NCE/16/00037 — Apresentação do pedido - Novo ciclo de estudos

Apresentação do pedido

Perguntas A1 a A4

A1. Instituição de ensino superior / Entidade instituidora:
Instituto Politécnico De Leiria

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

A2. Unidade(s) orgânica(s) (faculdade, escola, instituto, etc.):
Escola Superior De Tecnologia E Gestão De Leiria

A3. Designação do ciclo de estudos:
Cibersegurança e Informática Forense

A3. Study programme name:
Cibersecurity and Digital Forensics

A4. Grau:
Mestre

Perguntas A5 a A10

A5. Área científica predominante do ciclo de estudos:
Engenharia Informática

A5. Main scientific area of the study programme:
Informatics Engineering

A6.1. Classificação da área principal do ciclo de estudos (3 dígitos), de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF):
523

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

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

NA

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

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

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

A9. Número máximo de admissões:
40

A10. Condições específicas de ingresso:
Podem candidatar-se ao acesso ao ciclo de estudos conducente ao grau de mestre:
1) Titulares do grau de licenciado ou equivalente legal, na área de Engenharia Informática e áreas afins
2) Titulares de um grau académico superior estrangeiro conferido na sequência de um 1.º ciclo de estudos organizado de acordo com os princípios do Processo de Bolonha por um Estado aderente a este Processo, na área de Engenharia Informática e áreas afins
3) Titulares de um grau académico superior estrangeiro que seja reconhecido como satisfazendo os objetivos do grau de licenciado na área de Engenharia Informática e áreas afins, pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão
4)Detentores de um currículo escolar, científico ou profissional que seja reconhecido como atestando capacidade para a realização deste ciclo de estudos pelo Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão

A10. Specific entry requirements:
May apply for access to the course of study leading to a master degree:
a) Holders of an undergraduate degree or a legal equivalent In Computers Engineering or related fields.
b) Holders of a foreign higher education diploma, granted after a first cycle of studies, under the principles of the Bologna Process, by a State, which has subscribed this Process.
c) Holders of a foreign higher education diploma that is recognized as meeting the objectives of an undergraduate degree by the scientific body of ESTG-IPLeiria.
d) Holders of an academic, scientific or professional curriculum, recognized as adequate to attend the study cycle by the scientific body of ESTG-IPLeiria.

Pergunta A11

Pergunta A11

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

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

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

Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento: **Branch, option, specialization area of the master or speciality of the PhD:**

<sem resposta>

A12. Estrutura curricular

Mapa I - Não aplicável

A12.1. Ciclo de Estudos:
Cibersegurança e Informática Forense

A12.1. Study Programme:
Cibersecurity and Digital Forensics

A12.2. Grau:
Mestre

A12.3. Ramo, variante, área de especialização do mestrado ou especialidade do doutoramento (se aplicável):
Não aplicável

A12.3. Branch, option, specialization area of the master or speciality of the PhD (if applicable):
Not applicable

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

Área Científica / Scientific Area	Sigla / Acronym	ECTS Obrigatórios / Mandatory ECTS	ECTS Minímos Optativos* / Minimum Optional ECTS*
Engenharia Informática / Computers Engineering	EI	120	
(1 Item)		**120**	**0**

Perguntas A13 e A16

A13. Regime de funcionamento:
Pós Laboral

A13.1. Se outro, especifique:
<sem resposta>

A13.1. If other, specify:

<no answer>

A14. Local onde o ciclo de estudos será ministrado:
Escola Superior de Tecnologia e Gestão de Leiria (ESTG - Leiria)

A14. Premises where the study programme will be lectured:
Escola Superior de Tecnologia e Gestão de Leiria (ESTG - Leiria)

A15. Regulamento de creditação de formação e experiência profissional (PDF, máx. 500kB):
A15._regulamento_creditacao.pdf
A16. Observações:
<sem resposta>

A16. Observations:
<no answer>

Instrução do pedido

1. Formalização do pedido

1.1. Deliberações

Mapa II - Conselho Pedagógico da Escola Superior de Tecnologia e Gestão do I.P. Leiria

1.1.1. Órgão ouvido:
Conselho Pedagógico da Escola Superior de Tecnologia e Gestão do I.P. Leiria

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

Mapa II - Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão do I.P. Leiria

1.1.1. Órgão ouvido:
Conselho Técnico-Científico da Escola Superior de Tecnologia e Gestão do I.P. Leiria

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

Mapa II - Plenário do Departamento de Engenharia Informática da ESTG-I.P. Leiria

1.1.1. Órgão ouvido:

Plenário do Departamento de Engenharia Informática da ESTG-I.P. Leiria

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

Mapa II - Conselho Académico

1.1.1. Órgão ouvido:
Conselho Académico

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

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

1.2. Docente(s) responsável(eis) pela coordenação da implementação do ciclo de estudos
A(s) respetiva(s) ficha(s) curricular(es) deve(m) ser apresentada(s) no Mapa V.
Mário João Gonçalves Antunes

2. Plano de estudos

Mapa III - - 1ºano/1ºsemestre

2.1. Ciclo de Estudos:
Cibersegurança e Informática Forense

2.1. Study Programme:
Cibersecurity and Digital Forensics

2.2. Grau:
Mestre

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

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

2.4. Ano/semestre/trimestre curricular:
1ºano/1ºsemestre

2.4. Curricular year/semester/trimester:
1st year/1st semester

2.5. Plano de Estudos / Study plan

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Políticas e Análise de Risco na Segurança de Informação / Policy and Risk Analysis for Information Security	EI	Semestral	162	TP-30	6	Obrigatória
Segurança em Redes de Computadores / Computers Network Security	EI	Semestral	162	TP-30	6	Obrigatória
Análise Forense Digital I / Digital Forensics I	EI	Semestral	162	TP-30	6	Obrigatória
Administração Segura de Sistemas informáticos / Secure Administration of Computer Systems	EI	Semestral	162	TP-30	6	Obrigatória
Projeto de Segurança I / Project on Security I	EI	Semestral	162	TP-30	6	Obrigatória
(5 Items)						

Mapa III - - 1ºano/2ºsemestre

2.1. Ciclo de Estudos:
Cibersegurança e Informática Forense

2.1. Study Programme:
Cibersecurity and Digital Forensics

2.2. Grau:
Mestre

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

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

2.4. Ano/semestre/trimestre curricular:
1ºano/2ºsemestre

2.4. Curricular year/semester/trimester:
1sy year/2nd semester

2.5. Plano de Estudos / Study plan

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)

Laboratório de Testes de Penetração / Penetration Testing Laboratory	EI	Semestral	162	TP-30	6	Obrigatória
Gestão e Análise de Relatórios de Segurança / Management and Analysis of Security Reports	EI	Semestral	162	TP-30	6	Obrigatória
Tratamento de Incidentes Informáticos / Computer Incident Handling	EI	Semestral	162	TP-30	6	Obrigatória
Análise Forense Digital II / Digital Forensics II	EI	Semestral	162	TP-30	6	Obrigatória
Projecto de Segurança II / Project on Security II	EI	Semestral	162	TP-30	6	Obrigatória

(5 Items)

