

NCE/16/00134 — Apresentação do pedido - Novo ciclo de estudos

Apresentação do pedido

Perguntas A1 a A4

A1. Instituição de ensino superior / Entidade instituidora:
Universidade De Coimbra

A1.a. Outras Instituições de ensino superior / Entidades instituidoras:

A2. Unidade(s) orgânica(s) (faculdade, escola, instituto, etc.):
Faculdade De Ciências E Tecnologia (UC)

A3. Designação do ciclo de estudos:
Mestrado em Segurança Informática

A3. Study programme name:
Masters in Informatics Security

A4. Grau:
Mestre

Perguntas A5 a A10

A5. Área científica predominante do ciclo de estudos:
Informática

A5. Main scientific area of the study programme:
Informatics

A6.1. Classificação da área principal do ciclo de estudos (3 dígitos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF):
480

A6.2. Classificação da área secundária do ciclo de estudos (3 dígitos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF), se aplicável:
481

A6.3. Classificação de outra área secundária do ciclo de estudos (3 dígitos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF), se aplicável:
N/A

A7. Número de créditos ECTS necessário à obtenção do grau:
120

A8. Duração do ciclo de estudos (art.º 3 DL-74/2006, de 26 de Março):
2 anos (4 semestres)

A8. Duration of the study programme (art.º 3 DL-74/2006, March 26th):
2 years (4 semesters)

A9. Número máximo de admissões:**20****A10. Condições específicas de ingresso:***Serão admitidos no MSI os candidatos que reúnam uma das seguintes condições:*

1. Os titulares do grau de licenciado ou equivalente legal em: Engenharia Informática, Ciências da Computação, Comunicações e Multimédia, Engenharia de Sistemas e Informática, Engenharia Eletrotécnica, Engenharia Eletrotécnica e de Computadores, Engenharia Eletrotécnica e de Telecomunicações; 2. Os titulares do grau de licenciado ou equivalente legal em outras áreas da Engenharia e das Ciências Exatas e Naturais; 3. Os titulares de um grau académico superior estrangeiro que seja reconhecido como satisfazendo os objetivos do grau de licenciado numa das áreas referidas nas alíneas anteriores pela Comissão Científica do Departamento de Engenharia Informática; 4. Em casos devidamente justificados, os detentores de um currículo escolar, científico ou profissional, que seja reconhecido como atestando capacidade para realização deste ciclo de estudos pela Comissão Científica do Departamento de Engenharia Informática.

A10. Specific entry requirements:*The MSI candidates will be accepted if one of the following requirements is verified:*

1. Holders of a Bachelor's degree or legal equivalent in: Computer Engineering, Computer Science, Communications and Multimedia, Informatics and Systems Engineering, Electrical Engineering, Electrical and Computer Engineering, Electrical and Telecommunication Engineering;
2. Holders of the Bachelor's degree or legal equivalent in other areas of Engineering and Exact and Natural Sciences;
3. Holders of a foreign academic degree that is recognized by the Research Department of Computer Science to meet the objectives of a degree in the areas mentioned in the previous paragraphs;
4. In justified cases, holders of an academic, scientific or professional curriculum that is recognized to attest the capacity to complete this cycle of studies by the Scientific Committee of the Department of Computer Science.

Pergunta A11**Pergunta A11**

A11. Percursos alternativos como ramos, variantes, áreas de especialização do mestrado ou especialidades do doutoramento em que o ciclo de estudos se estrutura (se aplicável):

Não**A11.1. Ramos, variantes, áreas de especialização do mestrado ou especialidades do doutoramento (se aplicável)**

A11.1. Ramos, variantes, áreas de especialização do mestrado ou especialidades do doutoramento, em que o ciclo de estudos se estrutura (se aplicável) / Branches, options, specialization areas of the master or specialties of the PhD (if applicable)

Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento:

Branch, option, specialization area of the master or speciality of the PhD:

<sem resposta>

A12. Estrutura curricular**Mapa I -****A12.1. Ciclo de Estudos:****Mestrado em Segurança Informática****A12.1. Study Programme:****Masters in Informatics Security****A12.2. Grau:****Mestre**

A12.3. Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento (se aplicável):
<sem resposta>

A12.3. Branch, option, specialization area of the master or speciality of the PhD (if applicable):
<no answer>

A12.4. Áreas científicas e créditos que devem ser reunidos para a obtenção do grau / Scientific areas and credits that must be obtained for the awarding of the degree

Área Científica / Scientific Area	Sigla / Acronym	ECTS Obrigatórios / Mandatory ECTS	ECTS Mínimos Optativos* / Minimum Optional ECTS*
Segurança Informática / Informatics Security	SEC	102	0
Direito / Law	DIR	6	0
Opção Aberta / Open Option	OPT	0	12
(3 Items)		108	12

Perguntas A13 e A16

A13. Regime de funcionamento:
Pós Laboral

A13.1. Se outro, especifique:
O MSI funciona em modo pós-laboral com as aulas às quintas e sextas de tarde e aos sábados de manhã

A13.1. If other, specify:
The MSI classes will take place Thursday and Friday afternoon and Saturday morning

A14. Local onde o ciclo de estudos será ministrado:
O MSI será ministrado no Departamento de Engenharia Informática, da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

A14. Premises where the study programme will be lectured:
The MSI will be taught in the Department of Computer Engineering, Faculty of Science and Technology, University of Coimbra

A15. Regulamento de creditação de formação e experiência profissional (PDF, máx. 500kB):
[A15_Reg_191_2014_CreditacaoFormacaoAnterior_e_ExperienciaProfissional_UC.pdf](#)

A16. Observações:
A aprovação em 60 ECTS de UCs corresponde à conclusão do Curso de Especialização em Segurança Informática (CeSI), curso não conferente de grau, de que será emitido um Diploma.
A Dissertação/Estágio pode ser integralmente realizada em contexto de empresa, sob orientação do um docente da UC, enquadrada por um profissional Especialista em Informática. O processo de elaboração, acompanhamento e avaliação seguirá o procedimento já em utilização no DEI para os cursos de mestrado (MEI e MDM) em que a proposta pode partir do aluno ou da empresa e será validada pelo Coordenador do MSI. Estão previstos dois momentos de avaliação por um júri com, pelo menos, três docentes sendo um deles o Orientador: a avaliação intermédia ao fim de um semestre, e a avaliação final no fim de dois semestres.
A UC de Dissertação/Estágio terá duas modalidades: normal com início no 1º semestre e decorre num único ano letivo; plurianual com tem início no 2º semestre e decorre em dois anos letivos consecutivos.

A16. Observations:
The approval in UCs totalling 60 ECTS will correspond to the completion of the Specialization in Computer Security (CeSI), a non-degree course, that will entitle the student to a Diploma.

The Dissertation / Internship can be fully carried out in the context of the company, under the guidance of a faculty member of the UC (the Advisor), with local guidance in the company by Informatics Specialist. The process of preparation of the Dissertation / Internship and monitoring and evaluation will follow the procedure already in use in the DEI for master courses (MEI and MDM). The proposal can come from the student or from a company and will be validated by the Coordinator MSI, and then accompanied by the Advisor. Two moments of assessment by a jury

of at least three teachers (one being the Advisor) are planned: the mid-term review at the end of one semester of work, and the final evaluation at the end of two semesters.

The course of Dissertation / Internship will have two modes: normal mode, which begins in the first semester and will take a single school year; the multi-year modality that will start in the second semester and will take place two consecutive academic years.

Instrução do pedido

1. Formalização do pedido

1.1. Deliberações

Mapa II - Comissão Científica DEI, Conselho Científico FCTUC, Conselho Pedagógico

1.1.1. Órgão ouvido:

Comissão Científica DEI, Conselho Científico FCTUC, Conselho Pedagógico

1.1.2. Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada (PDF, máx. 100kB):

[1.1.2._Atas pdf_final.pdf](#)

Mapa II - Reitor

1.1.1. Órgão ouvido:

Reitor

1.1.2. Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada (PDF, máx. 100kB):

[1.1.2._Despacho_197_16_Criacao_Mest_Seg_Informatica.pdf](#)

1.2. Docente(s) responsável(eis) pela coordenação da implementação do ciclo de estudos

1.2. Docente(s) responsável(eis) pela coordenação da implementação do ciclo de estudos

A(s) respetiva(s) ficha(s) curricular(es) deve(m) ser apresentada(s) no Mapa V.

Edmundo Heitor da Silva Monteiro

2. Plano de estudos

Mapa III - - 1º ano / 1º semestre

2.1. Ciclo de Estudos:

Mestrado em Segurança Informática

2.1. Study Programme:

Masters in Informatics Security

2.2. Grau:

Mestre

2.3. Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento (se aplicável):

<sem resposta>

2.3. Branch, option, specialization area of the master or speciality of the PhD (if applicable):

<no answer>

2.4. Ano/semestre/trimestre curricular:

1º ano / 1º semestre

2.4. Curricular year/semester/trimester:

1st year / 1st semester**2.5. Plano de Estudos / Study plan**

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Criptografia / Cryptography	SEC	Semestral	162	T-30; PL-30; O-2	6	
Conceção e Desenvolvimento de Software Seguro / Design and Development of Secure Software	SEC	Semestral	162	T-30; PL-30; O-2	6	
Avaliação e Gestão de Cibersegurança Cyber Security Assessment and Management	SEC	Semestral	162	T-30; PL-30; O-2	6	
Direito e Segurança Informática / Informatics Security and Law	DIR	Semestral	162	T-30; PL-30; O-2	6	
Opcional 1 / Optional 1	Opção Aberta	Semestral	162	-	6	Qualquer UC do MEI (ou de outros mestrados mediante aprovação)

(5 Items)

Mapa III - - 1º ano / 2º semestre**2.1. Ciclo de Estudos:*****Mestrado em Segurança Informática*****2.1. Study Programme:*****Masters in Informatics Security*****2.2. Grau:*****Mestre*****2.3. Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento (se aplicável):*****<sem resposta>*****2.3. Branch, option, specialization area of the master or speciality of the PhD (if applicable):*****<no answer>*****2.4. Ano/semestre/trimestre curricular:*****1º ano / 2º semestre*****2.4. Curricular year/semester/trimester:*****1st year / 2nd semester*****2.5. Plano de Estudos / Study plan**

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Segurança e Privacidade / Security and Privacy	SEC	Semestral	162	T-30; PL-30; O-2	6	
Segurança em Tecnologia de Informação / Information Technologies Security	SEC	Semestral	162	T-30; PL-30; O-2	6	
Conceção e Desenvolvimento de Infraestruturas Seguras / Designing and Building Secure Infrastructures	SEC	Semestral	162	T-30; PL-30; O-2	6	

Auditoria de Segurança / Security Auditing	SEC	Semestral	162	T-30; PL-30; O-2	6	Qualquer UC do MEI (ou outros mestrados mediante aprovação)
Opcional 2 / Optional 2	Opção Aberta	Semestral	162	-	6	

(5 Items)

Mapa III - - 2º ano

2.1. Ciclo de Estudos:

Mestrado em Segurança Informática

2.1. Study Programme:

Masters in Informatics Security

2.2. Grau:

Mestre

2.3. Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento (se aplicável):

<sem resposta>

2.3. Branch, option, specialization area of the master or speciality of the PhD (if applicable):

<no answer>

2.4. Ano/semestre/trimestre curricular:

2º ano

2.4. Curricular year/semester/trimester:

2nd year

2.5. Plano de Estudos / Study plan

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Seminários de Acompanhamento / Followup Seminars	SEC	Semestral	162	S-30	6	
Dissertação/Estágio / Dissertation/Internship	SEC	Anual	1404	O-30	54	

(2 Items)

3. Descrição e fundamentação dos objetivos, sua adequação ao projeto educativo, científico e cultural da instituição, e unidades curriculares

3.1. Dos objetivos do ciclo de estudos

3.1.1. Objetivos gerais definidos para o ciclo de estudos:

O MSI visa formação especializada na área da Segurança Informática (Cibersegurança). Dando resposta a um conjunto de iniciativas a nível Internacional e Europeu, no sentido do reforço de competências na área da Cibersegurança (ex. US Cybersecurity Information Act, EU Directive for Security Across the Union) como forma de suportar o crescimento da economia digital, preservar a privacidade dos cidadãos e combater e prevenir o cibercrime e o ciberterrorismo, o MSI tem os seguintes objetivos:

- Complementar a formação de 1º ciclo, com de competências de conceção, desenvolvimento e avaliação de soluções de Segurança Informática;*
- Atualizar e especializar os profissionais já inseridos em ambiente profissional na área da Segurança Informática, nomeadamente os vários cargos da carreira de Oficial de Segurança de Informação;*
- Proporcionar formação avançada na áreas da Segurança Informática para os alunos vocacionados para uma*

carreira científica prosseguir em estudos de programa doutoral.

