre que possível em laboratório.

c. O ensino baseia – se fundamentalmente nos seguintes aspetos:

O método pedagógico utilizado é o afirmativo/expositivo e demonstrativo.

As técnicas pedagógicas utilizadas são a demonstração, os casos de estudo, a discussão de grupos e a simulação.

As aulas serão teóricas – práticas com a duração de três horas.

10. Métodos de Avaliação

Evaluation methodologies

a. A avaliação é composta por uma componente prática, constituída por quatro trabalhos de investigação aplicada de reduzida dimensão e por uma componente teórica constituída pela realização de duas provas de avaliação ou um exame final.

b.O peso na nota final de cada uma das componentes é definido no início de cada semestre de funcionamento da Unidade Curricular, sendo no mínimo de 30% a avaliação da componente prática.

11. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

Demonstration of the coherence between the teaching methodologies and the curricular unit's objectives

Utilizam-se métodos expositivos para desenvolver assuntos teóricos oralmente. No caso da implementação de tecnologias de segurança, utilizam-se métodos demonstrativos. Em ambos os métodos utilizam-se perguntas de controlo para auxiliar o discente a descobrir a solução e a mais facilmente memorizar uma possível solução para o problema. As técnicas mais utilizadas são a discussão de grupo (e.g., escolher os melhores controlos de segurança a implementar para mitigar um risco), a simulação (e.g., identificar cenários de incidentes de segurança da informação) e por fim a análise de Estudo de Casos (e.g., ciberataques à Estónia em 2007).

12. Língua de ensino

Português na apresentação da matéria e Inglês para a bibliografia de suporte.

13. Bibliografia principal

Main bibliography

Andress, J., & Winterfeld, S. (2011). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Boston: Syngress Media Inc.

Bosworth, S., Kabay, M. E. & Whyne, E. (2009). *Computer security handbook* (5th ed.), (vol. I, II). New Jersey: Wiley.

Carr, J. (2012). *Inside cyber warfare* (2nd ed.). Sebastopol: O´Reilly.

Correia, M. P. & Sousa, P. J. (2010). *Segurança no software*. Lisboa: FCA / Lidel. Dhillon, G. (2007). *Principles of information systems security*. New Jersey: Wiley.

Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures*. London: Gower Publishing Company.

Pfleeger, C. P. & Pfleeger, S. L. (2007). *Security in computing* (4th ed.). New Jersey: Prentice Hall.

Stallings, W. (2011). *Cryptography and network security: Principles and practice* (5th ed.). New Jersey: Prentice Hall.

Waltz, E. (1998). *Information warfare: Principles and operations*. Boston: Artech House

Academia Militar, ___/ ___/ 201_

Responsável pela UC

_____

_____

Anexo I – Cronograma de Planeamento da Lecionação da UC da AM

ACADEMIA MILITAR

Cronograma de Planeamento da Lecionação

2013 / 2014

Aprovado em _____

O COMANDANTE

_____

_____

Distribuição de horas totais de trabalho em semanas por conteúdos programáticos e por métodos pedagógicos

Curso:	Mestrado Integrado em Ciências Militares, na especialidade de Infantaria Mestrado Integrado em Ciências Militares, na especialidade de Artilharia Mestrado Integrado em Ciências Militares, na especialidade de Cavalaria Mestrado Integrado em Administração Militar Mestrado Integrado em Ciências Militares, na especialidade de Segurança (GNR) Mestrado Integrado em Administração da Guarda Nacional Republicana Mestrado Integrado em Engenharia Militar Mestrado Integrado em Engenharia Eletrotécnica Militar, na especialidade de Transmissões Mestrado Integrado em Engenharia Eletrotécnica Militar, na especialidade de Material Mestrado Integrado em Engenharia Mecânica Militar
Unidade Curricular:	*E361 – Segurança da Informação, dos Sistemas de Informação e Ciberdefesa*
Ano Curricular:	*2º e 3º*
Semestre:	*2º*

Sessão nº 01 – 1ª Semana

Dia:	Local/Sala:	Duração:	Sumário (conteúdo programático):	Método Pedagógico:
		3 Horas	Explicar os conceitos de Sistema, Dados/Informação/Conhecimento, Sistemas de Informação, Guerra de Informação, Operações de Informação, Competitive Intelligence, Infraestruturas Criticas, Ciberespaço, Cibersegurança e Ciberdefesa. Identificar as propriedades fundamentais da segurança da informação. Analisar o impacto da evolução das tecnologias nas organizações (e.g., na organização militar). Trabalho prático Nº1: análise do ciberataque à Estónia em 2007.	Método Afirmativo / Expositivo & Estudo de Casos

Sessão nº 02 – 2ª Semana

Dia:	Local/Sala:	Duração:	Sumário (conteúdo programático):	Método Pedagógico:
		3 Horas	Explicar as principais abordagens da segurança da informação, dos Sistemas de Informação e da ciberdefesa ao nível organizacional. Analisar algumas das principais políticas internacionais de cibersegurança e ciberdefesa.	Método Afirmativo / Expositivo & Estudo de Casos

Sessão nº 03 – 3ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Identificar alguns dos principais problemas típicos de segurança da informação, dos Sistemas de Informação e da ciberdefesa. Identificar as principais dimensões, categorias e controlos da segurança da informação, dos Sistemas de Informação e da ciberdefesa. Análise sumária da ISO / IEC 27001, das normas de segurança da NATO e do Exército Português.	Método Afirmativo / Expositivo