Mapa III - - 2ºano/1º e 2º semestres

2.1. Ciclo de Estudos:
Cibersegurança e Informática Forense

2.1. Study Programme:
Cibersecurity and Digital Forensics

2.2. Grau:
Mestre

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

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

2.4. Ano/semestre/trimestre curricular:
2ºano/1º e 2º semestres

2.4. Curricular year/semester/trimester:
2nd year/1st and 2nd semesters

2.5. Plano de Estudos / Study plan

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Projeto / Project	EI	Anual	1620	TP-60	60	Optativa
Dissertação / Dissertation	EI	Anual	1620	TP-60	60	Optativa
Estágio / Internship	EI	Anual	1620	TP-60	60	Optativa

(3 Items)

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

3.1. Dos objetivos do ciclo de estudos

3.1.1. Objetivos gerais definidos para o ciclo de estudos:

O ciclo de estudo que se propõe pretende atingir os seguintes objetivos gerais:
1) Dar continuidade à formação de 1ºciclo em Engenharia Informática existente na ESTG/IPLeiria
2) Desenvolver a oferta de 2ºciclo em Engenharia Informática na ESTG/IPLeiria.
3) Formar técnicos altamente qualificados nas área da cibersegurança e da computação forense.
4) Desenvolver a ligação com o tecido empresarial da região através da realização de estágios, projetos e dissertações, que possam permitir a aplicação de boas práticas na área da cibersegurança.
5) Desenvolver a investigação aplicada nas áreas da cibersegurança e computação forense, nomeadamente através da realização dos projetos e dissertações.
6) Promover a transferência de conhecimento avançado nas áreas de cibersegurança e computação forense para as organizações.
7) Promover uma aprendizagem ao longo da vida de um modo fundamentalmente auto-orientado ou autónomo.

3.1.1. Generic objectives defined for the study programme:

The study programme aims to achieve the following generic goals:
1) To enable the progress of the students from the 1st study cycle in computers engineering in ESTG-Leiria
2) To develop the 2nd cycle academic offer in the field of computers engineering in ESTG Leiria
3) To obtain highly qualified computers engineers and technicians in the fields of cybersecurity and digital forensics.
4) To develop partnerships with companies of the region through internships, projects and dissertations that may apply best practices in cybersecurity fields.
5) To develop applied research in the field of cybersecurity and digital forensics by the completion of projects and dissertations
6) To promote the transference of advanced knowledge in the fields of of cybersecurity and digital forensics to society
7) To promote a self-oriented and autonomous long-life learning study.

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

Este ciclo de estudo pretende dotar os seus diplomados de conhecimentos sólidos em:
1) Aplicar os conhecimentos e a capacidade de compreensão e de resolução de problemas em situações novas e não familiares, em contextos alargados e multidisciplinares;
2) Dominar aplicações, metodologias e tecnologias relacionadas com o planeamento, implementação e monitorização de soluções de cibersegurança nas organizações.
3) Dominar aplicações, metodologias e tecnologias relacionadas com a computação digital forense.
4) Integrar conhecimentos, lidar com questões complexas, desenvolver soluções ou emitir juízos em situações de informação limitada ou incompleta;
5) Comunicar as conclusões e os conhecimentos e raciocínios a elas subjacentes a especialistas e não especialista da área;
6) Desenvolver uma aprendizagem ao longo da vida de um modo fundamentalmente auto-orientado ou autónomo.
7) Possuir competências profissionais e de investigação científica em informática.

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

Graduates from this study cycle should have strong skills in the following issues:
1) To apply skills and comprehension ability to solve problems and situations in new and unfamiliar scenarios, in wide contexts and multidisciplinary.
2) To have strong skills on applications, methodologies and technologies related with planning, implementation and monitoring of cybersecurity applications in the organizations.
3) To have strong skills on applications, methodologies and technologies related with digital forensics.
4) To integrate skills, to deal with complex scenarios, to develop solutions or issue a judgment in situations of limited or incomplete information.
5) To communicate the conclusions and the knowledge and reasoning underlying them to specialists and non-specialists in the area.
6) To develop a long-life learning strategy in a self-oriented or autonomous way.
7) To possess professional and scientific research skills in computer science.

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

O Instituto Politécnico de Leiria (IPL) é uma instituição pública de ensino superior comprometida com a formação integral dos cidadãos, a aprendizagem ao longo da vida, a investigação, a difusão e transferência do conhecimento e cultura, a qualidade e a inovação. Promove ativamente o desenvolvimento regional e nacional e a internacionalização.

Valoriza a inclusão, a cooperação, a responsabilidade, a criatividade e o espírito crítico e empreendedor.
A Escola Superior de Tecnologia e Gestão (ESTG) é uma das unidades orgânicas do IPL, tendo como missão formar pessoas altamente qualificadas, numa perspetiva interdisciplinar e num contexto de excelência, com capacidade de adaptação à mudança, promover a investigação, inovação e empreendedorismo e a aprendizagem ao longo da vida, sendo uma força motriz de desenvolvimento regional numa perspetiva global.
O Mestrado em Cibersegurança e Computação Forense enquadra-se na área da tecnologia, uma das áreas de enfoque da ESTG. Os objetivos definidos para este Mestrado vão ao encontro do estabelecido na missão da ESTG, visto que se pretende promover a aprendizagem ao longo da vida, formando profissionais competentes, dotados de capacidade de adaptação à mudança e com autonomia na aprendizagem, quer durante a frequência do curso, quer após a entrada no mercado de trabalho, sem esquecer os valores da inclusão, da cooperação, da responsabilidade, da criatividade, do espírito crítico e do espírito empreendedor.

3.1.3. Insertion of the study programme in the institutional training offer strategy against the mission of the institution:
The Polytechnic Institute of Leiria (IPL) is a public institution of higher education committed to the education of citizens, learning through life, research, dissemination and transfer of knowledge and culture, quality and innovation. Actively promotes regional and national development and internationalization. The IPL promotes inclusion, cooperation, responsibility, creativity and critical thinking and entrepreneurial.
The School of Technology and Management (ESTG) is one of the basic units of the IPL, with the mission to train highly qualified people, in a perspective and in a context of interdisciplinary excellence that are able to adapt to change, to promote research, innovation and entrepreneurship and lifelong learning. The ESTG is a driving force for regional development in a global perspective.
A Master degree in Cybersecurity and Digital Forensics fits in the area of technology, one of the ESTG areas of focus. The defined objectives of this master degree will meet the established mission of ESTG, since it is intended to promote lifelong life learning and to train professionals that have the capacity to adapt to change and learning autonomy, both during the course or after entering the labor market, without forgetting the values of inclusion, cooperation, responsibility, creativity, critical thinking and entrepreneurial spirit.

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

3.2.1. Projeto educativo, científico e cultural da Instituição:
O Instituto Politécnico de Leiria (IPL) é uma instituição pública de ensino superior comprometida com a formação integral dos cidadãos, a aprendizagem ao longo da vida, a investigação, a difusão e transferência do conhecimento e cultura, a qualidade e a inovação. Promove ativamente o desenvolvimento regional e nacional e a internacionalização. Valoriza a inclusão, a cooperação, a responsabilidade, a criatividade e o espírito crítico e empreendedor.
Entre as diversas escolas do Instituto Politécnico de Leiria, encontram-se a Escola Superior de Tecnologia e Gestão (ESTG), e a Escola Superior de Artes e Design (ESAD). A ESTG supervisiona a oferta formativa nas áreas da Tecnologia e nas áreas da Gestão, enquanto a ESAD supervisiona a oferta formativa na área das artes e do design.