3.1.1. Generic objectives defined for the study programme:

MSI aims at specialized training in Informatics Security (Cybersecurity). Giving response to a set of initiatives that have been developed at International and European level, targeting the development of knowledge competences in the field of Cybersecurity (e.g. US Cybersecurity Information Sharing Act, EU Directive for security across the Union) as a way to support the growth of the digital economy, preserving the privacy of citizens and to combat and prevent cybercrime and cyberterrorism, the MSI has the following objectives:

- *Complement the training of students from 1st cycles, specializing in design, development, and evaluation skills related with Informatics Security.*
- *Upgrade and specialize the IT professionals, providing them with knowledge to perform functions in the field of Information Security, namely the role of Information Security Officer;*
- *Provide advanced training in the different areas of IT Security, allowing students to follow a doctoral program*

3.1.2. Objetivos de aprendizagem (conhecimentos, aptidões e competências) a desenvolver pelos estudantes:

Espera-se que, ao concluírem o Mestrado em Segurança Informática (MSI), os estudantes possuam os seguintes conhecimentos, aptidões e competências:

- *Conhecimento profundo dos aspetos tecnológicos, humanos e organizacionais e relevantes nas diferentes áreas da Segurança Informática.*
- *Competências de conceção, desenvolvimento e avaliação de soluções de Segurança Informática;*
- *Aptidão para o desempenho de funções na área da Segurança Informática, nomeadamente os vários cargos e tarefas da carreira de Oficial de Segurança de Informação (Information Security Officer);*
- *Aptidão para integrar e liderar equipas de projeto de investigação na área da Segurança Informática e de realização de trabalho autónomo de investigação e desenvolvimento de novos conhecimentos na área;*
- *Conhecimento dos aspetos legais, éticos e deontológicos, relacionados com a Segurança Informática.*

3.1.2. Intended learning outcomes (knowledge, skills and competences) to be developed by the students:

It is expected that, upon completion of the Master in Informatics Security (MSI) students will have the following knowledge, skills and competences :

- *Thorough knowledge of the technological aspects, human and organizational and relevant in different areas of IT Security*
- *Design, development and evaluation skills of informatics security solutions;*
- *Ability to perform functions in the field of Information Security, in particular the various positions and career of Information Security Officer;*
- *Ability to integrate and lead research project teams in the field of Informatics Security and ability to conduct of autonomous research and development work and development of new knowledge in the field;*
- *Knowledge of legal, ethical and moral aspects, related to IT Security.*

3.1.3. Inserção do ciclo de estudos na estratégia institucional de oferta formativa face à missão da instituição:

O ciclo de estudos insere-se na missão da Universidade de Coimbra que visa promover uma oferta de ensino qualificada, sobretudo em áreas em que existam carências de profissionais. O ciclo de estudos visa ainda contribuir para atividades de transferência de tecnologia e realizar trabalho de investigação de relevo em áreas do conhecimento, que são também vertentes da missão da UC

3.1.3. Insertion of the study programme in the institutional training offer strategy against the mission of the institution:

The study cycle is part of the mission of the University of Coimbra to promote a qualified educational opportunities , especially in areas where there are shortages of professionals. The MSI course aims to contribute to technology transfer activities, and conduct relevant research work in relevant areas of knowledge, which are also inline with the UC mission.

3.2. Adequação ao projeto educativo, científico e cultural da Instituição

3.2.1. Projeto educativo, científico e cultural da Instituição:

A UC é uma instituição de criação, análise crítica, transmissão e difusão de cultura, de ciência e de tecnologia que, através da investigação, do ensino e da prestação de serviços à comunidade, contribui para o desenvolvimento económico e social, para a defesa do ambiente, para a promoção da justiça social e da cidadania esclarecida e responsável e para a consolidação da soberania assente no conhecimento.

São fins da UC:

- a) *A formação humanística, filosófica, científica, cultural, tecnológica, artística e cívica;*
- b) *A promoção e valorização da língua e da cultura portuguesas;*
- c) *A realização de investigação fundamental e aplicada e do ensino dela decorrente;*
- d) *A contribuição para uma política de desenvolvimento económico e social sustentável, assente na difusão do conhecimento e da cultura e na prática de atividades de extensão universitária;*
- e) *O intercâmbio cultural, científico e técnico com instituições congéneres nacionais e estrangeiras;*

- f) A resposta adequada à necessidade de aprendizagem ao longo da vida;*
- g) A preservação, afirmação e valorização do seu património científico, cultural, artístico, arquitetónico, natural e ambiental;*
- h) A contribuição, no seu âmbito de atividade, para a cooperação internacional e para a aproximação entre os povos, com especial relevo para os países de expressão oficial portuguesa e os países europeus, no quadro dos valores democráticos e da defesa da paz.*

O ensino é adaptado às exigências do mercado de trabalho, internacionalizado e tem a investigação científica como elemento central. A UC conta com centros de investigação em vários domínios e desenvolve também um conjunto extenso de atividades de transferência de saberes, apoio ao empreendedorismo e desenvolvimento do tecido empresarial.

A Universidade promove ainda, de forma ativa e concertada, o empreendedorismo e inovação para toda a comunidade. O programa, catalisado pela própria Universidade, envolve todas as partes intervenientes no processo, destacando-se o importante papel de estruturas como o Biocant ou a incubadora do IPN, recentemente proclamada a melhor incubadora de base tecnológica do mundo e que, na última década, gerou mais de 140 empresas, muitas delas spin-offs da Universidade que hoje representam um volume de vendas anual acima dos 70 milhões de euros (35% dos quais para exportação), empregando mais de 500 profissionais altamente qualificados.

3.2.1. Institution's educational, scientific and cultural project:

University of Coimbra goals:

- a) Humanistic, philosophical, scientific, cultural, technologic, artistic and civic education;*
- b) Promotion and valorisation of the Portuguese language and culture;*
- c) Fundamental and applied research and resulting teaching;*
- d) Contribution to the implementation of a policy of economic and social development, based on the diffusion of knowledge and culture, and practice of university extension activities, namely to provide specialized services to the community in benefit of the city, region and country;*
- e) Cultural, scientific and technical exchange with similar national and international institutions;*
- f) Appropriate response to the lifelong learning demands;*
- g) Preservation, affirmation and valorisation of its scientific, cultural, artistic, natural, environmental and architectural patrimony;*
- h) Contribution to the international cooperation and to approach between nations, specially with PALOPs and European countries, on the basis of democratic values and peace defence.*

The teaching is adjusted to the demands of the labour market, it is strongly internationalized and scientific research has a central role. The UC develops an extensive amount of activities supporting the knowledge transfer and entrepreneurship.

The University also promotes, in an active and concerted manner, entrepreneurship and innovation for the entire community. The program, catalyzed by the University, involves all stakeholders in the process, highlighting the important role of structures such as the incubator Biocant or Instituto Pedro Nunes, recently proclaimed the best technology-based incubator in the world. IPN, in the last decade has generated more than 140 companies, many of them University's spin-offs, and now represents an annual turnover of over EUR 70 million (35% of which for export) with over 500 highly qualified professionals.

3.2.2. Demonstração de que os objetivos definidos para o ciclo de estudos são compatíveis com o projeto educativo, científico e cultural da Instituição:

Os objetivos definidos para o ciclo de estudos são compatíveis com o projeto educativo, científico e cultural da Universidade de Coimbra, sendo claramente enquadrados no projeto educativo (formação avançada em áreas em que existam carências de recursos humanos), científico (desenvolvimento de projetos de investigação desenvolvimento de novo conhecimento) e de transferência de tecnologia (transferência de tecnologia em áreas economicamente relevantes para Portugal e para o espaço Europeu)

3.2.2. Demonstration that the study programme's objectives are compatible with the Institution's educational, scientific and cultural project:

The objectives defined for the study cycle are consistent with the educational, scientific and cultural project of the University of Coimbra, being clearly in the scope of the educational project (advanced training in areas where there is a lack of human resources), scientific project (research and development of new knowledge), and the technology transfer project (technology transfer in economically relevant areas for Portugal and the European space).

3.3. Unidades Curriculares

Mapa IV - Criptografia / Cryptography

3.3.1. Unidade curricular:

Criptografia / Cryptography

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Edmundo Heitor da Silva Monteiro

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
João Paulo da Silva Machado Garcia Vilela (25%)
António Jorge Costa Granjal (25%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta unidade curricular tem como objetivo a aquisição de conhecimentos sobre técnicas e algoritmos de criptografia. Os alunos deverão dominar os mecanismos base de criptografia e da segurança de segurança informática. Espera-se que os estudantes adquiram/desenvolvam as seguintes competências-chave:
 - *Competências em avaliação e gestão de cibersegurança, análise e gestão de risco de segurança informática, avaliação e gestão de risco de segurança, no âmbito de sistemas informáticos e das organizações em que estes se inserem.*
 - *Aplicação prática do conhecimento teórico na avaliação e gestão de segurança, competências de análise e síntese, e capacidade de autoaprendizagem em novos contextos no domínio da segurança informática.*

E ainda as seguintes competências complementares:

- *Resolução de problemas, comunicação oral e escrita, relações interpessoais e capacidade de trabalho em equipa.*

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This curricular unit aims to acquire knowledge about encryption algorithms. At the end of the course students should master basic cryptography and security mechanisms. It is also intended that the students acquire/develop the following core competencies:
 - *Skills on cyber security assessment and management, security risk analysis, security risk assessment and management at organization and system level.*
 - *Practical application of the theoretical knowledge on security assessment and management, competences in analysis and synthesis, critical reasoning, and self-learning.*

and the following secondary competencies:

- *Problem solving, oral and written communication, interpersonal relations, and team work*

3.3.5. Conteúdos programáticos:

- *História da criptografia*
- *Fundamentos de criptografia*
- *Fundamentos de teoria da informação*
- *Computabilidade dos algoritmos de criptografia*
- *Criptografia de chave simétrica*
- *Criptografia de chave pública*
- *Algoritmos e técnicas de garantia de confidencialidade*
- *Algoritmos e técnicas de autenticação*
- *Algoritmos e técnicas de controlo de integridade*
- *Algoritmos e técnicas de não repudição*
- *Técnicas de criptoanálise*
- *Aspetos avançados de criptografia*

3.3.5. Syllabus:

- *History of cryptography*
- *Cryptography Basics*
- *Information theory basics*
- *Computability of encryption algorithms*
- *Symmetric key cryptography*
- *Public-key cryptography*
- *Algorithms and techniques for confidentiality*
- *Authentication algorithms and techniques*
- *Algorithms and techniques for integrity control*
- *Algorithms and techniques for non-repudiation*
- *Cryptanalysis techniques*
- *Advanced cryptography*

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área dos mecanismos

e algoritmos de criptografia. Nesse sentido, são abordadas as técnicas e algoritmos (com ênfase nos algoritmos de criptografia) para a garantia de segurança e privacidade nas comunicações e processamento de informação.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

This course aims to acquire knowledge and skills about encryption algorithms and mechanisms. In this sense, this curricular unit will address the techniques and algorithms (with emphasis on encryption algorithms) to guarantee security and privacy in communications and information processing.

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes.

Exame 50%; Projeto 25%; Resolução de problemas 25%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 25%; Problem resolving report 25%

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

A estratégia e o método de ensino adotado procuram envolver os alunos no processo de aprendizagem e na sua valorização pessoal, e assim levar ao desenvolvimento, para além de competências técnicas específicas, de competências genéricas, de natureza instrumental, pessoal e sistémicas.

Serão criadas condições para o desenvolvimento das competências para análise e síntese, resolução de problemas, tomada de decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, e em aplicar na prática os conhecimentos teóricos adquiridos nas aulas teóricas e teórico-práticas.

Serão criadas condições para o desenvolvimento das competências para análise e síntese, resolver problemas, decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, em aplicar na prática os conhecimentos teóricos adquiridos nas aulas.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The strategy and teaching methodology adopted seek to include students in the learning, leading to the development of not only specific technical competences, but also generic competences of instrumental, personal and systemic nature.

Examples and practical exercises presented in T and TP classes provide the conditions for the analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations and applying theoretical concepts learned to practical situations.

With the practical group project, students can develop their analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations, applying theoretical concepts learned to practical situations, planning and management as well as researching.

3.3.9. Bibliografia principal:

- William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 1999
- Schneier, Bruce (1996). *Applied Cryptography*, 2 ed, Wiley, (ISBN 0-471-11709-9).
- Bruce Schneier, *Secrets and lies (Segredos e mentiras sobre a protecção na vida digital)*, Editora Campus, 2001.
- Stinson, Douglas (2005). *Cryptography: Theory and Practice* ISBN 1-58488-508-4.
- Paar, Christof and Jan Pelzl (2009). *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, ISBN 978-3-642-04100-6
- Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, *Cryptography Engineering; Design Principles and Practical Applications*, John Wiley & Sons, 2010.
- Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography (Second Edition)*, CRC Press, 2014.

