Pós-Graduação em
Cibersegurança e Ciberdefesa
2ª Edição

Local: Academia Militar (Lisboa) e Universidade do Minho (Guimarães) Iniciativa:

1. ENQUADRAMENTO GERAL

A rápida evolução tecnológica e a crescente utilização da Internet constituem hoje um fator essencial de geração de riqueza e inclusão social, desempenhando um papel determinante não só no desenvolvimento e bem-estar das modernas sociedades mas também na sua Segurança.

A juntar aos tradicionais cenários de conflito e domínios operacionais (Terra, Mar, Ar e Espaço), onde se materializam os riscos e as ameaças à Segurança e Defesa Nacional, surgiu recentemente um novo *Global Common* criado pelo Homem: o Ciberespaço.

A exploração segura e eficiente deste espaço aberto de interação global requer o desenvolvimento de novas estratégias, doutrinas e capacidades, constituindo por essa razão uma preocupação crescente para todas as Organizações, Governos, Forças Armadas e Forças de Segurança.

Materializando o Ciberespaço um novo ambiente operacional de carácter potencialmente assimétrico, onde se torna necessário desenvolver e mobilizar novas competências, este Mestrado procura dar resposta à procura crescente de formação especializada em Cibersegurança e Ciberdefesa, registada tanto no contexto nacional como internacional.

2. OBJETIVOS

Esta Pós-Graduação orienta-se para as necessidades de formação avançada de quadros superiores e de profissionais, militares e civis, responsáveis pela gestão de processos e pela coordenação de iniciativas no domínio da Cibersegurança e Ciberdefesa, tendo por objetivos:

- Criar e desenvolver competências avançadas na área da segurança e defesa do ciberespaço, no contexto das atividades civis e militares, para fazer face aos diversos tipos de ataques cibernéticos e atividades maliciosas.
- Fomentar a reflexão sobre o binómio proteção - defesa, tendo em conta tanto os requisitos de prevenção, recuperação, mitigação de ciberataques e a adoção de operações de defesa ativa, tanto no plano nacional como internacional.
- Identificar e analisar ferramentas para avaliação de vulnerabilidades, código malicioso, ameaças e riscos cibernéticos, de forma a permitir a gestão dinâmica do risco.
- Analisar metodologias destinadas a garantir uma adequada consciência da situação, a tomada de decisão em tempo oportuno e uma eficiente gestão de crises no ciberespaço.
- Atendendo ao processo de edificação das capacidades de Cibersegurança e Ciberdefesa, às responsabilidades e domínios de atuação dos diversos atores tanto no plano nacional como internacional, contribuir para uma visão integradora e sinérgica dos esforços a desenvolver;
- Promover a reflexão e contribuir para o desenvolvimento de uma cultura estratégica de Cibersegurança e Ciberdefesa.

3. ESTRUTURA DO PROGRAMA

Procurando dar resposta aos principais desafios que as ameaças emergentes no ciberespaço colocam hoje aos indivíduos, às organizações e ao pleno exercício da soberania dos Estados, este programa de formação pós-graduada foi desenvolvido de forma a cobrir as lacunas existentes tanto no domínio operacional da cibersegurança, da ciberdefesa e da gestão de crises no ciberespaço, como no enquadramento legal das atividades conduzidas no seu âmbito.

O plano curricular e as atividades a desenvolver no seu âmbito foram articulados de forma a explorar a complementaridade e articulação coerente dos conteúdos ministrados.

3.1 Duração

A Pós-Graduação em Cibersegurança e Ciberdefesa tem uma duração de 2 semestres curriculares, perfazendo um total de 60 créditos (ECTS).

3.2 Plano Curricular

Este programa de formação especializada desenvolve-se ao longo de um ano letivo, conferindo um diploma de Pós-Graduação.

O plano curricular integra cinco módulos obrigatórios, conforme se apresenta na tabela em Anexo A. Cada um dos módulos apresenta uma natureza teórico-prática e inclui um conjunto de disciplinas que conferem ao aluno conhecimentos e competências avançadas na área da ciberdefesa, tendo por base o seu enquadramento geral no domínio da cibersegurança.

3.3 Módulos e Objetivos

MÓDULO 1 – Enquadramento da Cibersegurança e Ciberdefesa (11 ECTS)

Este módulo, constituindo um enquadramento geral do tema central da Pós-Graduação, apresenta os fundamentos e os conceitos básicos que caracterizam a cibersegurança e a ciberdefesa. Neste contexto, para além da caracterização sumária do impacto individual, organizacional e nacional/internacional dos ciberataques, são também abordadas as suas envolventes tecnológicas, sociais e estratégicas.