3.2.1. Institution's educational, scientific and cultural project:
The Polytechnic Institute of Leiria (IPL) is a public institution of college education committed to the education of citizens, lifelong learning, research, dissemination and transfer of knowledge and culture, quality and innovation. The institutes actively promotes regional and national development and internationalization. It values inclusion, cooperation, responsibility, creativity and critical thinking. Among the five schools of the Polytechnic Institute of Leiria, are the School of Technology and Management (ESTG), and the School of Art and Design (ESAD). ESTG oversees the training offer in the areas of technology and in the areas of management, while ESAD oversees the training offer in arts and design.

3.2.2. Demonstração de que os objetivos definidos para o ciclo de estudos são compatíveis com o projeto educativo, científico e cultural da Instituição:
O mestrado em Cibersegurança e Informática Forense enquadra-se no projeto educativo, científico e cultural da Instituição pelas seguintes razões:
1) Estar incluído nos domínios nucleares de formação na instituição, nomeadamente na área das tecnologias, mais concretamente da Informática.
2) Responder à dinâmica de desenvolvimento do projeto educativo e científico, nomeadamente pela oferta de formação avançada que responda às necessidades do meio em que está inserida.
3) Ter como objetivo o desenvolvimento de parcerias empresariais na realização de estágios, projetos e dissertações com vista à implementação de soluções de cibersegurança nas empresas e organizações.
4) Ter como objetivo o desenvolvimento da investigação, nomeadamente pela realização de projetos e dissertações, visando a transferência do conhecimento.

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

The master degree in Cybersecurity and Digital Forensics is coherent with the educational, scientific and cultural project of the institution due to the following reasons:
1) It is included in training fields of the institution, particularly in Technology studies and more precisely in computers engineering.
2) It answers to the dynamics in the development of scientific and educational project, namely the provision of advanced training that meets the needs of the environment in which it operates.
3) It aims to develop business partnerships with the internships, projects and dissertations focused in the implementation of cybersecurity solutions in the organizations.
4) It aims to develop research, in particular by carrying out projects and dissertations focused in knowledge transference.

3.3. Unidades Curriculares

Mapa IV - Políticas e Análise de Risco na Segurança de Informação

3.3.1. Unidade curricular:
Políticas e Análise de Risco na Segurança de Informação

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Carlos Manuel da Silva Rabadão

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
C1.Compreensão das bases da segurança da informação
C2.Compreensão da importância dos Sistemas de Gestão de Segurança da Informação (SGSI)
C3.Conhecimento da legislação, regulamentação e normas associadas aos SGSI
C4.Compreensão dos principais componentes dos SGSI e processo de implementação
C5.Proceder à análise de risco de sistemas de informação empresarial, identificando os riscos, vulnerabilidades e ameaças
C6.Proceder à definição das políticas de segurança, adotando normas, procedimentos e boas práticas
C7.Identificar objetivos de cada regra adotada e a sua relação com normas e legislação em vigor, bem como descrever o papel dos vários elementos da organização e definir medidas a implementar e mecanismos a adotar (tecnológicos/logísticos/legais)
C8.Capacidade para definir e implementar cenários práticos de SGSI
C9.Capacidade para pesquisar informação em diferentes meios e formatos e de proceder à sua utilização de forma eficaz
C10.Capacidade de realizar projetos em equipa

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
C1.Understanding of information security fundamentals
C2.Understanding the importance of Information Security Management Systems (ISMS)
C3. Knowledge of the laws, regulations and standards associated with the ISMS
C4.Understanding of the main components of the ISMS and its implementation
C5.Carry out the risk analysis of business information systems, identifying risks, vulnerabilities and threats.
C6.Ability to define security policies, adopting key standards, procedures and best practices in the area
C7.Ability to identify the objectives of each adopted rule and its relationship with standards and legislation, as well as describe the role of the various elements of the organization and define the measures to implement and mechanisms to adopt (technologics / logistics / legals)
C8.Ability to define and implement practical scenarios of ISMS
C9.Ability to research information in different sources and formats and proceed to it effective application
C10.Ability to carry out teams projects

3.3.5. Conteúdos programáticos:

1. Princípios fundamentais da segurança
2. Regulamentação, investigação, conformidade e ética
3. Sistemas de Gestão de Segurança da Informação
4. Políticas, normas, linhas orientadoras, diretrizes e procedimentos
5. Definição do programa de segurança da informação
6. Gestão, avaliação e análise de risco
7. Modelos e práticas de gestão de segurança informática

3.3.5. Syllabus:

1. Fundamental principles of security
2. Regulation, investigation, compliance and ethics
3. Information security management systems
4. Policies, Standards, Baselines, Guidelines and Procedures
5. Information Security Program
6. Risk Management, Assessment and Analysis
7. Security management models and practices

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

1. Princípios fundamentais da segurança (C1)
2. Regulamentação, investigação, conformidade e ética (C3)
3. Sistemas de Gestão de Segurança da Informação (C2, C4)
4. Políticas, normas, linhas orientadoras, diretrizes e procedimentos (C3, C6, C7)
5. Definição do programa de segurança da informação (C6, C7, C8, C9, C10)
6. Gestão, avaliação e análise de risco (C1, C5, C9, C10)
7. Modelos e práticas de gestão de segurança informática (C3, C7, C8, C9, C10)

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

1. Fundamental principles of security (C1)
2. Regulation, investigation, compliance and ethics (C3)
3. Information security management systems (C2, C4)
4. Policies, Standards, Baselines, Guidelines and Procedures (C3, C6, C7)
5. Information Security Program (C6, C7, C8, C9, C10)
6. Risk Management, Assessment and Analysis (C1, C5, C9, C10)
7. Security management models and practices (C3, C7, C8, C9, C10)

3.3.7. Metodologias de ensino (avaliação incluída):

Presencial

Teórico-Prático (TP): exposição e compreensão dos conteúdos programáticos relacionados com os capítulos 1 a 7, e sua consolidação com discussão de casos práticos.
Autónoma
Estudo autónomo: Leitura de materiais da unidade curricular e bibliografia.
Projeto: Realização de um projeto em equipa por forma a promover a organização do trabalho e o desenvolvimento de capacidades de autonomia, iniciativa e análise crítica.

3.3.7. Teaching methodologies (including assessment):

Contact teaching
Theoretical/practical (TP): Teacher presentation of the syllabus relating to chapters 1 to 7 and its assimilation by the students. Consolidation of theoretical knowledge thought out the discussion of practical cases.
Autonomous learning
Autonomous study: reading of course materials and recommended bibliography.
Project implementation in order to promote the organization of team work and the development of autonomy, initiative and critical analysis skills.