Mapa IV - Conceção e Desenvolvimento de Software Seguro / Design and Development of Secure Software

3.3.1. Unidade curricular:

Conceção e Desenvolvimento de Software Seguro / Design and Development of Secure Software

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Marco Paulo Amorim Vieira

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

Nuno Manuel dos Santos Antunes (50%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo a aquisição de conhecimentos sobre técnicas avançadas para o desenvolvimento de software seguro. Os alunos deverão dominar os diferentes aspetos do desenvolvimento de software com requisitos de segurança estritos, sendo capazes de identificar alternativas e de escolher e aplicar as mais adequadas a cada situação. Serão consideradas as diferentes fases do ciclo de vida do software. Pretende-se que o aluno adquira competências na análise, desenho, desenvolvimento e validação de software seguro.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The aim of this course is to provide knowledge on advanced techniques for the development of secure software. It is expected that students master the different aspects of developing software with security requirements, being able to identify existing alternatives and selecting and implementing the most adequate ones. The course considers the different phases of the software development lifecycle, from requirements engineering to testing. Beyond acquiring knowledge on the fundamentals of the area, students are expected to gain competences in the analysis, design, development and validation of secure software through their application in real-world case studies

3.3.5. Conteúdos programáticos:

- *Conceitos sobre segurança: Vulnerabilidades, Ameaças e Ataques*
- *Fundamentos sobre segurança de software*
- *Engenharia de requisitos para software seguro*
- *Arquitetura e desenho de software seguro*
- *Programação segura*
- *Deteção de vulnerabilidades e testes de segurança*
- *Segurança de software de uma perspetiva organizacional*
- *Fundamentos de avaliação de segurança: Métricas, Medição, Testes Padronizados e Análise de Riscos*

3.3.5. Syllabus:

- *Security Concepts: Vulnerabilities, Threats, and Attacks*
- *Software Security Foundations*
- *Requirements Engineering for Secure Software*
- *Secure Software Architecture and Design*
- *Secure Programming*
- *Vulnerability Detection and Security Testing*
- *Software Security from an Organization Perspective*
- *Security evaluation fundamentals: Metrics, Measurements, Benchmarking, and Risk Analysis*

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências em software seguro. Nesse sentido, são abordados conceitos, técnicas e ferramentas nas diferentes fases do ciclo de desenvolvimento de software, desde a engenharia de requisitos e desenho de arquitetura, até à codificação, validação e avaliação. Para além de aulas expositivas de conteúdos, serão usados exemplos e casos de estudo que facilitem a compreensão destes temas. Serão estudados conceitos fundamentais sobre software seguro, estabelecendo as bases para entender as principais ameaças e ataques existentes. Os aspetos relacionados com deteção de vulnerabilidades e testes são depois apresentados, completando a visão sobre as diferentes fases do ciclo de vida do desenvolvimento. Finalmente, são apresentados fundamentos sobre avaliação de segurança em diferentes perspetivas, nomeadamente em métricas e medição de segurança, testes padronizados e análise de risco.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

The aim of this course is providing knowledge and developing competences in secure software. With that goal in

mind, we address concepts, techniques, and tools for the different phases of the software development lifecycle, ranging from requirements engineering and architectural design, to coding, assessment and validation. In addition to traditional classes for presenting the fundamentals, case studies and examples will be used to facilitate understanding the different topics addressed.

The course starts by studying fundamental concepts on secure software, establishing the basis for understanding the main threats and attacks nowadays. From the architectural design the focus goes to detailed design and coding applying adequate techniques and guidelines. Finally, are presented fundamental concepts on security assessment from different perspectives, including security metrics and measurement, benchmarking and risk analysis

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes.

Exame 50%; Projeto 50%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 50%

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

A estratégia e o método de ensino adotado procuram envolver os alunos no processo de aprendizagem e na sua valorização pessoal, e assim levar ao desenvolvimento, para além de competências técnicas específicas, de competências genéricas, de natureza instrumental, pessoal e sistémicas.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolução de problemas, tomada de decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, e em aplicar na prática os conhecimentos teóricos adquiridos nas aulas teóricas e teórico-práticas.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolver problemas, decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, em aplicar na prática os conhecimentos teóricos adquiridos nas aulas teóricas e práticas-laboratoriais, planejar e gerir, e investigar.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The strategy and teaching methodology adopted seek to include students in the learning, leading to the development of not only specific technical competences, but also generic competences of instrumental, personal and systemic nature.

Examples and practical exercises presented in T and TP classes provide the conditions for the analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations and applying theoretical concepts learned to practical situations.

With the practical group project, students can develop their analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations, applying theoretical concepts learned to practical situations, planning and management as well as researching

3.3.9. Bibliografia principal:

- J. Viegas and G. McGraw, Building secure software: how to avoid security problems the right way. Addison-Wesley, 2001.

- M. Howard and D. E. Leblanc, Writing Secure Code, 2nd ed., Microsoft Press, 2002.

- G. Hoglund and G. McGraw, Exploiting Software: How To Break Code. Pearson Education, 2004.

- M. Howard, et al. , 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, McGraw-Hill, 2005.

- C. J. Berg, C. Berg, and P. G. Neumann, High-Assurance Design: Architecting Secure and Reliable Enterprise Applications, Addison-Wesley Professional, 2005.

- M. Schumacher et al , Security Patterns: Integrating Security and Systems Engineering, Wiley, 2006.

- G. McGraw, Software Security: Building Security In. Addison-Wesley Professional, 2006.

- J. H. Allen et al, *Software Security Engineering: A Guide for Project Managers*, Addison-Wesley Professional, 2008.
- M. Howard and S. Lipner, *The security development lifecycle*. O'Reilly Media, Incorporated, 2009.

Mapa IV - Avaliação e Gestão de Cibersegurança / Cyber Security Assessment and Management

3.3.1. Unidade curricular:

Avaliação e Gestão de Cibersegurança / Cyber Security Assessment and Management

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Henrique Santos Carmo Madeira

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

Carlos Nuno Bizarro e Silva Laranjeiro (50%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo a aquisição de conhecimentos sobre avaliação e gestão de cibersegurança na perspetiva dos sistemas informáticos. Espera-se que os estudantes dominem os conceitos fundamentais em segurança informática, na perspetiva organizacional e empresarial. Será dada ênfase particular à perspetiva de risco de segurança. Os conhecimentos adquiridos serão instanciados em áreas de aplicação relevantes incluindo cloud, smart-cards e sistemas de pagamento, sistemas ciber-físicos e proteção de infraestruturas críticas.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The aim of this curricular unit is to provide knowledge regarding the foundations of cyber security assessment and management. It is expected that students master the fundamentals of security, with focus on the enterprise perspective. A strong emphasis is put on the security risk assessment and risk management, covering the whole process from the organization/system security requirements. Besides acquiring knowledge on the fundamentals of these areas, specific domains will be targeted, such as cloud, smart-cards and payment, cyber-physical systems, and critical infrastructure protection.

3.3.5. Conteúdos programáticos:

- *Introdução à avaliação e gestão de cibersegurança.*
- *Risco de segurança em sistemas informáticos: requisitos, elementos do risco e gestão de risco.*
- *Técnicas e ferramentas de avaliação de segurança em sistemas informáticos.*
- *Segurança na perspetiva de sistema de operação, deteção de malware, mecanismos de defesa e de tolerância a intrusões.*
- *Segurança e privacidade na perspetiva das organizações*
- *Aspetos económicos da segurança informática*
- *Avaliação e gestão de segurança em domínios específicos, tais como:*
 - o Segurança em Cloud*
 - o Smart cards e sistemas de pagamento*
 - o Sistemas ciber-físicos*
 - o Proteção de infraestruturas críticas*

3.3.5. Syllabus:

- *Introduction to cyber security assessment and management*
- *System security risk perspective: requirements, risk elements, and management frameworks*
- *Security assessment techniques and tools*
- *Computer security, malware detection and defense*
- *Enterprise security and privacy*
- *Economics of information security*
- *Security assessment and management in specific domain*
 - o Cloud Security*
 - o Smart cards and payment security*
 - o Cyber-physical systems security*
 - o Critical infrastructure protection*

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área dos modelos e metodologias de segurança da informação. Nesse sentido, são abordados modelos e técnicas que permitem

avaliar o cumprimento de requisitos como o adequado investimento/retorno de investimento em segurança, focando domínios de aplicação tais como segurança em cloud, sistemas de pagamento, sistemas ciber-físicos e proteção de infraestruturas críticas.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

The aim of this course is to provide knowledge and develop competences in models and methodologies for managing and assessing cyber security at system and enterprise level. With that goal in mind, we address models and techniques for analyzing and managing enterprise security and also privacy, as well as techniques for specific (but security-critical) domains, such as cloud, payment security, cyber-physical systems security, and critical infrastructure protection.

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes.

Exame 50%; Projeto 50%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 50%

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

Nesta unidade curricular procura-se motivar e envolver os estudantes através de um processo contínuo de aprendizagem dos conceitos e discussão da sua aplicação prática em exemplos nos domínios de aplicação selecionados na unidade curricular. Para além de aulas magistrais, para explanação e discussão dos conceitos, serão usados pequenos projetos focando a aplicação prática dos conceitos aprendidos de forma a assegurar que os estudantes adquiram as competências esperadas. O facto de estes projetos serem efetuados em pequenos grupos ajuda a adquirir as competências técnicas num contexto mais realista, de trabalho em equipa, desenvolvendo também as competências de interação pessoal e de trabalho em equipa. Os projetos também complementa a aprendizagem com competências de comunicação escrita e oral (escrita de relatório final e apresentação e defesa, como parte da avaliação da unidade curricular) e de resolução de problemas em ambiente de equipa.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

In this curricular unit the teaching methodologies promote students involvement since the beginning, with the goal of a continuous acquisition of knowledge and competences. In addition to lecturers, practical assignments targeting key aspects of the concepts taught and their applicability will play an important role in the learning process. With the comprehension of the concepts, with the resolution and oral defenses of the proposed problems and with the exam the conditions are set for the acquisition of competences in computer skills related to the study field, problem solving, autonomous learning, application of theoretical knowledge in practical activities, and oral and written communication. The fact that the assignments are carried out in small group allows the acquisition of competences in team work and interpersonal relationships

3.3.9. Bibliografia principal:

- Lawrence Gordon and Martin Loeb, "Managing Cybersecurity Resources: A Cost-Benefit Analysis", McGraw-Hill
- Ross Anderson, "Security Engineering", Wiley
- Ross Anderson, et al., "Security Economics and the Internal Market", ENISA, 2008
- Charles P. Pfleeger, et al., "Security in Computing", Prentice Hall, 2015
- Shimon K. Modi, "Biometrics in Identity Management: Concepts to Applications", Artech House 2011
- William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Pearson 2014
- Sumeet Dua, Xian Du, "Data Mining and Machine Learning in Cybersecurity", CRC Press, 2011
- Ralph Gross, Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks", ACM WPES, 2005.
- Arvind Narayanan, Vitaly Shmatikov, "De-anonymizing Social Networks", IEEE SP, 2009.

- Yves-Alexandre de Montjoye, et al., “Unique in the crowd: The privacy bounds of human mobility”, *Nature Scientific Reports*, 2013.

Mapa IV - Direito e Segurança Informática / Informatics Security and Law

3.3.1. Unidade curricular:

Direito e Segurança Informática / Informatics Security and Law

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Alexandre Libório Dias Pereira

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

- 1º - Identificar as fontes e compreender a natureza do Direito da Informática e da Segurança Informática.*
- 2º - Compreender o comércio eletrónico e ser capaz de mobilizar as suas ferramentas normativas, em especial no que respeita ao princípio do país de origem, à contratação eletrónica (incluindo a certificação de assinaturas digitais e a proteção do consumidor), e à responsabilidade civil dos provedores de internet.*
- 3º - Dominar o regime jurídico de proteção de dados pessoais, da privacidade nas comunicações eletrónicas, proteção de programas e bases de dados e dos direitos de autor na Internet.*
- 4º - Relacionar o regulamento dos nomes de domínio da internet com a tutela dos sinais distintivos.*
- 5º - Identificar o tribunal competente e a lei aplicável em litígios relacionados com a utilização da Internet e reconhecer a existência de meios alternativos de resolução de litígios.*
- 6º - Compreender a lei do crime informático e aspetos de ética e deontologia da Segurança Informática.*

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

- 1 - Identify the sources and understand the nature of Computer Law and Computer Security Law.*
- 2 - Understanding e-commerce and be able to use its legal tools, especially with regard to the country of origin, e-contracts (including certification of digital signatures and consumer protection), and the civil liability of Internet providers.*
- 3 - Knowing the legal framework for personal data protection and privacy in electronic communications and the legal protection of computer programs and databases as well as copyright on the Internet.*
- 4 - Relate the regulation of Internet domain names with the protection of distinctive signs (brands, etc.).*
- 5 - Identifying the competent court and applicable law in disputes related to the use of Internet and to acknowledge the existence of alternative means of dispute resolution.*
- 6 - Understanding the law of computer crime (cybercrime) and aspects of ethics and deontology of Computer Security.*

3.3.5. Conteúdos programáticos:

- § 1. Objeto, fontes e natureza do Direito da Informática e da Segurança Informática.*
- § 2. Comércio eletrónico e o princípio do país de origem.*
- § 3. Contratação eletrónica, certificação e proteção do consumidor*
- § 4. Programas de computador, bases de dados e direitos de autor na internet*
- § 5. Nomes de domínio da Internet e sinais distintivos*
- § 6. Dados pessoais e privacidade nas comunicações eletrónicas*
- § 7. Responsabilidade civil dos provedores de Internet e computação em nuvem.*
- § 8. Jurisdição na internet: tribunal competente, lei aplicável e meios alternativos de resolução de litígios.*
- § 9. Crime informático*
- § 10. Aspetos de ética e deontologia.*

3.3.5. Syllabus:

- § 1. Object, sources and nature of Computer Law and Computer Security Law.*
- § 2. E-commerce and the principle of country of origin.*
- § 3. Electronic contracting , certification and consumer protection.*
- § 4. Computer programs, databases and copyright on the Internet.*
- § 5. Internet domain names and distinctive signs.*
- § 6. Personal data and privacy in electronic communications.*
- § 7. Liability of Internet service providers and cloud computing.*
- § 8. Jurisdiction on the Internet: competent court , applicable law and alternative means of dispute resolution.*
- § 9. Computer crime*
- § 10. Ethical and deontological issues*

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Para alcançar o 1º objetivo é lecionada matéria relativa às fontes e à natureza do Direito da Informática e da Segurança Informática (§ 1). Para alcançar o 2º objetivo são lecionadas as matérias relativas ao comércio eletrónico e princípio do país de origem, contratação eletrónica, certificação e proteção do consumidor, e responsabilidade civil dos provedores de Internet (§§ 2, 3 e 7). Para o 3º objetivo é lecionado o conteúdo relativo a dados pessoais e privacidade nas comunicações eletrónicas e sobre programas de computador, bases de dados e direitos de autor na internet (§§ 6 e 7). O 4º objetivo é servido pelos conteúdos da § 5 sobre nomes de domínio na Internet e sinais distintivos. Para o 5º objetivo é lecionada a matéria relativa ao tribunal competente, à lei aplicável e aos meios alternativos de resolução de litígios (§ 8). Finalmente, o objetivo 6º será alcançado através do estudo do crime informático e dos aspetos de ética e deontologia da segurança informática (§§ 9 e 10).

