

# ACEF/1213/06927 — Guião para a auto-avaliação

---

## Caracterização do ciclo de estudos.

**A1. Instituição de Ensino Superior / Entidade Instituidora:**  
*Universidade De Lisboa*

**A1.a. Outras Instituições de Ensino Superior / Entidades Instituidoras:**

**A2. Unidade(s) orgânica(s) (faculdade, escola, instituto, etc.):**  
*Instituto Superior Técnico*

**A3. Ciclo de estudos:**  
*Segurança de Informação*

**A3. Study cycle:**  
*Information Security*

**A4. Grau:**  
*Doutor*

**A5. Publicação do plano de estudos em Diário da República (n.º e data):**  
*Diário da República, 2.ª série — N.º 145 — 27 de julho de 2012 (Despacho n.º 10158/2012)*

**A6. Área científica predominante do ciclo de estudos:**  
*Segurança de Informação*

**A6. Main scientific area of the study cycle:**  
*Information Security*

**A7.1. Classificação da área principal do ciclo de estudos (3 algarismos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF):**  
*481*

**A7.2. Classificação da área secundária do ciclo de estudos (3 algarismos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF), se aplicável:**  
*n.a*

**A7.3. Classificação de outra área secundária do ciclo de estudos (3 algarismos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF), se aplicável:**  
*n.a*

**A8. Número de créditos ECTS necessário à obtenção do grau:**  
*240*

**A9. Duração do ciclo de estudos (art.º 3 DL-74/2006, de 26 de Março):**  
*4 Anos*

**A9. Duration of the study cycle (art.º 3 DL-74/2006, March 26th):**  
*4 Years*

**A10. Número de vagas aprovado no último ano lectivo:**  
*<sem resposta>*

**A11. Condições de acesso e ingresso:****Requisitos de Acesso**

**Diploma de 2º Ciclo, nacional ou estrangeiro, ou de licenciatura (pré-Bolonha) com 5 anos, em Electrotecnia, Informática, Matemática ou em áreas afins. Aprovação em 2 exames de qualificação. Conclusão da parte curricular do Programa com média superior ou igual a 14 valores.**

**A11. Entry Requirements:****Access Requisites**

**Master's degree or equivalent in science and engineering. Approval in 2 qualifying exams. Completion of the curricular component of the Program with a final grade of at least 14 out of 20.**

**A12. Ramos, opções, perfis...****Pergunta A12**

**A12. Ramos, opções, perfis, maior/menor ou outras formas de organização de percursos alternativos em que o ciclo de estudos se estrutura (se aplicável):**

**Não**

**A12.1. Ramos, opções, perfis, maior/menor, ... (se aplicável)**

**A12.1. Ramos, opções, perfis, maior/menor, ou outras formas de organização de percursos alternativos em que o ciclo de estudos se estrutura (se aplicável) / Branches, options, profiles, major/minor, or other forms of organisation of alternative paths compatible with the structure of the study cycle (if applicable)**

**Opções/Ramos/... (se aplicável):**

Tronco Comum

**Options/Branches/... (if applicable):**

Common Branch

**A13. Estrutura curricular****Mapa I - Tronco Comum****A13.1. Ciclo de Estudos:**

**Segurança de Informação**

**A13.1. Study Cycle:**

**Information Security**

**A13.2. Grau:**

**Doutor**

**A13.3. Ramos, opções, perfis, maior/menor, ou outras (se aplicável)**

**Tronco Comum**

**A13.3. Branches, options, profiles, major/minor, or other forms (if applicable)**

**Common Branch**

**A13.4. Áreas científicas e créditos que devem ser reunidos para a obtenção do grau / Scientific areas and credits that must be obtained before a degree is awarded**

**Área Científica / Scientific Area**

**Sigla /  
Acronym**

**ECTS Obrigatórios /  
Mandatory ECTS**

**ECTS Optativos /  
Optional ECTS\***

Metodologia e Tecnologia da Programação/Methodology and Programming Theory	MTP	0	25.5
Lógica e Computação/Logic and Computing	LogCom	0	67.5
Sistemas, Decisão e Controlo/Systems, Decision and Control	SDC	0	12
Telecomunicações/Telecommunications	Tele	0	12
Computadores/Computers	Comp	0	12
Competências Transversais/Crosscutting Skills	CT	0	27
Opção Livre/Free Option	OL	0	12
Arquitetura e Sistemas Operativos/Architecture and Operating Systems	ASO	0	31.5
<b>(8 Items)</b>		<b>0</b>	<b>199.5</b>

## A14. Plano de estudos

### Mapa II - Tronco Comum - 1º ano / 1º Semestre

**A14.1. Ciclo de Estudos:**  
*Segurança de Informação*

**A14.1. Study Cycle:**  
*Information Security*

**A14.2. Grau:**  
*Doutor*

**A14.3. Ramos, opções, perfis, maior/menor, ou outras (se aplicável)**  
*Tronco Comum*

**A14.3. Branches, options, profiles, major/minor, or other forms (if applicable)**  
*Common Branch*

**A14.4. Ano/semestre/trimestre curricular:**  
*1º ano / 1º Semestre*

**A14.4. Curricular year/semester/trimester:**  
*1 year / 1º Semester*

#### A14.5. Plano de estudos / Study plan

Unidades Curriculares / Curricular Units	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Aprendizagem Automática/Machine Learning	SDC	Semestral	168	T-42,0;TP-0,0;PL-28,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Compressão e Codificação de Dados/Data Coding and Compression	Tele	Semestral	168	T-42,0;TP-21,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Criptografia e Protocolos de Segurança/Cryptography and Security Protocols	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS.
Engenharia de Segurança de Informação/Security Engineering	MTP	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Fundamentos de Lógica e Teoria da Computação/Foundations of Logic and Theory of Computation	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS.

Fundamentos Modernos de Redes de Computadores/Modern Foundations of Computer Networking	Comp	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Lógica Cleística/Kleistic Logic	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS.
Modelos Computacionais em Segurança/Computational Models in Security	MTP	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Opção Livre I/Free Option I	OL	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	V Opção de escolher uma unidade curricular
Segurança em Linguagens de Programação/Language Based Security	MTP	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Segurança Informática em Redes e Sistemas/Network and Computer Security	ASO	Semestral	210	T-42,0;TP-0,0;PL-21,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Seminário de Investigação em Segurança de Informação I A/Information Security Research Seminar I (A)	CT	Semestral	84	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-14,0;	3	IV(x) Escolher uma unidade curricular IV(x) para um total de 9 a 12 ECTS.
Seminário de Investigação em Segurança de Informação I B/Information Security Research Seminar I (B)	CT	Semestral	126	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-21,0;	4.5	IV(x) Escolher uma unidade curricular IV(x) para um total de 9 a 12 ECTS.
Seminário de Investigação em Segurança de Informação I C/Information Security Research Seminar I (C)	CT	Semestral	168	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-28,0;	6	IV(x) Escolher uma unidade curricular IV(x) para um total de 9 a 12 ECTS.
Segurança em Redes Móveis/Mobile Network Security	Comp	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Tópicos Avançados em Segurança de Informação I/Advanced Topics in Information Security I	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS.
Algoritmos Probabilísticos/Probabilistic Algorithms	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS
Lógica e Verificação de Modelos/Logic and Model Checking	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS

(18 Items)

## Mapa II - Tronco Comum - 1º Ano / 2º Semestre

### A14.1. Ciclo de Estudos: *Segurança de Informação*

#### A14.1. Study Cycle: *Information Security*

#### A14.2. Grau: *Doutor*

#### A14.3. Ramos, opções, perfis, maior/menor, ou outras (se aplicável) *Tronco Comum*

#### A14.3. Branches, options, profiles, major/minor, or other forms (if applicable) *Common Branch*

#### A14.4. Ano/semestre/trimestre curricular:

**1º Ano / 2º Semestre****A14.4. Curricular year/semester/trimester:  
1º Year / 2º Semester****A14.5. Plano de estudos / Study plan**

Unidades Curriculares / Curricular Units	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Sistemas de Biometria/Biometrics	SDC	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Aprendizagem Estatística/Statistical Learning	Tele	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	I Escolher unidades curriculares I para um total de 6 a 18 ECTS
Protocolos de Segurança para Sistemas Distribuídos/Distributed Systems Security Protocols	ASO	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Tolerância a Falhas Distribuída/Distributed Fault Tolerance	ASO	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Tolerância, Detecção e Resposta a Intrusões/Intrusion Tolerance, Detection and Response	ASO	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Tópicos Avançados em Segurança de Informação II/Advanced Topics in Information Security II	ASO	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Algoritmos Avançados/Advanced Algorithms	MTP	Semestral	210	T-42,0;TP-21,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	II Escolher unidades curriculares II para um total de 12 a 27 ECTS
Computabilidade e Complexidade/Computability and Complexity	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS
Computação, Informação e Lógica Quânticas/Quantum Computation, Information and Logic	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS
Lógica Funcional e Teoria da Demonstração/Functional Logic and Proof Theory	LogCom	Semestral	210	T-56,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	7.5	III Escolher unidades curriculares III para um total de 18 a 31,5 ECTS
Seminário de Investigação em Segurança de Informação II A/Research Seminar in Information Security II (A)	CT	Semestral	84	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-14,0;	3	IV(y) Escolher uma unidade curricular IV(y) para um total de 9 a 12 ECTS
Seminário de Investigação em Segurança de Informação II B/Research Seminar in Information Security II (B)	CT	Semestral	126	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-21,0;	4.5	IV(y) Escolher uma unidade curricular IV(y) para um total de 9 a 12 ECTS.
Seminário de Investigação em Segurança de Informação II C/Research Seminar in Information Security II (C)	CT	Semestral	168	T-0,0;TP-0,0;PL-0,0;TC-0,0;S-14,0;E-0,0;OT-28,0;	6	IV(y) Escolher uma unidade curricular IV(y) para um total de 9 a 12 ECTS.
Opção Livre II/Free Option II	OL	Semestral	168	T-42,0;TP-0,0;PL-0,0;TC-0,0;S-0,0;E-0,0;OT-0,0;	6	V Opção de escolher uma unidade curricular

(14 Items)

**Perguntas A15 a A16****A15. Regime de funcionamento:  
Diurno**

**A15.1. Se outro, especifique:**

*<sem resposta>*

**A15.1. If other, specify:**

*<no answer>*

**A16. Docente(s) responsável(eis) pela coordenação do ciclo de estudos (a(s) respectiva(s) Ficha(s) Curricular(es) deve(m) ser apresentada(s) no Mapa VIII)**

*Diogo Luís de Castro Vasconcelos de Aguiar Gomes*

## **A17. Estágios e Períodos de Formação em Serviço**

### **A17.1. Indicação dos locais de estágio e/ou formação em serviço**

---

Mapa III - Protocolos de Cooperação

Mapa III - N/A

**A17.1.1. Entidade onde os estudantes completam a sua formação:**

*N/A*

**A17.1.2. Protocolo (PDF, máx. 100kB):**

*<sem resposta>*

Mapa IV. Mapas de distribuição de estudantes

**A17.2. Mapa IV. Plano de distribuição dos estudantes pelos locais de estágio.(PDF, máx. 100kB)**

Documento com o planeamento da distribuição dos estudantes pelos locais de formação em serviço demonstrando a adequação dos recursos disponíveis.

*<sem resposta>*

**A17.3. Recursos próprios da instituição para acompanhamento efectivo dos seus estudantes no período de estágio e/ou formação em serviço.**

---

**A17.3. Indicação dos recursos próprios da instituição para o acompanhamento efectivo dos seus estudantes nos estágios e períodos de formação em serviço.**

*N/A*

**A17.3. Indication of the institution's own resources to effectively follow its students during the in-service training periods.**

*N/A*

### **A17.4. Orientadores cooperantes**

---

**A17.4.1. Normas para a avaliação e selecção dos elementos das instituições de estágio responsáveis por acompanhar os estudantes (PDF, máx. 100kB).**

**A17.4.1. Normas para a avaliação e selecção dos elementos das instituições de estágio responsáveis por acompanhar os estudantes (PDF, máx. 100kB)**

Documento com os mecanismos de avaliação e selecção dos monitores de estágio e formação em serviço, negociados entre a instituição de ensino e as instituições de formação em serviço.

*<sem resposta>*

Mapa V. Orientadores cooperantes de estágio e/ou formação em serviço (para ciclos de estudos de formação de professores).

**Mapa V. Orientadores cooperantes de estágio e/ou formação em serviço (para ciclo de estudos de formação de professores) / Map V. External supervisors responsible for following the students' activities (only for teacher training study cycles)**

Nome / Name	Instituição ou estabelecimento a que pertence / Institution	Categoria Profissional / Professional Title	Habilitação Profissional / Professional Qualifications	Nº de anos de serviço / No of working years
----------------	--	--	---	--

<sem resposta>

## Pergunta A18 e A19

### A18. Observações:

*No ponto 7.1.4. da secção 4 é importante referir:*

*A plataforma neste ponto aceita apenas números, razão pela qual aparece o número “100” em vez de “não disponível” ou “não aplicável”.*

*Inexistência de diplomados aquando da aplicação do inquérito em 2012 aos diplomados 2008/2009 e 2009/2010*

### A18. Observations:

*As for paragraph 7.1.4, section 4, it is important to note that:*

*The platform only accepts numbers; that is why ‘100’ appears instead of “not available” or “not applicable”.*

*There were no graduate when the survey was implemented in 2012 and targeted to 2008/2009 and 2009/2010 graduates*

### A19. Participação de um estudante na comissão de avaliação externa

A Instituição põe objecções à participação de um estudante na comissão de avaliação externa?

*Não*

## 1. Objectivos gerais do ciclo de estudos

### 1.1. Objectivos gerais definidos para o ciclo de estudos.

*O Programa visa formar especialistas capazes de desenvolver investigação autónoma na área interdisciplinar de segurança informática, o que requer o domínio de matérias de Matemática, Engenharia Informática e Engenharia Electrotécnica, incluindo complexidade computacional, criptografia, segurança de sistemas e teoria da informação.*

*Os doutores em Segurança de Informação poderão realizar actividades de investigação e desenvolvimento em universidades, unidades de investigação e empresas hightech, nacionais ou estrangeiras ou liderar equipas responsáveis pela segurança informática na indústria e serviços, em Portugal ou no estrangeiro.*

### 1.1. Study cycle's generic objectives.

*The Program aims at training experts capable of carrying out autonomous research activities in the broad area of information security, mastering relevant subjects in Mathematics, Computer Science and Electrical Engineering, including computational complexity, cryptography, systems security and information theory.*

*Those successfully completing the Program will be capable of performing research activity in national and international universities, research units and hightech companies and leading teams responsible for information security at industry and services.*

### 1.2. Coerência dos objectivos definidos com a missão e a estratégia da instituição.

*Nos termos do n.º 1 do Artigo 3.º dos Estatutos do IST, homologados pelo Despacho n.º 9523/2012 publicado em Diário da Republica de 13 de Julho de 2012, “É missão do IST, como instituição que se quer prospectiva no ensino universitário, assegurar a inovação constante e o progresso consistente da sociedade do conhecimento, da cultura, da ciência e da tecnologia, num quadro de valores humanistas.”*

*Nos termos do n.º 2 do mesmo artigo estabelece-se que, no cumprimento da sua missão, o IST: Privilegia a investigação científica, o ensino, com ênfase no ensino pós-graduado, e a formação ao longo da vida, assim como o desenvolvimento tecnológico; Promove a difusão da cultura e a valorização social e económica do conhecimento científico e tecnológico;*

*Procura contribuir para a competitividade da economia nacional através da transferência de tecnologia, da inovação e da promoção do empreendedorismo; Efetiva a responsabilidade social, na prestação de serviços científicos e técnicos à comunidade e no apoio à inserção dos diplomados no mundo do trabalho e à sua formação permanente.*

### 1.2. Coherence of the study cycle's objectives and the institution's mission and strategy.

*Pursuant to paragraph 1 of article 3 of the Statute of the IST, approved by order No. 9523/2012 published in Diário da Republica de July 13, 2012, "Is the mission of the IST as an institution that foresight in university education, ensure constant innovation and consistent progress of the knowledge society, culture, science and technology in the context of humanist values."*

*Pursuant to paragraph 2 of the same article provides that, in carrying out its task, the IST: focused on scientific research, teaching, with an emphasis on graduate education, and lifelong learning, as well as technological development; Promotes the dissemination of culture and the social and economic promotion of scientific and technological knowledge; Seeks to contribute to the competitiveness of the national economy through technology transfer, innovation and promoting entrepreneurship; Effective social responsibility in providing scientific and technical services to the community and supporting the integration of graduates in the labour market and their ongoing formation.*

### 1.3. Meios de divulgação dos objectivos aos docentes e aos estudantes envolvidos no ciclo de estudos.

*O Programa foi criado em 2007 no IST na sequência do crescente interesse na formação de pós-graduação neste domínio. A equipa docente lecciona desde 2001 disciplinas avançadas no domínio, tendo também uma vasta experiência de orientação de alunos de doutoramento e de pós-doutoramento. Estes docentes desenvolvem as suas actividades de investigação em grupos com objectivos no domínio de unidades de investigação de topo a nível nacional, nomeadamente o IT e o INESC-ID, com especial relevância para o SQIG e o DSG.*

*O programa tem como objetivo atrair estudantes nacionais e internacionais de alta qualidade com um mestrado em ciência ou engenharia e que pretendem seguir uma carreira científica ou técnica na vanguarda da pesquisa e desenvolvimento em segurança da informação. Para este efeito um número de acções de divulgação e recrutamento são organizadas, incluindo páginas web, emails para listas de divulgação e sessões de esclarecimento.*

### 1.3. Means by which the students and teachers involved in the study cycle are informed of its objectives.

*The Program was created in 2007 as a consequence of the increasing interest in graduate studies on this domain. The faculty has been teaching advanced courses in Information Security since 2001, and has a wide experience in supervising PhD and post-doc students. The faculty belongs to top Portuguese research units, namely IT and INESC, working in research groups specially focused on Information Security, such as SQIG and DSG.*

*The program aims to attract national and international top quality students with a Master's degree in science or engineering and who intend to pursue a scientific or technical career in the forefront of research and development in information security. To this effect a number of actions are organized including web pages, email and outreach sessions.*

## 2. Organização Interna e Mecanismos de Garantia da Qualidade

### 2.1 Organização Interna

#### 2.1.1. Descrição da estrutura organizacional responsável pelo ciclo de estudo, incluindo a sua aprovação, a revisão e actualização dos conteúdos programáticos e a distribuição do serviço docente.

*A Coordenação Científica dos CE conducentes ao grau de doutor é da responsabilidade da Comissão Científica do CE, que é constituída por um Coordenador e Professores ou investigadores doutorados, que representem as áreas científicas dos departamentos e estruturas transversais que participam no CE, incluindo mais do que um professor catedrático.*

*A Coordenação Pedagógica é da responsabilidade de uma Comissão, constituída por um Coordenador e Professores ou investigadores doutorados e estudantes.*

*A criação,extinção ou alteração de CE tem procedimentos aprovados pelo IST disponíveis na página WEB do CG. Os Departamentos ou Estruturas elaboram propostas e remetem-nas ao Presidente. Os processos passam pelos vários órgãos (CC,CP,CG,CE) terminando com a aprovação,ou não,do Reitor.A distribuição do serviço docente é proposta pelos Departamentos, aprovada pelo CC e homologada pelo Presidente do IST.As normas e mecanismos estão definidos no Regulamento de Prestação de Serviço dos Docentes do IST.*

#### 2.1.1. Description of the organisational structure responsible for the study cycle, including its approval, the syllabus revision and updating, and the allocation of academic service.

*The Scientific Coordination of the CE leading to a PhD degree is up to the CE Executive Committee, which includes a Coordinator and Teachers or PhD researchers, which represent the scientific areas of the departments that participate in the CE, including more than one Full Professor.*

*The Pedagogical Coordination is up to one Committee, which includes a Coordinator and Teachers of PhD researchers*



and students.

*The creation, windup or amendment of CE involves procedures approved by IST available at the webpage of the Governing Board. The Departments or Structures elaborate proposals and send them to the President. The processes are subject to the approval of the different bodies of IST (CC,CP,CG,CE) and are ultimately approved or not by the Rector. The distribution for the teaching service is proposed by the Departments, approved by the CC and authorized by the President of IST. The standards and mechanisms are defined in the Service Provision Regulations of IST Teaching staff.*

2.1.2. Forma de assegurar a participação activa de docentes e estudantes nos processos de tomada de decisão que afectam o processo de ensino/aprendizagem e a sua qualidade.