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Ensino Presencial
Teórico-prático: C1, C2, C3, C4
Aprendizagem Autónoma
Estudo autónomo: C1, C2, C3, C4, C5, C9
Projeto: C5, C6, C7, C8, C9, C10

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
Contact teaching
Theoretical/practical (TP): C1, C2, C3, C4
Autonomous learning
Autonomous study: C1, C2, C3, C4, C5, C9
Project: C5, C6, C7, C8, C9, C10

3.3.9. Bibliografia principal:
- Management of Information Security, 5th Edition. Michael E. Whitman and Herbert J. Mattord.Cengage Learning, 2016. ISBN: 978-1305501256
- Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, 1st Edition. Evan Wheeler. Syngress, 2011. ISBN: 978-1597496155
- IT Governance: An international guide to data security and ISO27001/ISO27002, 5th edition. Alan Calder & Steve Watkins. - KoganPage, 2013. ISBN: 978-0749464851
Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, 1st Edition. Corey Schou and Steven Hernandez. McGraw-Hill Education, 2014. ISBN: 978-0071821650
- NIST Special Publication 800-30 - Rev.1. Information Security: Guide for Conducting Risk Assessments. Joint task force transformation initiative. NIST, 2012.
- NIST Special Publication 800-39 - Rev.1. Information Security: Managing Information Security Risk – Organization, Mission, and Information System View. Joint task force. NIST, 2011

Mapa IV - Segurança em Redes de Computadores

3.3.1. Unidade curricular:
Segurança em Redes de Computadores

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

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
Paulo Manuel Gonçalves Oliveira Valente da Cruz, 15h

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

C1 - Compreender as principais noções e protocolos relacionados com a segurança em redes.
C2 - Identificar os principais desafios na segurança física de uma infraestrutura de rede.
C3 - Conhecer de forma aprofundada o funcionamento da pilha protocolar TCP/IP e identificar os principais protocolos relacionados com a segurança da comunicação na Internet.
C4 - Configurar os principais serviços de rede tendo em conta preocupações relacionadas com a segurança.
C5 - Utilizar aplicações de filtragem de pacotes e detecção de ataques.
C6 - Desenvolver cenários práticos de implementação de soluções seguras de interligação de redes.
C7 - Elaborar relatórios técnicos e justificar decisões tomadas.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
C1 - To understand network security fundamentals and protocols.
C2 - To identify the main challenges on physically securing a network infrastructure.
C3 - To understand in depth the TCP/IP functioning and to identify its main protocols related with secure communications on the Internet.
C4 - To configure the main Internet services, concerning security issues.
C5 - To use applications for packet filtering and intrusion detections.
C6 - To deploy and implement networking scenarios for secure internetworking solutions.
C7 - To elaborate technical reports and to justify technical decisions.

3.3.5. Conteúdos programáticos:
1 - Tópicos avançados de comunicação TCP/IP
2 - Tópicos fundamentais de segurança em sistemas e redes
3 - Aspectos de segurança em IPv6
4 - Segurança física de redes - cablagem e datacenters
5 - Segurança lógica: protocolo IP e TCP
6 - Segurança nos serviços de resolução de nomes e DHCP
7 - Protocolos e serviços de segurança em redes: IPSec, SSL/TLS
8 - Firewalls
9 - Sistemas de deteção de intrusões

3.3.5. Syllabus:
1 - Advanced topics on TCP/IP communication
2 - Fundamentals on systems and networking security
3 - IPv6 security issues
4 - Physical security - cabling and datacenters
5 - Logical security - IP e TCP protocols
6 - Naming and DHCP protocols
7 - Networking security protocols and services: IPSec, SSL/TLS
8 - Firewalls
9 - Intrusion detection systems

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Os conteúdos programáticos lecionados contribuem para as competências gerais estabelecidas para a UC da seguinte forma:

1 - Tópicos avançados de comunicação TCP/IP (C1,C3)
2 - Tópicos fundamentais de segurança em sistemas e redes (C1,C2,C3)
3 - Aspectos de segurança em IPv6 (C1, C2,C3)
4 - Segurança física de redes - cablagem e datacenters (C2)
5 - Segurança lógica: protocolo IP e TCP (C3,C4)

6 - Segurança nos serviços de resolução de nomes e DHCP (C3,C4,C6,C7)
7 - Protocolos e serviços de segurança em redes:IPSec e SSL (C3,C4,C6,C7)
8 - Firewalls (C5,C6)
9 - Sistemas de deteção de intrusões (C5,C6)

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
The topics covered contribute to achieve the goals defined for the curricular unit in the following manner:

1 - Advanced topics on TCP/IP communication (C1, C3)
2 - Fundamentals in systems and networking security (C1, C2, C3)
3 - IPv6 security issues (C1, C2, C3)
4 - Physical security - cabling and datacenters (C2)
5 - Logical security - IP e TCP protocols (C3, C4)
6 - Naming and DHCP servers security (C3, C4, C6, C7)
7 - Networking security protocols and services: IPSec and SSL/TLS (C3, C4, C6, C7)
8 - Firewalls (C5, C6)
9 - Intrusion detection systems (C5, C6)

3.3.7. Metodologias de ensino (avaliação incluída):
Ensino presencial e teórico-prático - os conceitos serão ilustrados com casos práticos a apresentar na aulas

Estudo autónomo - leitura da bibliografia recomendada e resolução de exercícios

1) Avaliação Periódica
1 teste teórico
1 teste prático
1 trabalho prático realizado fora das aulas

Classificação final: teórico = 30%, prático = 35% e trabalho prático = 35%

2) Exame
1 teste teórico (30%) e 1 teste prático (70%)

3.3.7. Teaching methodologies (including assessment):
Presential, in classroom and theoretical-practice (TP) - contents are presented with practical scenarios in the classroom.

Autonomous - complementar and recommended readings, with exercises.

Evaluation
1) Periodical evaluation:
1 theoretical test
1 practical assessment
1 working group assessment

Final evaluation: theoretical= 30%, practical = 35% and working group = 35%

2) Final assessment - Exam
1 written test (30%) and one lab test (70%)

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Presencial
Ensino teórico-prático - C3, C4, C5, C6, C7, C8, C9
Estudo autónomo
Leitura da bibliografia recomendada e resolução de exercícios - C1, C2, C7

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
Presential, in classroom:
Theoretical-practice (TP) - C3, C4, C5, C6, C7, C8, C9

Autonomous study:
Recommended and complementary readings, with exercises - C1, C2, C7

3.3.9. Bibliografia principal:
- W. Stallings; "Network Security Essentials: Applications and Standards"; Pearson; 5th edition; ISBN: 0273793365; 2013
- Allan Liska, Geoffrey Stowe; "DNS Security: Defending the Domain Name System"; ISBN: 0128033061; ;2016
- Kurose, Ross; "Computer Networking: A Top-Down Approach"; Pearson; ISBN: 0132856204; 2012
- Michel Thomatis; "Network Design Cookbook: Architecting Cisco Networks"; lulu.com; ISBN: 1257750240; 2016
- RFC-Editor: www.rfc-editor.org

Mapa IV - Análise Forense Digital I

3.3.1. Unidade curricular:
Análise Forense Digital I

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

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
A análise forense digital dedica-se à recolha, identificação, preservação, documentação, análise e apresentação de provas digitais a partir de computadores, redes e outros dispositivos eletrónicos. A área forense digital pode ser dividida em: computação forense, análise forense de redes de dados e análise forense de dispositivos móveis.

Após a conclusão desta Unidade Curricular, o estudante deverá ser capaz de:
1- Identificar os diferentes tipos de provas digitais forenses
2- Conhecer a terminologia, técnicas e processos de investigação forense digital
3- Recolher provas digitais em suportes de armazenamento
4- Conhecer as limitações das técnicas atuais de investigação forense digital
5- Compreender o método científico e a necessidade da sua utilização
6- Aplicar o método científico na investigação forense digital
7- Utilizar ferramentas e técnicas de investigação forense digital
8- Interpretar relatórios de análise forense

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

Digital forensics is dedicated to the collection, identification, preservation, documentation, analysis and presentation of digital evidence from computers, data networks and other electronic devices. The digital forensics field can be divided into: computer forensics, data networks forensics and mobile forensics.