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

To achieve the 1st goal it is taught the object, sources and nature of Computer Law (§ 1). Matters relating to e-commerce and the country of origin, e-contracts, including certification of digital signatures and consumer protection, and civil liability of Internet service providers (§§ 2, 3 and 7) are taught to reach the 2nd objective. For the 3rd goal it is provided the content concerning personal data and privacy in electronic communications as well as the legal protection of computer programs, databases and copyright on the Internet (§§ 6 and 7). The 4th goal is served by the contents of § 5 on domain names on the Internet and distinctive signs. For the 5th goal it is taught the contents concerning the competent court, applicable law and alternative means of dispute resolution (§ 8). Finally, the 6th goal will be achieved through the study of computer crime and aspects of ethics and deontology of computer security (§§ 9 and 10)

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manha, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes

Exame 50%; Projeto 50%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 50%

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

O método de ensino do Direito da Informática e da Segurança Informática é teórico-prático, analisando-se em duas componentes fundamentais. Por um lado, é usado o método expositivo para fazer uma breve exposição das matérias, apresentando os problemas e os respetivos instrumentos legais, e expondo sucintamente os seus princípios fundamentais. Por outro lado, é proposta a análise de jurisprudência, sobretudo acórdãos do Tribunal de Justiça da União Europeia, promovendo desse modo uma aprendizagem dinâmica dos regimes jurídicos aplicáveis a partir de casos concretos. Será privilegiada a utilização da informática para a realização de pesquisa de materiais de estudo, incluindo legislação, jurisprudência e bibliografia.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The teaching method of Computer Law and Computer Security is both theoretical and practical. It has two key components. On the one hand, the lecture method is used to make a brief presentation of the contents, presenting the problems and the legal instruments found to solve them and briefly exposing its basic principles. On the other hand, it undertakes case-law analysis, especially the relevant rulings of the European Court of Justice, thus providing a dynamic learning of the legal regimes applicable to and from concrete cases. Attention will turn to the use of information technology to carry out research of study materials, such as legislation, case law and literature.

3.3.9. Bibliografia principal:

Base: Martins, Lourenço; Marques, Garcia, Direito da Informática, 2.ª ed., Almedina, 2006

Monteiro, António Pinto, "A responsabilidade civil na negociação informática", Direito da Sociedade da Informação, vol. I, Coimbra Editora, 1999, 229-239.

Monteiro, J. Sinde, "Direito Privado Europeu – Assinatura Electrónica e Certificação (A Directiva 1999/93/CE e o

Decreto – Lei n.º 290 – D/99, de 2 de Agosto)” Revista de Legislação e de Jurisprudência. n.º 3918 (2001), 262
Pereira, Alexandre Dias, Direito da Informática – Elementos, Coimbra, 2016 (em preparação

Mapa IV - Segurança e Privacidade / Security and Privacy

3.3.1. Unidade curricular:

Segurança e Privacidade / Security and Privacy

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

João Paulo da Silva Machado Garcia Vilela

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

António Jorge Costa Granjal (25%)

Tiago José dos Santos Martins da Cruz (25%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo a aquisição de conhecimentos sobre técnicas e modelos avançados para segurança e privacidade da informação e comunicações. Os alunos deverão dominar modelos económicos para examinar a relação custo-benefício em segurança da informação, técnicas para anonimização e aferição do nível de segurança de comunicação de dados anonimizados, bem como metodologias de processamento de dados (data mining e machine learning) para segurança e privacidade, em particular aplicadas à deteção de intrusões e autenticação. Além da aquisição dos fundamentos nestas áreas, pretende-se que o aluno adquira competências de análise e validação dos modelos e técnicas de segurança apresentados através do estudo de casos práticos de aplicação.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The aim of this curricular unit is to provide knowledge on advanced models and techniques for security and privacy of data and communications. It is expected that students master the use of economic models to examine the cost-benefit tradeoff of information security, techniques for anonymization and assessment of the security level of anonymized data communications, as well as data mining methods for security and privacy, particularly when applied to intrusion detection and authentication systems. Beyond acquiring knowledge on the fundamentals of these areas, students are expected to gain competences in the analysis and validation of the presented security models and techniques through their application in real-world case studies.

3.3.5. Conteúdos programáticos:

- *Economia de segurança e privacidade.*
- *Teoria de jogos.*
- *Aspetos económicos de investimento em segurança.*
- *Seguros e gestão de riscos de segurança.*
- *Aspetos económicos de divulgação de vulnerabilidades de segurança e privacidade.*

- *Técnicas de privacidade e anonimato.*
- *Princípios de privacidade: k-anonymity, l-diversity, t-closeness.*
- *Gestão de informação – anonimização e de-anonimização.*
- *Anonimato em comunicações: crowds, onion routing, ToR.*
- *Anonimato em redes sociais e móveis.*

- *Processamento e análise de dados para segurança e privacidade.*
- *Sistemas de deteção de intrusões.*
- *Autenticação e mecanismos de biometria.*
- *Técnicas experimentais em segurança informática*

3.3.5. Syllabus:

- *Economics of information security and privacy.*
- *Game theory.*
- *Economics of security investment.*
- *Cyber-insurance for security risk management.*
- *Economics of security and privacy vulnerability disclosure.*

- *Privacy and anonymity techniques.*
- *Privacy principles: k-anonymity, l-diversity, t-closeness.*
- *Data management – anonymization and de-anonymization.*
- *Anonymous networking: crowds, onion routing, ToR.*

- **Security and privacy aspects of social and mobile networks.**

- **Data processing and analysis for security and privacy.**
- **Intrusion detection systems.**
- **User authentication and biometrics.**
- **Experimental techniques in informatics security**

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área dos modelos e metodologias de segurança da informação. Nesse sentido, são abordados modelos e técnicas que permitem avaliar o cumprimento de requisitos como o adequado investimento/retorno de investimento em segurança, técnicas para anonimização e processamento de dados para segurança e privacidade

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área dos modelos e metodologias de segurança da informação. Nesse sentido, são abordados modelos e técnicas que permitem avaliar o cumprimento de requisitos como o adequado investimento/retorno de investimento em segurança, técnicas para anonimização e processamento de dados para segurança e privacidade

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes

Exame 50%; Projeto 25%; Resolução de problemas 25%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 25%; Problem resolving report 25%

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

A estratégia e o método de ensino adotado procuram envolver os alunos no processo de aprendizagem e na sua valorização pessoal, e assim levar ao desenvolvimento, para além de competências técnicas específicas, de competências genéricas, de natureza instrumental, pessoal e sistémicas.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolução de problemas, tomada de decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, e em aplicar na prática os conhecimentos teóricos adquiridos nas aulas teóricas e teórico-práticas.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolver problemas, decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, em aplicar na prática os conhecimentos teóricos adquiridos nas aulas.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The strategy and teaching methodology adopted seek to include students in the learning, leading to the development of not only specific technical competences, but also generic competences of instrumental, personal and systemic nature.

Examples and practical exercises presented in the classes provide the conditions for the analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations and applying theoretical concepts learned to practical situations.

With the practical group project, students can develop their analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations, applying theoretical concepts learned to practical situations, planning and management as well as researching.

3.3.9. Bibliografia principal:

- Lawrence Gordon and Martin Loeb, “Managing Cybersecurity Resources: A Cost-Benefit Analysis”, McGraw-Hill, 2005
- Ross Anderson, “Security Engineering”, Wiley, 2008
- Ross Anderson, Rainer Böhme, Richard Clayton, Tyler Moore, “Security Economics and the Internal Market”, ENISA, 2008
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, “Security in Computing”, Prentice Hall, 2015
- Shimon K. Modi, “Biometrics in Identity Management: Concepts to Applications”, Artech House, 2011
- William Stallings, Lawrie Brown, “Computer Security: Principles and Practice”, Pearson, 2014
- Sumeet Dua, Xian Du, “Data Mining and Machine Learning in Cybersecurity”, CRC Press, 2011

Mapa IV - Segurança em Tecnologias da Informação / Communication System Security**3.3.1. Unidade curricular:**

Segurança em Tecnologias da Informação / Communication System Security

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Edmundo Heitor da Silva Monteiro

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

António Jorge Costa Granjal (50%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular pretende dotar os alunos das capacidades técnicas necessárias à administração da segurança em tecnologias da informação. É dada particular ênfase os aspetos relativos aos sistemas de comunicação, redes informáticas, aos sistemas de informação organizacionais e aos sistemas distribuídos no geral. É objectivo compreender o conjunto de métodos e ferramentas que permitam capacitar os alunos para a realização das tarefas normalmente associadas a um especialista em Segurança em Tecnologias da Informação.

Os objectivos concretos da disciplina são os seguintes:

- *Segurança em Redes e Sistemas de Comunicação, com ênfase na Segurança na Internet*
- *Segurança das Aplicações, com ênfase nos aspectos de Privacidade dos Utilizadores*
- *Segurança de Sistemas de Informação, com ênfase nos aspectos relativos à Segurança em Bases de Dados, Comércio electrónico e sistemas distribuídos no geral.*

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The main objectives of this course are the following:

- *Informatics security*
- *Network security*
- *Security of informatics systems*

The student will gain knowledge and decision skills in the following areas:

- *Security mechanisms and technologies*
- *Most relevant security tools*
- *Security in informatics systems*
- *Security problems resolution in informatics systems*
- *Definition and implementation of organizational security politics*
- *Performance of tasks concerning security monitoring and auditing*
- *Conception and installation of security solutions for informatics networks*

3.3.5. Conteúdos programáticos:

1. *Aspectos fundamentais*
2. *Segurança em sistemas de comunicação*
3. *Segurança em sistemas de informação*
4. *Segurança na Internet*
5. *Segurança em comércio e transacções electrónicas*
6. *Controlo de acesso e detecção e prevenção de intrusões*
7. *Auditorias de segurança e aspetos organizacionais*

3.3.5. Syllabus:

1. *Basic information security concepts*
2. *Security in communication systems*
3. *Security in information systems*

4. Internet security
5. Security in e-commerce and electronic transactions
6. Access control, intrusion detection and prevention
7. Security audits and organizational aspects

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

O capítulo 1 debruça-se no essencial sobre os conceitos básicos e as metodologias e ferramentas fundamentais para a construção de infraestruturas informáticas organizacionais que sejam seguras. Os capítulos 2, 3 e 4 focam dimensões diferentes da segurança, em diferentes níveis de suporte da infraestrutura, nomeadamente: a segurança nas comunicações e nas ligações através da Internet, e a segurança nos sistemas de informação, incluindo a camada de dados nos os sistemas multicamada distribuídos. O capítulo 5 foca nos aspetos relativos às transações financeiras e comércio electrónico. O capítulo 6 foca-se nos aspectos relativos à detecção de intrusões e controlo de acesso em infraestruturas de comunicação e informação. Finalmente, o capítulo 7 debruçam-se sobre diferentes aspectos a nível organizacional, desde a realização da auditorias, até à aplicação de normas e linhas orientadoras.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

Chapter 1 essentially focus on the basic concepts and on the fundamental methodologies and tools for deploying secure organizational computer infrastructures. Chapters 2 to 4 focus different security dimensions, at different levels of the infrastructure, namely: data layer, distributed systems, and external links via the Internet. On the other hand, chapter 5 addresses the detection of intrusions and access control. Finally, chapter 7 focus on different aspects at the organizational level, from audits to the application standards and guidelines

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manha, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes

Exame 25%; Projeto 50%; Trabalho de síntese 25%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers

Exam 25%; Project 50%; Synthesis work 25%

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

Nesta disciplina o método de ensino fomenta o envolvimento do aluno desde o início da disciplina, procurando uma aprendizagem de conhecimentos e competências continua. É com este objectivo que são propostos trabalhos práticos que abordam aspectos centrais dos conceitos leccionados. A metodologia adoptada pretende induzir o desenvolvimento de algumas competências genéricas, de natureza instrumental, pessoal e sistémicas. Com o conhecimento e a compreensão das matérias lecionadas nas aulas teóricas e os exercícios de aplicação prática que se procura que os alunos resolvam nas aulas práticas estão criadas as condições para o desenvolvimento das competências em resolver problemas, capacidade de abstração e generalização, em raciocínio matemático e crítico, em aplicar na prática os conhecimentos teóricos e, num nível mais avançado, da competência em análise e síntese. Estas últimas competências são ainda reforçadas pelos trabalhos práticos propostos que obrigam à instanciação dos conhecimentos em domínios específicos.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

In this course the teaching approach stimulates continuous student involvement in order to achieve a continuous learning and acquisition of knowledge and competences. It is with this goal in mind that students have to perform regular homework assignments, usually motivated by discussions or doubts raised in theoretical classes, as well as to solve problems. The adopted teaching strategy intends to foster the acquisition of some generic instrumental personal and systematic competences.