MÓDULO 2 – Segurança da Informação (16 ECTS)

Partido do facto de a Segurança da Informação constituir um pilar estruturante das áreas de estudo do Curso, este módulo integra um conjunto de unidades curriculares orientadas para a caracterização dos diferentes domínios da segurança dos sistemas e infraestruturas de informação, preparando os alunos para um melhor entendimento dos seus requisitos e desafios técnicos assim como dos vários métodos e técnicas de ataque cibernético.

MÓDULO 3 – Operações no Ciberespaço (15 ECTS)

Tendo como tema de fundo a condução de operações no ciberespaço, serão aqui caracterizados os princípios subjacentes ao seu planeamento, analisada a aplicação da doutrina militar à Ciberdefesa, promovendo-se a sua adaptação, quando ajustado, ao domínio da Cibersegurança e ao próprio ciberespaço. Neste contexto, serão também estudadas as áreas emergentes dos ataques de engenharia social, os processos de Cyber Intelligence necessários à formação de uma consciência situacional no ciberespaço e o desenvolvimento de capacidades de cibersegurança e ciberdefesa.

MÓDULO 4 – Gestão de Crises (12 ECTS)

Este módulo procura preparar os alunos para a utilização de métodos e ferramentas de avaliação de vulnerabilidades, código malicioso, ameaças e riscos cibernéticos, de forma a permitir a gestão estática e dinâmica do risco. Neste âmbito, será atribuída especial atenção aos ciberataques que procuram explorar as vulnerabilidades das infraestruturas críticas e dos sistemas responsáveis pelo seu controlo caracterizando e identificando, através de casos de estudo e simulação, as principais defesas a implementar para garantir a integridade e disponibilidade destes sistemas. Como corolário natural dos módulos anteriores, de forma a promover a aplicação dos conhecimentos adquiridos em contexto operacional, serão aqui também desenvolvidos cenários e treinados, em contexto de exercício, os processos de decisão associados a uma situação de gestão de crises no ciberespaço.

MÓDULO 5 – Projeto ou Estágio Profissional (6 ECTS)

Com o objetivo de garantir a ligação entre a componente letiva à prática dos conhecimentos adquiridos, os alunos realizarão um trabalho individual de carácter prático, numa organização ou empresa de referência (nacional ou internacional). Este trabalho, ligado obrigatoriamente à área da

Cibersegurança ou da Ciberdefesa, incidirá sob a aplicação dos conceitos, metodologias, capacidades ou ferramentas com que o aluno tomou contacto durante o curso, permitindo avaliar o nível de aquisição e mobilização de novas competências. O período de estágio decorre durante os dois primeiros semestres do Curso, sendo a avaliação realizada com base num projeto ou relatório de estágio. Este trabalho será desenvolvido sob a orientação de um docente e de um representante da instituição de acolhimento do estágio profissional.

3.4 Metodologia de Aprendizagem

Esta Pós-Graduação pretende ser aberta e global, combinando aulas de natureza presencial com o conceito de sala de aula virtual, procurando também sempre que possível explorar métodos de ensino *on-line* (*B-Learning*).

A metodologia de ensino inclui uma componente iminentemente prática, incluindo a análise de casos de estudo e um estágio profissional, onde o aluno poderá tomar contacto com um conjunto alargado de ferramentas e capacidades que caraterizam o estado da arte da envolvente tecnológica desta área de estudo.

A componente letiva (presencial, via VTC e *on-line*) será complementada com um conjunto de visitas, seminários e conferências, realizadas por especialistas de relevância nacional e internacional, docentes e profissionais ligados ao sector da Cibersegurança e da Ciberdefesa. Dentro deste contexto, algumas sessões letivas serão ministradas em língua inglesa.

O corpo docente é composto por reputados especialistas nacionais e internacionais, provenientes do meio académico, da indústria e de organizações de referência ligadas à cibersegurança e ciberdefesa. De forma a garantir uma metodologia de ensino flexível, prática e orientada para as possibilidades de cada aluno, o curso será ministrado em diferentes localizações físicas e a grupos não superiores a 30 alunos.

3.5 Bloco de Homogeneização de Conhecimentos

Atendendo à diversidade e possível heterogeneidade da formação de base dos alunos, existirá a possibilidade de estes frequentarem um período letivo de homogeneização de conhecimentos. Este período extra curricular, incidirá em matérias de tecnologias de informação, fundamentos de redes e estratégia.