Upon completion of this course, the student should be able to:
1- To identify the different types of digital forensic evidence
2- To know the terminology, techniques and processes of a digital forensic investigation
3- To collect digital evidence from storage media
4- To know the limitations of digital forensics current techniques
5- To understand the scientific method and the need for its use
6- To apply the scientific method in a digital forensics investigation
7- To use digital forensics' tools and techniques
8- To comprehend forensic analysis reports

3.3.5. Conteúdos programáticos:

1. Introdução à investigação forense digital
1.1 Método científico
1.2 Privacidade e ética
1.3 Conceitos técnicos
bytes, hexadecimal e unicode
ordem de volatilidade

2. Obtenção de provas
2.1 Procedimentos de 1ª intervenção e recolha de equipamentos
2.2 Fontes de provas
Suportes de armazenamento e zonas escondidas
Redes de dados, live e mobile
2.3 Suportes de armazenamento
Bloqueadores de escrita
Cópias forenses
Partições e volumes
Sistemas de ficheiros FAT e NTFS
Integridade de cópia, colisões e assinaturas digitais

3. Análise de imagens forenses com Autopsy
Espaço desalocado e slack
Ficheiros apagados
Arquivos e metadados
Padrões de pesquisa
Incongruência do tipo de ficheiro e a sua extensão
Navegação web
Clientes de email
Artefactos dos SO Windows

4. Documentação e comunicação
4.1 Limitações da análise forense digital
esconder informação
remoção de provas
adulteração de registos

4.2 Interpretação de relatórios forenses
casos de estudo

3.3.5. Syllabus:

1. Introduction to digital forensics
1.1 Scientific method
1.2 Privacy and ethics
1.3 Technical concepts
bytes, hexadecimal and unicode
order of volatility

2. Obtaining evidences
2.1 1st intervention procedures and equipment seizure
2.2 Evidence sources
Storage media and hidden areas
Data networks, live and mobile
2.3 Storage media
Write blockers
Forensic copies
Partitions and volumes
FAT and NTFS file systems
Copy integrity, collisions and digital signatures

3. Analysis of forensic images with Autopsy
Unallocated and slack space
Deleted files
Files and metadata
Search patterns
File extension mismatch
Web browsing
Email clients
Windows OS artefacts

4. Documentation and report
4.1 Digital forensics limitations
Hidden information
Evidences removal
Records tampering
4.2 Forensic report comprehension
Case studies

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

O tópico 1 visa dotar os estudantes das competências relacionadas com a aplicação do método científico (objectivos de aprendizagem 5 e 6). O tópico 2 visa dotar os estudantes das competências relacionadas com a identificação e recolha de provas (objectivos de aprendizagem 1, 2 e 3). O tópico 3 permitirá dotar os estudantes com competências relacionadas com a análise de provas digitais (6 e 7). Por último, o tópico 4 foca as competências relacionadas com as insuficiências das técnicas de investigação forense digital e com a elaboração de relatórios forenses (4 e 8).

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

Topic 1 aims to provide students with skills for the application of the scientific method (learning objectives 5 and 6). Topic 2 aims to give students skills for the identification and collection of evidences (learning objectives 1, 2 and 3). Topic 3 will equip students with skills to analyse digital evidences (6 and 7). Finally, topic 4 focus on the skills to identify the shortcomings of digital forensics techniques and comprehend digital forensics reports (4 and 8).

3.3.7. Metodologias de ensino (avaliação incluída):

A metodologia a adotar para a generalidade das aulas Teóricas será o método expositivo. Nas aulas práticas será aplicado o método ativo onde os alunos desenvolverão guiões de exercícios, bem como dois trabalhos práticos.

A avaliação dos estudantes será através de 2 testes escritos individuais (tópicos 1 e 4 do programa) e 2 trabalhos práticos (tópicos 2 e 3). Os trabalhos práticos serão realizados em grupo de onde terá de resultar um relatório.

Nota final = 10% Teste escrito 1 + 25% Trabalho prático 1 + 50% Trabalho prático 2 + 15% Teste escrito 2

3.3.7. Teaching methodologies (including assessment):

The methodology to adopt for most of the theoretical classes is the expository method. In practical classes the active method will be applied, where students will develop exercises guidelines as well as two team projects.

Students will be evaluated through two individual written tests (for topics 1 and 4) and 2 projects (for topics 2 and 3). The projects will be carried out by teams where they have to elaborate a report.

Final grade = 10% Written test 1 + 25% Team Project 1 + 50% Team Project 2 + 15% Written test 2

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

As metodologias de ensino estão em coerência com os objetivos da unidade curricular dado que:
1) Os métodos de ensino utilizados, ajustam-se à natureza dos conteúdos programáticos e dos objetivos a atingir em cada sessão. A realização de exposições sobre as diferentes matérias (demonstração e discussão), quer por parte do docente, quer dos estudantes, conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos.
2) Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC.
O regime de avaliação foi concebido para avaliar a extensão e o nível de aquisição das competências a desenvolver.

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

The teaching methodologies are consistent with the objectives of the course given that:
1) The used teaching methods adjust to the nature of the syllabus and objectives to achieve in each session. The lectures on different topics (demonstration and discussion), either by the teacher or by students, is combined with the defined evaluation methodology to achieve the learning objectives;
2) Complementary skills such as teamwork, written and verbal communication will also be explored in the context of this course;
The evaluation process was designed to assess the extent and level of acquired and developed skills.

3.3.9. Bibliografia principal:

- John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 2nd edition. Amsterdam ; Boston: Syngress, 2014.
- B. Carrier, File System Forensic Analysis, 1st edition. Boston, Mass. ; London: Addison-Wesley Professional, 2005.
- Cory Altheide and Harlan Carvey, Digital Forensics with Open Source Tools, 1st edition. Burlington, MA: Syngress, 2011.
- Brett Shavers, Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, 1st edition. Waltham, MA: Syngress, 2013.

Mapa IV - Administração Segura de Sistemas Informáticos

3.3.1. Unidade curricular:
Administração Segura de Sistemas Informáticos

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

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
No término desta unidade curricular, o estudante deverá ser capaz de:

Objetivos Gerais
C1 - Compreender o funcionamento dos principais sistemas e serviços da responsabilidade do administrador de sistemas
C2 - Aplicar boas práticas de administração de sistemas visando promover a segurança dos serviços e sistemas
C3 - Compreender as principais implicações de falhas de segurança em serviços e sistemas da organização

Objetivos Específicos
C4 - Conhecer a terminologia própria à administração segura de sistemas
C5 - Configurar e manter sistemas de diretoria e credenciais para acesso a sistemas e serviços
C6 - Definir metodologias e gerir de forma segura mecanismos de salvaguarda de dados
C7 - Configurar e gerir de forma segura os serviços de ficheiros
C8 - Conhecimento das metodologias e práticas para validação da integridade de sistemas de ficheiros
C9 - Configurar e gerir de forma segura os serviços de WEB
C10 - Configurar e gerir de forma segura os serviços de correio eletrónico

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
At the end of this course, the student should be able to:

Generic goals:
C1 - Understand the inner working of the main systems and services that are the responsibility of the system administrator
C2 - Apply the proper system administration practices to promote safety of services and systems
C3 - Understand the implications of security flaws in services and systems

Specific goals:
C4 - To get acquainted with the proper terminology regarding safe management systems
C5 - Setup and maintain management systems and credentials for access to systems and services
C6 - Define methodologies and manage safely guard mechanisms and safeguard data
C7 - Setup and manage file services in a secure way
C8 - Knowledge of methodologies and practices to validate the integrity of files and file systems
C9 - Setup and manage securely WEB services
C10 - Setup and manage securely email services