*A participação ativa destes elementos na gestão da qualidade do CE está assegurada de várias formas, sendo exemplo disso a Coordenação Científico-Pedagógica de curso que para além do coordenador, inclui na sua constituição uma representação de vários docentes e investigadores doutorados e estudantes, e nalguns casos inclui Comissões de Acompanhamento de Tese.*

*Mais adiante serão referidas outras formas de contribuição dos estudantes e docentes, referindo-se como exemplo alguns inquéritos tais como o QUC (avaliação das UC), que prevê a auscultação de alunos e docentes, e inquérito de avaliação da empregabilidade dos diplomados, cujos resultados são incorporados num relatório Anual de Autoavaliação de cada CE(R3A). Neste momento está definido o modelo para este relatório no 3º ciclo, estando em curso o alargamento do QUC.*

2.1.2. Means to ensure the active participation of academic staff and students in decision-making processes that have an influence on the teaching/learning process, including its quality.

*The active participation of these elements in the quality management process of the Studies Cycle can be ensured in different ways, for example, through the Scientific and Pedagogical Coordination which, in addition to the programme coordinator, includes students' representatives and teachers and researchers' representatives, and in some cases include a Committee for the monitoring of the thesis development.*

*Other forms of contribution in the quality management process will be provided below. For example some regular surveys, such as the QUC survey, whose regulations provides for the consultation of teachers and students, and survey for the assessment of graduates' employability, whose results are incorporated into an annual self-assessment report (R3A). At the moment the model for this 3rd cycle report is already defined, and the QUC extension is in progress.*

## 2.2. Garantia da Qualidade

2.2.1. Estruturas e mecanismos de garantia da qualidade para o ciclo de estudos.

*Nos últimos anos o IST assumiu como objetivo estratégico da escola o desenvolvimento de um Sistema Integrado de Gestão da Qualidade (SIQuIST), com o objetivo de promover e valorizar a cultura de qualidade desenvolvida no IST, com a institucionalização de um conjunto de procedimentos que imprimam a melhoria contínua e o reajustamento, em tempo real, dos processos internos. O modelo abrange as 3 grandes áreas de atuação do IST-Ensino, I&DI, e atividades de ligação à sociedade - assumindo-se como áreas transversais os processos de governação, gestão de recursos e internacionalização da escola. No Ensino estão instituídos vários processos de garantia da qualidade, destacando-se: o Guia Académico, Programa de Tutorado, QUC (subsistema de garantia de qualidade das unidades curriculares), e R3A (Relatórios anuais de autoavaliação) que incluem indicadores decorrentes do desenvolvimento de inquéritos e estudos vários. A funcionar em pleno no 1º e 2º ciclos, está em curso a extensão destes dois últimos ao 3º ciclo.*

2.2.1. Quality assurance structures and mechanisms for the study cycle.

*Over the last years, the IST has invested in the development of an Integrated Quality Management System (SIQuIST), with the ultimate purpose of promoting and enhancing the culture of quality developed at the IST, with the institutionalization of a set of procedures leading to continuous improvement and readjustment, in real time, of internal procedures. It covers IST's 3 large areas of action - Teaching, R&DI, and activities reaching out to society - establishing the processes of governance, resource management and internationalization as crosscutting areas.*

*The area "Education" provides several quality assurance processes, among which the Academic Guide, the Tutoring Programme, the QUC (quality assurance sub-system for course units) which include indicators arising from the development of surveys and different studies. It became fully operational for 1st and 2nd cycles and the extension of these two cycles to the 3rd cycle is being analysed.*

2.2.2. Indicação do responsável pela implementação dos mecanismos de garantia da qualidade e sua função na instituição.

*A coordenação e gestão do SIQuIST cabe ao Conselho para a Gestão da Qualidade da instituição (CGQ), o qual é dirigido pelo Presidente do IST, ou pelo membro do CGQ em quem este delegar essas competências.*

*Compete ao CGQ, no quadro do sistema nacional de acreditação e avaliação, nos termos da lei e no respeito pelas orientações emanadas pelos órgãos do IST, propor e promover os procedimentos relativos à avaliação da qualidade a prosseguir pelo IST no âmbito das atividades de ensino, I&DI, transferência de tecnologia e gestão, bem como analisar o funcionamento do SIQuIST, elaborar relatórios de apreciação e pronunciar-se sobre propostas de medidas de correção que considere adequadas ao bom desempenho e imagem da Instituição.*

*Para além do Presidente do IST integram o CGQ: um membro do Conselho Científico, um docente e um aluno do Conselho Pedagógico, os Coordenadores da Áreas de Estudos e Planeamento e de Qualidade e Auditoria Interna, e o*

**Presidente da Associação de Estudantes do IST.**

**2.2.2. Responsible person for the quality assurance mechanisms and position in the institution.**

*The SIQuIST is coordinated and managed by the institution's Quality Management Council (CGQ), which is chaired by the President of IST, or by the member of the CGQ to whom he delegates that power.*

*Under the national accreditation and evaluation framework and under the law and in compliance with the guidelines issued by the IST's bodies, the CGQ is responsible for proposing and promoting the procedures regarding the quality evaluation to be pursued by the IST under its activities of teaching, R&DI, technology transfer and management, as well as analyzing how the SIQuIST works, elaborating assessment reports and giving an opinion on proposals of corrective measures deemed fit to the sound performance and image of the institution.*

*The CHQ comprises the President of IST, a member of the Scientific Board, a teacher and a student of the Pedagogical Council, the Coordinators of the Planning and Studies and Internal Quality and Audit Offices and the President of Students' Association of IST.*

**2.2.3. Procedimentos para a recolha de informação, acompanhamento e avaliação periódica do ciclo de estudos.**

*A principal fonte de informação para todos os processos de acompanhamento e avaliação periódica dos CE é o sistema de informação e gestão Fénix, complementado com informação recolhida através de inquéritos à comunidade académica, e outras fontes externas à instituição quando necessário.*

*O acompanhamento e avaliação periódica dos cursos são feitos através dos mecanismos descritos em 2.2.1, destacando-se os R3A que se traduzem num pequeno documento de publicação anual onde se sintetizam indicadores considerados representativos de três momentos distintos – Ingresso, Processo Educativo e Graduação – que permitem uma visão global e objetiva do curso num determinado ano.*

*Os R3A, a funcionar em pleno no 1º e 2º ciclos estando em curso a extensão ao 3º ciclo, permitem uma visão global e a identificação dos aspetos críticos e constrangimentos de cada curso num determinado ano, e deverão estar na base de um relatório síntese anual das atividades das coordenações de curso.*

**2.2.3. Procedures for the collection of information, monitoring and periodic assessment of the study cycle.**

*The main source of information for all periodic follow-up and assessment processes of the study cycles is the Fénix information and management system, completed with information obtained through academic surveys and other external sources, when necessary.*

*The periodic follow-up and assessment processes of the programmes are carried out through mechanisms described in paragraph 2.2.1, of which the R3A are worth of note, which consist of a small, annually published document that summarizes the indicators deemed representative of three distinct stages – Admission, Educational Process and Graduation – which allow for a global and objective view of the programme in a certain year.*

*Operational in the 1st and 2nd cycles, the R3A allow for a global view and the identification of the critical aspects and constraints of each programme in a certain year and should be the basis for a summary report of the activities of every course coordination board.*

**2.2.4. Ligação facultativa para o Manual da Qualidade**

<https://dspace.ist.utl.pt/bitstream/2295/1099487/1/Manual%20da%20Qualidade%20IST%20V00-29-05-2012-1.pdf>

**2.2.5. Discussão e utilização dos resultados das avaliações do ciclo de estudos na definição de acções de melhoria. não aplicável**

**2.2.5. Discussion and use of study cycle's evaluation results to define improvement actions.**

*not applicable*

**2.2.6. Outras vias de avaliação/acreditação nos últimos 5 anos.**

*O Doutoramento em Segurança de Informação foi acreditado preliminarmente pela A3ES em 2010, sem qualquer tipo de recomendação.*

**2.2.6. Other forms of assessment/accreditation in the last 5 years.**

*The Phd Program in Information Security was accredited by A3ES in 2010, without any recommendation.*

## **3. Recursos Materiais e Parcerias**

### **3.1 Recursos materiais**

**3.1.1 Instalações físicas afectas e/ou utilizadas pelo ciclo de estudos (espaços lectivos, bibliotecas, laboratórios, salas de computadores, etc.).**

**Mapa VI. Instalações físicas / Mapa V. Spaces**

Tipo de Espaço / Type of space	Área / Area (m2)
1 Sala de apoio a laboratórios/1 Laboratory support room	59.3
2 Salas de informática/2 Computer rooms	71.6
3 Salas de reuniões/3 Meeting rooms	108.9
5 Gabinetes/5 Offices	174.1
9 laboratórios de ensino/9 Teaching laboratories	326.0
9 Salas de estudo/9 Study rooms	593.5
1 Biblioteca/1 Library	929.2

**3.1.2 Principais equipamentos e materiais afectos e/ou utilizados pelo ciclo de estudos (equipamentos didácticos e científicos, materiais e TICs).****Mapa VII. Equipamentos e materiais / Map VII. Equipments and materials**

Equipamentos e materiais / Equipment and materials	Número / Number
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Fujitsu Siemens CTM 5020/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Fujitsu Siemens CTM 5020	10
Impressora HP Color Laserjet 1320/Impressora HP Color Laserjet 1320	1
PCs: •CPU P4 2.53 GHz •RAM 512MB •Disco 80GB •Placa Gráfica Nvidia GeForce 4 MX440SE •Placa de Rede Admtek AN983 •Rato não Óptico; Monitor Fujitsu Siemens CTM 5020/PCs: •CPU P4 2.53 GHz •RAM 512MB •Disco 80GB •Placa Gráfica Nvidia GeForce 4 MX440SE •Placa de Rede Admtek AN983 •Rato não Óptico; Monitor Fujitsu Siemens CTM 5020	18
Sistema de seguimento por laser composto por duas câmaras Canon PAL VC-C4R e um PC HP XW6200 equipado com grabber DTRAM/Sistema de seguimento por laser composto por duas câmaras Canon PAL VC-C4R e um PC HP XW6200 equipado com grabber DTRAM	1
HP workstation WX4200 /HP workstation WX4200	2
Microfones sem fios Microsoft LifeChat ZX6000/Microfones sem fios Microsoft LifeChat ZX6000	2
Microfones unidireccionais AKG SE30B /Microfones unidireccionais AKG SE30B	2
Amplificador AV Denon AVR 1804/Amplificador AV Denon AVR 1804	1
Sistema de Som 5.1 AudioPhysic Yara/Sistema de Som 5.1 AudioPhysic Yara	1
Multitouch MiniWall de 1,36m2/Multitouch MiniWall de 1,36m2	1
Space Mouse SpaceBall 5000 /Space Mouse SpaceBall 5000	1
Space Mouse HP SpacePilot USB/Space Mouse HP SpacePilot USB	1
Óculos de realidade virtual eMagin Z800 HMD /Óculos de realidade virtual eMagin Z800 HMD	1
Squeezy Ball para controlo no espaço 3D com seis graus de liberdade/Squeezy Ball para controlo no espaço 3D com seis graus de liberdade	1
Óculos StereoGraphics CrystalEyes3 /Óculos StereoGraphics CrystalEyes3	1
Impressora HP Laserjet 1320/Impressora HP Laserjet 1320	2
Sistema de seguimento por marcadores composto por seis câmaras Motion Capture da Natural Point e um PC HP xw4200/Sistema de seguimento por marcadores composto por seis câmaras Motion Capture da Natural Point e um PC HP xw4200	1
PCs Fujitsu Siemens: •CPU P4 2.26GHz •RAM 512MB •Disco 40GB •Placa Gráfica ATI Radeon 7000 •Placa de Rede IntelPro100 •Rato não Óptico; Monitor Fujitsu Siemens 1760V/PCs Fujitsu Siemens: •CPU P4 2.26GHz •RAM 512MB •Disco 40GB •Placa Gráfica ATI Radeon 7000 •Placa de Rede IntelPro100 •Rato não Óptico; Monitor Fujitsu Siemens 1760V	10
Rede de sensores ultrasons para detecção de posicionamento de utilizadores/Rede de sensores ultrasons para detecção de posicionamento de utilizadores	1
Diaplay wall de 9m2 e 8.5 Megapixels de resolução. Composto por 12 projectores DLP HP VP 6120 controlados por um cluster de doze PCs HP xw4100 e um servidor HP xw8000/Diplay wall de 9m2 e 8.5 Megapixels de resolução. Composto por 12 projectores DLP HP VP 6120 controlados por um cluster de doze PCs HP xw4100 e um servidor HP xw8000	1
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit	2
Scanner Epson Perfection 4490 PHOTO/Scanner Epson Perfection 4490 PHOTO	1
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway	10
Impressora HP Lsaerjet 5M/Impressora HP Lsaerjet 5M	2
PCs HP: •CPU P4 1.5GHz •RAM 640MB •Disco 20GB •Placa Gráfica ATI Rage 128 Pro II •Placa de Rede Intel Pro 100 •Rato não Óptico; Monitor HP 72/PCs HP: •CPU P4 1.5GHz •RAM 640MB •Disco 20GB •Placa Gráfica ATI Rage 128 Pro II •Placa de Rede Intel Pro 100 •Rato não Óptico; Monitor HP 72	10

Switch's gigabit /Switch's gigabit	7
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway	23
PCs Gateway: •CPU P4 3.2 GHz •RAM 1024MB •Disco 60GB •Placa Gráfica Nvidia GeforceFX5200 •Placa de Rede Intel Pro1000 •Rato não Óptico; Monitor Acer AL1715/PCs Gateway: •CPU P4 3.2 GHz •RAM 1024MB •Disco 60GB •Placa Gráfica Nvidia GeforceFX5200 •Placa de Rede Intel Pro1000 •Rato não Óptico; Monitor Acer AL1715	10
PCs Gateway: •CPU P4 3.4GHz •RAM 2048MB •Disco 160GB •Placa Gráfica Nvidia Quadro FX3000 •Placa de Rede Intel Pro1000 •Rato Óptico; Monitor Acer AL1912/PCs Gateway: •CPU P4 3.4GHz •RAM 2048MB •Disco 160GB •Placa Gráfica Nvidia Quadro FX3000 •Placa de Rede Intel Pro1000 •Rato Óptico; Monitor Acer AL1912	10
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Fujitsu Siemens CTM 5020	10
Fato para Captura de Movimento NaturalPoint /Fato para Captura de Movimento NaturalPoint	1
Impressora/Impressora	1
Computador pessoal/Computador pessoal	22
Eq. Video-conferência/Eq. Video-conferência	1
PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway/PCs: •CPU P4 3.0GHz •RAM 1GB •Disco 80GB •Placa Gráfica Intel 82915G/82910GL •Placa de Rede Realtek 8169/8110 gigabit •Rato Óptico; Monitor Gateway	9

## 3.2 Parcerias

### 3.2.1 Eventuais parcerias internacionais estabelecidas no âmbito do ciclo de estudos.

*O programa de segurança de informação é um dos programas de doutoramento em Portugal que participa no programa de cooperação CMU|Portugal.*

### 3.2.1 International partnerships within the study cycle.

*The information security PhD program is one of the Portuguese PhD programs that participates in the CMU|Portugal cooperation program.*

### 3.2.2 Colaborações com outros ciclos de estudos, bem como com outras instituições de ensino superior nacionais.

*Existe uma interacção muito forte entre o programa de segurança de informação e os programas de mestrado e doutoramento em matemática, engenharia electrotécnica e informática, dada a natureza interdisciplinar deste programa.*

### 3.2.2 Collaboration with other study cycles of the same or other institutions of the national higher education system.

*There is a strong interaction between the PhD program in information security and the PhD and MSc programs in mathematics, electrical engineering and informatics, given the interdisciplinary nature of the program.*

### 3.2.3 Procedimentos definidos para promover a cooperação interinstitucional no ciclo de estudos.

*Há cooperação protocolada entre o IST e diversas Universidades Públicas Portuguesas. Com entidades públicas ou privadas são feitos protocolos específicos associados a cada projecto de investigação.*

### 3.2.3 Procedures to promote inter-institutional cooperation within the study cycle.

*There is cooperation between the IST and several Portuguese public universities. With public or private entities are made specific protocols associated with each research project.*

### 3.2.4 Práticas de relacionamento do ciclo de estudos com o tecido empresarial e o sector público.

*Protocolo de Cooperação Pedagógica, Científica e Técnica entre a Escola Naval, a Faculdade de Direito da Universidade de Lisboa e o Instituto Superior Técnico, na área da Segurança de Informação e do Direito no Ciberespaço.*

### 3.2.4 Relationship of the study cycle with business network and the public sector.

*Pedagogical, Scientific and Technical cooperation agreement between the Naval School, the Law School of the Lisbon University and IST in the area of Information security and cyberspace law.*

## 4. Pessoal Docente e Não Docente

### 4.1. Pessoal Docente

---

#### 4.1.1. Fichas curriculares

Mapa VIII - José Félix Gomes da Costa

4.1.1.1. Nome do docente (preencher o nome completo):

*José Félix Gomes da Costa*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

*Professor Associado ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):

*100.000000*

4.1.1.6. Ficha curricular de docente:

[Mostrar dados da Ficha Curricular](#)

Mapa VIII - João Luís da Costa Campos Gonçalves Sobrinho

4.1.1.1. Nome do docente (preencher o nome completo):

*João Luís da Costa Campos Gonçalves Sobrinho*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

*Professor Associado ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):

*100.000000*

4.1.1.6. Ficha curricular de docente:

[Mostrar dados da Ficha Curricular](#)

Mapa VIII - Ana Luísa Nobre Fred

4.1.1.1. Nome do docente (preencher o nome completo):

*Ana Luísa Nobre Fred*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

**Professor Auxiliar ou equivalente**

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Nikola Paunkovic**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Nikola Paunkovic*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

4.1.1.4. Categoria:  
*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*25*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Carlos Nuno da Cruz Ribeiro**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Carlos Nuno da Cruz Ribeiro*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
*<sem resposta>*

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
*<sem resposta>*

4.1.1.4. Categoria:  
*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Miguel Nuno Dias Alves Pupo Correia**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Miguel Nuno Dias Alves Pupo Correia*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
*<sem resposta>*

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
*<sem resposta>*

4.1.1.4. Categoria:

**Professor Associado ou equivalente**

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Mário Alexandre Teles de Figueiredo**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Mário Alexandre Teles de Figueiredo*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
*<sem resposta>*

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
*<sem resposta>*

4.1.1.4. Categoria:  
*Professor Catedrático ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Luís Henrique Martins Borges de Almeida**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Luís Henrique Martins Borges de Almeida*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
*<sem resposta>*

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
*<sem resposta>*

4.1.1.4. Categoria:  
*Professor Catedrático ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Luís Eduardo Teixeira Rodrigues**

4.1.1.1. Nome do docente (preencher o nome completo):  
*Luís Eduardo Teixeira Rodrigues*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
*<sem resposta>*

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
*<sem resposta>*

**4.1.1.4. Categoria:**

*Professor Catedrático ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**

*100.000000*

**4.1.1.6. Ficha curricular de docente:**

[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Paulo Alexandre Carreira Mateus****4.1.1.1. Nome do docente (preencher o nome completo):**

*Paulo Alexandre Carreira Mateus*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**

*<sem resposta>*

**4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):**

*<sem resposta>*

**4.1.1.4. Categoria:**

*Professor Associado ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**

*100.000000*

**4.1.1.6. Ficha curricular de docente:**

[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Carlos Manuel Costa Lourenço Caleiro****4.1.1.1. Nome do docente (preencher o nome completo):**

*Carlos Manuel Costa Lourenço Caleiro*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**

*<sem resposta>*

**4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):**

*<sem resposta>*

**4.1.1.4. Categoria:**

*Professor Associado ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**

*100.000000*

**4.1.1.6. Ficha curricular de docente:**

[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Ricardo Jorge Fernandes Chaves****4.1.1.1. Nome do docente (preencher o nome completo):**

*Ricardo Jorge Fernandes Chaves*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**

*<sem resposta>*



**4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):**  
<sem resposta>

**4.1.1.4. Categoria:**  
*Professor Auxiliar ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**  
*100.000000*

**4.1.1.6. Ficha curricular de docente:**  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Pedro Miguel dos Santos Alves Madeira Adão**

**4.1.1.1. Nome do docente (preencher o nome completo):**  
*Pedro Miguel dos Santos Alves Madeira Adão*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**  
<sem resposta>

**4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):**  
<sem resposta>

**4.1.1.4. Categoria:**  
*Professor Auxiliar ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**  
*100.000000*

**4.1.1.6. Ficha curricular de docente:**  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Alexandre Paulo Lourenço Francisco**

**4.1.1.1. Nome do docente (preencher o nome completo):**  
*Alexandre Paulo Lourenço Francisco*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**  
<sem resposta>