With the knowledge and comprehension of the topics taught in the theoretical classes and the exercises developed in the theoretical-practical classes, conditions are raised to develop competences in problem solving, capacity of abstraction and generalization, in mathematical and critical reasoning, practical application of the theoretical

knowledge acquired, and, at an advanced level, analysis and synthesis. The latter competences are further developed through the research in finding solutions for practical problems

3.3.9. Bibliografia principal:

- **André Zúquete, *Segurança em Redes Informáticas* (4ª edição), FCA Editora, 2014.**
- **Edmundo Monteiro e Fernando Boavida, *Engenharia de Redes Informáticas*, FCA Editora, 2011 (cap 7)**
- **Jorge Granjal, *Gestão de Sistemas e Redes em Linux*, FCA Editora 2013.**
- **Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, 2004.**
- **William Stallings, *Cryptography and Network Security: Principles and Practice* (6th edition), Prentice Hall, 2013**
- **Alberts, C.J. and Dorofee, A.J., "Managing Information Security Risks: The Octave Approach", ISBN: 9780321118868, SEI Series in Software Engineering, 2003**

Mapa IV - Conceção e Desenvolvimento de Infraestruturas Seguras /Designing and Building Secure Infrastructures

3.3.1. Unidade curricular:

Conceção e Desenvolvimento de Infraestruturas Seguras /Designing and Building Secure Infrastructures

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Paulo Alexandre Ferreira Simões

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

António Jorge Costa Granjal (25%)

Tiago José dos Santos Martins da Cruz (25%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo a aquisição de conhecimentos sobre técnicas avançadas para o desenvolvimento de infraestruturas seguras. No final da cadeira os alunos deverão dominar os diferentes aspetos do desenvolvimento de infraestruturas com requisitos de segurança estritos, sendo capazes de identificar alternativas e de escolher e aplicar as mais adequadas a cada situação. Além da aquisição dos fundamentos nesta área, pretende-se que o aluno adquira competências na análise, desenho, desenvolvimento e validação de infraestruturas críticas da aplicação em casos de estudo reais.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The aim of this curricular unit is to provide knowledge on advanced techniques for the development of secure infrastructures. It is expected that students master the different aspects of developing software with security requirements, being able to identify existing alternatives and selecting and implementing the most adequate ones. The course considers the different phases of the secure infrastructure development lifecycle, from requirements to evaluation

3.3.5. Conteúdos programáticos:

- ***Desenho de infraestruturas seguras para ambientes Cloud***
- ***Sistemas de deteção e prevenção de intrusão (IDS/IPS)***
- ***Mecanismos de alarmística***
- ***Segurança em ambientes móveis***
- ***Segurança na Internet das Coisas (IoT)***
- ***Proteção de redes de controlo industrial e outras infraestruturas críticas***
- ***Serviços de comunicação para cenários de Public Protection & Disaster Relief***
- ***Segurança de serviços de rede***

3.3.5. Syllabus:

- ***Design of secure infrastructures for Cloud environments***
- ***Intrusion detection and prevention systems (IDS/IPS)***
- ***Alarms mechanisms***
- ***Security in mobile environments***
- ***Security in the Internet of Things (IoT)***
- ***Protection of industrial control networks and other critical infrastructures***
- ***Communication services for scenarios of Public Protection & Disaster Relief***
- ***Security in communication services***

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área da auditoria de

segurança. Nesse sentido, são abordadas as técnicas, normas, procedimentos e ferramentas para a realização de auditorias de segurança informática em organizações. Os conhecimentos adquiridos serão postos em prática pelos alunos num caso de estudo.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

This curricular unit aims to acquire knowledge and skills in the security audit area. In this sense, techniques, standards, procedures and tools to carry out computer security audits in organizations are addressed. The knowledge gained will be implemented by the students on a case study .

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes.

Exame 50%; Projeto 50%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 50%; Project 50%

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

A estratégia e o método de ensino adotado procuram envolver os alunos no processo de aprendizagem e na sua valorização pessoal, e assim levar ao desenvolvimento, para além de competências técnicas específicas, de competências genéricas, de natureza instrumental, pessoal e sistémicas.

Serão criadas condições para o desenvolvimento das competências para análise e síntese, resolução de problemas, tomada de decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, e em aplicar na prática os conhecimentos teóricos adquiridos.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolver problemas, decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, em aplicar na prática os conhecimentos teóricos adquiridos nas aulas, planear e gerir, e investigar.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The strategy and teaching methodology adopted seek to include students in the learning, leading to the development of not only specific technical competences, but also generic competences of instrumental, personal and systemic nature.

Examples and practical exercises presented in T and TP classes provide the conditions for the analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations and applying theoretical concepts learned to practical situations.

With the practical group project, students can develop their analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations, applying theoretical concepts learned to practical situations, planning and management as well as researching.

3.3.9. Bibliografia principal:

Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.

Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley, 2010.

Fei Hu, Security and Privacy in Internet of Things (IoT): Models, Algorithms, and Implementations, CRC Press 2016.

F. Flammini, Critical Infrastructure Security, Assessment, Prevention, Detection, Response, WIT Press 2012.

Sajal K. Das, Krishna Kant and Nan Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Science Direct, 2012.

Mapa IV - Auditoria de Segurança / Security Auditing

3.3.1. Unidade curricular:

Auditoria de Segurança / Security Auditing

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Marco Paulo Amorim Vieira

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

Paulo Alexandre Ferreira Simões (50%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Esta unidade curricular tem como objetivo fazer a integração dos conhecimentos obtidos nas várias disciplinas do MSI em contexto de auditoria, num caso de estudo a definir para cada grupo de alunos e tendo em conta as metodologias, procedimento, normas e ferramentas para realização de auditoria de segurança em organizações. Espera-se que os estudantes adquiram/desenvolvam as seguintes competências-chave:

- *Competências em avaliação e gestão de cibersegurança, análise e gestão de risco de segurança informática, avaliação e gestão de risco de segurança, no âmbito de sistemas informáticos e das organizações em que estes se inserem.*
- *Aplicação prática do conhecimento teórico na avaliação e gestão de segurança, competências de análise e síntese, e capacidade de autoaprendizagem em novos contextos no domínio da segurança informática.*
- *Resolução de problemas, comunicação oral e escrita, relações interpessoais e capacidade de trabalho em equipa.*

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

This curricular unit aims to integrate the knowledge obtained in the various disciplines of MSI in the audit context , a case study to be defined for each group of students, taking into account the methodologies, procedures, standards and tools for conducting security auditing in organizations. It is also intended that the students acquire/develop the following core competencies:

- *Skills on cyber security assessment and management, security risk analysis, security risk assessment and management at organization and system level.*
- *Practical application of the theoretical knowledge on security assessment and management, competences in analysis and synthesis, critical reasoning, and self-learning.*

and the following secondary competencies:

- *Problem solving, oral and written communication, interpersonal relations, and team work.*

3.3.5. Conteúdos programáticos:

- *Introdução à auditoria de segurança informática.*
- *Certificação de segurança da informação.*
- *Normas e procedimentos de certificação e auditoria de segurança .*
- *Ferramentas de auditoria informática.*
- *Ética e deontologia na auditoria informática.*
- *Casos de estudo*

3.3.5. Syllabus:

- *Introduction to IT security auditing.*
- *Information security certification.*
- *Standards and certification procedures and security audit.*
- *Tools of communications and information security auditing .*
- *Ethics and deontology in computer audit.*
- *Study cases*

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta unidade curricular tem como objetivo a aquisição de conhecimento e competências na área da auditoria de segurança. Nesse sentido, são abordadas as técnicas, normas, procedimentos e ferramentas para a realização de auditorias de segurança informática em organizações. Os conhecimentos adquiridos serão postos em prática pelos alunos num caso de estudo.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

This curricular unit aims to acquire knowledge and skills in the security audit area. In this sense, techniques, standards, procedures and tools to carry out computer security audits in organizations are addressed. The knowledge gained will be implemented by the students on a case study

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas teóricas (T) : apresentações e discussão sobre os tópicos da unidade curricular.

Aulas práticas (PL): aplicação dos conceitos teóricos em exercícios e projetos.

As aulas teóricas serão também difundidas por teleconferência e serão gravadas para os alunos poderem acompanhar remotamente.

As aulas práticas serão marcadas, preferencialmente, às sextas-feiras de manhã, podendo também os trabalhos práticos ser desenvolvidos pelos alunos, em regime remoto e assíncrono, com apoio remoto dos docentes.

Exame 25%; Projeto 75%

3.3.7. Teaching methodologies (including assessment):

Lecture classes (T): presentation and discussion around the topics of the course.

Lab classes (PL): application of theoretical concepts in projects.

The MSI theoretical classes will take place, preferably, Friday afternoon and Saturday morning. Theoretical classes will also be broadcast by teleconference and will be recorded to allow the students to follow the classes remotely.

The practical classes will be preferably booked Friday morning. The practical assignments may also be developed by the students in remote and asynchronous mode with remote support of teachers.

Exam 25%; Project 75%

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

A estratégia e o método de ensino adotado procuram envolver os alunos no processo de aprendizagem e na sua valorização pessoal, e assim levar ao desenvolvimento, para além de competências técnicas específicas, de competências genéricas, de natureza instrumental, pessoal e sistémicas.

Serão criadas as condições para o desenvolvimento das competências para análise e síntese, resolução de problemas, tomada de decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, e em aplicar na prática os conhecimentos teóricos adquiridos nas aulas teóricas e teórico-práticas.

Serão criadas as condições para o desenvolvimento das competências de análise e síntese, resolver problemas, decisão, raciocínio crítico, aprendizagem autónoma, adaptabilidade a novas situações, em aplicar na prática os conhecimentos teóricos adquiridos. A escrita do relatório cria as condições para que os alunos adquiram competências em aprendizagem autónoma em comunicação escrita. As apresentações orais das metas do projeto ajudam a desenvolver a capacidade de explicar soluções e descobertas a especialistas e não especialistas.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The strategy and teaching methodology adopted seek to include students in the learning, leading to the development of not only specific technical competences, but also generic competences of instrumental, personal and systemic nature.

Examples and practical exercises presented in T and TP classes provide the conditions for the analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations and applying theoretical concepts learned to practical situations.

With the practical group project, students can develop their analysis and synthesis, problem solving, decision making and critical thinking, autonomous learning, adaptability to new situations, applying theoretical concepts learned to practical situations, planning and management as well as researching. The written report creates the conditions for students to acquire competences in autonomous learning in written communication. The oral presentations help students to better explain solutions and finds to both experts and non-experts

3.3.9. Bibliografia principal:

ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing, 2011.

Chris Jackson, Network Security Auditing Tools and Techniques, 2010.

Kvong, Javier F., Computer Auditing, Security, and Internal Control Manual, 2015.

Hassan A. Afyouni, Database Security and Auditing: Protecting Data Integrity and Accessibility, 2013.

Richard E. Cascarino, Auditor's Guide to Information Systems Auditing, 2007.

Robert E. Davis, Auditing Information Security Management, 2008

Mapa IV - Seminários de Acompanhamento / Followup Seminars**3.3.1. Unidade curricular:**

Seminários de Acompanhamento / Followup Seminars

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Carlos Nuno Bizarro e Silva Laranjeiro

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:

Tiago José dos Santos Martins da Cruz (50%)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

A Internet está a evoluir com novos requisitos e aplicações, criando novos desafios na área da segurança e privacidade da informação e das comunicações.

Esta unidade curricular visa explorar conceitos fundamentais e tópicos avançados na área científica da segurança informática, fornecendo uma visão abrangente do estado da arte, da oferta tecnológica, incluindo questões de investigação em aberto e projetos de investigação.

Estes objetivos apoiarão os alunos na formação avançada em segurança informática, no aprofundamento das suas competências de análise crítica de trabalho científico, escrita científica, apresentação e discussão orais, e revisão científica entre pares, que constituirão competências chave para a realização da dissertação e a publicação dos resultados de investigação.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The Internet is evolving with new requirements and applications, creating new challenges in the areas of security and privacy of communications and information.

This course aims to exploit fundamental concepts and advanced topics in the scientific area of informatics security, providing a comprehensive view of the state-of-the-art, including relevant open research questions and research projects.

These objectives will assist the students in gaining advanced knowledge of their area of research, further developing their competencies in the areas of critical analysis of scientific work, scientific writing, oral presentation and discussion, scientific peer reviewing, which will be key assets for the successful completion of the dissertation and the publication of the research results.

3.3.5. Conteúdos programáticos:

Serão explorados tópicos nas seguintes áreas:

- Metodologias de investigação***
- Motivações e desafios para a segurança informática***
- Fundamentos de segurança, privacidade e confiança***
- Arquiteturas resilientes, confiáveis e energeticamente eficientes para a Internet***
- Segurança no desenvolvimento de software e sistemas informação***
- Segurança em redes de sensores sem fios, IoT***
- Avaliação de segurança e confiabilidade de sistemas***
- Segurança em infraestruturas críticas***
- Segurança em infraestruturas e sistemas para computação na nuvem***
- Outros tópicos relacionados com Segurança Informática***

Outros tópicos poderão ser alvo de análise e discussão, dentro da área genérica da segurança nas comunicações e software, dependendo do seu interesse para o alcance dos objetivos do curso.