3.3.5. Conteúdos programáticos:
1 - Conceitos básicos de administração de sistemas
- Deveres e direitos
- Ética

- Documentação
- Pontos centrais de falhas
2 - Noção de serviço
- Definição de serviço
- Instalação e configuração de serviços
- Manutenção
- Atualizações de segurança
3 - Gestão de utilizadores
- Direito e deveres
- Interação com utilizadores
4 - Serviços de autenticação e de diretoria
- Conceitos gerais
- Credenciais de acesso
- LDAP, DAP e Active Directory
5 - Armazenamento e gestão segura de ficheiros
- Integridade de ficheiros
- Sistemas de ficheiros (locais, distribuídos)
- Salvaguarda segura de ficheiros
- Eliminação segura de ficheiros
- Ficheiros na nuvem
6 - Serviços HTTP e HTTPS
- Protocolo HTTP/1.x e HTTP/2
- Vulnerabilidades do HTTP/1.x e HTTP/2
- Segurança dos serviços HTTP e HTTPS
7 - Serviços de Correio Eletrónico
- Funcionamento geral
- Vulnerabilidades
- SPF, DKIM

3.3.5. Syllabus:

1 - Basic concepts of sysadmin
- Duties and rights
- Ethics
-Documenting
- Central fault points
2 - Notion of service
- Definition of Service
- Installation and configuration of services
- Maintaining services
- Management of security updates
3 - User Management
- Rights and duties
- Interacting with users
4 - Authentication Services and board
- General Concepts
- Management of access credentials
- LDAP, DAP and Active Directory systems
5 - Storage and secure management of files
- File integrity validation mechanisms
- File systems (local, distributed)

- Secure save files (backups, data transfer)
- Safe disposal of content stored in persistent memory devices
- File storage services in the cloud
6 - HTTP and HTTPS services
- HTTP / 1.x and HTTP / 2 protocols
- Key vulnerabilities of the HTTP / 1.x and HTTP/2 protocols
- Security mechanisms and methodologies of HTTP and HTTPS services
7 - e-mail Services
- Main operations
- Key vulnerabilities
- SPF and DKIM mechanisms

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Os conteúdos programáticos lecionados contribuem para as competências gerais estabelecidas para a UC da seguinte forma:

1 - Conceitos básicos de administração de sistemas (C1, C2, C3, C4)
- Deveres e direitos (C1,C2)
- Ética (C1)
- Documentação (C1,C2)
- Pontos centrais de falhas (C3)
2 – Noção de serviço (C2,C3,C4)
- Definição de serviço (C4)
- Instalação e configuração de serviços (C2,C4)
- Manutenção de serviços (C2,C4)
- Gestão das atualizações de segurança (C2,C3,C4)
3 – Gestão de utilizadores (C2,C3,C4,C5)
- Direito e deveres dos utilizadores (C2,C3,C4)
- Interação com os utilizadores (C2)
4 - Serviços de autenticação e de diretoria (C4,C5,C6)
- Conceitos gerais (C4,C5)
- Gestão de credenciais de acesso (C4,C5)
- Sistemas LDAP, DAP e Active Directory (C5,C6)
5 - Armazenamento e gestão segura de ficheiros (C4, C6, C7, C8)
- Mecanismos de validação da integridade de ficheiros (C4, C6, C8)
- Sistemas de ficheiros (locais, distribuídos) (C6, C7, C8)
- Salvaguarda segura de ficheiros (backups; transporte de dados) (C6, C7, C8)
- Eliminação segura de conteúdo armazenado em dispositivos de memória persistente (C6, C7)
- Serviços de armazenamento de ficheiros na nuvem (C6, C8)
6 - Serviços HTTP e HTTPS (C4, C9)
- Protocolo HTTP/1.x e HTTP/2 (C4, C9)
- Principais vulnerabilidades dos protocolos HTTP/1.x e HTTP/2 (C4, C9)
- Mecanismos e metodologias de segurança dos serviços HTTP e HTTPS (C4, C9)
7 - Serviços de Correio Eletrónico (C4, C10)
- Funcionamento geral (C10)
- Principais vulnerabilidades (C10)
- Mecanismos SPF, DKIM (C4,C10)

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

1 - Basic concepts of sysadmin (C1, C2, C3, C4)
- Duties and rights of sysadmin (C1, C2)
- Ethics of sysadmin(C1)
- Documenting in system administration (C1, C2)
- Central fault points (C3)
2 - Notion of service (C2, C3, C4)
- Definition of Service (C4)
- Installation and configuration of services (C2, C4)
- Maintaining services (C2, C4)
- Management of security updates (C2, C3, C4)
3 - User Management (C2, C3, C4, C5)
- Rights and duties of users (C2, C3, C4)
- Interacting with users (C2)
4 - Authentication Services and board (C4, C5, C6)
- General Concepts (C4, C5)
- Management of access credentials (C4, C5)
- LDAP, DAP and Active Directory systems (C5, C6)
5 - Storage and secure management of files (C4, C6, C7, C8)
- File integrity validation mechanisms (C4, C6, C8)
- File systems (local, distributed) (C6, C7, C8)
- Secure save files (backups, data transfer) (C6, C7, C8)
- Safe disposal of content stored in persistent memory devices (C6, C7)
- File storage services in the cloud (C6, C8)
6 - HTTP and HTTPS services (C4, C9)
- HTTP / 1.x and HTTP / 2 protocols (C4 -C9)
- Key vulnerabilities of the HTTP / 1.x and HTTP/2 protocols (C4, C9)
- Security mechanisms and methodologies of HTTP and HTTPS services (C4, C9)
7 - e-mail Services (C4, C10)
- Main operations (C10)
- Key vulnerabilities (C10)
- SPF and DKIM mechanisms (C4,C10)

3.3.7. Metodologias de ensino (avaliação incluída):

Ensino presencial e teórico-prático - os conceitos mais relevantes serão apresentados nas aulas com recurso a casos práticos.

Estudo autónomo - leitura da bibliografia recomendada e resolução de exercícios

Avaliação
i) Periódica
1 prova teórica
1 prova prática
1 trabalho de pesquisa bibliográfica (a realizar fora das aulas)

Classificação final: prova teórica = 40%; prova prática = 40%; trabalho de pesquisa bibliográfica = 20%

ii) Exame (Normal, Recurso e Especial)
1 teste global com duas componentes: teórico = 40%, prático = 60%

3.3.7. Teaching methodologies (including assessment):

Presential, in classroom and theoretical-practice (TP) - contents are presented with practical scenarios in the classroom.
Autonomous - complementar and recommended readings, with exercises.