**4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):**  
<sem resposta>

**4.1.1.4. Categoria:**  
*Professor Auxiliar ou equivalente*

**4.1.1.5. Regime de tempo na instituição que submete a proposta (%):**  
*100.000000*

**4.1.1.6. Ficha curricular de docente:**  
[Mostrar dados da Ficha Curricular](#)

**Mapa VIII - Vítor João Rocha Vieira**

**4.1.1.1. Nome do docente (preencher o nome completo):**  
*Vítor João Rocha Vieira*

**4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):**

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

*Professor Catedrático convidado ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):

*33.000000*

4.1.1.6. Ficha curricular de docente:

[Mostrar dados da Ficha Curricular](#)

Mapa VIII - Maria Margarida Campos da Silveira

4.1.1.1. Nome do docente (preencher o nome completo):

*Maria Margarida Campos da Silveira*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):

*100.000000*

4.1.1.6. Ficha curricular de docente:

[Mostrar dados da Ficha Curricular](#)

Mapa VIII - Amílcar dos Santos Costa Sernadas

4.1.1.1. Nome do docente (preencher o nome completo):

*Amílcar dos Santos Costa Sernadas*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):

<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):

<sem resposta>

4.1.1.4. Categoria:

*Professor Catedrático ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):

*100.000000*

4.1.1.6. Ficha curricular de docente:

[Mostrar dados da Ficha Curricular](#)

Mapa VIII - Artur Miguel do Amaral Arsénio

4.1.1.1. Nome do docente (preencher o nome completo):

*Artur Miguel do Amaral Arsénio*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
<sem resposta>

4.1.1.4. Categoria:  
*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

#### Mapa VIII - João Filipe Quintas dos Santos Rasga

4.1.1.1. Nome do docente (preencher o nome completo):  
*João Filipe Quintas dos Santos Rasga*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
<sem resposta>

4.1.1.4. Categoria:  
*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

#### Mapa VIII - Vasco Miguel Gomes Nunes Manquinho

4.1.1.1. Nome do docente (preencher o nome completo):  
*Vasco Miguel Gomes Nunes Manquinho*

4.1.1.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):  
<sem resposta>

4.1.1.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):  
<sem resposta>

4.1.1.4. Categoria:  
*Professor Auxiliar ou equivalente*

4.1.1.5. Regime de tempo na instituição que submete a proposta (%):  
*100.000000*

4.1.1.6. Ficha curricular de docente:  
[Mostrar dados da Ficha Curricular](#)

4.1.2 Equipa docente do ciclo de estudos (preenchimento automático após submissão do guião)

**4.1.2. Equipa docente do ciclo de estudos / Study cycle's academic staff**

<b>Nome / Name</b>	<b>Grau / Degree</b>	<b>Área científica / Scientific Area</b>	<b>Regime de tempo / Employment link</b>	<b>Informação/ Information</b>
José Félix Gomes da Costa	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
João Luís da Costa Campos Gonçalves Sobrinho	Doutor	ENG. ELECTROTECNICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Ana Luísa Nobre Fred	Doutor	ENG. ELECTROTECNICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Nikola Paunkovic	Doutor	Theoretical Physics	25	<a href="#">Ficha submetida</a>
Carlos Nuno da Cruz Ribeiro	Doutor	ENGENHARIA INFORMATICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Miguel Nuno Dias Alves Pupo Correia	Doutor	INFORMATICA	100.000000	<a href="#">Ficha submetida</a>
Mário Alexandre Teles de Figueiredo	Doutor	ENG. ELECTROTECNICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Luís Henrique Martins Borges de Almeida	Doutor	ENGENHARIA ELECTROTECNICA	100.000000	<a href="#">Ficha submetida</a>
Luís Eduardo Teixeira Rodrigues	Doutor	ENG. ELECTROTECNICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Paulo Alexandre Carreira Mateus	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
Carlos Manuel Costa Lourenço Caleiro	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
Ricardo Jorge Fernandes Chaves	Doutor	Secure Comput on Reconfigurable Systems	100.000000	<a href="#">Ficha submetida</a>
Pedro Miguel dos Santos Alves Madeira Adão	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
Alexandre Paulo Lourenço Francisco	Doutor	ENGENHARIA INFORMATICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Vítor João Rocha Vieira	Doutor	CIENCIAS "FISICA DA MATERIA CONDENSADA"	33.000000	<a href="#">Ficha submetida</a>
Maria Margarida Campos da Silveira	Doutor	ENG. ELECTROTECNICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
Amílcar dos Santos Costa Sernadas	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
Artur Miguel do Amaral Arsénio	Doutor	Electrical Engineering and Comp Science	100.000000	<a href="#">Ficha submetida</a>
João Filipe Quintas dos Santos Rasga	Doutor	MATEMATICA	100.000000	<a href="#">Ficha submetida</a>
Vasco Miguel Gomes Nunes Manquinho	Doutor	ENGENHARIA INFORMATICA E DE COMPUTADORES	100.000000	<a href="#">Ficha submetida</a>
			<b>1858</b>	

**<sem resposta>****4.1.3. Dados da equipa docente do ciclo de estudos****4.1.3.1.a Número de docentes em tempo integral na instituição****20****4.1.3.1.b Percentagem dos docentes em tempo integral na instituição (campo de preenchimento automático, calculado após a submissão do formulário)****107,6****4.1.3.2.a Número de docentes em tempo integral com uma ligação à instituição por um período superior a três anos****20****4.1.3.2.b Percentagem dos docentes em tempo integral com uma ligação à instituição por um período superior a três anos (campo de preenchimento automático, calculado após a submissão do formulário)****107,6**

**4.1.3.3.a Número de docentes em tempo integral com grau de doutor**

20

**4.1.3.3.b Percentagem de docentes em tempo integral com grau de doutor (campo de preenchimento automático, calculado após a submissão do formulário)**

107,6

**4.1.3.4.a Número (ETI) de docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano**

23

**4.1.3.4.b Percentagem dos docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (campo de preenchimento automático calculado após a submissão do formulário)**

123,8

**4.1.3.5.a Número (ETI) de docentes do ciclo de estudos não doutorados com grau de mestre (pré-Bolonha)**

&lt;sem resposta&gt;

**4.1.3.5.b Percentagem dos docentes do ciclo de estudos não doutorados com grau de mestre (pré-Bolonha) (campo de preenchimento automático calculado após a submissão do formulário)**

&lt;sem resposta&gt;

**Perguntas 4.1.4. e 4.1.5****4.1.4. Procedimento de avaliação do desempenho do pessoal docente e medidas para a sua permanente actualização**

*A avaliação do desempenho do pessoal docente do IST assenta no sistema multicritério definido no "Regulamento de Avaliação de Desempenho dos Docentes do Instituto Superior Técnico (RADIST)" (Despacho Reitoral n.º 4576/2010, DR 2ª Série, n.º 51 de 15 de Março), sendo aplicado a cada docente, individualmente e nos períodos estipulados por Lei. Permite a avaliação quantitativa da actuação do pessoal docente nas diferentes vertentes, e reflecte-se, nomeadamente, sobre a distribuição de serviço docente regulamentada pelo Despacho Reitoral n.º 8985/2011 (DR, 2ª Série, N.º 130 de 8 de Julho). O Conselho Coordenador da Avaliação do Docente (CCAD) do IST, no exercício das competências previstas no RADIST, elaborou um relatório sobre as avaliações de desempenho dos docentes relativas aos períodos 2004-2007 e 2008-2009 que já foram realizadas. Este relatório que fornece ampla informação sobre as avaliações realizadas, respeitando escrupulosamente o princípio da confidencialidade dos resultados da avaliação de cada docente estabelecido no artigo 30º do RADIST, foi objecto de discussão nos diferentes Órgãos do IST. Em resultado desta discussão, da experiência adquirida nas avaliações anteriores e das audiências sindicais, que foram efectuadas nos termos previstos na lei, foram produzidas actualizações do RADIST que foram recentemente aprovadas pelos Órgãos competentes do IST e que aguardam homologação do Reitor da Universidade Técnica de Lisboa para publicação em Diário da República. Paralelamente, a avaliação das actividades pedagógicas é efectuada recorrendo ao Sistema de Garantia da Qualidade das Unidades Curriculares. Este sistema baseia-se na realização de inquéritos pedagógicos aos alunos, na avaliação por parte de coordenadores de curso e delegados de curso, na realização de auditorias de qualidade e na elaboração de códigos de boas práticas.*

**4.1.4. Assessment of academic staff performance and measures for its permanent updating**

*The performance assessment of IST teaching-staff relies on the multicriterion system defined in the "Performance bylaw of the IST Teaching-staff" (Rectorial Order 4576/2010, Government Journal 2nd Series, No. 51 of 15 March), which is applied individually to each teacher during the periods established by law. The quantitative assessment of the teaching staff performance is reflected in different strands, namely, on the allocation of teaching tasks that is governed by the Rectorial Order 8985/2011 (Government Journal, 2nd Series, No. 130 of 8th July). Pursuant to the powers and responsibilities conferred upon it under the RADIST, the Coordinating Board for Teacher Evaluation (CCAD) elaborated a teachers' performance report for the periods 2004-2007 and 2008-2009, which were already carried out. This report, which provides extensive information on such evaluations, with scrupulous regard for the principle of confidentiality of each teacher's results established in article 30 of RADIST, was discussed in the different bodies of IST. After this discussion, the experience acquired in previous evaluations and several union audiences, which were carried out under the terms set out in the law, the RADIST went through updates, which were adopted by the relevant bodies of IST, which are still awaiting approval from the Rector of the Technical University of Lisbon for publication in the Official Journal. In parallel, the teaching activities evaluation is performed using the Quality Guarantee System of the curricular units. This system is based on pedagogic surveys to the students, on the performance evaluation implemented by the course coordinators and student delegates and on quality audits and elaboration of good practice codes.*

**4.1.5. Ligação facultativa para o Regulamento de Avaliação de Desempenho do Pessoal Docente**

<https://dspace.ist.utl.pt/bitstream/2295/685495>

</1/Regulamento%20de%20avaliacao%20de%20desempenho%20dos%20docentes%20-%20IST%20Alteracao%2029Jun2010.pdf>

## 4.2. Pessoal Não Docente

---

### 4.2.1. Número e regime de dedicação do pessoal não docente afecto à leccionação do ciclo de estudos.

*O programa é apoiado por 1 funcionário não docente partilhado com os programas de doutoramento em matemática e doutoramento em estatística e processos estocásticos.*

### 4.2.1. Number and work regime of the non-academic staff allocated to the study cycle.

*We have 1 staff member for support of the program shared with the PhD program in mathematics and statistics and stochastic processes.*

### 4.2.2. Qualificação do pessoal não docente de apoio à leccionação do ciclo de estudos.

*12º ano.*

### 4.2.2. Qualification of the non academic staff supporting the study cycle.

*12th grade.*

### 4.2.3. Procedimentos de avaliação do desempenho do pessoal não docente.

*O IST implementa o SIADAP desde a sua criação jurídica, em 2004. Após a revisão de 2007, com a Lei n.º 66-B/2007, de 28 de Dezembro, que o IST integra os subsistemas:*

*- de Avaliação do Desempenho dos Dirigentes da Administração Pública - SIADAP 2*

*- de Avaliação do Desempenho dos Trabalhadores da Administração Pública - SIADAP 3*

*Todo este processo foi desmaterializado e está disponível no sistema de informação do IST, FENIX, sendo acedido pelos vários intervenientes (avaliadores e avaliados) electronicamente.*

*Mais informação disponível na página do IST na Internet (Pessoal/ Direcção de Recursos Humanos/Não Docentes/Avaliação (SIADAP))*

### 4.2.3. Procedures for assessing the non academic staff performance.

*Back in 2004, since its legal creation, the IST implemented the SIADAP. After being reviewed in 2007 with Law 66-B/2007 of December 28th, the IST has participated in the following subsystems:*

*Assessment of Performance of the Senior Officials of the State Administration - SIADAP 2*

*Assessment of Performance of the Employees of the State Administration - SIADAP 3*

*All this process has been dematerialised, is available at IST's information System, FENIX, and can be accessed by the different stakeholders (assessors and assessed) electronically.*

*Further info available at IST webpage (Staff/Staff Area/Não Docentes/Avaliação (SIADAP))*

### 4.2.4. Cursos de formação avançada ou contínua para melhorar as qualificações do pessoal não docente.

*O IST tem uma política de gestão de recursos humanos que afirma a formação como factor crítico para melhorar a performance dos seus profissionais, visando aumentar os níveis de produtividade. Em 2006 desenhou um Plano de Formação para formar os colaboradores em temáticas relevantes para a sua actividade: TIC; Comunicação; Gestão; Língua Inglesa. Incluiu a aprendizagem do Sistema de Informação que suporta a Gestão Académica na Escola. Foi proporcionada formação avançada a quadros dirigentes do IST no INA. Em 2012 submeteu uma candidatura ao QREN para desenvolver acções de formação para o quadro de pessoal do IST dotando-o de competências adequadas às exigências do mundo global que obriga todas as instituições a pautar-se pela excelência em toda a sua organização. Esta candidatura foi aprovada e encontra-se em execução durante o corrente ano lectivo, abrangendo exclusivamente os funcionários não docentes do IST em áreas temáticas críticas.*

### 4.2.4. Advanced or continuing training courses to improve the qualifications of the non academic staff.

*IST's resource management policy focuses on training as the critical factor to improve the performance of its professionals, with a view to increasing productivity levels. In 2006 a Training Plan was designed to training its collaborators in areas that are relevant to its activity: ICT; Communication; Management; English as a foreign language, including the Information System that supports its Academic Management. Senior officers have been provided with training at INA. In 2012, a proposal was submitted to QREN for the development of training actions oriented to IST staff. The purpose was to equip it with skills, which cater for the requirements of the global world, in that all institutions must guide their activity with excellence. This proposal was approved and is active during this academic year, exclusively targeted for IST non-teaching staff in critical issues.*

## 5. Estudantes e Ambientes de Ensino/Aprendizagem

## 5.1. Caracterização dos estudantes

---

### 5.1.1. Caracterização dos estudantes inscritos no ciclo de estudos, incluindo o seu género, idade, região de proveniência e origem socioeconómica (escolaridade e situação profissional dos pais).

#### 5.1.1.1. Por Género

##### 5.1.1.1. Caracterização por género / Characterisation by gender

Género / Gender	%
Masculino / Male	83
Feminino / Female	17

#### 5.1.1.2. Por Idade

##### 5.1.1.2. Caracterização por idade / Characterisation by age

Idade / Age	%
Até 20 anos / Under 20 years	0
20-23 anos / 20-23 years	0
24-27 anos / 24-27 years	67
28 e mais anos / 28 years and more	33

#### 5.1.1.3. Por Região de Proveniência

##### 5.1.1.3. Caracterização por região de proveniência / Characterisation by region of origin

Região de proveniência / Region of origin	%
Norte / North	0
Centro / Centre	0
Lisboa / Lisbon	100
Alentejo / Alentejo	0
Algarve / Algarve	0
Ilhas / Islands	0

#### 5.1.1.4. Por Origem Socioeconómica - Escolaridade dos pais

##### 5.1.1.4. Caracterização por origem socioeconómica - Escolaridade dos pais / By Socio-economic origin – parents' education

Escolaridade dos pais / Parents	%
Superior / Higher	67
Secundário / Secondary	17
Básico 3 / Basic 3	0
Básico 2 / Basic 2	0
Básico 1 / Basic 1	17

#### 5.1.1.5. Por Origem Socioeconómica - Situação profissional dos pais

##### 5.1.1.5. Caracterização por origem socioeconómica - Situação profissional dos pais / By socio-economic origin – parents' professional situation

Situação profissional dos pais / Parents	%
--	---

Empregados / Employed	58
Desempregados / Unemployed	0
Reformados / Retired	25
Outros / Others	17

### 5.1.2. Número de estudantes por ano curricular

#### 5.1.2. Número de estudantes por ano curricular / Number of students per curricular year

Ano Curricular / Curricular Year	Número / Number
Doutoramento	6
	6

### 5.1.3. Procura do ciclo de estudos por parte dos potenciais estudantes nos últimos 3 anos.

#### 5.1.3. Procura do ciclo de estudos / Study cycle demand

	2010/11	2011/12	2012/13
N.º de vagas / No. of vacancies	0	0	0
N.º candidatos 1.ª opção / No. 1st option candidates	0	0	0
N.º colocados / No. enrolled students	0	0	0
N.º colocados 1.ª opção / No. 1st option enrolments	0	0	0
Nota mínima de entrada / Minimum entrance mark	0	0	0
Nota média de entrada / Average entrance mark	0	0	0

## 5.2. Ambiente de Ensino/Aprendizagem

### 5.2.1. Estruturas e medidas de apoio pedagógico e de aconselhamento sobre o percurso académico dos estudantes.

*O percurso académico dos estudantes de doutoramento e nomeadamente a dissertação é acompanhada não só pelo orientador como também pelo coordenador do programa.*

*Os alunos podem recorrer a apoio psicológico no núcleo de Serviços Médicos, Apoio e Avaliação Psicológica (SMAP) que tem como compromisso diagnosticar e tratar de forma célere e eficaz quem a ele recorre.*

### 5.2.1. Structures and measures of pedagogic support and counseling on the students' academic path.

*The PhD students' academic path and in particular the dissertation is followed carefully not only by the advisor but also by the program coordinator. Students may also have psychological support at the Medical Unit (SMAP) which aims at diagnosing and treat patients in a quick manner.*

### 5.2.2. Medidas para promover a integração dos estudantes na comunidade académica.

*Seminários de investigação regulares. Encontros informais.*

### 5.2.2. Measures to promote the students' integration into the academic community.

*Regular research seminars. Informal meetings.*

### 5.2.3. Estruturas e medidas de aconselhamento sobre as possibilidades de financiamento e emprego.

*O Núcleo de Parcerias Empresarias do IST dinamiza as relações com as empresas, o apoio ao empreendedorismo e o desenvolvimento de carreiras dos alunos. Neste âmbito mantém os programas: IST Job Bank (plataforma de emprego); IST Career Sessions (sessões de informação sobre os processos de recrutamento); IST Career Workshops (ações de formação de preparação para o recrutamento para as quais é realizado o concurso de bolsas IST Career Scholarships); IST Career Weeks (semanas de apresentação das empresas divididas por área); AEIST Jobshop (feira e semana de negociação de emprego) IST Summer Internships (estágios de verão em empresas). No fomento ao empreendedorismo destaca-se: a Comunidade IST SPIN-OFF com empresas cujas origens estão ligadas ao IST e o fundo de capital de risco ISTART I promovido pelo IST. Coordena também os múltiplos eventos ligados ao empreendedorismo que ocorrem regularmente no IST e faz a ligação às incubadoras associadas ao IST: Taguspark, Lispolis e Startup Lisboa.*



### 5.2.3. Structures and measures for providing advice on financing and employment possibilities.

*The Corporate Partnerships Unit of IST seeks to foster the relationship with companies, the support to entrepreneurship and the development of student careers. Thus, it maintains the following programs: IST Job Bank(recruitment platform);IST Career Sessions(information sessions regarding the recruitment processes);IST Career Workshops(training actions for the preparation of recruitment for which the IST Career Scholarships are available);IST Career Weeks(company presentations divided by area);AEIST Jobshop (employment fair and negotiation week)IST Summer Internships(student internships in companies).Regarding fostering entrepreneurship, the following should be pointed out: the IST SPIN-OFF Community with companies whose origins are linked to IST and the venture capital fund ISTART I promoted by IST. It is also responsible for coordinating all the events linked to entrepreneurship that takes place at IST and links it to IST-associated incubators:Taguspark, Lispolis and StartupLisboa.*

### 5.2.4. Utilização dos resultados de inquéritos de satisfação dos estudantes na melhoria do processo ensino/aprendizagem.