3.3.5. Syllabus:

They will be explored topics in the following areas :

- Research methodologies***
- Motivations and challenges for computer security***
- Security, privacy and trust fundamentals***
- Resilient Architectures, reliable and energy efficiency for the Internet***
- Secure software and information systems development***
- Security in wireless sensor networks and IoT***
- Security and reliability evaluation***
- Security in critical infrastructures***
- Security for cloud computing infrastructures***
- Other topics related to communications and software security***

Other topics will be the subject of analysis and discussion within the area of communications and software security, depending on the interest to the achievement of the course objectives.

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade

curricular:

Os tópicos a abordar são atuais e estão fortemente ligados com a atividade de investigação do CISUC e, consequentemente, com a atividade de investigação relacionada com o programa quadro H2020 na área das segurança em tecnologias da informação e comunicação. Através da apresentação e discussão destes tópicos fornece-se aos alunos uma visão atualizada dos desafios de investigação e potenciam-se competências de análise e síntese, comunicação oral e escrita, raciocínio crítico, aprendizagem autónoma, e investigação.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

The topics addressed in the course are up-to-date and strongly related to the research activity carried out at CISUC and, consequently, to the H2020 European Framework research. Through presentation and discussion of these topics, the students are provided with an updated view on ICT research challenges and develop competences in analysis and synthesis, written and oral communication, critical reasoning, autonomous learning, and research.

3.3.7. Metodologias de ensino (avaliação incluída):

Aulas Serão desenvolvidas duas atividades complementares:

1 – Seminários (30h): apresentação e discussão de tópicos relacionados com a investigação a desenvolver pelos estudantes no âmbito das suas dissertações.

2 – Elaboração de um artigo de síntese, revisão pelos pares, apresentação e discussão numa workshop.

Avaliação:

- Participação ativa nos seminários e apresentação de questões: 10%

- Qualidade das revisões dos artigos: 20%

- Artigo de síntese (qualidade global, apresentação, discussão): 70%

É obrigatória a presença em 75% nos seminários (pode ser por teleconferência)

3.3.7. Teaching methodologies (including assessment):

Two complementary activities will be developed:

1 - Seminars (30h) : presentation and discussion of topics related to the curricular dissertation research work.

2 - Preparation of a survey article, peer review, presentation and discussion at a workshop .

Evaluation:

- Active participation in seminars and presentation of issues: 10 %

- Quality of reviews of articles: 20 %

- Drafted Article (overall quality , presentation, discussion): 70 %

It is compulsory to attend 75 % in seminários (may be by teleconference)

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

Sendo esta uma disciplina de apoio ao desenvolvimento da investigação, é fundamental que os alunos estejam a par das metodologias e das questões tecnológicas e de investigação mais atuais na área em causa e, para além disso, que adquiram competências para estudar uma dada área, analisar a investigação que nela é feita e ter uma visão crítica do estado da arte. A discussão, escrita e apresentação de artigos é fundamental para exercitar essas competências.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

Being this a course to develop research skills, it is fundamental that the students are abreast with the current tecnológicas and research issues in the area and, in addition, acquire competences to study a given area, analyze the research being done in it, and form a critical view on the state-of-the-art. Discussing, writing and presenting papers is fundamental in order to exercise these competences.

3.3.9. Bibliografia principal:

Para cada tópico abordado será fornecida aos alunos uma lista de referências.

For each topic to be addressed, a list of references will be provided to the students

Mapa IV - Dissertação/Estágio / Thesis/Projet**3.3.1. Unidade curricular:**

Dissertação/Estágio / Thesis/Projet

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:

Coordenador do MSI | MSI Coordinator**3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:**

Edmundo Heitor da Silva Monteiro, Henrique Santos Carmo Madeira, Marco Paulo Amorim Vieira, Paulo Alexandre Ferreira Simões, João Paulo da Silva Machado Garcia Vilela, António Jorge Costa Granjal, Carlos Nuno Bizarro e Silva Laranjeiro, Tiago José dos Santos Martins da Cruz, Nuno Manuel dos Santos Antunes (all O:30)

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Os objectivos principais do estágio são os seguintes:

- *Técnicas de projeto e desenvolvimento de segurança em sistemas informação e comunicação*
- *Realização de projetos de desenvolvimento tecnológico*
- *Contacto com a elaboração de projetos em ambiente empresarial*
- *Iniciação a atividades de investigação de base e aplicada*
- *Integração no mercado laboral*
- *Realização de um documento com a proposta de estágio / dissertação incluindo os seguintes aspectos:*
 - *Análise do estado da arte*
 - *Escolha justificada das ferramentas e metodologias a utilizar*
 - *Análise de requisitos relativamente ao tema a desenvolver*
 - *Especificação de alto nível do sistema a desenvolver / trabalho a realizar incluindo objectivos concretos calendarização para o segundo semestre*

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):

The main goals of this course are the following:

- *Project techniques and development of security in information and communication systems*
- *Development of technological projects*
- *Experience of project development in enterprise environment*
- *Experience with basic and applied research*
- *Integration in the working world*
- *Writing of a document with the internship / thesis proposal including the following topics:*
 - *Analysis of the state of the art*
 - *Justified selection of tools and methodologies to be used*
 - *Requirements analysis related with the topic to be developed*
 - *High level specification of the system to be developed / work to be performed including specific objectives and scheduling for the second semester*

3.3.5. Conteúdos programáticos:

Todos os conteúdos na área da segurança de informação e comunicações com ênfase para as metodologias de concepção e acompanhamento de projetos na área

3.3.5. Syllabus:

All the contents in the area of information and communication security with emphasis on the conception and follow-up of projects in the area

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:

Esta disciplina visa a integração dos conhecimentos obtidos na licenciatura e mestrado e a transição dos estudantes para o mercado de trabalho ou para o 3º ciclo

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:

This course targets the integration of the knowledge obtained in the BsC and MsC courses and the transition of the students to the working field or for the 3rd cycle.

3.3.7. Metodologias de ensino (avaliação incluída):

Desenvolvimento em contexto de empresa ou laboratório de investigação acompanhado pelo orientador da instituição e pelo orientador do DEI em caso de estágios realizados em instituições externas.

A avaliação no final do primeiro semestre é realizada com base no documento da proposta e numa apresentação realizada pelo aluno, por um júri nomeado pela Comissão Científica que integra o presidente, o vogal e os orientadores, de acordo com o regulamento da disciplina. A avaliação é qualitativa com cinco níveis. Além da avaliação, são também fornecidas ao aluno um conjunto de comentários / recomendações que deverão ser tidas em consideração durante o segundo semestre.

A avaliação no final do segundo semestre é realizada com base no documento do estágio / dissertação e numa apresentação realizada pelo aluno, por um júri nomeado pela Comissão Científica que integra o presidente, o vogal e o orientador, de acordo com o regulamento da unidade curricular.

Projeto 100%

3.3.7. Teaching methodologies (including assessment):

Development in a company or research laboratory under the supervision of the institution advisor and by an advisor from DEI for the internships in companies.

The evaluation at the end of the first semester is based on the proposal document and a presentation by the student, by a jury nominated by the Scientific Commission that includes the president, non-supervisor jury member, and the supervisors, according to the rules of this course. Evaluation is qualitative with five levels. With the evaluation, the student will receive comments / recommendations that must be taken into consideration in the second semester.

The final evaluation will be based on the Dissertation and in a presentation held the student to the jury appointed by the Scientific Committee. The jury includes the president, the vowel and the supervisor according to the rules of course.

Project 100%

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

As metodologias de ensino estão em sintonia com concretização dos objectivos da disciplina de estágio / dissertação.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:

The teaching methodologies are inline with the fulfilment of the objectives of this course.

3.3.9. Bibliografia principal:

Dependente de cada estágio / dissertação | Depend on the type and nature of the internship / thesis.

4. Descrição e fundamentação dos recursos docentes do ciclo de estudos

4.1 Descrição e fundamentação dos recursos docentes do ciclo de estudos

4.1.2 Equipa docente do ciclo de estudos

4.1.2. Equipa docente do ciclo de estudos / Teaching staff of the study programme

Nome / Name	Grau / Degree	Área científica / Scientific Area	Regime de tempo / Employment link	Informação/ Information
Alexandre Libório Dias Pereira	Doutor	Direito	100	Ficha submetida
António Jorge da Costa Granjal	Doutor	Engenharia Informática	100	Ficha submetida
Carlos Nuno Bizarro e Silva Laranjeiro	Doutor	Ciências e Tecnologias da Informação	100	Ficha submetida
Edmundo Heitor da Silva Monteiro	Doutor	Engenharia Eletrotécnica – Opção de Informática	100	Ficha submetida
Henrique Santos do Carmo Madeira	Doutor	Engenharia Eletrotécnica – Opção de Informática	100	Ficha submetida
João Paulo da Silva Machado Garcia Vilela	Doutor	Ciência de Computadores	100	Ficha submetida
Marco Paulo Amorim Vieira	Doutor	Informática	100	Ficha submetida
Tiago José dos Santos Martins da Cruz	Doutor	Engenharia Informática	100	Ficha submetida
Paulo Alexandre Ferreira Simões	Doutor	Engenharia Informática	100	Ficha submetida
Nuno Manuel dos Santos Antunes	Doutor	Ciências e Tecnologias da Informação	100	Ficha submetida
(10 Items)			1000	

<sem resposta>

4.2. Dados percentuais dos recursos docentes do ciclo de estudos

4.2.1. Corpo docente próprio do ciclo de estudos

4.2.1. Corpo docente próprio do ciclo de estudos / Full time teaching staff

Corpo docente próprio / Full time teaching staff	ETI / FTE	Percentagem* / Percentage*
Nº de docentes do ciclo de estudos em tempo integral na instituição / No. of full time teachers:	10	100

4.2.2. Corpo docente do ciclo de estudos academicamente qualificado

4.2.2. Corpo docente do ciclo de estudos academicamente qualificado / Academically qualified teaching staff

Corpo docente academicamente qualificado / Academically qualified teaching staff	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos com o grau de doutor (ETI) / Teaching staff with a PhD (FTE):	10	100

4.2.3. Corpo docente do ciclo de estudos especializado

4.2.3. Corpo docente do ciclo de estudos especializado / Specialized teaching staff

Corpo docente especializado / Specialized teaching staff	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos com o grau de doutor especializados nas áreas fundamentais do ciclo de estudos (ETI) / Teaching staff with a PhD, specialized in the main areas of the study programme (FTE):	9	90
Especialistas, não doutorados, de reconhecida experiência e competência profissional nas áreas fundamentais do ciclo de estudos (ETI) / Specialists, without a PhD, of recognized professional experience and competence, in the main areas of the study programme (FTE):	0	0

4.2.4. Estabilidade do corpo docente e dinâmica de formação

4.2.4. Estabilidade do corpo docente e dinâmica de formação / Teaching staff stability and training dynamics

Estabilidade e dinâmica de formação / Stability and training dynamics	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos em tempo integral com uma ligação à instituição por um período superior a três anos / Full time teaching staff with a link to the institution for a period over three years:	10	100
Docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (ETI) / Teaching staff registered in a doctoral programme for more than one year (FTE):	0	0

4.3. Procedimento de avaliação do desempenho

4.3. Procedimento de avaliação do desempenho do pessoal docente e medidas para a sua permanente atualização:

O procedimento de avaliação dos docentes da Universidade de Coimbra (UC) tem por base o disposto no "Regulamento de Avaliação de Desempenho dos Docentes da Universidade de Coimbra", Regulamento n.º 398/2010 publicado no DR n.º 87, 2.ª Série, de 5 de Maio de 2010, retificado no DR. 2.ª Série, de 17 de Maio de 2010. Este regulamento define os mecanismos para a identificação dos objetivos de desempenho dos docentes para cada período de avaliação, explicitando a visão da instituição, nos seus diversos níveis orgânicos, e traçando, simultaneamente, um quadro de referência claro para a valorização das atividades dos docentes, com vista à melhoria da qualidade do seu desempenho. A avaliação do desempenho dos docentes da UC é efetuada relativamente a períodos de três anos e tem em consideração quatro vertentes: investigação; docência; transferência e valorização do conhecimento; gestão universitária e outras tarefas. Relativamente a cada uma das vertentes, a avaliação dos docentes pode incluir duas componentes: avaliação quantitativa e avaliação qualitativa. A avaliação quantitativa tem por base um conjunto de indicadores e de fatores. Cada indicador retrata um aspeto bem definido da atividade do docente e os fatores representam uma apreciação valorativa, decidida pelo Conselho Científico ou pelo Director da Unidade Orgânica (UO) para cada área disciplinar. Os fatores permitem assim ajustar

a avaliação quantitativa ao contexto de cada área. A avaliação qualitativa é efetuada por painéis de avaliadores que avaliam o desempenho do docente em cada vertente.

O processo de avaliação compreende cinco fases (autoavaliação, validação, avaliação, audiência, homologação) e prevê os seguintes intervenientes: Avaliado, Director da UO, Conselho Científico da UO, Comissão de Avaliação da UO, Paineis de Avaliadores, Conselho Coordenador da Avaliação do Desempenho dos Docentes e Reitor. O resultado final da avaliação de cada docente é expresso numa escala de quatro posições: excelente, muito bom, bom e não relevante.

Antes de cada novo ciclo de avaliação, cada UO define, para as suas áreas disciplinares, o conjunto de parâmetros que determinam os novos objetivos do desempenho dos docentes e cada uma das suas vertentes, garantindo, assim, permanente atualização do processo

4.3. Teaching staff performance evaluation procedures and measures for its permanent updating:

The academic staff performance evaluation procedures of the University of Coimbra (UC) are set in the “Regulation of Teachers’ Performance Evaluation of UC” – regulation n.º 398/2010, published on the 5th of May, and amended on the 17th of May.