Evaluation
i) Periodical evaluation:
1 theoretical test
1 practical assessment
1 bibliographical research work

Final evaluation: theoretical= 40%, practical = 40% and bibliographical research work = 20%

ii) Final assessment - Exam
1 global assessment with two components: theoretical = 40% and practical = 60%

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Presencial
Ensino teórico-prático - C1, C3, C4, C5, C6, C7, C8, C9, C10

Estudo autónomo
Leitura da bibliografia recomendada; resolução de exercícios - C2, C7

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
Presential, in classroom:
Theoretical-practice (TP) - C1, C3, C4, C5, C6, C7, C8, C9, C10

Autonomous study:
Recommended and complementary readings, with exercises - C2, C7

3.3.9. Bibliografia principal:
- Limoncelli, T., Hogan, C. J., & Chalup, S. R. (2016). The practice of system and network administration. 3rd edition. Pearson Education.
- Lee Brotherston, Amanda Berlin (2016). Defensive Security Handbook - Best Practices for Securing Infrastructure. O'Reilly Media.
- Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley (2011). UNIX and Linux System Administration Handbook. 4th edition. Pearson Education.
- Shinder, T. W., Diogenes, Y., & Shinder, D. L. (2013). Windows server 2012 security from end to edge and beyond: Architecting, designing, planning, and deploying windows server 2012 security solutions. Newnes.
- Documentação disponibilizada pelo docente.

Mapa IV - Projeto de Segurança I

3.3.1. Unidade curricular:
Projeto de Segurança I

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Carlos Manuel da Silva Rabadão

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

<sem resposta>

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

C1. Desenvolvimento de competências para compreender, enquadrar e formular problemas de Cibersegurança.
C2. Desenvolvimento de competências para a aplicação de métodos, tecnologias e normas vocacionadas para a prevenção, detecção, recuperação e reporte de incidentes em Cibersegurança.
C3. Desenvolvimento de competências para a adoção de métodos, tecnologias, normas e legislação adequados à investigação de cibercrimes.
C4. Desenvolvimento de competências para a resolução de problemas novos, de forma autónoma.
C5. Desenvolvimento de competências para organizar, documentar e produzir relatórios nas áreas da Cibersegurança e Computação Forense.
C6. Desenvolvimento de competências para apresentar e defender publicamente estudos em Cibersegurança e Computação Forense, destinados a públicos diversos (gestores, juristas, forças policiais).
C7. Desenvolvimento de competências de iniciação à investigação científica.

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

C1. Developing skills to understand, contextualize and formulate cybersecurity problems.
C2. Developing skills for the application of methods, technologies and standards aimed for the prevention, detection, recovery, and reporting cybersecurity incidents.
C3. Developing skills for the adoption of methods, technologies, standards and legislation appropriate to the investigation of cybercrimes.
C4. Developing skills to solve new problems autonomously.
C5. Developing skills to organize, document and produce reports in the areas of Cybersecurity and Computer Forensics.
C6. Developing skills to present and defend publicly studies in Cybersecurity and Computer Forensics, aimed at different audiences (managers, lawyers, police).
C7. Development of initiation skills for scientific research.

3.3.5. Conteúdos programáticos:

A unidade curricular não possui conteúdos previamente definidos, dependendo estes dos projetos a ser realizados em grupos de dois estudantes.

3.3.5. Syllabus:

The course has no pre-defined content, the content depends on the projects to be carried out in groups of two student.

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

Nesta unidade curricular é atribuído ao grupo o enunciado de um problema de média complexidade, cuja motivação pode partir do docente, dos estudantes ou do ambiente empresarial, implicando uma abordagem multidisciplinar centrada na Cibersegurança e/ou Computação Forense (C1, C2, C3, C4, C5, C6, C7).

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

In this course groups of two students are assigned medium complexity problems, whose motivation can be originated on teachers, students or the business environment, involving a multidisciplinary approach focused on Cybersecurity and/or Computer Forensics (C1, C2, C3, C4 , C5, C6, C7).

3.3.7. Metodologias de ensino (avaliação incluída):

Sessões de orientação em pequenos grupos para conduzir o processo de aprendizagem, o trabalho de grupo e individual dos estudantes.
Leitura da bibliografia indicada e realização de experimentação relacionada com os trabalhos dos grupos.
Consulta do material disponibilizado na plataforma de e-learning do curso.
A avaliação desta unidade curricular é realizada em três momentos, com peso de 1/3 (33%) cada. Dois momentos de avaliação de progresso e um momento de avaliação final do trabalho.

3.3.7. Teaching methodologies (including assessment):

Orientation sessions in small groups to conduct the process of learning, group work and individual progress.
Reading the bibliography and conducting experiments related to group work.
Consultation of the material available on the e-learning course platform.
The evaluation of this course is held in three stages, with a weight of 1/3 (33%) each. Two moments of progress evaluation and a final evaluation of the work.

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Sessões de orientação em pequenos grupos para conduzir o processo de aprendizagem, o trabalho de grupo e individual dos estudantes. (C1, C2, C3, C4, C5, C6, C7)
Leitura da bibliografia indicada e realização de experimentação relacionada com os trabalhos dos grupos. (C4, C5, C7)
Consulta do material disponibilizado na plataforma de e-learning do curso. (C4, C5, C7)

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
Orientation sessions in small groups to conduct the process of learning, group work and individual progress. (C1, C2, C3, C4, C5, C6, C7)
Reading the bibliography and conducting experiments related to group work. (C4, C5, C7)
Consultation of the material available on the e-learning course platform. (C4, C5, C7)

3.3.9. Bibliografia principal:
A bibliografia é definida individualmente de acordo com as especificidades de cada projeto.

The bibliography is defined individually according to the specificities of each project.

Mapa IV - Laboratório de Testes de Penetração

3.3.1. Unidade curricular:
Laboratório de Testes de Penetração

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Patrício Rodrigues Domingues, 15h

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
Carlos Manuel Gonçalves Antunes, 15h

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
A Segurança Ofensiva (Ethical Hacking) testa as vulnerabilidades dos sistemas que pretende proteger. Nesta UC utiliza-se a segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas, redes e aplicações. A UC procura dar uma visão global da exploração e mitigação de falhas. São profusamente realçadas as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração.

O1.Conhecer restrições éticas e legais do ethical hacking
O2.Realizar testes de penetração
O3.Identificar atividade maliciosa na rede
O4.Implementar aplicações úteis na exploração de falhas
O5.Identificar medidas para mitigar ataques de engenharia social
O6.Mitigar falhas de segurança
O7.Identificar e resolver problemas nas aplicações e serviços web
O8.Determinar falhas de segurança em redes

O9. Reforçar competências de planeamento/implementação de sistemas IDS/IPS
O10. Reforçar capacidades de planeamento/implementação de serviços de autenticação e controlo de acesso

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

Offensive security (here in the context of Ethical Hacking) tests for vulnerabilities of systems that it aims to protect. In this curricular unit, offensive security is used to assess and mitigate vulnerabilities in systems, networks and applications. It aims to provide a global overview of the exploitation and mitigation of security failures. Great emphasis is given to legal and ethical issues regarding ethical hacking.