*No âmbito do sistema de gestão da qualidade do IST (ver 2.2 para mais detalhes) foi desenvolvido o subsistema de Garantia da Qualidade do Processo de Ensino e Aprendizagem no IST (QUC). Este subsistema tem como objetivos centrais: a monitorização em tempo útil do funcionamento de cada UC face aos objetivos para ela estabelecidos nos planos curriculares dos cursos oferecidos pelo IST; e a promoção da melhoria contínua do processo de ensino, aprendizagem e avaliação do aluno e do seu envolvimento no mesmo. Um dos instrumentos de recolha de informação previsto no QUC é um inquérito aos estudantes congregando as suas opiniões sobre vários aspetos do processo de ensino e aprendizagem de cada UC, contudo, por ora este sistema apenas está disponível para formações de 1º e 2º ciclo, nos casos de unidades curriculares com funcionamento em regime regular, mas em breve prevê-se o seu alargamento a outras UC/ciclos.*

### 5.2.4. Use of the students' satisfaction inquiries on the improvement of the teaching/learning process.

*As part of the IST's quality management system (see 2.2 for further details), the Quality Assurance Subsystem of the Teaching and Learning process of IST was developed. It provides real time monitoring how each course unit is run in view of the desired goals in the curricula of the programmes offered by IST, and promoted continuous improvement of the teaching, learning and evaluation process of students and their involvement in it. One of its data collection instruments, at the end of each semester is to conduct a student survey and to ask students' representatives to complete a report, putting together their opinions on different aspects of the teaching and learning process of each course unit. This system is only available for 1st and 2nd cycle programmes, in common course units, but it will soon be extended to other course units/cycles.*

### 5.2.5. Estruturas e medidas para promover a mobilidade, incluindo o reconhecimento mútuo de créditos.

*O IST tem reforçado as ações de internacionalização, através da participação em redes de escolas de referência, como o CLUSTER, MAGALHÃES, TIME e CESAER. Além da oferta de programas de Mestrado e Doutoramento, o IST aumentou a atratividade e o número de estudantes internacionais, nomeadamente do Norte da Europa, através de uma política de utilização da Língua Inglesa no ensino. Além dos graus de mestrado duplo na rede CLUSTER ou TIME, o IST participa ativamente no programa Erasmus Mundus II, tendo atualmente em curso 2 programas de M.Sc e 4 de PhD, além de mais de 5 Projectos Partnership. Prossegue o forte envolvimento do IST nas parcerias com o MIT, CMU, UTAustin e EPFL. O IST é a ainda única instituição Portuguesa full partner de uma Knowledge and Innovation Community do EIT, no âmbito da KIC Innoenergy. No âmbito dos vários programas de mobilidade o período de estudos é reconhecido através do sistema ECTS.*

### 5.2.5. Structures and measures for promoting mobility, including the mutual recognition of credits.

*The IST has sought to reinforce internationalization initiatives by participating in reference university networks, such as CLUSTER, MAGALHAES, TIME and CESAER. In addition to its MSc and PhD programmes, the IST has increased its attractiveness and the number of international students, namely those from Northern Europe through a policy of widespread use of the English language in its programmes. In addition to the double master's degrees at the CLUSTER network (which presides over it) or TIME, the IST has actively participated in the Erasmus Mundus II programme, currently running 2 MSC and 4 PhD programmes, besides more than 5 Partnership Projects. The IST has been increasingly involved in partnerships with MIT, CMU, UTAustin and EPFL. The IST is the only Portuguese full partner institution of a Knowledge and Innovation Community of EIT, as part of KIC Innoenergy. Under different mobility programmes the period of study is recognized through the ECTS system.*

## 6. Processos

### 6.1. Objectivos de ensino, estrutura curricular e plano de estudos

6.1.1. Objectivos de aprendizagem (conhecimentos, aptidões e competências) a desenvolver pelos estudantes, operacionalização dos objectivos e medição do seu grau de cumprimento.

***O doutoramento visa o aprofundamento do conhecimento em áreas específicas de segurança de informação e em áreas de fronteira com outros ramos do conhecimento. Tem como objectivo a habilitação para o desempenho de actividades de investigação científica e desenvolvimento tecnológico independente, de qualidade internacionalmente reconhecida, em instituições de ensino superior, em laboratórios de investigação e em serviços especializados da administração pública e do sector empresarial.***

**6.1.1. Learning outcomes to be developed by the students, their translation into the study cycle, and measurement of its degree of fulfillment.**

***The aim of a PhD programme is to provide and create specialized knowledge in emerging scientific, technical and or technological areas in information security.***

***Its purpose is to provide the qualification necessary to carry out scientific research and independent technological development activities, of internationally renowned quality, in higher education institutions, research laboratories and specialized services of the public administration and of the business sector.***

**6.1.2. Demonstração de que a estrutura curricular corresponde aos princípios do Processo de Bolonha.**

***O processo de Bolonha consagrou a implementação de três importantes linhas de atuação no ES: o modelo de organização em três ciclos; o sistema de créditos ECTS; a transição de um sistema de ensino baseado na ideia da transmissão de conhecimentos para um baseado no desenvolvimento de competências. Todos os ciclos de estudo do IST foram adequados a Bolonha no ano lectivo de 2006/2007. Assim, às cargas de trabalho foi alocada uma correspondência ECTS. Para além disso, o IST tem um ensino fortemente baseado em três vectores estruturantes: uma sólida formação em ciências básicas (estruturante sobretudo a nível do 1º ciclo); uma forte componente de aplicação à prática de engenharia (estruturante sobretudo a nível do 2º ciclo); uma forte componente de investigação (estruturante sobretudo a nível do 3º ciclo). A implementação e contínua melhoria destes três vectores asseguram que o IST garante o cumprimento dos princípios de Bolonha ao mais elevado nível em todos os seus ciclos de estudo.***

**6.1.2. Demonstration that the curricular structure corresponds to the principles of the Bologna process.**

***The Bologna process enshrined the implementation of three important lines of action in HE: the adoption of a 3-cycle organization model; the adoption of the ECTS credit system; the transition of a knowledge-based system into a skill development based system. All study cycles taught at IST have been suited to the Bologna requirements in 2006/2007. The workloads have been allocated a number of ECTS. In addition, the IST provides teaching based on three strands: sound background in basic sciences (which is structural in particular for the 1st cycle); strong experimental component (which is structural in particular for the 2nd cycle); strong research component (which is structural in particular for the 3rd cycle). The implementation and steady improvement of these strands ensure that the IST fully complies with the Bologna standards at the highest level of its study cycles.***

**6.1.3. Periodicidade da revisão curricular e forma de assegurar a actualização científica e de métodos de trabalho.**

***As revisões curriculares não têm periodicidade pré-determinada. As revisões curriculares - propostas pelas coordenações de curso, ouvidas as comissões científicas e pedagógicas de curso, e submetidas a parecer do conselho científico, pedagógico e de gestão – são efectuadas sempre que há necessidade de atualizar conteúdos programáticos das unidades curriculares, necessidade de otimizar percursos académicos ou imposições exógenas ao curso, tais como atualização de áreas científicas ou disciplinares, criação ou extinção de unidades académicas.***

**6.1.3. Frequency of curricular review and measures to ensure both scientific and work methodologies updating.**

***Curriculum review is not carried out on a regularly basis. The curricula, proposed by the program coordinators, in consultation with the scientific and pedagogical committees of each program and submitted to the opinion of the scientific, pedagogical and management boards – undergo reviews whenever there is the need to update the syllabuses, to optimize academic paths or obligations that are exogenous to the program, such as the update of scientific or discipline areas or the creation or extinctions of academic units.***

**6.1.4. Modo como o plano de estudos garante a integração dos estudantes na investigação científica.**

***A formação a adquirir durante o ciclo de estudos conducente ao Doutoramento em Segurança de Informação tem uma componente curricular e uma componente de investigação (tese).***

***A parte curricular é constituído por unidades curriculares (UCs) de base científica adequadas à formação para a investigação proposta. É requerida a aprovação em 10 unidades curriculares (60 ECTS). Para prosseguir no Programa, o aluno tem de obter aprovação, nos 2 anos após a matrícula, em 2 exames de qualificação, a escolher entre os seguintes:***

***Exame de qualificação em Lógica, Complexidade e Criptografia***

***Exame de qualificação em Segurança de Sistemas***

***Exame de qualificação em Teoria da Informação***

***A proposta de tese deverá ser apresentada publicamente até 24 meses após a matrícula. A proposta deve indicar o(s) problema(s) em aberto em que o candidato vai trabalhar com vista a produzir contribuições originais significativas.***

#### 6.1.4. Description of how the study plan ensures the integration of students in scientific research.

*The course of studies leading to a PhD in Information Security has a curricular component and a research component (thesis).*

*The curriculum component consists of units (CUs) of adequate scientific basis.*

*It is required the approval in 10 curricular units (60 ECTS).*

*Before starting the thesis work, the student must be approved, no later than the beginning of the third year, in 2 qualifying exams chosen among the following:*

*-Qualifying exam in Logic, Complexity and Cryptography (at DM);*

*-Qualifying exam in Systems Security (at DEI);*

*-Qualifying exam in Information Theory (at DEEC).*

*The thesis proposal must be presented in public within 24 months after enrollment with the agreement of the supervisor(s).*

*The proposal should indicate the open problem(s) in which the student wants to work towards producing significant original contributions. The proposal should also sketch the work plan so that submission is possible no later than 5 years after enrollment in the Program.*

## 6.2. Organização das Unidades Curriculares

---

### 6.2.1. Ficha das unidades curriculares

#### Mapa IX - Computação, Informação e Lógica Quânticas

##### 6.2.1.1. Unidade curricular:

*Computação, Informação e Lógica Quânticas*

##### 6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):

*Paulo Alexandre Carreira Mateus (0.0)*

##### 6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:

*Nikola Paunkovic (0.0)*

##### 6.2.1.3. Other academic staff and lecturing load in the curricular unit:

*Nikola Paunkovic (0.0)*

##### 6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

*Dominar os conceitos, resultados e técnicas emergentes da computação e informação quânticas, com ênfase no desenvolvimento e análise de correcção e complexidade de algoritmos e protocolos quânticos.*

##### 6.2.1.4. Learning outcomes of the curricular unit:

*Master the emerging concepts, results and techniques of quantum computation and information, with emphasis on the development and analysis of the correctness and computational complexity of quantum algorithms and protocols.*

##### 6.2.1.5. Conteúdos programáticos:

*Revisão dos conceitos e resultados relevantes de álgebra linear e teoria de operadores. Notação de Dirac. Postulados da mecânica quântica.*

*Lógica exógena quântica proposicional: concepção a partir dos postulados, sintaxe, semântica, sistema dedutivo de Hilbert, decidibilidade e completude fraca. Comparação com as lógicas de Birkhoff e von Neumann. Autómatos e sistemas de transições quânticos. Lógica dinâmica quântica.*

*Circuitos quânticos e conjuntos completos de portas quânticas. Classes de complexidade computacional quântica. Algoritmo de Deutsch-Jozsa. Transformada de Fourier quântica. Algoritmo de Shor. Pesquisa quântica: algoritmo de Grover, aceleração canónica de algoritmos de pesquisa. Passeios quânticos. Aceleração exponencial - algoritmo de Childs et al.*

*Entropia de von Neumann, majoração de Holevo. Entrelaçamento e desigualdades de Bell. Comunicação sobre canais quânticos. Correcção quântica de erros. ...*

**6.2.1.5. Syllabus:**

*Review of relevant concepts and results in linear algebra and operator theory. Dirac notation. Postulates of quantum mechanics.*

*Exogenous quantum propositional logic: design from the postulates, syntax, semantics, axiomatic system, decidability and weak completeness. Comparison with Birkhoff and von Neumann quantum logics. Quantum automata and transition systems. Dynamical quantum logic.*

*Quantum circuits and complete sets of quantum gates. Classes of quantum computational complexity. Deutsch-Jozsa algorithm. Quantum Fourier transform. Shor algorithm. Quantum search: Grover algorithm and variations, canonical speedup of search algorithms. Quantum walks. Exponential speedup - Child et al algorithm.*

*Von Neumann entropy and Holevo bound. Entanglement and Bell inequalities. Communication over quantum channels. Quantum error-correction. Cloning theorem. Quantum security: key distribution, key sharing, authentication, zero knowledge proof systems with quantum adversary, ...*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Exercícios (60%) e exame final (40%).*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Homework assignments (60%) and final exam (40%).*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*John Wiley, (volumes One and Two); Springer-Verlag, (Second Edition). ; Cambridge University Press*

**Mapa IX - Segurança Informática em Redes e Sistemas****6.2.1.1. Unidade curricular:**

*Segurança Informática em Redes e Sistemas*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Ricardo Jorge Fernandes Chaves (42.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

*Artur Miguel do Amaral Arsénio (105.0)*

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

*Artur Miguel do Amaral Arsénio (105.0)*

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*O objectivo desta cadeira é fornecer ao aluno um conjunto de conceitos, metodologias e ferramentas de segurança informática que lhe permita abordar o tema face a um conjunto de tecnologias alargado, tais como: redes locais, redes pessoais, redes globais, desenvolvimento de software, sistemas operativos, sistemas distribuídos, bases de dados, e sistemas de ficheiros.*

*A cadeira começará por definir um conjunto de conceitos de segurança informática, para depois identificar os componentes críticos da arquitectura de segurança de uma organização. Por fim para cada um destes componentes serão identificadas as suas vulnerabilidades, e descritas algumas metodologias e ferramentas para as eliminar.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*The main course goal is to provide the student with a set of security concepts, methodologies and tools which gives him the ability to handle security problems on a large spectrum of technologies, namely: local, personal and wide area networks, secure software development, operating systems, distributed systems, data bases, and file systems. The course starts by defining a set of security concepts and the elements comprising an organization security architecture. It then analyses the key elements of identifying the common vulnerabilities and the methodologies and tools to eliminate or mitigate them.*

**6.2.1.5. Conteúdos programáticos:**

*Introdução*

*Arquitectura de segurança de uma organização*

*Autenticação*

*Protocolos de Autenticação*

*Gestão de chaves e certificados*

*Controlo de Acessos*

*Modelos de Autorização*

*Gestão de confiança distribuída*

*Desenvolvimento de Software*

*Escrita de Código Seguro*

*Desenvolvimento de Protocolos Seguros*

*Redes*

*Firewalls e Sistemas de detecção de intrusos*

*Comunicação segura*

*Redes privadas virtuais*

*Gestão segura de redes*

*Sistemas de informação*

*Sistemas de ficheiros*

*Bases de dados*

**6.2.1.5. Syllabus:**

*Introduction*

*Organizations Security Architectures*

*Authentication*

*Authentication protocols*

*Key and certificate management*

*Access Control*

*Authorization Models*

*Distributed Trust Management*

*Software Development*

*Secure Code*

*Safe Protocols*

*Networks*

*Firewalls and Intrusion Detection Systems*

*Secure Communication*

*Virtual Private Networks*

*Secure Network Management*

*Secure storage*

*File systems*

*Databases*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points*

**syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

***A avaliação da cadeira será efectuada através de exame e um projecto laboratorial. O projecto e o exame contribuem cada um com 50% da avaliação final.***

***Para o aluno ser aprovado é necessário que a nota do projecto seja igual ou superior a 10 numa escala de 0 a 20, que a nota do exame seja igual ou superior a 8,0 numa escala de 0 a 20, e que a nota final seja igual ou superior a 10.***

**6.2.1.7. Teaching methodologies (including evaluation):**

***The course evaluation is comprised of two components: a project and an exam. Both, the project and the exam accounts for 50% of the total grade. Course approval is achieved when: the student achieved a score of 10 or more in the project, a score of 8,0 or more in the exam, and a combined score of 10, all in the scale from 0 to 20.***

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

***A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.***

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

***The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.***

**6.2.1.9. Bibliografia principal:**

***John Wiley and Sons ; ISBN: 0130351288; ISBN: 9727223990; Addison Wesley***

**Mapa IX - Protocolos de Segurança para Sistemas Distribuídos**

**6.2.1.1. Unidade curricular:**

***Protocolos de Segurança para Sistemas Distribuídos***

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

***Carlos Nuno da Cruz Ribeiro (0.0)***

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

**-**

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

**-**

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

***Efectuar uma análise e avaliação alargadas de diferentes protocolos de segurança para sistemas distribuídos.***

**6.2.1.4. Learning outcomes of the curricular unit:**

***Analyze security protocols for distributed systems.***

**6.2.1.5. Conteúdos programáticos:**

***Pretende-se avaliar protocolos com diferentes objectivos e para diferentes modelos de ameaças. A cadeira de segurança leccionada no segundo ciclo abordou alguns protocolos básicos de garantia de integridade e confidencialidade para o modelo de ameaças clássico de Dolev-Yao. Nesta cadeira pretende-se abordar protocolos para outros modelos de ameaças, nomeadamente aqueles em que não existe confiança nos interlocutores. Pretende-se também abordar protocolos para aplicações específicas, tais como: dinheiro electrónico, votação electrónica, negociação de contratos, redes de sensores, etc.***

**6.2.1.5. Syllabus:**

***The goal of the course is to evaluate and analyse different security protocols for distributed systems, considering different goals and different usage scenarios. Protocol goals will range from simple goals like connection authentication***

*to more complex ones like e-cash management. The course will analyse solutions for different goals under different scenarios, e.g. wireless sensor networks or large scale web services enrolment. The course will also analyse how changes to the classic Dolev-Yao threat model have impact on different protocols and evaluate solutions to the problem.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**  
*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**  
*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**  
*Exam + Project.*

**6.2.1.7. Teaching methodologies (including evaluation):**  
*Exame + Project.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**  
*Security for Wireless Sensor Networks, D. Liu and P. Ning, 2006, <http://www.springer.com/east/home?SGWID=5-102-22-173660373-0&changeHeader=true&SHORTCUT=www.springer.com/978-0-387-32723-5>*

## Mapa IX - Seminário de Investigação em Segurança de Informação I (C)

**6.2.1.1. Unidade curricular:**  
*Seminário de Investigação em Segurança de Informação I (C)*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**  
*Paulo Alexandre Carreira Mateus (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**  
 -

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**  
 -

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**  
*Contactar com tópicos de investigação recente em Segurança de Informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**  
*To make contact with recent research topics in Information Security.*

**6.2.1.5. Conteúdos programáticos:**  
*Frequentar e realizar apresentações em seminários da especialidade.*

**6.2.1.5. Syllabus:**

*To attend and prepare specialized seminars.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Criptografia e Protocolos de Segurança****6.2.1.1. Unidade curricular:**

*Criptografia e Protocolos de Segurança*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Conhecer os sistemas e protocolos criptográficos em uso, desenvolver protocolos para resolução de problemas específicos e perspetivar desenvolvimentos futuros.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Master cryptosystems and cryptographic protocols in current use, develop protocols to solve specific problems and forecast future developments.*

**6.2.1.5. Conteúdos programáticos:**

*Motivação: conceitos básicos e problemas centrais da criptografia.*



**Sistemas criptográficos de chave privada. Cifras sequenciais. Contributo da teoria da informação. Formas de ataque: dividir para conquistar e correlação rápida. Cifras por blocos. Exemplos típicos: DES e AES. Segurança perfeita e computacional.**

**Sistemas criptográficos de chave pública. Sistema RSA. Algoritmos de factorização e primalidade. Análise criptográfica quântica. Coordenadas projectivas. Curvas elípticas. Inteiros de Gauss. Algoritmo de Euclides para polinómios. Teorema de Hilbert. Bases de Gröbner. Sistemas criptográficos elípticos e hiperelípticos.**

**Protocolos de chave pública. Esquema de assinatura ElGamal e DSS. Algoritmos de assinatura digital baseados em curvas elípticas. Assinaturas cegas. Funções de dispersão. Esquemas de distribuição de chaves de Diffie-Hellman. Distribuição quântica de chaves. Protocolo estação para estação e MTI. ...**

#### 6.2.1.5. Syllabus:

**Basic concepts and central problems in cryptography.**

**Private key cryptosystems. Sequential ciphers. Contribution of information theory. Attacks: divide to conquer and fast correlation. Block ciphers. Examples: DES and AES. Perfect and computational security.**

**Public key cryptosystems. RSA cryptosystem. Factoring and primality algorithms. Quantum cryptoanalysis. Projective coordinates. Elliptic curves. Gauss integers. Euclidean algorithm for polynomials. Hilbert theorem. Gröbner bases. Elliptic and hyperelliptic cryptosystems.**

**Public key protocols. ElGamal signature scheme and DSS. Elliptic curve digital signature algorithms. Blind signatures. Hash functions. Diffie-Hellman key exchange scheme. Quantum key distribution protocols. Station to station and MTI protocols. Authentication codes. Shamir secret sharing scheme. Zero-knowledge proof systems. Schnorr and Fiat-Shamir identification protocols. Multi-party secure computation and applications.**

#### 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

#### 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

#### 6.2.1.7. Metodologias de ensino (avaliação incluída):

**Projecto (20%) e exame final (80%).**

#### 6.2.1.7. Teaching methodologies (including evaluation):

**Project (20%) and final examination (80%).**

#### 6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.

**A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

#### 6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.

**The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

#### 6.2.1.9. Bibliografia principal:

**DMIST, in preparation.; CRC Press**

### Mapa IX - Seminário de Investigação em Segurança de Informação II (A)

#### 6.2.1.1. Unidade curricular:

**Seminário de Investigação em Segurança de Informação II (A)**

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**  
*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**  
*Contactar com tópicos de investigação recente em Segurança de Informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**  
*To make contact with recent research topics in Information Security.*