This regulation defines the mechanisms to identify teachers’ performance goals for each time span of evaluation, clearly stating the institution’s vision, across its different levels, and outlining simultaneously a clear reference board to value teachers’ activities with the purpose to improve their performance. The teachers’ performance evaluation at UC is made on a three years basis and takes into account four dimensions: investigation, teaching, knowledge transfer, university management and other tasks. For each dimension, the teachers’ evaluation may include two variables: quantitative and qualitative. Quantitative evaluation is based on a set of performance indicators and factors. Each performance indicator is a well-defined aspect of the teacher’s activity and the factors represent an evaluation, defined by the Scientific Board or the Director of the Organizational Unit (OU), for each subject area. Thus, factors allow quantitative evaluation to adjust the context of each subject area. The qualitative evaluation is made by a panel of reviewers who evaluate teachers’ performance in each dimension.

The evaluation procedures have five stages (self-evaluation, validation, evaluation, audience, and homologation) and include the following participants: teacher, OUs’ Director, OUs’ Scientific Board, OUs’ Evaluation Commission, Evaluators Panel, Coordinator Council of Teachers’ Performance Evaluation and Rector. The final evaluation of each teacher is expressed in a four point scale: excellent, very good, good and not relevant.

Before each new evaluation cycle each OU identifies, for the subject areas, a set of parameters that define the new goals of teachers’ performance and its components, thus ensuring the continuous updating of the process

5. Descrição e fundamentação de outros recursos humanos e materiais

5.1. Pessoal não docente afeto ao ciclo de estudos:

O pessoal não docente do DEI-UC,, está distribuído por varias áreas de apoio à lecionação: Secretariado (3), Recursos Letivos (1), Investigação (1), Biblioteca do Polo 2 (1), Recursos Informáticos (2). A dedicação do pessoal não docente às varias formações académicas em que o DEI tem responsabilidade é partilhada pelos vários ciclos de estudos com qualificações desdeo 9º ano (assistentes), licenciatura ou mestrado (4 elementos). Os vários ciclos de estudo beneficiam ainda de serviços de limpeza diária a cargo de uma empresa de limpeza contratada pela UC e com serviços afetos ao Departamento de Engenharia Informática.

5.1. Non teaching staff allocated to the study programme:

The administrative staff of the DEI-UC working in full time, spreads its activity over several areas in support of the teaching activities: Secretariat (3), Academic resources (1), Research support (1), Polo 2 Library services (1), IT Resources (3) and technical or operational assistance (4). All the administrative staff members of the DEI have appropriate qualifications for the activities assigned to each one of them, with qualifications ranging from grade nine (assistants) to bachelor or Master degrees (4 staff). All the cycles of study still enjoy daily maid services, in charge of a cleaning company hired by UC and with services allocated to the Department of Informatics Engineering.

5.2. Instalações físicas afetas e/ou utilizadas pelo ciclo de estudos (espaços letivos, bibliotecas, laboratórios, salas de computadores, etc.):

O Departamento de Engenharia Informática está instalado num edifício recente com instalações adequadas às atividades letivas e de investigação. Para o MSI serão disponibilizadas: salas de aula (as necessárias), salas de estudo, Biblioteca do Polo 2, laboratórios de investigação, várias salas de computadores, várias salas com equipamento laboratorial; salas de seminários, 3 salas de videoconferência; sala de Conselho, salas de reuniões, secretariado, gabinetes, bar, cantinas do Polo 2, zonas de convívio de alunos, instalações sanitárias

5.2. Facilities allocated to and/or used by the study programme (teaching spaces, libraries, laboratories, computer rooms, etc.):

The Department of Computer Engineering is housed in a new building with adequate facilities for teaching activities

and research. For the MSI the following facilities be available: classrooms (the necessary) , study rooms, Polo library 2, research laboratories, several computer rooms, several rooms with laboratory equipment, seminar rooms, video conference rooms, meeting rooms, secretariat, offices, bar, canteens, social areas for students, sanitary facilities.

5.3. Indicação dos principais equipamentos e materiais afetos e/ou utilizados pelo ciclo de estudos (equipamentos didáticos e científicos, materiais e TICs):

Cluster de alto desempenho de suporte a atividades de investigação, composto por 1 servidor e 30 nós com máquinas virtuais Equipamento de segurança de redes 3 Bastidores de comunicações 12 Equipamento de controlo de acessos RFID Equipamento de videovigilância CCTV Servidores de máquinas Virtuais – VMWare ESX 3 Sala equipada com 12 Routers Cisco 1700 1 Sala equipada com 6 Switches 3Com 4200 1 Sala equipada com 12 Access Points Linksys 1 Salas equipadas com PC com Windows XP e Linux Fedora 12 Sala de videoconferência com suporte de IP 5 Sala de aulas com suporte de videoconferência em IP 1 Equipamento de gestão de videoconferências – MCU 1 Equipamento de gravação de videoconferências – IPVRC 1 Quiosques multimédia 3 Pontos de acesso a Internet físicos 850 Pontos de Acesso Wireless (APs) 26 Equipamentos de projeção 35

5.3. Indication of the main equipment and materials allocated to and/or used by the study programme (didactic and scientific equipments, materials and ICTs):

High performance cluster for the support of research activities, composed by 1 server and 30 nodes with virtual machines Network security equipment 3 Communications racks 12 RFID1 access control equipment CCTV surveillance equipment 1 Room equipped with 18 PC with Windows XP and Linux Fedora 10 Room equipped with 12 Cisco 1700 routers 1 Room equipped with 6 3Com 4200 Switches 1 Room equipped with 12 Linksys access points 1 Rooms equipped with 14 PC with Windows and Linux Fedora 12 Videoconference room with IP support 5 Classroom with IP videoconference support 1 Videoconference management equipment - MCU 1 Videoconference recordingg equipment - IPVRC 1 Multimedia Kiosk 3 Pontos de acesso a Internet físicos 850 Wireless Access Points (APs) 26 Video projector 35

6. Atividades de formação e investigação

Mapa VI - 6.1. Centro(s) de investigação, na área do ciclo de estudos, em que os docentes desenvolvem a su. Atividade científica

6.1. Mapa VI Centro(s) de investigação, na área do ciclo de estudos, em que os docentes desenvolvem a sua atividade científica / Research Centre(s) in the area of the study programme, where the teachers develop their scientific activities

Centro de Investigação / Research Centre	Classificação (FCT) / Mark (FCT)	IES / Institution	Observações / Observations
CISUC	Muito Bom	UC	9 Docentes envolvidos
Instituto Jurídico	Muito Bom	UC	1 Docente envolvido

Perguntas 6.2 e 6.3

6.2. Mapa resumo de publicações científicas do corpo docente do ciclo de estudos, na área predominante do ciclo de estudos, em revistas internacionais com revisão por pares, nos últimos cinco anos (referenciação em formato APA):

<http://a3es.pt/si/iportal.php/cv/scientific-publication/formId/966cd136-436b-ce05-fa98-57ea5544df8f>

6.3. Lista dos principais projetos e/ou parcerias nacionais e internacionais em que se integram a. Atividades científicas, tecnológicas, culturais e artísticas desenvolvidas na área do ciclo de estudos:

H2020 ATENA

H2020 EUBrasilCloudFORUM: Fostering an International dialogue between Europe & Brazil

H2020 EUBra-BIGSEA

IRES: Practical Physical-Layer Security in Coimbra, Portugal

FP7 DEVASSES: DEsign, Verification and VALidation of large-scale, dynamic Service SystEmS

COST Action IC1303: AAPELE - Algorithms, Architectures and Platforms for Enhanced Living Environments

CECRIS – CERTification of CRItical Systems

TRUST - Towards Trust in Quality Assurance Systems

TRONE: Trustworthy and Resilient Operations in a Network Environment (CMU-PT/RNQ/0015/2009)

FP7 CockpitCI: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

Menon@WS - Methodologies for the Development of Non-Vulnerable Web Services

ADAAS: Assuring Dependability in Architecture-based Adaptive Systems
AFFIDAVIT - Automating the Proof of Quality Attributes for Large Scale Software Architectures
FP7 ICT MICIE
FP7 AMBER - Assessing, Measuring, and Benchmarking Resilience

6.3. List of the main projects and/or national and international partnerships, integrating the scientific, technological, cultural and artistic activities developed in the area of the study programme:

H2020 ATENA
H2020 EUBrasilCloudFORUM: Fostering an International dialogue between Europe & Brazil
H2020 EUBra-BIGSEA
IRES: Practical Physical-Layer Security in Coimbra, Portugal
FP7 DEVASSES: DEsign, Verification and VALidation of large-scale, dynamic Service SystEmS
COST Action IC1303: AAPELE - Algorithms, Architectures and Platforms for Enhanced Living Environments
CECRIS – CErtification of CRITICAL Systems
TRUST - Towards Trust in Quality Assurance Systems
TRONE: Trustworthy and Resilient Operations in a Network Environment (CMU-PT/RNQ/0015/2009)
FP7 CockpitCI: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
Menon@WS - Methodologies for the Development of Non-Vulnerable Web Services
ADAAS: Assuring Dependability in Architecture-based Adaptive Systems
AFFIDAVIT - Automating the Proof of Quality Attributes for Large Scale Software Architectures
FP7 ICT MICIE
FP7 AMBER - Assessing, Measuring, and Benchmarking Resilience

7. Atividades de desenvolvimento tecnológico e artísticas, prestação de serviços à comunidade e formação avançada

7.1. Descreva esta. Atividades e se a sua oferta corresponde às necessidades do mercado, à missão e aos objetivos da instituição:

O grupo de docentes envolvido no MSI participa regularmente em atividade de transferência de tecnologia e prestação de serviços de consultoria na área da Segurança Informática envolvendo empresas e entidades públicas e privada a nível nacional e Internacional. A título de exemplo podem referir-se projetos de auditoria de segurança com várias entidades, consultoria na avaliação de projetos na área de segurança para entidades nacionais e internacionais (incluindo União Europeia) e colaboração nacional e internacional na definição de políticas na área da cibersegurança.
Estas atividades são normalmente canalizadas através do Laboratório de Informática e Sistemas do Instituto Pedro Nunes (instituição de transferência de tecnologia da UC).

7.1. Describe these activities and if they correspond to the market needs and to the mission and objectives of the institution:

The group of teachers involved in MSI regularly participates in technology transfer activity and providing consulting services in the field of IT Security involving companies and public bodies at national and international level. As an example it can be mentioned the involvement in security audit projects, consulting and project evaluation in security for national and international organizations (including the EU) and national and international collaboration in defining policies in the area of cyber security.
These activities are usually channelled through the Informatics Laboratory and the Pedro Nunes Institute (UC technology transfer institution).

8. Enquadramento na rede de formação nacional da área (ensino superior público)

8.1. Avaliação da empregabilidade dos graduados por ciclos de estudos similares com base nos dados do Ministério que tutela o emprego:

Os dados de empregabilidade do Ministério da Economia, relativos a cursos na área das TIC revelam valores muito elevados, próximos dos 100% de empregabilidade. Tratando-se de um curso de especialização numa área dentro das TIC em que existe grande carência de profissionais e dadas as prioridades nacionais e internacionais na área da Cibersegurança espera-se uma forte procura de profissionais do MSI. Esta análise é corroborada pelos dados de empregabilidade dos cursos semelhantes oferecidos pelas principais universidades em Portugal e no espaço Europeu.

8.1. Evaluation of the graduates' employability based on Ministry responsible for employment data:

Employability data of the Ministry of Economy, on the courses in the ICT area reveal very high values , close to 100% employability. In the case of a specialization course in an area within ICT where there is a great shortage of professionals, and given the national and international priorities in the area of cybersecurity expected strong demand for MSI professionals. This analysis is supported by the employment data of similar courses offered by major universities in Portugal and in the European space.

8.2. Avaliação da capacidade de atrair estudantes baseada nos dados de acesso (DGES):

Os dados de empregabilidade da DGES confirmam a elevada empregabilidade dos cursos semelhantes existentes nas instituições de ensino superior portuguesas

8.2. Evaluation of the capability to attract students based on access data (DGES):

The employability of DGES data confirms the high employability of similar degrees existing in Portuguese higher education institutions.

8.3. Lista de eventuais parcerias com outras instituições da região que lecionam ciclos de estudos similares:

Está em curso o estabelecimento de parceria com a Universidade do Luxemburgo com a qual o Universidade de Coimbra tem um protocolo de colaboração para intercâmbio de alunos e docentes e um historial já longo de projetos Europeus de investigação conjuntos na área da da Segurança Informática e da Segurança em Infraestruturas Críticas.

8.3. List of eventual partnerships with other institutions in the region teaching similar study programmes:

The establishment of partnership is ongoing with the University of Luxembourg with which the University of Coimbra has a collaboration agreement for the exchange of students and teachers and an already long history of European research projects in Informatics and Security Security in Critical Infrastructure areas.

9. Fundamentação do número de créditos ECTS do ciclo de estudos

9.1. Fundamentação do número total de créditos ECTS e da duração do ciclo de estudos, com base no determinado nos artigos 8.º ou 9.º (1.º ciclo), 18.º (2.º ciclo), 19.º (mestrado integrado) e 31.º (3.º ciclo) do Decreto-Lei n.º 74/2006, de 24 de Março:

A generalidade dos cursos de 2º ciclo na Universidade de Coimbra (e também da oferta nacional) funciona em regime semestral, com uma duração de 4 semestres letivos e um total de 120 ECTS. Esta configuração também se justifica por uma questão de harmonização da oferta dentro do Departamento de Engenharia Informática, em termos de serviços docente, uso de recursos e reutilização de unidades curriculares como opcionais.