3.6 Avaliação

Três vertentes orientam a avaliação das várias unidades curriculares do curso:

- Avaliação individual aferida em exame final e/ou provas intermédias;
- Avaliação individual decorrendo da participação oral;
- Avaliação da aplicação prática de conhecimentos (resolução de casos práticos ou desenvolvimento de projetos) quando a especificidade das disciplinas o justifique.
-

4. DESTINATÁRIOS

A Pós-Graduação em Cibersegurança e Ciberdefesa é dirigida a quadros superiores e gestores ligados a este domínio emergente da segurança na Era da Informação, incluindo profissionais civis e militares ligados às Forças Armadas e às Forças de Segurança, que necessitem de adquirir competências e desenvolver conhecimentos estruturantes desta área do saber. O papel destes gestores revela-se de particular importância não só para apoiar os decisores estratégicos de topo mas também para garantir uma integração operacional coerente das diversas áreas técnicas e funcionais associadas à cibersegurança e ciberdefesa.

O público-alvo deste Programa é assim constituído por candidatos com licenciatura em áreas disciplinares afins ou ligadas, preferencialmente, às áreas dos Sistemas e Tecnologias de Informação, Engenharia, Gestão, Ciências Militares e Ciências da Informação.

5. CANDIDATURAS

5.1. Condições de Candidatura

Podem candidatar-se a este curso de formação especializada todos os interessados nesta temática. No entanto, será atribuída uma condição de acesso preferencial a:

- Titulares do grau de licenciado ou equivalente legal;
- Titulares de um grau académico superior estrangeiro que seja reconhecido como satisfazendo os objetivos do grau de licenciado;
- Titulares de um grau académico superior estrangeiro conferido na sequência de um primeiro ciclo de estudos organizado de acordo com o Processo de Bolonha;
- Detentores de um currículo escolar, científico ou profissional reconhecido, pelo Conselho Científico do Mestrado, como atestando capacidade para a realização do ciclo de estudos conducente ao grau de mestre.

Número mínimo de vagas preenchidas para a realização do curso - 15

5.2. Documentação Necessária

No momento da formalização da candidatura, deverão ser entregues os seguintes documentos:

- Requerimento de candidatura/inscrição;
- Certificado de habilitações, contendo a classificação obtida nas diferentes unidades curriculares e certidão de licenciatura (se existente);
- Certidão/certificado comprovativo da atribuição de uma equivalência/reconhecimento de habilitações, no caso de obtenção de grau académico no estrangeiro;
- Fotocópia do Cartão de Cidadão (CC) ou documento equivalente;
- Fotocópia do cartão de contribuinte;
- Duas fotografias, a cores, tipo passe;
- Curriculum Vitae (1 exemplar).

5.3. Períodos de Candidatura e Início das Aulas

20 de agosto a 22 de setembro de 2017

Publicação da relação dos candidatos admitidos: 29 de setembro de 2017

Início das aulas (previsão) - **13 de outubro de 2017**

5.4. Horário das Aulas

As aulas são lecionadas em regime pós-laboral, no horário semanal com a seguinte distribuição:

Sexta-Feira:	Sábado:
Noite (18h00-23h00) 2 Aulas (3 +2 horas)	**Manhã** (09h00-14h00) 2 Aulas (3+2 horas)

Excecionalmente, para efeitos de compensação de aulas ou ocorrência de visitas, conferências e seminários poderão ser utilizados tempos letivos em outros dias e/ou horários a agendar.

6. PARCERIAS E SINERGIAS NACIONAIS

Explorando a complementaridade de saberes e a especialização inerente às áreas de estudo, este Programa será ministrado, em regime de parceria, por docentes de várias Instituições de Ensino Universitário:

- **UNIVERSIDADES:**
  Academia Militar - AM, Universidade de Lisboa (Faculdade de Ciências – FCUL e Instituto Superior Técnico – IST), Universidade do Minho (Escola de Engenharia - EE) e Universidade do Porto (Faculdade de Ciências – FCUP), Universidade Católica Portuguesa (Pólo de Braga - FFCS) e Universidade Portucalense (UPT);

- **OUTRAS INSTITUIÇÕES DE ENSINO SUPERIOR:**

  Instituto Politécnico de Beja (IPBeja), Instituto Politécnico do Porto (IPP), Instituto Politécnico de Viana do Castelo (IPVC) e Instituto Politécnico de Leiria (IPLeiria).

Materializando o Ciberespaço e a área da Cibersegurança e Ciberdefesa em especial um domínio em constante evolução tecnológica, este programa de formação especializada procura também, sempre que ajustado, uma ligação à Indústria e às Entidades Públicas e Privadas mais relevantes nesta área.

A estrutura modular das várias unidades curriculares e a existência de uma ligação ao Projeto NATO Multinational Cyber Defence Education and Training (MNCDE&T), que conta já com 102 Entidades e Empresas Nacionais, favorece esta ligação e confere um carácter mais pratico à formação ministrada.