**6.2.1.5. Conteúdos programáticos:**  
*Frequentar e realizar apresentações em seminários da especialidade.*

**6.2.1.5. Syllabus:**  
*To attend and prepare specialized seminars.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**  
*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**  
*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**  
*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**  
*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

## Mapa IX - Aprendizagem Automática

**6.2.1.1. Unidade curricular:**  
*Aprendizagem Automática*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

**Luís Henrique Martins Borges de Almeida (42.0)**

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

***Maria Margarida Campos da Silveira (42.0)***

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

***Maria Margarida Campos da Silveira (42.0)***

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

***Adquirir conhecimentos fundamentais sobre aprendizagem automática em geral, e sobre diversas técnicas de aprendizagem automática. Adquirir a capacidade de utilizar essas técnicas em aplicações concretas e de escolher as técnicas que melhor se adequem a cada situação.***

**6.2.1.4. Learning outcomes of the curricular unit:**

***To acquire basic knowledge about machine learning in general, and about several machine learning techniques. To acquire the capacity to use those techniques in applications and to choose the techniques that are more adequate for each situation.***

**6.2.1.5. Conteúdos programáticos:**

***Conceito de aprendizagem. Aprendizagem supervisionada e não supervisionada. Perspectiva histórica. Perceptrões multicamada. Aspectos estatísticos da aprendizagem supervisionada. O problema da generalização. Máquinas de suporte vectorial. Árvores de decisão. Agregação de dados e quantificação vectorial. Estimação de densidades de probabilidade. Análise em componentes principais***

**6.2.1.5. Syllabus:**

***Concept of machine learning. Supervised and unsupervised learning. Historical perspective. Multilayer perceptrons. Statistical aspects of supervised learning. The problem of generalization. Support vector machines Decision trees. Clustering and vector quantization. Estimation of probability densities. Principal components analysis.***

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

***Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.***

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

***Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.***

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

***Oito trabalhos de laboratório (peso de 50%) e exame final (peso de 50%).***

**6.2.1.7. Teaching methodologies (including evaluation):**

***Eight lab assignments (50% weight) and final exam (50% weight).***

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

***A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.***

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

***The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.***

**6.2.1.9. Bibliografia principal:**

***Machine Learning, Tom M. Mitchell, 1999, Prentice-Hall***

***Reconhecimento de Padrões: Métodos Estatísticos e Neurais, Jorge Salvador Marques, 1998, IST Press***

**Mapa IX - Lógica e Verificação de Modelos****6.2.1.1. Unidade curricular:**

*Lógica e Verificação de Modelos*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Aplicar lógica na verificação de sistemas de hardware e de software.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Apply logic to the verification of hardware and software.*

**6.2.1.5. Conteúdos programáticos:**

*Lógica proposicional. Diagramas de decisão binária. Lógica CTL. Verificação de modelos. Fairness. Caracterização dos operadores CTL como pontos fixos. Outras lógicas temporais. Verificação de sistemas concorrentes e distribuídos. Simulação e bi-simulação de modelos. Lógica de Hoare. Lógica modal e agentes. Lógica dinâmica. Lógica de 1a ordem, teorias decidíveis e aplicações.*

**6.2.1.5. Syllabus:**

*Propositional logic. Binary decision diagrams. Computation Tree Logic (CTL). Model checking. Fairness. Fixed-point characterization of CTL operators. Other temporal logics. Verification of concurrent and distributed systems. Simulation and bisimulation. Hoare logic. Modal logic and agents. Dynamic logic. First-order logic, decidable theories and applications.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Projecto (50%) + Exame Final (50%).*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Project (50%) + Final exam (50%).*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Cambridge University Press; MIT Press*

**Mapa IX - Seminário de Investigação em Segurança de Informação I (B)****6.2.1.1. Unidade curricular:**

*Seminário de Investigação em Segurança de Informação I (B)*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Paulo Alexandre Carreira Mateus (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Contactar com tópicos de investigação recente em Segurança de Informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*To make contact with recent research topics in Information Security.*

**6.2.1.5. Conteúdos programáticos:**

*Frequentar e realizar apresentações em seminários da especialidade.*

**6.2.1.5. Syllabus:**

*To attend and prepare specialized seminars.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

## Mapa IX - Algoritmos Avançados

### 6.2.1.1. Unidade curricular:

*Algoritmos Avançados*

### 6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):

*Alexandre Paulo Lourenço Francisco (48.069)*

### 6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:

*Vasco Miguel Gomes Nunes Manquinho (14.93100000000001)*

### 6.2.1.3. Other academic staff and lecturing load in the curricular unit:

*Vasco Miguel Gomes Nunes Manquinho (14.93100000000001)*

### 6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

*Formação avançada em técnicas de desenvolvimento de algoritmos eficientes e aplicações. Algoritmos para a resolução de problemas computacionalmente difíceis (NP-Hard). Identificação de aplicações de problemas computacionalmente difíceis. Métodos de procura para problemas NP-Hard. Algoritmos eficientes de aproximação e com escolhas aleatórias. Algoritmos eficientes para processamento online e em tempo real. Algoritmos paralelos e com acesso a memória externa.*

### 6.2.1.4. Learning outcomes of the curricular unit:

*Advanced training in techniques for the development of efficient algorithms and applications. Algorithms for solving computationally hard problems (NP-Hard). Identification of applications of computationally hard problems. Search methods for NP-Hard. Efficient algorithms for approximation and random choices. Efficient algorithms for online and real-time. Parallel algorithms and access to external memory.*

### 6.2.1.5. Conteúdos programáticos:

*Algoritmos de Aproximação para problemas NP-Hard. Métodos de procura completos para problemas NP-Hard: branch and bound; identificação de planos de corte; procura com retrocesso. Algoritmos gananciosos; programação dinâmica e algoritmos fracamente polinomiais. Métodos de procura local. Aplicações de Problemas NP-Hard. Algoritmos paralelos e com recurso memória externa. Algoritmos Online e em Tempo Real. Algoritmos com escolhas aleatórias. Algoritmos de aproximação para problemas polinomiais, e.g., algoritmos lineares para MSTs e algoritmos rápidos para cortes mínimos.*

### 6.2.1.5. Syllabus:

*Approximation Algorithms for NP-Hard problems. Complete search methods for NP-Hard problems: branch and bound; identifying cutting plans, backtrack search. Greedy algorithms, dynamic programming algorithms and weakly polynomial. Local search methods. Applications of NP-Hard problems. Parallel algorithms and using external memory. Online and real-time algorithms. Algorithms with random choices. Approximation algorithms to polynomial problems, e.g., linear algorithms for MSTs and fast algorithms for minimum cuts.*

### 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

### 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

### 6.2.1.7. Metodologias de ensino (avaliação incluída):

*Projecto (40%) + Exame (60%)*

### 6.2.1.7. Teaching methodologies (including evaluation):

*Project (40%) + Exam (60%)*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Wolsey: Integer and Combinatorial Optimization, G. L. Nemhauser and L. A, 1999, Wiley  
 Combinatorial Optimization, 2nd Edition, C. H. Papadimitriou and K. Steiglitz, 1998, Dover*

## Mapa IX - Algoritmos Probabilísticos

**6.2.1.1. Unidade curricular:**

*Algoritmos Probabilísticos*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*José Félix Gomes da Costa (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Desenvolver algoritmos probabilísticos, caracterizar classes computacionais probabilísticas, e verificar a correcção de programas*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Design probabilistic algorithms, characterize probabilistic classes, and perform program verification.*

**6.2.1.5. Conteúdos programáticos:**

*Máquinas de Turing probabilísticas. Máquinas-PP, -BPP-, -R-, e -ZPP. Monte Carlo versus Las Vegas. A hierarquia polinomial. Relação da hierarquia polinomial com as classes probabilísticas. Complexidade de problemas de optimização: classes PO e NPO. Aproximabilidade: classes APX, PAS, e FPAS. Sistemas de prova interactivos (Arthur versus Merlin). Classes IP and DIP. Verificação probabilística de provas. Limites de Chernoff: packet routing. Grafos aleatórios: hashing e circuitos hamiltonianos. Cadeias de Markov em tempo discreto e contínuo. Aplicações a máquinas de Boltzmann e redes neuronais estocásticas. Relativização de relações estruturais entre classes probabilísticas.*

**6.2.1.5. Syllabus:**

*Probabilistic Turing machines. PP-, BPP-, R-, and ZPP-machines. Monte Carlo versus Las Vegas. The polynomial time hierarchy. Probabilistic complexity classes and the polynomial time hierarchy. The complexity of optimization problems: classes PO and NPO. Approximability: classes APX, PAS, and FPAS. Interactive proof systems (Arthur-Merlin). Classes IP and DIP. Probabilistic checking of proofs. Chernoff bounds: packet routing. Random graphs: hashing and Hamiltonian cycles. Discrete and continuous-time Markov chains. Applications to Boltzmann machines and stochastic neural nets. Relativization of structural relations between probabilistic classes.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes*

*described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Fichas (60%) + Exame Final (40%).*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Work assignments (60%) + Final exam (60%).*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Introduction to the Theory of Complexity., Daniel P. Bovet and Pierluigi Crescenzi, 1994, C.A.R. Hoare Series Editor, Prentice-Hall International Series in Computer Science*

*Algorithmic Randomness and Complexity, Rodney G. Downey and Denis R. Hirschfeldt, 2010, Springer*

*Theory of Computation: Classical and Contemporary Approaches, Dexter C. Kozen, 2006, Springer*

*Probability and Computing, Randomized Algorithms and Probabilistic Analysis, Michael Mitzenmacher and Eli Upfal., 2005, Cambridge University Press*

**Mapa IX - Seminário de Investigação em Segurança de Informação II (B)**

**6.2.1.1. Unidade curricular:**

*Seminário de Investigação em Segurança de Informação II (B)*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

*-*

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

*-*

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Contactar com tópicos de investigação recente em Segurança de Informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*To make contact with recent research topics in Information Security.*

**6.2.1.5. Conteúdos programáticos:**

*Frequentar e realizar apresentações em seminários da especialidade.*

**6.2.1.5. Syllabus:**

*To attend and prepare specialized seminars.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*



**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Tópicos Avançados em Segurança de Informação I****6.2.1.1. Unidade curricular:**

*Tópicos Avançados em Segurança de Informação I*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Amílcar dos Santos Costa Sernadas (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Contacto com tema especializado de investigação em segurança da informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Advanced research topic in information security.*

**6.2.1.5. Conteúdos programáticos:**

*Programa variável dependendo do especialista visitante encarregado pelo DM da sua leccionação.*

**6.2.1.5. Syllabus:**

*The syllabus depends of the research topic of the specialist appointed by DM to teach the course.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points*

**syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

**6.2.1.7. Teaching methodologies (including evaluation):**

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular. A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes. The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Tolerância, Detecção e Resposta a Intrusões**

**6.2.1.1. Unidade curricular:**

***Tolerância, Detecção e Resposta a Intrusões***

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

***Miguel Nuno Dias Alves Pupo Correia (0.0)***

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

***Aprender os principais paradigmas, modelos e ferramentas para lidar com intrusões em sistemas e aplicações distribuídas.***

**6.2.1.4. Learning outcomes of the curricular unit:**

***To learn the main paradigms, models and tools to deal with intrusions in distributed computing systems and applications.***

**6.2.1.5. Conteúdos programáticos:**

***A maioria das abordagens de segurança informática visam prevenir que aconteçam intrusões. Esta cadeira é sobre tolerância a intrusões, uma abordagem baseada na premissa de que as intrusões acontecem, e que por isso devem ser criados mecanismos que as tolerem, ou seja, que mascarem os seus efeitos ou que as detectem e reajam.***

***Conceitos básicos: conceitos de confiabilidade, atributos de segurança, modelos de sistemas distribuídos;***

***Processo de intrusão: ataque-vulnerabilidade-intrusão, problemas de autenticação, buffer/integer overflows, vulnerabilidades de string de formato, injeção de SQL;***

***Tolerância a intrusões com criptografia de limiar: partilha de segredos, partilha de funções, assinaturas de limiar;***

***Sistemas de quorum bizantinos: semântica de memória partilhada, quorums de f-disseminação, quorums de f-mascaramento;***

***Replicação de máquinas de estados: replicação baseada ...***

**6.2.1.5. Syllabus:**

***Most computer security approaches aim to prevent that intrusions happen. This course is about intrusion tolerance, an approach based on the premise that intrusions do happen, so mechanisms have to be deployed to tolerate them, i.e., to mask their effects or detect and react.***

**Basic concepts: dependability concepts, security attributes, distributed system models**

**How intrusions happen: attack-vulnerability-intrusion, broken authentication, buffer/integer overflows, format string vulnerabilities, SQL injection**

**Intrusion tolerance with threshold cryptography: secret sharing, function sharing, threshold signatures**

**Byzantine quorum systems: shared memory semantics, f-dissemination BQS, f-masking BQS**

**State machine replication: leader-based SMR, reducing number of replicas, randomized algorithms, checkpointing**

**Intrusion-tolerant confidentiality: fragmentation, secret sharing, erasure codes**

**Proactive and reactive recovery**

**Diversity: off-the-shelf di ...**

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

**Exame (60%), projecto (40%).**

**6.2.1.7. Teaching methodologies (including evaluation):**

**Exam (60%), project (40%).**

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

**A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

**The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

**6.2.1.9. Bibliografia principal:**

**Network Intrusion Detection and Prevention: Concepts and Techniques. , Ali A. Ghorbani, Wei Lu, Mahbod Tavallae., 2009, Springer**

**Selected papers., Key conferences in security and dependability., 2011, -**

**Mapa IX - Tolerância a Faltas Distribuída**

**6.2.1.1. Unidade curricular:**

**Tolerância a Faltas Distribuída**

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

**Luís Eduardo Teixeira Rodrigues (0.0)**

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

**Compreender os problemas fundamentais que se colocam no desenvolvimento de aplicações distribuídas e seguras tolerantes a faltas.**

**Aprender um conjunto de abstrações chave para suportar o desenvolvimento de aplicações distribuídas tolerantes a faltas.**

**Aprender a aplicar estas abstrações através da experiência prática.**

#### 6.2.1.4. Learning outcomes of the curricular unit:

**To obtain an understanding of the fundamental problems in the design of reliable and secure distributed applications.**

**To learn a portfolio of abstractions to support the development of fault-tolerant applications.**

**To learn how to apply these abstractions through a concrete hands-on experiment.**

#### 6.2.1.5. Conteúdos programáticos:

**A fiabilidade e disponibilidade são hoje atributos fundamentais a ter em conta na concepção, concretização e instalação de sistemas distribuídos. No entanto, é surpreendentemente difícil assegurar a cooperação robusta entre processos quando estes podem falhar ou exibir um comportamento Bizantino. Para permitir que o arquitecto de sistema domine esta complexidade, o curso introduz um conjunto de abstrações fundamentais para o suporte ao desenvolvimento de aplicações distribuídas confiáveis e descreve os algoritmos que as concretizam. Nomeadamente, abordam-se os seguintes temas:**

- **Abstrações básicas: processos, elos, detectores de falhas.**
- **Difusão fiável: difusão melhor-esforço, regular, uniforme, probabilista, causal e Bizantina.**
- **Memória partilhada: registos regulares e registos atómicos. Registos Bizantinos.**
- **Consenso distribuído e acordo Bizantino.**
- **Variantes do consenso: difusão tota ...**

#### 6.2.1.5. Syllabus:

**Reliability and availability are fundamental concerns in the design, implementation and deployment of distributed systems. However, achieving robust cooperation in a distributed system, despite the failures or disconnections of some processes, is surprisingly hard. In order to allow the system designer to master this complexity, the course introduces a number of fundamental reliable distributed programming abstractions, and describes the algorithms that implement them. Namely, the course addresses:**

- **Basic abstractions: processes, links, failure detectors.**
- **Reliable broadcast: best-effort, regular, uniform, randomized, causal broadcast, secure broadcast.**
- **Shared memory: regular and atomic registers. Byzantine registers.**
- **Consensus and byzantine agreement.**
- **Consensus variants: total order broadcast, terminating reliable broadcast, atomic commit, group membership, view-synchronous communication.**
- **The Appia group communication fra ...**

#### 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

#### 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

#### 6.2.1.7. Metodologias de ensino (avaliação incluída):

**Participação nas aulas (30%), exame (70%). Projecto opcional.**

**6.2.1.7. Teaching methodologies (including evaluation):**

*Participation in classes(30%), exam (70%). The project is optional.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Introduction to Reliable and Secure Distributed Programming , Christian Cachin, Rachid Guerraoui and Luís Rodrigues , 2011, Springer*

**Mapa IX - Fundamentos de Lógica e Teoria da Computação****6.2.1.1. Unidade curricular:**

*Fundamentos de Lógica e Teoria da Computação*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

*-*

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

*-*

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Dominar resultados e técnicas chave para estabelecer a decidibilidade de teorias de primeira ordem.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Master key results and techniques for establishing the decidability of first-order theories.*

**6.2.1.5. Conteúdos programáticos:**

*Breve revisão da lógica e teorias de primeira ordem. Cálculo de sequentes. Eliminação do corte. Coerência da lógica de primeira ordem por via simbólica. Analiticidade versus decidibilidade. Técnicas de eliminação de quantificadores. Decidibilidade da teoria das ordens lineares densas. Decidibilidade da aritmética de Presburger. Decidibilidade da teoria dos corpos algebricamente fechados. Decidibilidade da teoria de Tarski dos corpos reais fechados. Avanços recentes na algoritmia da teoria de Tarski. Caracterizações complementares da eliminação de quantificadores.*

**6.2.1.5. Syllabus:**

*Short revision of first-order logic and theories. Sequent calculus. Cut elimination. Consistency of first-order logic by proof-theoretic means. Analyticity versus decidability. Quantifier elimination techniques. Decidability of the theory of dense linear orders. Decidability of Presburger arithmetic. Decidability of the theory of algebraically closed fields. Decidability of Tarski's theory of real closed fields. Recent improvements on the efficiency of the algorithms for deciding Tarski's theory. Model-theoretic characterizations of quantifier elimination. Applications: deciding the total correctness of non-deterministic, probabilistic and quantum programs with bounded resources.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points*

**syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

**Exame final.**

**6.2.1.7. Teaching methodologies (including evaluation):**

**Final examination.**

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular. A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

**The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

**6.2.1.9. Bibliografia principal:**

**Deciding First-order Theories, C. Sernadas and J. Rasga, In preparation, DMIST**

**Mapa IX - Seminário de Investigação em Segurança de Informação II (C)**

**6.2.1.1. Unidade curricular:**

**Seminário de Investigação em Segurança de Informação II (C)**

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

**STAFF**

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

**-**

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

**-**

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

**Contactar com tópicos de investigação recente em Segurança de Informação.**

**6.2.1.4. Learning outcomes of the curricular unit:**

**To make contact with recent research topics in Information Security.**

**6.2.1.5. Conteúdos programáticos:**

**Frequentar e realizar apresentações em seminários da especialidade.**

**6.2.1.5. Syllabus:**

**To attend and prepare specialized seminars.**

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes**

*described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Lógica Cleística**

**6.2.1.1. Unidade curricular:**

*Lógica Cleística*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Carlos Manuel Costa Lourenço Caleiro (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Dominar os modelos simbólicos de concepção e de análise de protocolos de segurança e perspetivar desenvolvimentos futuros.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Master formal methods and tools for designing and analysing security protocols and forecast future developments.*

**6.2.1.5. Conteúdos programáticos:**

*Cenários básicos de formalização: criptografia perfeita, intruso de Dolev-Yao.*

*Lógicas epistémicas, sistemas de agentes, conhecimento partilhado, lógica BAN e lógicas temporais. Aplicações.*

*Teorias de segurança em sistemas lógicos computacionais: teorias indutivas, programação em lógica. Verificação semântica de protocolos: limitações dos modelos finitos, técnicas de abstracção e verificação simbólica.*

*Cenários avançados de formalização: ataques probabilísticos, extensões ao intruso de Dolev-Yao, álgebras de mensagens. Resultados de fidelidade da representação.*

**6.2.1.5. Syllabus:**

*Basic formalization scenarios: perfect cryptography, Dolev-Yao intruder.*

*Kleistic logics: epistemic logics, knowledge, belief and awareness, multi-agent systems and common knowledge, BAN logic, evolving knowledge and temporal logics. Application examples in security.*

**Security theories in logic frameworks: inductive theories and inductive theorem proving, logic programming techniques. Model checking of security protocols: limitations of finite state models, abstraction techniques, infinite state and symbolic model checking.**

**Advanced formalization scenarios: probabilistic failure of cryptography, extended Dolev-Yao intruders, equations on the algebra of messages. First formalization attempts and faithfulness results.**

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**  
*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**  
*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