9.1. Justification of the total number of ECTS credits and of the duration of the study programme, based on articles no.8 or 9 (1st cycle), 18 (2nd cycle), 19 (integrated master) and 31 (3rd cycle) of Decreto-Lei no. 74/2006, March 24th:

The majority of 2nd cycle courses at the University of Coimbra (and the also in Portugal) are structured in semesters, with a duration of 4 semesters and a total of 120 ECTS. This setting is also justified for the sake of harmonization of the resource optimization within the Department of Informatics Engineering, in terms of educational services, resource use and reuse of other curricular units as Optional in the MSI.

9.2. Metodologia utilizada no cálculo dos créditos ECTS das unidades curriculares:

Reflexão do corpo docente sobre o esforço estimado para a cobertura dos vários tópicos e também normalização da oferta de unidades curricular dentro do Departamento de Engenharia Informática.

9.2. Methodology used for the calculation of the ECTS credits of the curricular units:

Discussion on the estimated effort to cover various topics and also normalization of the offer of curriculum units within the Department of Infomatics Engineering .

9.3. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de créditos ECTS das unidades curriculares:

São realizadas reuniões regulares com docentes e alunos em que é discutida a oferta formativa, os problemas existentes e a forma de os ultrapassar, na procura da melhoria contínua do DEI/FCTUC.

9.3. Process used to consult the teaching staff about the methodology for calculating the number of ECTS credits of the curricular units:

Meetings with teachers and students take place regularly, were the training offer is discussed, the problems and

how to overcome them, in the search for continuous improvement DEI / FCTUC.

10. Comparação com ciclos de estudos de referência no espaço europeu

10.1. Exemplos de ciclos de estudos existentes em instituições de referência do Espaço Europeu de Ensino Superior com duração e estrutura semelhantes à proposta:

Seguem-se alguns exemplos considerados relevantes.

Mestrado em Segurança Informática da Universidade do Porto : https://sigarra.up.pt/fcup/pt/cur_geral.cur_planos_estudos_view?pv_plano_id=10281&pv_ano_lectivo=2014&pv_tipo_cur_sigla=M&pv_origem=CUR

Mestrado em Segurança de Informação e Direito no Ciberespaço do IST Universidade de Lisboa <https://fenix.tecnico.ulisboa.pt/cursos/msidc/plano-curricular>

Mestrado em Segurança Informática da faculdade de Ciência da Universidade de Lisboa <http://msi.di.fc.ul.pt/program/structure>

Master in Cyber-security from University of Lancaster: <http://www.lancaster.ac.uk/study/postgraduate/postgraduate-courses/cyber-security-msc/>

Master in Cyber Security and Management, University of Warwick

http://www2.warwick.ac.uk/fac/sci/wmg/education/wmgmasters/courses/cyber_security_management/

Wiki sobre mestrados em Cibersecurity: https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security

10.1. Examples of study programmes with similar duration and structure offered by reference institutions of the European Higher Education Area:

Some examples follow.

MSc in Informatics Security of Universidade do Porto: https://sigarra.up.pt/fcup/pt/cur_geral.cur_planos_estudos_view?pv_plano_id=10281&pv_ano_lectivo=2014&pv_tipo_cur_sigla=M&pv_origem=CUR

MSc in Information Security and Ciberspace law of IST Universidade de Lisboa: <https://fenix.tecnico.ulisboa.pt/cursos/msidc/plano-curricular>

MSc in Informatics Security of Faculdade de Ciência da Universidade de Lisboa <http://msi.di.fc.ul.pt/program/structure>

Master in Cyber-security from University of Lancaster: <http://www.lancaster.ac.uk/study/postgraduate/postgraduate-courses/cyber-security-msc/>

Master in Cyber Security and Management, University of Warwick

http://www2.warwick.ac.uk/fac/sci/wmg/education/wmgmasters/courses/cyber_security_management/

Wiki about Cibersecurity MSc: https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security

10.2. Comparação com objetivos de aprendizagem de ciclos de estudos análogos existentes em instituições de referência do Espaço Europeu de Ensino Superior:

A comparação dos objetivos de aprendizagem do MSI com os objetivos de ciclos de estudos análogos existentes em instituições de referência do Espaço Europeu de Ensino Superior é relativamente complexa dada a grande diversidade da oferta e as diferentes tipologias. Podem, no entanto, identificar-se três tipos diferentes de oferta consoante o foco principal. Temos assim mestrados com um grande foco em técnicas e princípios de criptografia (como é o caso do mestrado da Universidade de Lovaina), mestrados com foco em segurança de software e segurança de informação (como é o caso do mestrado do IST- UTL) e mestrados com um foco em segurança nas comunicações. No caso do MSI tentou-se equilibrar as três vertentes descritas anteriormente, existindo 12 ECTS de criptografia e fundamentos de segurança e privacidade, 12 ECTS de segurança de informação e software e 12 ECTS de segurança de redes e sistemas de comunicação. Esta oferta é complementada com uma UC de integração de conhecimentos (Auditoria de Segurança com 6 ECTS), uma UC de aspetos legais e deontológicos (6 ECTS) e uma UC de seminários em tópicos emergentes (6 ECTS). Assim, o MSI apresenta uma estrutura equilibrada incluindo os aspetos mais relevantes na área de Cibersegurança, sem descurar os aspetos fundamentais, os aspetos tecnológicos e os aspetos legais e deontológicos.

10.2. Comparison with the intended learning outcomes of similar study programmes offered by reference institutions of the European Higher Education Area:

Comparison of the MSI learning objectives with similar study cycles goals existing in reference institutions of the European Higher Education Area is relatively complex given the great diversity and the different typologies. We may, however, identify three different types depending on the focus of the study cycles. There are MSc with a major focus on technical and cryptographic principles (such as the Master of the University of Louvain), MSc with a focus on security software and security information (such as the Master of IST- UTL) and MSc with a focus on security in communications. In the case of MSI we tried to balance the three components described above, there are 12 ECTS encryption and security and privacy fundamentals, 12 ECTS on information and software security and 12 ECTS of network and communication systems security. This offer is complemented by a UC focusing on knowledge integration (Security Auditing with 6 ECTS), a UC legal and ethical aspects (6 ECTS) and a UC dedicated to

seminars on emerging topics (6 ECTS). Overall the MSI presents a balanced structure including the most relevant aspects in the cybersecurity area, without neglecting the fundamental aspects, technological aspects and the legal and ethical aspects.

11. Estágios e/ou Formação em Serviço

11.1. e 11.2 Locais de estágio e/ou formação em serviço (quando aplicável)

Mapa VII - Protocolos de Cooperação

Mapa VII - Nos laboratórios de investigação do DEI ou em entidades externas (empresas ou instituições)

11.1.1. Entidade onde os estudantes completam a sua formação:

Nos laboratórios de investigação do DEI ou em entidades externas (empresas ou instituições)

11.1.2. Protocolo (PDF, máx. 150kB):

<sem resposta>

Mapa VIII. Plano de distribuição dos estudantes

11.2. Mapa VIII. Plano de distribuição dos estudantes pelos locais de estágio e/ou formação em serviço demonstrando a adequação dos recursos disponíveis.(PDF, máx. 100kB).

<sem resposta>

11.3. Recursos próprios da Instituição para acompanhamento efetivo dos seus estudantes nos estágios e/ou formação em serviço.

11.3. Recursos próprios da Instituição para o acompanhamento efetivo dos seus estudantes nos estágios e/ou formação em serviço:

Os estagiários ano exterior são enquadrados por um funcionário de empresa (Especialista em Informática com grau de Mestre em Engenharia Informática, ou equivalente) e orientados por um docente do DEI.

Os estagiários que realizam estágios em laboratórios de investigação do DEI são orientados por um Docente do DEI, e eventualmente enquadrados num projeto de investigação.

Todos os docentes envolvidos no MSI participam na orientação ou coorientação dos estagiários, tendo atribuído tempo letivo para reuniões de acompanhamento dos estagiários.

As regras de acompanhamento de estagiários pelos docentes do DEI estabelecem reuniões regulares para acompanhamento dos trabalhos em que estejam presentes o estagiário, o orientador do DEI e responsável pelo enquadramento na empresa.

Os estagiários devem entregar relatórios mensais de acompanhamento que são analisados nas reuniões e dos quais é dado feedback ao aluno.

Existe uma Plataforma de Estágios onde é arquivada toda a informação

11.3. Resources of the Institution to effectively follow its students during the in-service training periods:

The students while performing internships outside are supervised by a senior employee (Specialist Informatics with MS degree in Computer Science, or equivalent) and are advised by a teacher of DEI.

Students can also perform internships at DEI's research laboratories under the supervision of teacher at DEI. The research work can be developed in the scope of a research project.

All teachers involved in MSI can participate in supervision of students. Teaching time is allocated to supervisors to allow follow-up meetings and other student supervision activities.

The supervision procedures at DEI establish regular meetings with the students to follow up work the student work. These meetings can involve the DEI supervisor and the responsible for the student in the company.

Students must submit monthly monitoring reports that are analysed in meetings to provide feedback to the students.

There is an internship platform where all the information is filed and kept.

11.4. Orientadores cooperantes

Mapa IX. Normas para a avaliação e seleção dos elementos das instituições de estágio e/ou formação em serviço

responsáveis por acompanhar os estudantes

11.4.1 Mapa IX. Mecanismos de avaliação e seleção dos orientadores cooperantes de estágio e/ou formação em serviço, negociados entre a Instituição de ensino superior e as instituições de estágio e/ou formação em serviço (PDF, máx. 100kB):

<sem resposta>

Mapa X. Orientadores cooperantes de estágio e/ou formação em serviço (obrigatório para ciclo de estudos com estágio obrigatório por Lei)

11.4.2. Mapa X. Orientadores cooperantes de estágio e/ou formação em serviço (obrigatório para ciclo de estudos com estágio obrigatório por Lei) / External supervisors responsible for following the students' activities (mandatory for study programmes with in-service training mandatory by law)

Nome / Name	Instituição ou estabelecimento a que pertence / Institution	Categoria Profissional / Professional Title	Habilitação Profissional (1)/ Professional qualifications (1)	Nº de anos de serviço / N° of working years
----------------	--	--	--	--

<sem resposta>

12. Análise SWOT do ciclo de estudos

12.1. Pontos fortes:

- *O MSI é ancorado em dois grupos de investigação do DEI com largos anos de experiência de investigação e projetos internacionais na área da Segurança Informática.*
- *O MSI foi desenhado para dar resposta às necessidades das empresas e foi planeado para funcionar em regime tendencialmente pós-laboral com possibilidade de realização de algumas componentes (trabalhos práticos) em modo remoto*

12.1. Strengths:

- *The MSI is anchored in two DEI research groups with many years of research experience and international projects in the field of Information and Communication Security.*
- *The MSI is designed to meet the needs of companies and was designed to allow part-time, after-business hours compatibility, with the possibility of students to develop part of the work (practical work) in remote mode*

12.2. Pontos fracos:

- *Dificuldade de adaptação do corpo docente ao regime tendencialmente pós-laboral.*

12.2. Weaknesses:

- *Difficulty adapting faculty to tend to after business hours teaching mode*

12.3. Oportunidades:

- *Existência de mais de 500 profissionais em pequenas e médias empresas de TIC na região Cento, algumas delas spin-offs do DEI e muitas delas com ex-alunos;*
- *Envolvimento dos docentes em vários projetos nacionais e Europeus na área da cibersegurança;*
- *Existência de parcerias internacionais com entidades de referência na área da Cibersegurança*

12.3. Opportunities:

- *Existence of more than 500 professionals in small and medium ICT companies in Cento region, some of them spin- offs DEI and many of them involving former DEI students;*
- *Involvement of teachers in numerous national and European projects in the area of cyber-security;*
- *Existence of international partnerships with reference entities in the field of cybersecurity*

12.4. Constrangimentos:

- *Oferta semelhante das grandes universidades a Norte e a Sul de Coimbra;*
- *O funcionamento em Coimbra, longe dos locais onde estão instaladas empresas de grande dimensão e multinacionais na área das TIC*

12.4. Threats:

- *Offer of similar degrees by the major universities in the North and the South of Coimbra;*
- *Location in Coimbra, away from places where large and multinational companies in the ICT area are instaled*

12.5. CONCLUSÕES:

O MSI representa claramente um desafio para o Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra, por se tratar de uma oferta especializada, focada essencialmente no mercado empresarial, funcionando em regime pós-kaboral, com todas as vantagens e inconvenientes desses fatos.

A experiência do corpo docente na área da segurança informática, traduzida em publicações em revistas e conferências de referência, em teses de doutoramento e em projetos de investigação de âmbito internacional, nomeadamente em projetos Europeus será certamente um fator decisivo para minorar as fraquezas e os constrangimentos identificados (e as que venham a surgir) e transformar as oportunidades em pontos fortes!

12.5. CONCLUSIONS:

The MSI is clearly a challenge for the Department of informatics Engineering of the Faculty of Science and Technology of University of Coimbra, because it is a specialized training offered, focused mainly on the company's market, after business operation, with all the advantages and disadvantages related to the situations described.

The experience of the teaching staff in the security area, evaluated in publications in journals and reference conferences, in doctoral thesis, and international research projects, particularly in European projects, will certainly be a decisive factor to minimize the weaknesses and constraints identified (and those that may arise) and turn opportunities into strengths!