7. COOPERAÇÃO INTERNACIONAL

Aprofundando a sua matriz internacional, de forma a melhor enquadrar o levantamento das capacidades nacionais, este **Programa de Formação Pós-graduada em Cibersegurança e Ciberdefesa** será organizado de forma articulada com uma Pós-Graduação em "Direito, Cibersegurança e Ciberdefesa" e com duas iniciativas internacionais semelhantes, a lançar no ano letivo 2017/18.

Esta Pós-Graduação terá assim por base uma rede académica de excelência (ex: Erasmus+ e Erasmus Militar) onde áreas nacionais de especialização podem ser partilhadas e disponibilizadas tanto num contexto nacional como à NATO, União Europeia e a outras Nações, segundo uma lógica de cooperação bilateral ou multilateral. Nesta iniciativa, serão tidas em consideração as melhores práticas e o estudo de iniciativas similares já existentes.

8. Propina

O valor da propina é de 3000€.

Módulo	Unidade Curricular	Horas (Presencias)	ECTS	1º Sem	2º Sem	Obrigatória (O) Opção (OP)	Corpo Docente Responsável (Instituições)
Enquadramento da Cibersegurança e Ciberdefesa	Introdução à Cibersegurança e Ciberdefesa	**15**	**3**	**15**	**0**	***O***	***Luís Antunes (FCUP)***
	Enquadramento Legal do Ciberespaço e dos Ciber Conflitos	**20**	**4**	**20**	**0**	***O***	***Sofia de Vasconcelos Casimiro (AM)***
	Guerra de Informação	**20**	**4**	**0**	**20**	***O***	***Paulo Nunes (AM)*** *e Nuno Perry (CIIWA)*
Segurança da Informação	Gestão de Segurança da Informação	**20**	**4**	**20**	**0**	***O***	***Henrique Santos*** *(UM), José Martins (CIIWA); Teresa Pereira (IPVC); Pedro Fernandes (UPT);*
	Segurança SW e Aplicacional	**15**	**3**	**15**	**0**		***Miguel Correia (IST),*** *Nuno Neves (FCUL) e João Paulo Magalhães (IPP)*
	Testes de Penetração e *Hacking* Ético	**25**	**5**	**0**	**25**	***O***	***Rui Silva*** *(IPBeja) e Pedro Adão (IST)*
	Análise Forense Digital	**20**	**4**	**20**	**0**	***O***	***Miguel Frade*** *(IPL), Rogério Bravo (FCUL) e Alberto Pinto (IPP)*
Operações no Ciberespaço	Planeamento de Operações no Ciberespaço	**20**	**4**	**0**	**20**	***O***	***Paulo Nunes (AM)*** *e Nelson Rego (IUM)*
	Engenharia Social	**15**	**3**	**0**	**15**		***Vítor Sá*** *(UCP), Paulo Alexandre (CGD), Pedro Pinto (IPVC) e Ivone Patrão (ISPA).*
	Cyber Intelligence e Consciência Situacional no Ciberespaço	**25**	**5**	**25**	**0**	***O***	***João Paulo Magalhães*** *(IPP); Carlos Silva (S21 Sec), Indústria: Anubis Networks, Globinova, S21Sec.*
	Desenvolvimento de Capacidades de Cibersegurança e Ciberdefesa	**15**	**3**	**0**	**15**	***O***	***Paulo Nunes (AM)*** *e João Farinha (CCD/EMGFA)*
Gestão de Crises	Gestão de Incidentes e do Risco (Estático e Dinâmico)	**20**	**4**	**20**	**0**	***O***	***Ana Respício*** *(FCUL), Paulo Moniz (EDP) e Daniel Caçador (Montepio)*
	Proteção de Sistemas e Infraestruturas Críticas	**20**	**4**	**0**	**20**	***O***	***António Casimiro*** *(FCUL), Paulo Moniz (EDP) e Carlos Silva (S21Sec)*
	Desenvolvimento Cenários e Exerc Gestão de Crises no Ciberespaço	**20**	**4**	**0**	**20**	**O**	***Paulo Nunes (AM),*** *José Martins (CIIWA),* José Dinis (CDD) e Nuno Goes (DCSI/Exe)
Projeto ou Estágio	Relatório de Projeto ou de Estágio (*on job training*)	**40**	**6**	**20**	**20**	**O**	*Coordenação UMinho: docentes a indicar*
Sessões Presenciais	Visitas, Conferências e Seminários					**O**	
	TOTAL	**310**	**60**	**155**	**155**		