**6.2.1.7. Teaching methodologies (including evaluation):**

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**  
*Modal Logic, P. Blackburn, M. de Rijke, and Y. Venema, 2001, Cambridge University Press*  
*Reasoning about Knowledge, R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi, 1995, The MIT Press*  
*On the Security of Public Key Protocols, D. Dolev, and A. Yao, 1983, IEEE Transactions on Information Theory, vol. IT-29(2), pp. 198-208.*  
*A Logic of Authentication, M. Burrows, M. Abadi, and R. Needham, 1990, ACM Transactions on Computer Systems 8(1), pp. 18-36*

## Mapa IX - Lógica Funcional e Teoria da Demonstração

**6.2.1.1. Unidade curricular:**  
**Lógica Funcional e Teoria da Demonstração**

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**  
**Carlos Manuel Costa Lourenço Caleiro (0.0)**

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**  
**Dominar a teoria matemática da lógica funcional, sua semântica operacional e sistemas de tipos, bem como a semântica e sistemas dedutivos das lógicas proposicionais clássica e intuicionista. Compreender a relação fundamental entre os sistemas de tipos para a lógica funcional e a teoria da demonstração clássica e intuicionista, e suas implicações.**



**6.2.1.4. Learning outcomes of the curricular unit:**

*Master the mathematical theory of functional logic, its operational semantics and type systems, as well as the semantics and deductive systems of classical and intuitionistic propositional logics. Understand the fundamental relationship between type systems for functional logic and classical and intuitionistic proof theory, and its implications.*

**6.2.1.5. Conteúdos programáticos:**

*Cálculo-lambda, teorias, coerência. Redução, formas normais, confluência, teorema de Church-Rosser. Determinadores de pontos-fixos, recursão, definibilidade e computabilidade, tese de Church-Markov-Turing, teorema de Kleene. Resultados de indecidibilidade, teorema de Rice. Lógica combinatória. Tipos simples, redução e normalização. Decidibilidade da tipificação de termos e da verificação de tipos, teorema de Hindley-Milner. O problema da habitação de tipos. Lógicas proposicionais clássica e intuicionista (LPC and LPI), álgebras de Boole e de Heyting, axiomatizações e tertium non datur, correcção e completude. Semântica de Kripke da LPI, propriedade do modelo finito, decidibilidade. Cálculo de sequentes, eliminação do corte, normalização, decidibilidade. A interpretação de Brouwer-Heyting-Kolmogorov da LPI. Habitação de tipos simples e o fragmento implicativo da LPI. O isomorfismo de Curry-Howard, coerência, normalização, decidibilidade ...*

**6.2.1.5. Syllabus:**

*The lambda-calculus, theories, consistency. Reduction, normal forms, confluence, Church-Rosser's theorem. Fixed-point combinators, recursion, definability and computability, Church-Markov-Turing's thesis, Kleene's theorem. Undecidability results, Rice's theorem. Combinatory logic. Simple types, subject reduction and normalization. Decidability of term typability and type checking, Hindley-Milner's theorem. The type inhabitation problem. Classical and intuitionistic propositional logics (CPL and IPL), Boolean and Heyting algebras, axiomatizations and tertium non datur, soundness and completeness. Kripke semantics for IPL, finite-model property, model-theoretic decidability. Sequent calculi, cut-elimination, proof normalization, proof-theoretic decidability. The Brouwer-Heyting-Kolmogorov interpretation of IPL. Inhabitation of simple types and the implicative fragment of IPL. The Curry-Howard isomorphism, consistency, normalization, decidability of type inhabitation. Product and sum ...*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Exame final.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Final examination.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Lectures on the Curry-Howard Isomorphism, P. Urzyczyn, M. Sorensen, 2005, Elsevier Science  
Fundamentos de Programação Funcional, C. Caleiro, 2002, DMIST*

**Mapa IX - Aprendizagem Estatística****6.2.1.1. Unidade curricular:**

## Aprendizagem Estatística

### 6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):

*Mário Alexandre Teles de Figueiredo (0.0)*

### 6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:

-

### 6.2.1.3. Other academic staff and lecturing load in the curricular unit:

-

### 6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

*Fornecer aos alunos formação básica acerca de técnicas e teoria da aprendizagem estatística, incluindo estimação de densidades de probabilidade, regressão, classificação, agrupamento de dados ("clustering"). O objectivo central da disciplina é fornecer aos alunos a formação necessária para que possam ter acesso à moderna literatura nesta área.*

### 6.2.1.4. Learning outcomes of the curricular unit:

*The main goal of this course is to provide the students with fundamental knowledge on techniques and theory of statistical learning, covering density estimation, regression, classification, and clustering. The topics covered in the course aim at allowing the students to read the modern literature in this area.*

### 6.2.1.5. Conteúdos programáticos:

*1. Introdução à Aprendizagem Estatística. Aprendizagem supervisionada/não-supervisionada; aprendizagem generativa/não-generativa; aprendizagem paramétrica/não-paramétrica; generalização como problema central. 2. Introdução à Teoria da Decisão de Bayes. Funções de verosimilhança e probabilidades a priori; funções de custo, riscos esperados, decisões óptimas; priors conjugados; estatísticas suficientes; famílias exponenciais; priors não informativos (Jeffreys); modelos hierárquicos; inferência com dados em falta (algoritmo EM). 4. Regressão Linear. Critérios (mínimo erro quadrático, máxima verosimilhança); caracterização (teorema de Gauss-Markov); regressão "ridge" e LASSO (critérios e algoritmos); graus de liberdade e selecção de variáveis. 5. Classificação Linear. Regressão logística (interpretação generativa e algoritmos); discriminante Fisher; máquinas de v ...*

### 6.2.1.5. Syllabus:

*1. Introduction to Statistical Learning. Supervised/non-supervised learning; generative/non-generative learning; parametric/non-parametric learning; generalization as the central problem. 2. Introduction to Bayes Decision Theory. Likelihood function and a priori probability; loss functions, expected risks, optimal decisions; conjugate priors; sufficient statistics; exponential families; non-informative priors (Jeffreys); hierarchical modelling; inference with missing data (EM algorithm); 4. Linear Regression. Criteria (minimum mean squared error, maximum likelihood); characterization (Gauss-Markov theorem); ridge and LASSO regression (criteria and algorithms); degrees of freedom and variable selection: 5. Linear Classification. Logistic regression (generative interpretation and algorithms); Fisher discriminants; support vector machines; large margin methods. 6. Non-Linear Regression and Classification. Basis expansions ...*

### 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

### 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points*

***syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.***

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

***Um exame final e um projecto (50% + 50%).***

**6.2.1.7. Teaching methodologies (including evaluation):**

***Final exam and a research project (50% + 50%)***

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

***A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.***

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

***The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.***

**6.2.1.9. Bibliografia principal:**

***The Elements of Statistical Learning, T. Hastie, R. Tibshirani, J. Friedman, 2001, Springer-Verlag***

***Learning with Kernels, B. Schölkopf, A. Smola, 2002, MIT Press***

***Kernel Methods for Pattern Analysis, J. Shawe-Taylor, N. Cristianini, 2005, Cambridge University Press***

***A probabilistic Theory of Pattern Recognition, L. Devroye, L. Györfi, G. Lugosi, 1996, Springer-Verlag***

**Mapa IX - Segurança em Linguagens de Programação**

**6.2.1.1. Unidade curricular:**

***Segurança em Linguagens de Programação***

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

***STAFF***

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

***-***

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

***-***

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

***Dominar a segurança baseada em linguagens, com ênfase no controlo do fluxo de informação.***

**6.2.1.4. Learning outcomes of the curricular unit:**

***To become familiar with language based security, with focus on information flow control.***

**6.2.1.5. Conteúdos programáticos:**

***Complementos de semântica de linguagens, teoria de tipos, lógicas e cálculos para computação.***

***Mecanismos de segurança: dinâmicos e estáticos.***

***Formalização de políticas de segurança: confidencialidade, integridade, privacidade, anonimato.***

***Tipificação do fluxo seguro de informação: uso de sistemas de tipos para garantir propriedades de fluxo de informação (não-interferência e suas generalizações).***

***Outros tópicos em segurança baseada em linguagens: código portador de prova, compilação certificada, linguagem máquina tipificada, inspeção da pilha de segurança.***

**6.2.1.5. Syllabus:**

***Complementary topics in language semantics, type theory, logics and computation calculi. Enforcement mechanisms: dynamic and static. Formalization of security policies: confidentiality, integrity, privacy, anonymity. Typing secure information flow: using type systems to enforce information flow properties (non-interference and generalizations) Other***

*topics in language based security: proof carrying code, certifying compilation, typed assembly language, stack inspection.*

- 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**  
*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*
- 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**  
*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*
- 6.2.1.7. Metodologias de ensino (avaliação incluída):**  
*Exame + Projecto.*
- 6.2.1.7. Teaching methodologies (including evaluation):**  
*Exam + Project.*
- 6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*
- 6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*
- 6.2.1.9. Bibliografia principal:**  
*Computer Security, M. Bishop, 2003, <http://nob.cs.ucdavis.edu/book/>*

## Mapa IX - Computabilidade e Complexidade

- 6.2.1.1. Unidade curricular:**  
*Computabilidade e Complexidade*
- 6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**  
*João Filipe Quintas dos Santos Rasga (0.0)*
- 6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**  
 -
- 6.2.1.3. Other academic staff and lecturing load in the curricular unit:**  
 -
- 6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**  
*Caracterizar classes computacionais, identificar conjuntos completos, distinguir complexidade uniforme de não uniforme e executar reduções.*
- 6.2.1.4. Learning outcomes of the curricular unit:**  
*Characterize computational classes, identify complete sets, distinguish between uniform and nonuniform complexity classes and perform reductions.*
- 6.2.1.5. Conteúdos programáticos:**  
*Modelos de computação. Computabilidade. Computação com recursos limitados no espaço e no tempo. Postulados de Church-Turing e invariância. Classes de complexidade notáveis. Teorias de redução em tempo e espaço limitados.*

**Conjuntos P-completos, NP-completos e PSPACE-completos. Aplicações à Criptografia. Circuitos booleanos. Classes probabilísticas. Diagonalização uniforme. A hierarquia polinomial. Relativização de relações estruturais entre classes de complexidade.**

**6.2.1.5. Syllabus:**

***Models of computation. Computability. Time and space bounded computations. Church-Turing and invariance theses. Relevant complexity classes. Time and space bounded reducibilities. P-complete, NP-complete, and PSPACE-complete sets. Applications to Cryptography. Boolean circuits. Probabilistic classes. Uniform diagonalization. The polynomial time hierarchy. Relativization of structural relations between complexity classes.***

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

***Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.***

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

***Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.***

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

***Teste + Exame Final.***

**6.2.1.7. Teaching methodologies (including evaluation):**

***Mid-term exam + Final exam.***

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

***A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.***

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

***The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.***

**6.2.1.9. Bibliografia principal:**

***Computational Complexity , Arora & Barak , 2009, Cambridge University Press***

**Mapa IX - Seminário de Investigação em Segurança de Informação I (A)**

**6.2.1.1. Unidade curricular:**

***Seminário de Investigação em Segurança de Informação I (A)***

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

***Paulo Alexandre Carreira Mateus (0.0)***

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

**-**

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

**-**

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

***Contactar com tópicos de investigação recente em Segurança de Informação.***

**6.2.1.4. Learning outcomes of the curricular unit:**

*To make contact with recent research topics in Information Security.*

**6.2.1.5. Conteúdos programáticos:**

*Frequentar e realizar apresentações em seminários da especialidade.*

**6.2.1.5. Syllabus:**

*To attend and prepare specialized seminars.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Presença.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Presence.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Modelos Computacionais em Segurança**

**6.2.1.1. Unidade curricular:**

*Modelos Computacionais em Segurança*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Pedro Miguel dos Santos Alves Madeira Adão (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Dominar os modelos computacionais de concepção e de análise de protocolos de segurança e perspectivar desenvolvimentos futuros.*

**6.2.1.4. Learning outcomes of the curricular unit:**

**Master the computational models of design and analysis of security protocols and forecast future developments.**

**6.2.1.5. Conteúdos programáticos:**

**Cenários básicos de formalização: criptografia perfeita, intruso de Dolev-Yao, álgebra livre de mensagens. Revisão dos objectivos e protocolos de segurança.**

**Protocolos de segurança como sistemas concorrentes. Traços, álgebras de processos e CSP, reescrita, cálculos  $\pi$  e  $\text{spi}$ , estruturas de eventos, tranças, modelos computacionais e máquinas de Turing interactivas. Resultados de (in)decidibilidade e complexidade.**

**Análise da correcção e completude das abstracções simbólicas.**

**Ferramentas para verificação de propriedades de segurança, AVISPA, ProVerif, inter alia.**

**6.2.1.5. Syllabus:**

**Basic formalization scenarios: perfect cryptography, Dolev-Yao intruder, free algebra of messages. Security protocols and goals revisited. Security protocols as concurrent systems: trace models, process algebras and CSP, rewriting systems,  $\pi$  and  $\text{spi}$  calculus, event structures, braids, computational models and interactive Turing machines.**

**(Un)decidability and complexity results. Soundness and completeness of symbolic abstractions. Tools for verification of security properties: AVISPA, ProVerif, inter alia.**

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

**Exame + Projecto.**

**6.2.1.7. Teaching methodologies (including evaluation):**

**Exam + Project.**

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

**A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

**The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Engenharia de Segurança de Informação**

**6.2.1.1. Unidade curricular:**

**Engenharia de Segurança de Informação**

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

**STAFF**

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Conhecer as técnicas para desenvolver sistemas seguros. Estudar conceitos, métodos e ferramentas usadas nas diferentes actividades do ciclo de desenvolvimento de software para melhorar a segurança dos sistemas resultantes.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*To survey engineering techniques for developing secure systems. To understand the concepts, methods, and tools that can be applied within the different activities of the software development process, in order to improve the security of the resulting systems.*

**6.2.1.5. Conteúdos programáticos:**

*Introdução à segurança em engenharia de software. Engenharia de requisitos: requisitos de segurança e sua análise. Requisitos funcionais e não funcionais. Cenários de utilização correcta e incorrecta. Diagramas de sequência. Árvores de ataques. Modelação de segurança durante o desenho do sistema. Estrutura, comportamento e fluxo de informação. Diagramas de classe e diagramas de estado. Técnicas para controlo de acesso baseadas em modelos. A linguagem SecureUML: combinação de linguagens de modelação, semântica, geração. Padrões de segurança, desenho e implementação. Segurança da implementação: buffer overflow (transbordo da área tampão), análise estática de dados. Testes: testes baseados em modelos, testes a propriedades de segurança. Análise de risco. Risco: activos, ameaças, vulnerabilidades. Avaliação quantitativa e qualitativa de riscos. Salvaguardas. Procedimentos genéricos de análise de riscos. Critérios de avaliação, o processo CMMI.*

**6.2.1.5. Syllabus:**

*Introduction to information security in engineering. Requirements Engineering: security Requirements and Analysis; functional and non-functional requirements; use and misuse cases; sequence diagrams; attack trees. Modeling in the design activities: structure, behavior, and data flow; class diagrams, statecharts. Model-driven security for access control: design. SecureUML as a language for access control: combining Design Modeling Languages, semantics, generation. Security patterns: design and implementation. Implementation-level security: buffer overflows; input checking; injection attacks. Testing: model-based testing; testing security properties. Risk analysis and management: "risk" assets, threats, vulnerabilities; quantitative and qualitative risk assessment; safeguards; generic risk analysis procedure. Evaluation criteria: CMMI process.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Exame + Projecto + Apresentações*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Exam + Project + Presentations*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliar o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Security Engineering, R. Anderson, 2001, <http://www.cl.cam.ac.uk/~rja14/book.html>*

*Computer Security, M. Bishop, 2003, <http://nob.cs.ucdavis.edu/book/book-aands/index.html>*



*Information Security Risk Analysis, T. Peltier, 2001, <http://www.amazon.com/Information-Security-Risk-Analysis-Second/dp/0849333466>*

*Software Engineering, I. Sommerville, 2001, <http://www.cs.st-andrews.ac.uk/~ifs/Books/SE7/index.html>*

## Mapa IX - Compressão e Codificação de Dados

### 6.2.1.1. Unidade curricular:

*Compressão e Codificação de Dados*

### 6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):

*Mário Alexandre Teles de Figueiredo (84.0)*

### 6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:

-

### 6.2.1.3. Other academic staff and lecturing load in the curricular unit:

-

### 6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

*Aquisição dos conceitos fundamentais da teoria da informação e sua aplicação aos problemas da compressão e codificação de informação (dados, sinais e imagens).*

### 6.2.1.4. Learning outcomes of the curricular unit:

*Acquisition of the fundamental concepts of information theory and its application to problems of coding and compression and information (data, signals, and images).*

### 6.2.1.5. Conteúdos programáticos:

*Compressão com e sem perdas e aspectos psico-físicos. Conceitos básicos de teoria da informação (informação de um evento, entropia, informação mútua e suas propriedades). Compressão entrópica (desigualdade de Kraft-McMillan, código de Huffman e sua optimalidade, codificação de Shannon-Fano-Elias e aritmética). Comunicação em canais ruidosos (capacidade de de canal). Compressão baseada em dicionários (algoritmo de Ziv-Lempel).*

*Codificação/compressão de sinais (quantização). Codificação preditiva (DPCM, delta). Quantização vectorial.*

*Compressão por transformada (alocação de bits, transformadas de Karhunen-Loeve, DCT, de Walsh-Hadamard e de "wavelets"). Alguns exemplos práticos (sinais de voz, normas JPEG e MPEG).*

### 6.2.1.5. Syllabus:

*Lossless and lossy compression. Psychophysical aspects. Fundamental concepts of information theory (event information, entropy, mutual information and their properties). Entropic compression (Kraft-McMillan inequality, Huffman coding and its optimality, Shannon-Fano-Elias coding, and arithmetic coding). Communication over noisy channels (channel capacity). Dictionary-based compression (Lempel-Ziv coding). Predictive coding. Signal compression (quantization). Differential pulse code modulation and delta modulation. Vector quantization. Transform coding (bit allocation, Karhunen-Loeve transform, discrete cosine transform, Walsh-Hadamard transform, and wavelet transforms). Practical applications: JPEG and MPEG.*

### 6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

### 6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

### 6.2.1.7. Metodologias de ensino (avaliação incluída):

*Exame (50 %) + Trabalho (50%). Grupos de trabalho: Licenciatura - até dois alunos; Mestrado - um aluno.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Exam (50%) + Project in MATLAB (50%). The Project is to be developed by groups of at most two students. Minimum exam grade: 9.5*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

*Compressão e Codificação de Dados, Mário A. T. Figueiredo, 2005, Apontamentos disponíveis na página da disciplina*

**Mapa IX - Tópicos Avançados em Segurança de Informação II****6.2.1.1. Unidade curricular:**

*Tópicos Avançados em Segurança de Informação II*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*STAFF*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

*-*

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

*-*

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Contacto com tema especializado de investigação em segurança da informação.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Advanced research topic in information security.*

**6.2.1.5. Conteúdos programáticos:**

*Programa variável dependendo do especialista visitante encarregado pelo DEI da sua leccionação.*

**6.2.1.5. Syllabus:**

*The syllabus depends of the research topic of the specialist appointed by DEI to teach the course.*

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

*Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.*

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

*Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.*

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

*Ajustável ao programa.*

**6.2.1.7. Teaching methodologies (including evaluation):**

*Adjustable to the specific program.*

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

*A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objectivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.*

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

*The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.*

**6.2.1.9. Bibliografia principal:**

-

**Mapa IX - Sistemas de Biometria****6.2.1.1. Unidade curricular:**

*Sistemas de Biometria*

**6.2.1.2. Docente responsável e respectivas horas de contacto na unidade curricular (preencher o nome completo):**

*Ana Luísa Nobre Fred (0.0)*

**6.2.1.3. Outros docentes e respectivas horas de contacto na unidade curricular:**

-

**6.2.1.3. Other academic staff and lecturing load in the curricular unit:**

-

**6.2.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**

*Ajudar o estudante na compreensão dos conceitos fundamentais, das tecnologias e das limitações da biometria, preparando-o para a identificação de aplicações apropriadas e para o projecto de sistemas de biometria fiáveis e seguros.*

**6.2.1.4. Learning outcomes of the curricular unit:**

*Fundamentals of the major biometric technologies, as well as privacy and security concerns. It aims at preparing the students to understand these technologies, their limitations, and how to identify appropriate applications and design reliable biometric systems*

**6.2.1.5. Conteúdos programáticos:**

*Introdução à biometria: definições e modalidades em biometria. Sobre a necessidade de identificar indivíduos.*