Sessão nº 04 – 4ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Explicar os principais conceitos de segurança da informação, dos Sistemas de Informação e de Ciberdefesa (e.g., atacante, ameaça, vulnerabilidades). Analisar uma taxonomia de incidentes de segurança de computadores. Analisar uma ontologia de segurança da informação. Explicar a modelação de métodos de ataque, através das técnicas de árvores de ataque, do diagrama de fluxos de dados e da análise morfológica geral. Caraterizar os principais vetores de ataque de um possível adversário.	Método Afirmativo / Expositivo, demonstrativo e simulação & Estudo de Casos

Sessão nº 05 – 5ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Identificar e analisar algumas das principais normas e métodos de gestão do risco de segurança da informação e de SI (e.g., ISO 27001, OCTAVE). Identificar e analisar métodos de cálculo do risco de segurança da informação (e.g., método da Microsoft). Trabalho Nº2: Identificar e avaliar riscos de segurança da informação e de SI.	Método Afirmativo / Expositivo e demonstrativo

Sessão nº 06 – 6ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Explicar como construir uma política de segurança da informação e de Sistemas de Informação. Explicar como realizar um plano de Segurança da informação, dos Sistemas de Informação e da ciberdefesa. Explicar como planear e realizar um plano de auditorias relacionado com a Segurança da informação, dos Sistemas de Informação e da ciberdefesa.	Método Afirmativo / Expositivo e demonstrativo & Estudo de Casos

Sessão nº 07 – 7ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Realização da prova teórica Nº 1. Discussão dos trabalhos Nº 1 e 2.	Técnica Pedagógica: Discussão de Grupo

Sessão nº 08 – 8ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Resolver problemas de segurança da informação, dos Sistemas de Informação e de ciberdefesa ao nível da dimensão de segurança física de uma organização. Explicar alguns dos principais métodos de ataque físicos a uma organização. Identificar as principais categorias e controlos da segurança da informação, dos Sistemas de Informação e da ciberdefesa ao nível da dimensão de segurança física de uma organização. **Trabalho Nº 3:** Identificar e caracterizar métodos de ataque e principais controlos de segurança a aplicar para mitigar o risco ao nível das diversas dimensões de segurança de uma organização.	Método Afirmativo / Expositivo & Estudo de Casos

Sessão nº 09 – 9ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Resolver problemas de segurança da informação, dos Sistemas de Informação e de ciberdefesa ao nível da dimensão de segurança humana de uma organização. Explicar alguns dos principais métodos de ataque de engenharia social a uma organização. Identificar as principais categorias e controlos da segurança da informação, dos Sistemas de Informação e da ciberdefesa ao nível da dimensão de segurança humana de uma organização. Analisar sumariamente as principais técnicas militares de *Intelligence*.	Método Afirmativo / Expositivo & Estudo de Casos

Sessão nº 10 – 10ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Explicar o funcionamento geral da Internet e de uma rede de computadores local a uma organização. Resolver problemas de segurança da informação, dos Sistemas de Informação e de ciberdefesa ao nível da dimensão de segurança da infraestrutura tecnológica de uma organização. Explicar os principais métodos de ataque tecnológicos a uma organização. Identificar as principais categorias e controlos da segurança da informação, dos Sistemas de Informação e da ciberdefesa ao nível da dimensão de segurança da infraestrutura tecnológica de uma organização.	Método Afirmativo / Expositivo & Estudo de Casos

Sessão nº 11 – 11ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Explicar os principais conceitos de criptografia. Enunciar os princípios gerais de funcionamento dos principais algoritmos simétricos e assimétricos de encriptação, da autenticação de uma mensagem pela utilização de funções de *hash* (e.g., MD5, SHA-1) e das assinaturas digitais (e.g., certificados X.509). Explicar os princípios gerais de funcionamento da estenografia.	Método Afirmativo / Expositivo e demonstrativo

Sessão nº 12 – 12ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	**Realização do trabalho Nº3:** criptografia e estenografia aplicada.	Método Afirmativo / Expositivo e demonstrativo

Sessão nº 13 – 13ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Implementar alguns dos principais procedimentos e tecnologias de segurança da informação, dos Sistemas de Informação e de ciberdefesa na ótica do utilizador (e.g., antivírus, firewall, anti-spam, backups, atualizações de software, segurança do browser, gestão de logs, segurança do sistema operativo e identificação/autenticação/ autorização).	Método Afirmativo / Expositivo e demonstrativo

Sessão nº 14 – 14ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Explicar as principais metodologias para realizar testes de penetração, no âmbito de uma auditoria. **Trabalho Nº4:** utilizar técnicas de recolha de informação na Internet.	Método Afirmativo / Expositivo e demonstrativo

Sessão nº 15 – 15ª Semana				
Dia:	**Local/Sala:**	**Duração:**	**Sumário (conteúdo programático):**	**Método Pedagógico:**
		3 Horas	Realização da prova teórica Nº 2. Discussão dos trabalhos Nº 3 e 4.	Técnica Pedagógica: Discussão de Grupo

Academia Militar, __de _____ de 201_

Responsável pela UC

_____

_____