*Aplicações emergentes.*

*Conceitos básicos: os sistemas de biometria como sistemas de reconhecimento de padrões. Projecto de um sistema de biometria: componentes do sistema. Um classificador de dados biométricos. Características e classificação de padrões.*

*Fases de um sistema de biometria. Projecto de um sistema de biometria: modos de operação. Cenários de autenticação e de identificação. Taxas de acerto e de rejeição e curvas de ROC.*

*Tecnologias de biometria: biometria fisiológica e comportamental. Descrição e revisão dos tipos mais relevantes:*

*impressão digital, íris, face, assinatura, geometria da mão, orelha, voz, dinâmica de digitação e movimentos de teclado, sinais electrofisiológicos, ADN. Preocupações potenciais e vulnerabilidades. Requisitos na escolha de uma tecnologia de biometria.*

*Biometria multimod ...*

**6.2.1.5. Syllabus:**

*Overview of Biometrics: definitions, biometric modalities and course outline. The need to identify individuals. Emerging biometric applications Basic Concepts: a biometric system as a pattern recognition system. Design of a biometric system: building blocks. A biometric classifier. Features and pattern classifiers. Biometric systems phases. Design of a biometric system: modes of operation. Authentication and identification scenarios. True and false accept/reject and receiver operating characteristic curves. Major Biometric Technologies: physiological and behavioural biometrics.*

**Description and overview of principal biometric types: fingerprint, iris, facial, signature, hand geometry, ear, voice, keystroke dynamics and mouse movements, electrophysiological signals, DNA. Potential concerns of vulnerability. The key requirements to consider when choosing a biometric technology Multimodal Biometrics: limitations of unimodal systems. Multibiometric scenarios, levels of fusion. Score fu ...**

**6.2.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**

**Atendendo aos objetivos de aprendizagem da UC, descritos em 6.2.1.4, qualquer especialista na matéria poderá constatar que todos os pontos dos conteúdos, descritos em 6.2.1.5, programáticos visam dotar os alunos com os conhecimentos e competências necessárias ao seu cumprimento e à aquisição dos referidos objetivos.**

**6.2.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**

**Considering the objectives of this the UC, any expert in the field can reach to the conclusion that that all the points syllabus (point 6.2.1.5) aim to equip students with the required knowledge and skills to reach the learning outcomes described in point 6.2.1.4.**

**6.2.1.7. Metodologias de ensino (avaliação incluída):**

-

**6.2.1.7. Teaching methodologies (including evaluation):**

-

**6.2.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**

**A metodologia de ensino basear-se-á na transferência de conceitos teóricos e práticos através da utilização intensiva de aulas de demonstração e trabalhos experimentais. Esta abordagem permitirá não só cumprir os objetivos como auxiliará o nivelamento do conhecimento de estudantes com diferentes proveniências e formações.**

**6.2.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**

**The teaching methodologies, based on the transfer of theoretical and practical concepts through the extensive use of demonstration classes and experimental work, will allow to fulfill the intended learning outcomes, as well as to level the knowledge of students with different backgrounds and formations.**

**6.2.1.9. Bibliografia principal:**

**Biometric Systems, Technology, Design and Performance Evaluation, A. Ross, K. Nandakumar, and A. K. Jain, 2005, Springer  
Handbook of Multibiometrics, tbd, 2006, Springer,**

### **6.3. Metodologias de Ensino/Aprendizagem**

---

**6.3.1. Adaptação das metodologias de ensino e das didáticas aos objectivos de aprendizagem das unidades curriculares.**

**As metodologias de ensino são definidas pelo respectivo grupo de disciplinas de modo a serem coerentes com os objetivos da aprendizagem da unidade curricular. São aqui discutidas as técnicas didáticas, incluindo métodos que facilitem a aprendizagem e interliguem estas, sempre que possível com a investigação em curso. Estas metodologias são objecto de aprovação pela Comissão Científica do Curso de Doutoramento.**

**6.3.1. Adaptation of methodologies and didactics to the learning outcomes of the curricular units.**

**Teaching methodologies are set by the respective group of disciplines so as to be consistent with the objectives of the learning curriculum unit. Didactic techniques are discussed here, including methods to facilitate learning and connect these, where possible with the ongoing investigation. These methodologies are subject to approval by the Scientific Commission of the doctorate.**

**6.3.2. Verificação de que a carga média de trabalho necessária aos estudantes corresponde ao estimado em ECTS.**

**No âmbito do QUC está previsto a recolha e tratamento de dados para esta aferição, contudo, por ora este sistema apenas está disponível para formações de 1º e 2º ciclo, mas em breve prevê-se o seu alargamento a este nível de formação.**

**6.3.2. Verification that the required students average work load corresponds the estimated in ECTS.**

**As part of the QUC system, the collection and processing of data are foreseen, but this system is only available for the 1st 1nd 2nd cycles but it will soon be extended to this cycle.**

### 6.3.3. Formas de garantir que a avaliação da aprendizagem dos estudantes é feita em função dos objectivos de aprendizagem da unidade curricular.

*O QUC prevê a avaliação do processo de ensino e aprendizagem em 5 dimensões: Carga de Trabalho, Organização, Avaliação, Competências e Corpo Docente, as quais refletem a relação entre a aprendizagem dos estudantes e os objectivos de aprendizagem previstos pela unidade curricular.*

*Com base nas respostas dos alunos estas dimensões são classificadas de acordo com o seu funcionamento como “Inadequado”, “A melhorar” ou “Regular”, sendo que nos 2 primeiros casos existem mecanismos de recolha de informação mais detalhados sobre as causas destes resultados. Em casos mais graves (vários resultados inadequados ou a melhorar) está previsto um processo de auditoria, do qual resulta uma síntese das causas apuradas para o problema, e um conjunto de conclusões e recomendações para o futuro.*

*Por ora este sistema apenas está disponível para formações de 1º e 2º C, nos casos de unidades curriculares com funcionamento em regime regular, mas em breve prevê-se o seu alargamento a outras UC/ciclos.*

### 6.3.3. Means to ensure that the students learning assessment is adequate to the curricular unit's learning outcomes.

*The QUC system comprises 5 categories: Workload, Organization, Evaluation, Skills and Teaching Staff which reflect upon the relationship between students and the purposes of learning expected by the course unit.*

*Based on the students' answers these categories are ranked according their functioning as “Inadequate”, “To Be Improved” or “Regular”, in which the 2 former categories are provided with more detailed information collection mechanisms on the causes of these results. In acute cases (different inadequate results or results to be improved) an auditing process is foreseen, which will give rise to a summary of the causes found for the problem, and a set of conclusions and recommendations for the future.*

*This system is only available for the 1st and 2nd cycles, for regular course units, but it will soon be extended to other course units/cycles.*

### 6.3.4. Metodologias de ensino que facilitam a participação dos estudantes em actividades científicas.

*As metodologias de ensino são definidas pelo respectivo grupo de disciplinas de modo a serem coerentes com os objectivos da aprendizagem da unidade curricular. São aqui discutidas as técnicas didácticas, incluindo métodos que facilitem a aprendizagem e interliguem estas, sempre que possível com a investigação em curso. Estas metodologias são objecto de aprovação pela Comissão Científica do Curso de Doutoramento.*

### 6.3.4. Teaching methodologies that promote the participation of students in scientific activities.

*Teaching methodologies are set by the respective group of disciplines so as to be consistent with the objectives of the learning curriculum unit. Didactic techniques are discussed here, including methods to facilitate learning and connect these, where possible with the ongoing investigation. These methodologies are subject to approval by the Scientific Commission of the doctorate.*

## 7. Resultados

### 7.1. Resultados Académicos

#### 7.1.1. Eficiência formativa.

##### 7.1.1. Eficiência formativa / Graduation efficiency

	2009/10	2010/11	2011/12
N.º diplomados / No. of graduates	0	0	0
N.º diplomados em N anos / No. of graduates in N years*	0	0	0
N.º diplomados em N+1 anos / No. of graduates in N+1 years	0	0	0
N.º diplomados em N+2 anos / No. of graduates in N+2 years	0	0	0
N.º diplomados em mais de N+2 anos / No. of graduates in more than N+2 years	0	0	0

#### Perguntas 7.1.2. a 7.1.3.

#### 7.1.2. Comparação do sucesso escolar nas diferentes áreas científicas do ciclo de estudos e respectivas unidades curriculares.

*Ainda no âmbito do QUC está prevista a apresentação dos resultados semestrais de cada UC não só ao coordenador de curso, como também aos presidentes de departamento responsáveis pelas várias UC, em particular os resultados da*

*componente de avaliação da UC que engloba o sucesso escolar. Paralelamente, o coordenador de curso tem ao seu dispor no sistema de informação um conjunto de ferramentas analíticas que permitem analisar e acompanhar o sucesso escolar nas várias UC ao longo do ano letivo.*

*Por ora o QUC apenas está disponível para formações de 1º e 2º ciclo, nos casos de unidades curriculares com funcionamento em regime regular, mas em breve prevê-se o seu alargamento a outras UC/ciclos.*

#### 7.1.2. Comparison of the academic success in the different scientific areas of the study cycle and related curricular units.

*As part of the QUC system, half yearly results of each course unit are must also be submitted not only to the course coordinator, but also to the heads of departments that are responsible for the course units, particularly the results of evaluation of the course unit that comprises academic success. The course coordinator also has a set of analytical tools that allow him/her to analyze and monitor the academic achievement of the different course units throughout the academic year.*

*This system is only available for the 1st and 2nd cycles, for regular course units, but it will soon be extended to other course units/cycles.*

#### 7.1.3. Forma como os resultados da monitorização do sucesso escolar são utilizados para a definição de acções de melhoria do mesmo.

*De acordo com o descrito em 6.3.3 o sistema QUC prevê a realização de auditorias a UC que apresentem resultados inadequados ou a melhorar em várias dimensões de análise, das quais decorrem recomendações para melhoria dos processos associados que devem ser seguidas pelos departamentos responsáveis, pelo coordenador de curso, e o pelo conselho pedagógico. Paralelamente, anualmente é publicado relatório anual de autoavaliação (R3A) que engloba um conjunto de indicadores chave sobre o sucesso escolar do curso, entre outros, e sobre o qual é pedido aos coordenadores de curso uma análise dos pontos fortes e fracos, bem como propostas de atuação futura. Periodicamente são também desenvolvidos alguns estudos sobre o abandono e sucesso escolar que permitem analisar esta dimensão. Por ora, tanto o QUC como o R3A apenas estão disponíveis para formações de 1º e 2º ciclo, mas em breve prevê-se o seu alargamento ao 3º ciclo, eventualmente com formatos ajustados à especificidade deste nível de estudos.*

#### 7.1.3. Use of the results of monitoring academic success to define improvement actions.

*According to point 6.3.3, the QUC system includes course unit audits, which result from recommendations for improvement of related processes that must be observed by the departments at issue, by the course coordinator and the pedagogical council.*

*An annual self-assessment report (R3A) is also published, which comprises a set of key indicators on the academic achievement of the course, among other items, and on which course coordinators are asked to make an analysis of the strengths and weaknesses and proposals for future action.*

*Some studies are also carried out on a regular basis on dropouts and academic achievement, which allow for analyzing this dimension.*

*Both the QUC system and the R3A are only available for the 1st and 2nd cycles, but it will soon be extended to the 3rd cycle, adapted to the particular features of this level of studies.*

#### 7.1.4. Empregabilidade.

##### 7.1.4. Empregabilidade / Employability

	%
Percentagem de diplomados que obtiveram emprego em sectores de actividade relacionados com a área do ciclo de estudos / Percentage of graduates that obtained employment in areas of activity related with the study cycle area	100
Percentagem de diplomados que obtiveram emprego em outros sectores de actividade / Percentage of graduates that obtained employment in other areas of activity	100
Percentagem de diplomados que obtiveram emprego até um ano depois de concluído o ciclo de estudos / Percentage of graduates that obtained employment until one year after graduating	100

## 7.2. Resultados das actividades científicas, tecnológicas e artísticas.

### Pergunta 7.2.1. a 7.2.6.

#### 7.2.1. Indicação do(s) Centro(s) de Investigação devidamente reconhecido(s), na área científica predominante do ciclo de estudos e respectiva classificação.

*Instituto de Telecomunicação (classificação: Excelente)*

*INESC - ID (classificação: Excelente)*

#### 7.2.1. Research centre(s) duly recognized in the main scientific area of the study cycle and its mark.

**Telecommunications Institute (classification: Excellent).**  
**INESC - ID (classification: Excellent)**

**7.2.2. Número de publicações do corpo docente do ciclo de estudos em revistas internacionais com revisão por pares, nos últimos 5 anos e com relevância para a área do ciclo de estudos.**

147

**7.2.3. Outras publicações relevantes.**

N/A

**7.2.3. Other relevant publications.**

N/A

**7.2.4. Impacto real das actividades científicas, tecnológicas e artísticas na valorização e no desenvolvimento económico.**

N/A

**7.2.4. Real impact of scientific, technological and artistic activities on economic enhancement and development.**

N/A

**7.2.5. Integração das actividades científicas, tecnológicas e artísticas em projectos e/ou parcerias nacionais e internacionais.**

*O Programa visa formar especialistas capazes de desenvolver investigação autónoma na área interdisciplinar de segurança informática, o que requer o domínio de matérias de Matemática, Engenharia Informática e Engenharia Electrotécnica, incluindo complexidade computacional, criptografia, segurança de sistemas e teoria da informação. O programa colabora activamente no âmbito do programa CMU|Portugal.*

**7.2.5. Integration of scientific, technological and artistic activities in national and international projects and/or partnerships.**

*The Program aims at training experts capable of carrying out autonomous research activities in the broad area of information security, mastering relevant subjects in Mathematics, Computer Science and Electrical Engineering, including computational complexity, cryptography, systems security and information theory. The program has a very active partnership under the CMU|Portugal program.*

**7.2.6. Utilização da monitorização das actividades científicas, tecnológicas e artísticas para a sua melhoria.**

*Para além das avaliações promovidas pela FCT, o IST está a rever a sua estratégia no que diz respeito à avaliação das atividades de ID&I, que incluiu uma reflexão sobre o posicionamento nac/intern das unidades de ID&I(UID&I). Deste modo, foi produzido em 2011 um documento provisório para diagnóstico/planeamento estratégico das UID&I, incluindo alguma partilha de experiências com instituições nacionais e internacionais (Ex: EPFL e UNL). Em 2012, este trabalho foi reforçado com a elaboração de um estudo sobre a produção científica da Escola, baseado numa análise bibliométrica comparativa das UID&I e dos departamentos, na sua dimensão financeira, de recursos humanos e de infraestruturas, com um enfoque especial na na construção de indicadores de comparação com base em parâmetros nac/intern. A partir de 2013, a metodologia será aplicada anualmente permitindo uma monitorização permanente dos objetivos estratégicos das UID&I e das atividades cient./tecn. do IST.*

**7.2.6. Use of scientific, technological and artistic activities' monitoring for its improvement.**

*Besides the evaluation processes conducted by FCT, IST has been updating its strategy regarding the evaluation of its RD&I activities, with a reflection on the national and international positioning of its RD&D units. In 2011 a methodological draft document came out, aiming to diagnose and plan its RD&I activities, together with sharing experiences with international and national institutions (i.e.. EPFL and UNL). In 2012, this work was reinforced with a study based on a bibliometric analysis, which compares the RD&D units and the departments, in terms of funding, human resources, and infrastructure, with emphasis on the construction of comparative indicators based on national and international parameters. From 2013, this methodology will be applied annually, thus making it possible to constantly monitor the strategic objectives of the RD&I units of IST and its scientific and technological activities.*

## 7.3. Outros Resultados

---

Perguntas 7.3.1 a 7.3.3

**7.3.1. Actividades de desenvolvimento tecnológico e artístico, prestação de serviços à comunidade e formação avançada.**

*O Programa visa formar especialistas capazes de desenvolver investigação autónoma na área interdisciplinar de segurança informática, o que requer o domínio de matérias de Matemática, Engenharia Informática e Engenharia Electrotécnica, incluindo complexidade computacional, criptografia, segurança de sistemas e teoria da informação.*

*Destaca-se, por exemplo o acordo de cooperação Pedagógica, Científica e Técnica entre a Escola Naval, a Faculdade de Direito da Universidade de Lisboa e o Instituto Superior Técnico, na área da Segurança de Informação e do Direito no Ciberespaço.*

#### 7.3.1. Activities of technological and artistic development, consultancy and advanced training.

*The Program aims at training experts capable of carrying out autonomous research activities in the broad area of information security, mastering relevant subjects in Mathematics, Computer Science and Electrical Engineering, including computational complexity, cryptography, systems security and information theory. We can single out, for instance, the Scientific and Technological Cooperation between the Naval School, Lisbon University Law school and IST in the area of Information Security and Ciberspace Law.*

#### 7.3.2. Contributo real para o desenvolvimento nacional, regional e local, a cultura científica, e a acção cultural, desportiva e artística.

*O Programa visa formar especialistas capazes de desenvolver investigação autónoma na área interdisciplinar de segurança informática, o que requer o domínio de matérias de Matemática, Engenharia Informática e Engenharia Electrotécnica, incluindo complexidade computacional, criptografia, segurança de sistemas e teoria da informação.*

#### 7.3.2. Real contribution for national, regional and local development, scientific culture, and cultural, sports and artistic activities.

*The Program aims at training experts capable of carrying out autonomous research activities in the broad area of information security, mastering relevant subjects in Mathematics, Computer Science and Electrical Engineering, including computational complexity, cryptography, systems security and information theory.*

#### 7.3.3. Adequação do conteúdo das informações divulgadas ao exterior sobre a instituição, o ciclo de estudos e o ensino ministrado.

*O IST assume total responsabilidade sobre a adequação de toda a informação divulgada ao exterior pelos seus serviços, relativa aos ciclos de estudo ministrados sob sua esponsabilidade.*

#### 7.3.3. Adequacy of the information made available about the institution, the study cycle and the education given to students.

*The IST is fully responsible for the adequacy of all the information reported externally by its services, regarding the study cycles taught under its responsibility.*

#### 7.3.4. Nível de internacionalização

##### 7.3.4. Nível de internacionalização / Internationalisation level

	%
Percentagem de alunos estrangeiros / Percentage of foreign students	17
Percentagem de alunos em programas internacionais de mobilidade / Percentage of students in international mobility programs	33
Percentagem de docentes estrangeiros / Percentage of foreign academic staff	0

## 8. Análise SWOT do ciclo de estudos

### 8.1. Objectivos gerais do ciclo de estudos

#### 8.1.1. Pontos fortes

- *Preparação de doutorados em segurança de informação com elevada formação científica, tanto para a docência, como para a investigação científica e empresarial;*
- *Interdisciplinaridade do programa.*

#### 8.1.1. Strengths

- *Training of highly skilled PhD both for teaching and for scientific and entrepreneurial research;*
- *Interdisciplinary nature of the program.*

#### 8.1.2. Pontos fracos

- *Número reduzido de candidatos.*



### 8.1.2. Weaknesses

- *Small number of candidates*

### 8.1.3. Oportunidades

- *Internacionalização e atracção de estudantes de países estrangeiros;*
- *Colaborações interdisciplinares.*
- *Colaboração com a indústria.*

### 8.1.3. Opportunities

- *Internationalization and attraction of students from foreign countries*
- *Interdisciplinary collaborations.*
- *Collaborations with the industry.*

### 8.1.4. Constrangimentos

- *Financiamento reduzido em especial no que diz respeito a bolsas de investigação para alunos estrangeiros.*
- *Orçamento de estado, leis e regulamentos que bloqueiam as actividades de investigação e a realização dos doutoramentos de projectos financiados;*

### 8.1.4. Threats

- *Insufficient funding, specially in what concerns PhD fellowships for foreign students.*
- *State budget, laws and regulations that create obstacles to the research activities and the carrying out of PhDs of funded projects;*

## 8.2. Organização interna e mecanismos de garantia da qualidade

---

### 8.2.1. Pontos fortes

- *Natureza interdisciplinar e flexível do programa.*

### 8.2.1. Strengths

- *Interdisciplinary and flexible nature of the program.*

### 8.2.2. Pontos fracos

- *interacção entre alunos e indústria.*

### 8.2.2. Weaknesses

- *interaction between students and industry*

### 8.2.3. Oportunidades

- *Possibilidade de expansão das ofertas a alunos de outros países;*
- *Criação de redes de ensino temáticas a nível nacional e/ou internacional.*

### 8.2.3. Opportunities

- *Possibility of increasing offer to students form other countries;*
- *Creation of thematic teaching networks at national and/or international level.*

### 8.2.4. Constrangimentos

- *Financiamento reduzido;*
- *Propinas elevadas para alunos que não tenham bolsa.*

### 8.2.4. Threats

- *Insufficient funding;*
- *High tuition fees for students that have not been awarded a scholarship.*

## 8.3. Recursos materiais e parcerias

---

### 8.3.1. Pontos fortes

- *Grande actividade de investigação com ligação a diversas universidades estrangeiras como CMU e UTAustin.*

**- Colaborações interdisciplinares**

**8.3.1. Strengths**

- *Very active in research with a link to other national and foreign universities such as CMU and UTAustin.*
- *Interdisciplinary collaborations*

**8.3.2. Pontos fracos**

- *Não existência de bolsas de doutoramento associados com o programa (com a exceção das do programa CMU|Portugal)*

**8.3.2. Weaknesses**

- *Non existence of PhD grants associated with the program (with the exception of the CMU|Portugal partnership)*

**8.3.3. Oportunidades**

- *Desenvolvimento de colaboração com a indústria*
- *Colaboração com organizações militares nacionais e internacionais (eg gabinete nacional de segurança, NATO, etc)*

**8.3.3. Opportunities**

- *New collaborations with industry*
- *Collaborations with national and international military organization (eg National Security Office, NATO, etc)*

**8.3.4. Constrangimentos**

- *Financiamento reduzido.*

**8.3.4. Threats**

- *There has been insufficient funding.*

---

**8.4 Pessoal docente e não docente**

**8.4.1. Pontos fortes**

- *Uma grande e competente equipa de professores cobrindo todas as áreas de segurança de informação*

**8.4.1. Strengths**

- *A large and competent team of teachers cover all areas of information security.*

**8.4.2. Pontos fracos**

- *número reduzido de pessoal não docente, especialmente no que diz respeito ao acompanhamento e inserção de alunos internacionais.*

**8.4.2. Weaknesses**

- *reduced number of staff, specially in what concerns the support to international students.*

**8.4.3. Oportunidades**

- *Possibilidade de formar novo pessoal docente de qualidade numa área emergente.*

**8.4.3. Opportunities**

- *The possibility to provide training to new teaching and research staff in an emerging area.*

**8.4.4. Constrangimentos**

- *Legislação dificulta novas contratações de pessoal docente e não docente;*

**8.4.4. Threats**

- *Legislation makes it hard for recruiting new teaching and non-teaching staff;*

---

**8.5. Estudantes e ambientes de ensino/aprendizagem**

#### 8.5.1. Pontos fortes

- *Bons alunos frequentam os programas de doutoramento;*
- *Bom ambiente de investigação, com colaboração entre grupos.*

#### 8.5.1. Strengths

- *Good students attend PhD programs;*
- *Good research environment, with cooperation between groups.*

#### 8.5.2. Pontos fracos

- *Poucos candidatos.*

#### 8.5.2. Weaknesses

- *Few candidates.*

#### 8.5.3. Oportunidades

- *Forma de os alunos adquirirem uma formação elevada.*

#### 8.5.3. Opportunities

- *A chance that students have to acquire sound background.*

#### 8.5.4. Constrangimentos

- *Falta de bolsas para os candidatos.*

#### 8.5.4. Threats

- *Insufficient scholarships for candidates.*

### 8.6. Processos

---

#### 8.6.1. Pontos fortes

- *Boa organização do curso sem problemas processuais.*

#### 8.6.1. Strengths

- *Good program organization without any procedural problems.*

#### 8.6.2. Pontos fracos

- *dado o número reduzido de alunos e a natureza interdisciplinar do programa, alguns processos podem ser aperfeiçoados especialmente no que diz respeito ao recrutamento de alunos de diversos backgrounds*

#### 8.6.2. Weaknesses

- *given the reduced number of students and the interdisciplinary nature of the program, some processes can be improved specially in what concerns recruiting of students of diverse backgrounds.*

#### 8.6.3. Oportunidades

- *Desenvolver a capacidade de os alunos encontrarem soluções.*

#### 8.6.3. Opportunities

- *To develop the student's ability to find out solutions.*

#### 8.6.4. Constrangimentos

- *O Orçamento de Estado e reduzido financiamento.*

#### 8.6.4. Threats

- *The State Budget and insufficient funding.*

## 8.7. Resultados

---

### 8.7.1. Pontos fortes

- *Alunos de elevada qualidade.*
- *Investigação de elevada qualidade.*

### 8.7.1. Strengths

- *Very high quality students.*
- *High quality research.*

### 8.7.2. Pontos fracos

- *Número ainda reduzido de alunos*

### 8.7.2. Weaknesses

- *Small number (so far) of students.*

### 8.7.3. Oportunidades

- *Competição entre professores pelos melhores alunos;*
- *Estabelecimento de redes de investigação nacionais e internacionais como forma de progredir;*
- *Competição por financiamentos públicos e privados.*

### 8.7.3. Opportunities

- *Teachers compete for the best students;*
- *National and international research networks are established as a way to move forward;*
- *There is a competition for public and private funding.*

### 8.7.4. Constrangimentos

- *Falta de financiamento decorrente da crise financeira;*
- *Percepção negativa de Portugal no estrangeiro devido à crise actual;*
- *Falta de visibilidade nos rankings internacionais.*

### 8.7.4. Threats

- *Funding squeeze as a result of the financial crisis;*
- *Negative perception of Portugal abroad due to the current crisis;*
- *Lack of visibility in international rankings.*

## 9. Proposta de acções de melhoria

### 9.1. Objectivos gerais do ciclo de estudos

---

#### 9.1.1. Debilidades

*São pontos fracos do ciclo de estudos o número reduzido de candidatos. Tal deve-se em parte ao facto do programa ser relativamente recente e à ausência de financiamento directo associado ao programa para apoio a novos alunos. No entanto dadas as características inovadoras e interdisciplinares do programa bem como o número importante de aplicações, esta situação não tardará a ser invertida.*

#### 9.1.1. Weaknesses

*One of the weak points is the small number of candidates. This is due in part to the program being relatively recent as well as the lack of fellowships administered directly by the program. We believe, however that given the interdisciplinary characteristics of this program as well as the number of important areas of application, that this situation will soon be changed.*

#### 9.1.2. Proposta de melhoria

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*

- *Promoção do curso junto da Indústria e no estrangeiro para aumentar o número de alunos;*
- *Maior inserção em programas de doutoramento nacionais e internacionais (eg CMU|Portugal);*
- *Aumento do esforço na captação de bolsas de doutoramento.*

**9.1.2. Improvement proposal**

*Measures to tackle the previously mentioned gaps:*

- *To promote the program among Industry stakeholders and abroad to increase the number of students;*
- *To provide greater integration in national and international PhD programs;*
- *To increase efforts to attract PhD scholarships.*

**9.1.3. Tempo de implementação da medida**

*Em permanência.*

**9.1.3. Implementation time**

*Permanently.*

**9.1.4. Prioridade (Alta, Média, Baixa)**

*Alta.*

**9.1.4. Priority (High, Medium, Low)**

*High.*

**9.1.5. Indicador de implementação**

*Monitorização do número de alunos de doutoramento.*

**9.1.5. Implementation marker**

*Monitoring of the number of PhD students.*

**9.2. Organização interna e mecanismos de garantia da qualidade.**

---

**9.2.1. Debilidades**

*Um dos pontos fracos diz respeito à interação entre alunos e indústria.*

*Seria importante uma divulgação e partilha, interna e externa, dos resultados dos projetos de investigação dos doutorandos. Sendo esses projetos enquadrados pela atividade das unidades de investigação, fica a elas muito condicionada a potenciação de sinergias e a partilha de experiências.*

**9.2.1. Weaknesses**

*On of the weaknesses concerns the interaction between students and industry.*

*It would be importnat to increase the dissemination and sharing, both internally and externally, of the outcomes of the PhD research projects. As these projects fall into the scope of the activity of the research units, synergies and the sharing of experiences is greatly influenced by it.*

**9.2.2. Proposta de melhoria**

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*

- *Aumento da divulgação e partilha dos resultados dos projectos de investigação.*
- *Aumento do esforço para obtenção de maior número de alunos de doutoramento;*
- *Possibilidade de atrair alunos de outros países;*
- *Criação de redes de ensino temáticas a nível nacional e/ou internacional, como forma de aumentar a massa crítica de alunos por disciplina;*

**9.2.2. Improvement proposal**

*Measures to tackle the previously mentioned gaps:*

- *To increase the dissemination and sharing of the outcomes of research projects.*
- *To increase efforts to attract more PhD students;*
- *The possibility to attract foreign students;*
- *To create teaching networks nationally and/or internationally as a way to increase the critical mass of students per course unit;*

**9.2.3. Tempo de implementação da medida**

*Em permanência.*

**9.2.3. Improvement proposal**

*Em permanência.*

**9.2.4. Prioridade (Alta, Média, Baixa)****Alta****9.2.4. Priority (High, Medium, Low)****High****9.2.5. Indicador de implementação**

- *Número de alunos de doutoramento;*
- *Divulgação dos projectos de investigação e de doutoramentos concluídos.*

**9.2.5. Implementation marker**

- *Number of PhD students;*
- *Dissemination of research projects and PhDs concluded.*

**9.3 Recursos materiais e parcerias**

---

**9.3.1. Debilidades**

*Ainda no contexto das parcerias, é essencial reforçar a formalização de relações privilegiadas com as empresas que atuam no sector.*

**9.3.1. Weaknesses**

*Still within the context of partnerships, it is essential to reinforce the establishment of privileged relationships with companies that operate in this sector.*

**9.3.2. Proposta de melhoria**

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*

- *Aumento de colaboração com Indústria em projectos de investigação financiados;*
- *Criação de redes de ensino e investigação temáticas a nível nacional e/ou internacional, como forma de aumentar a massa crítica de alunos por disciplina, por exemplo através do aproveitamento do programa CMU|Portugal;*

**9.3.2. Improvement proposal**

*Measures to tackle the previously mentioned gaps:*

- *To increase the cooperation with Industry in sponsored research projects;*
- *To create thematic teaching and research networks nationally and/or internationally, as a way to increase the critical mass of students per course unit, as an example through the reinforcement of the CMU|Portugal program.*

**9.3.3. Tempo de implementação da medida**

*Em permanência.*

**9.3.3. Implementation time**

*Permanently*

**9.3.4. Prioridade (Alta, Média, Baixa)****Alta****9.3.4. Priority (High, Medium, Low)****High****9.3.5. Indicador de implementação**

- *Número de teses financiadas por projectos em colaboração com a Indústria;*
- *Número de teses orientadas por docentes de mais de uma Escola;*

**9.3.5. Implementation marker**

- *Number of thesis funded per project in cooperation with Industry;*
- *Number of supervised thesis per teacher of more than one University;*

## 9.4. Pessoal docente e não docente

---

### 9.4.1. Debilidades

*O número reduzido de pessoal não docente torna especialmente difícil o acompanhamento e inserção de alunos internacionais. Além disso existe uma clara sobrecarga administrativa sobre os docentes responsáveis pelo programa.*

### 9.4.1. Weaknesses

*The reduced number of support staff makes it particularly hard to help incoming international students. Furthermore there is a clear overload on the professors in charge of the program.*

### 9.4.2. Proposta de melhoria

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*  
*- Aumentar o número e a formação do pessoal de apoio de secretariado com meios próprios ou através de pessoal de empresas públicas e privadas.*

### 9.4.2. Improvement proposal

*Measures to tackle the previously mentioned gaps:*  
*- To increase the number and background level of secretariat staff with its own means or through the staff tied to state-owned and private companies.*

### 9.4.3. Tempo de implementação da medida

*A contratação de mais pessoal não depende presentemente da Escola.*

### 9.4.3. Implementation time

*The recruitment of more staff does not currently depend on IST itself.*

### 9.4.4. Prioridade (Alta, Média, Baixa)

*Alta*

### 9.4.4. Priority (High, Medium, Low)

*High*

### 9.4.5. Indicador de implementação

*- Número de funcionários de apoio e respectivo nível de formação de base;*  
*- Verbas para contratação de pessoal não docente.*

### 9.4.5. Implementation marker

*- Number of staff and respective background level;*  
*- Sums to recruit non-teaching staff.*

## 9.5. Estudantes e ambientes de ensino/aprendizagem

---

### 9.5.1. Debilidades

*O número de estudantes e a sua inserção em ambientes de investigação em colaboração com a indústria é um dos aspectos que deve ser reforçado. Outro aspecto onde progresso importante pode ser obtido é na atracção de mais alunos, quer de Portugal quer do estrangeiro.*

### 9.5.1. Weaknesses

*The number of students and its insertion in research environments in collaboration with industry is one of the aspects that must be reinforced. Also significant progress can be obtained in the attraction of students both from Portugal and abroad.*

### 9.5.2. Proposta de melhoria

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*  
*- Aumentar o número de alunos, obtendo financiamento da Indústria através de projectos conjuntos;*  
*- Necessidade de uma maior agressividade ao nível do financiamento Europeu (ex: Erasmus Mundus);*  
*- Maior esforço na obtenção de empregos pós-doutoramento.*

#### 9.5.2. Improvement proposal

*Measures to tackle the previously mentioned gaps:*

- *To increase the number of students, obtaining funding from Industry through joint projects;*
- *To need to be more aggressive in terms of getting funds from Europe (ex: Erasmus Mundus);*
- *To make further efforts to obtain post-doctoral jobs.*

#### 9.5.3. Tempo de implementação da medida

*Em curso.*

#### 9.5.3. Implementation time

*In progress.*

#### 9.5.4. Prioridade (Alta, Média, Baixa)

*Alta*

#### 9.5.4. Priority (High, Medium, Low)

*High*

#### 9.5.5. Indicador de implementação

- *Número de alunos de doutoramento;*
- *Taxa de empregabilidade pós-doutoramento;*
- *Bolsas de doutoramento da Indústria*

#### 9.5.5. Implementation marker

- *Number of PhD students;*
- *Post-PhD employability rate;*
- *PhD Scholarships from Industry*

### 9.6. Processos

---

#### 9.6.1. Debilidades

*Um dos pontos fortes do programa é a sua interdisciplinaridade, o que permitiria atrair alunos de diferentes backgrounds.*

*É essencial que esta vantagem seja utilizada de uma forma mais intensa para permitir atrair um maior número de alunos.*

#### 9.6.1. Weaknesses

*One of the strong points of this program is the interdisciplinarity which should enable to attract students from different backgrounds. It is essential this advantage be used in a more intense and systematic way to attract a larger number of students.*

#### 9.6.2. Proposta de melhoria

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*

- *Sensibilizar as entidades competentes para maior apoio financeiro;*
- *Divulgação mais intensa quer a nível nacional quer internacional.*

#### 9.6.2. Improvement proposal

*Measures to tackle the previously mentioned gaps:*

- *To make the competent authorities aware of the situation to get additional financial support;*
- *More intense publicity for the program both at national and international level.*

#### 9.6.3. Tempo de implementação da medida

*Em permanência*

#### 9.6.3. Implementation time

*Permanently*

#### 9.6.4. Prioridade (Alta, Média, Baixa)

*Alta*



**9.6.4. Priority (High, Medium, Low)****High****9.6.5. Indicador de implementação**

- *Apoios financeiros;*
- *Número de alunos.*

**9.6.5. Implementation marker**

- *Financial support;*
- *Number of students.*

**9.7. Resultados**

---

**9.7.1. Debilidades**

*Em termos de resultados, o aspeto mais fraco é o subaproveitamento da capacidade instalada, especialmente em recursos humanos, face ao número de doutorandos captados no país e no estrangeiro. Seria desejável aumentar a inserção do curso em parcerias, tanto nacionais como internacionais.*

**9.7.1. Weaknesses**

*In terms of results, the weakest aspect is the poor utilization of the installed capacity, particularly human resources as compared to the number of PhD students attracted across the country and abroad. The integration of the program in national and international partnerships is expected to increase.*

**9.7.2. Proposta de melhoria**

*Prevêem-se como medidas para colmatar as debilidades acima referidas as seguintes actuações:*

- *Aumentar o número de alunos de doutoramento;*
- *Aumentar as inserções em parcerias de investigação;*
- *Aumentar as formações associadas à Indústria e a prestação de serviços.*

**9.7.2. Improvement proposal**

*Measures to tackle the previously mentioned gaps:*

- *To increase the number of PhD students;*
- *To increase integrations in research partnerships;*
- *To increase programs associates with Industry and service provision.*

**9.7.3. Tempo de implementação da medida**

*Em curso.*

**9.7.3. Implementation time**

*In progress.*

**9.7.4. Prioridade (Alta, Média, Baixa)****Alta****9.7.4. Priority (High, Medium, Low)****High****9.7.5. Indicador de implementação**

- *Número de alunos de doutoramento;*
- *Número de doutoramentos em parceria com a Indústria*

**9.7.5. Implementation marker**

- *Number of PhD students;*
- *Number of PhD programs in partnership with Industry.*

## 10. Proposta de reestruturação curricular

### 10.1. Alterações à estrutura curricular

---

#### 10.1. Alterações à estrutura curricular

##### 10.1.1. Síntese das alterações pretendidas

*N/A*

##### 10.1.1. Synthesis of the intended changes

*N/A*

#### 10.1.2. Nova estrutura curricular pretendida

##### Mapa XI - Nova estrutura curricular pretendida

##### 10.1.2.1. Ciclo de Estudos:

*Segurança de Informação*

##### 10.1.2.1. Study Cycle:

*Information Security*

##### 10.1.2.2. Grau:

*Doutor*

##### 10.1.2.3. Ramos, opções, perfis, maior/menor, ou outras (se aplicável)

*<sem resposta>*

##### 10.1.2.3. Branches, options, profiles, major/minor, or other forms (if applicable)

*<no answer>*

#### 10.1.2.4 Nova estrutura curricular pretendida / New intended curricular structure

Área Científica / Scientific Area	Sigla / Acronym	ECTS Obrigatórios / Mandatory ECTS	ECTS Optativos / Optional ECTS*
(0 Items)		0	0

*<sem resposta>*

### 10.2. Novo plano de estudos

---

#### Mapa XII – Novo plano de estudos

##### 10.2.1. Ciclo de Estudos:

*Segurança de Informação*

##### 10.2.1. Study Cycle:

*Information Security*

##### 10.2.2. Grau:

*Doutor*

##### 10.2.3. Ramos, opções, perfis, maior/menor, ou outras (se aplicável)

*<sem resposta>*

**10.2.3. Branches, options, profiles, major/minor, or other forms (if applicable)***<no answer>***10.2.4. Ano/semestre/trimestre curricular:***<sem resposta>***10.2.4. Curricular year/semester/trimester:***<no answer>***10.2.5 Novo plano de estudos / New study plan**

Unidades Curriculares / Curricular Units	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
---	--	---------------------------	---------------------------------------	---------------------------------------	------	-----------------------------------

(0 Items)

*<sem resposta>***10.3. Fichas curriculares dos docentes****Mapa XIII****10.3.1. Nome do docente (preencher o nome completo):***<sem resposta>***10.3.2. Instituição de ensino superior (preencher apenas quando diferente da instituição proponente mencionada em A1):***<sem resposta>***10.3.3 Unidade Orgânica (preencher apenas quando diferente da unidade orgânica mencionada em A2.):***<sem resposta>***10.3.4. Categoria:***<sem resposta>***10.3.5. Regime de tempo na instituição que submete a proposta (%):***<sem resposta>***10.3.6. Ficha curricular de docente:***<sem resposta>***10.4. Organização das Unidades Curriculares (apenas para as unidades curriculares novas)****Mapa XIV****10.4.1.1. Unidade curricular:***<sem resposta>***10.4.1.2. Docente responsável e respectiva carga lectiva na unidade curricular (preencher o nome completo):***<sem resposta>***10.4.1.3. Outros docentes e respectivas cargas lectivas na unidade curricular:***<sem resposta>***10.4.1.3. Other academic staff and lecturing load in the curricular unit:***<no answer>*

**10.4.1.4. Objectivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):**  
<sem resposta>

**10.4.1.4. Learning outcomes of the curricular unit:**  
<no answer>

**10.4.1.5. Conteúdos programáticos:**  
<sem resposta>

**10.4.1.5. Syllabus:**  
<no answer>

**10.4.1.6. Demonstração da coerência dos conteúdos programáticos com os objectivos da unidade curricular.**  
<sem resposta>

**10.4.1.6. Demonstration of the syllabus coherence with the curricular unit's objectives.**  
<no answer>

**10.4.1.7. Metodologias de ensino (avaliação incluída):**  
<sem resposta>

**10.4.1.7. Teaching methodologies (including evaluation):**  
<no answer>

**10.4.1.8. Demonstração da coerência das metodologias de ensino com os objectivos de aprendizagem da unidade curricular.**  
<sem resposta>

**10.4.1.8. Demonstration of the coherence between the teaching methodologies and the learning outcomes.**  
<no answer>

**10.4.1.9. Bibliografia principal:**  
<sem resposta>