O1. Learn the legal and ethical constraints of ethical hacking
O2. Perform penetration tests
O3. Identify malicious activity on the network
O4. Develop applications for the exploitation of failures
O5. Identify measures to mitigate social engineering-based attacks
O6. Mitigate security failures
O7. Identify and solve problems in applications and web services
O8. Detect security failures of networks
O9. Strengthen competencies for planning/implementing IDS/IPS systems
O10. Strengthen capabilities for planning/implementing authentication and access control services

3.3.5. Conteúdos programáticos:

C1. Introdução aos conceitos do Ethical hacking
C2. Tipos de ameaças e ataques a redes
C3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN), 802.16 (wireless WAN)
C4. Fragilidades protocolares dos sistemas de comunicações
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes
C6. Metodologias para testes de penetração
C7. Caracterização e implementação de ataques contra redes e sistemas
C8. Planeamento de soluções de comunicação segura em redes e sistemas
C9. Identificação e deteção de vulnerabilidades nos sistemas

3.3.5. Syllabus:

C1. Introduction to the main concepts of Ethical hacking
C2. Types of menaces and attacks to networks
C3. Security protocols and algorithms for networks 802.11 (Wireless LAN), 802.15 (wireless PAN), 802.16 (wireless WAN)
C4. Protocol weaknesses of communication systems
C5. Technologies for confidentiality, privacy and availability in networks
C6. Methodologies for penetration tests
C7. Characterization and implementation of attacks against networks and systems
C8. Planning of secure communications for networks and systems
C9. Identification and detection of vulnerabilities in systems

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

C1. Introdução aos conceitos do Ethical hacking (O1, O2)
C2. Tipos de ameaças e ataques a redes (O3, O5)
C3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN) e 802.16 (wireless WAN) (O5, O6)
C4. Fragilidades protocolares dos sistemas de comunicações (O4)
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes (O3,O9,O10)
C6. Metodologias para testes de penetração (O7, O8)

C7. Caracterização e implementação de ataques contra redes (O3, O8)
C8. Planeamento de soluções de comunicação segura em redes e sistemas (O8,O9)
C9. Identificação e deteção de vulnerabilidades nos sistemas (O3,O8,O9)

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
C1. Introduction to the main concepts of Ethical hacking (O1,O2)
C2. Types of menaces and attacks to networks (O3,O5)
C3. Security protocols and algorithms for networks 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN) (O5,O6)
C4. Protocol weaknesses of communication systems (O4)
C5. Technologies for confidentiality, privacy and availability in networks (O3,O9,O10)
C6. Methodologies for penetration tests (O7,O8)
C7. Characterization and implementation of attacks against networks and systems (O3,O8)
C8. Planning of secure communications for networks and systems (O8,O9)
C9. Identification and detection of vulnerabilities in systems (O3,O8,O9)

3.3.7. Metodologias de ensino (avaliação incluída):
EP.1.Teórico-prático: i) Exposição pelo professor dos conteúdos programáticos e respetiva assimilação por parte dos estudantes

EP.2. i) Consolidação dos conhecimentos teórico-práticos, através da especificação e execução de procedimentos de ethical hacking associados a exemplos de serviços e sistemas; ii) Realização de projeto laboratorial, que corresponde à consolidação dos conhecimentos adquiridos nas fases anteriores

3.3.7. Teaching methodologies (including assessment):
EP.1.theoretical/practical: i) Presentation by the teacher of the contents of the course and respective assimilation by students

EP.2. i) Consolidation of theoretical and practical knowledges through the specification and implementation of ethical hacking procedures associated with examples of services and systems; ii) Realization of a laboratory project, to consolidate knowledge acquired along previous stages

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
A metodologia de ensino teórico-prático baseia-se na transmissão de conhecimentos sobre a segurança ao nível da segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas ubíquos, redes e aplicações. Pretende-se dar uma visão global do processo de exploração e mitigação de falhas, tendo sempre em linha de conta as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração. Permite desenvolver nos estudantes as competências (O1,O2, O3).

A metodologia utilizada na componente laboratorial incide, numa primeira fase, na consolidação dos conhecimentos transmitidos na componente teórico-prática atraves da realização de trabalhos laboratoriais (O1, O2, O3) e, numa fase posterior, na realização de um projeto prático, e que contempla as seguintes fases: a) estudo do cenário proposto, b) identificação de falhas e vulnerabilidades do cenário, c) seleção de mecanismos adequados à exploração de vulnerabilidades, d) realização de testes de penetração, e) mitigação de falhas detetadas e e) escrita de relatório e f) apresentação do projeto realizado. Isto permite desenvolver nos estudantes os objetivos (O4, O5, O6, O7, O8, O9, O10).

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
The methodology of theoretical/practical teaching is based on lessons regarding security at the offensive level in order to assess and mitigate vulnerabilities in ubiquitous systems, networks and applications. The goal is to provide an overview of the main processes for exploring and mitigate security failures, keeping in mind the restrictions, ethical and legal directives of the activities associated to a penetration test. The goal is to reach objectives O1, O2 and O3.

The methodology adopted for the lab part aims to strengthen the knowledge taught in the theoretical-practical lessons. This is achieved through solving lab exercises (O1,O2,O3), and in a second stage, through the realization of a practical project that comprises the following stages: a) study of the proposed scenario; b) detection of failures and vulnerabilities of the scenario; c) selection of the proper mechanisms to exploit the failures; d) performing penetration tests; e) writing of the report and f) presentation of developed project. This strengthens the objectives O4,O5,O6,O7,O8,O9,O10.

3.3.9. Bibliografia principal:

- Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012

- Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; ISBN: 978-0071832380; McGraw-Hill Education; 4 ed., 2015

- Documentação disponibilizada pelo docente.

Mapa IV - Gestão e Análise de Relatórios de Segurança

3.3.1. Unidade curricular:

Gestão e Análise de Relatórios de Segurança

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

Maria Beatriz Guerra Piedade, 15h

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

José Vítor Martins Ramos, 15h

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

As organizações são confrontadas com um enorme volume de dados provenientes de equipamentos de rede, assumindo os sistemas SIEM (Security Information and Event Management) uma importância fulcral na gestão e análise de eventos (incidentes) de segurança.

C1. Compreensão da importância da gestão e análise de eventos de segurança
C2. Conhecimento da arquitetura dos sistemas SIEM
C3. Conhecimento aprofundado dos componentes de um sistema SIEM (recolha de logs, processamento, armazenamento, análise, relatórios e alertas)
C4. Identificação dos desafios, em termos de processamento, análise de dados e identificação de padrões em tempo-real
C5. Configuração e gestão dos principais componentes de um sistema SIEM
C6. Utilização de sistemas SIEM para a resolução de problemas reais de segurança
C7. Capacidade de pesquisar informação em diferentes meios e formatos
C8. Capacidade de desenvolver cenários práticos de implementação de soluções SIEM
C9. Capacidade de realizar projetos em equipa

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

Organizations are confronted with a huge volume of data from network equipment, so that the SIEM (Security Information and Event Management) systems are more important than ever in the management and analysis of security events (incidents).

C1. Understand the importance of management and analysis of security events
C2. Understand the architecture of SIEM systems
C3. Understand in depth the modules of a SIEM system (collection of logs, processing, storage, analysis, reporting and alerts)
C4. Identification of challenges for different scenarios in terms of processing, real-time data analysis and pattern recognition
C5. Configuration and management of the main components of a SIEM system
C6. Use SIEM systems to solve real security problems
C7. The ability to search information in different media and formats

C8. The ability to develop practical deployment scenarios of SIEM solutions
C9. The ability to develop projects in a team

3.3.5. Conteúdos programáticos:

1. Gestão de eventos de segurança
2. Arquitetura dos sistemas SIEM
3. Recolha de dados de eventos de segurança (logs)
4. Processamento dos dados
5. Análise dos dados e identificação de padrões em tempo-real
6. Relatórios de segurança e alertas (dashboards)
7. Sistemas SIEM open-source (OSSEC, OSSIM, Graylog, …)
8. Cenários de testes reais
9. Sistemas SIEM em ambientes Big Data
10. Analítica de segurança

3.3.5. Syllabus:

1. Management of security events
2. Architecture of SIEM systems
3. Collection of security event data (logs)
4. Data processing
5. Real-time data analysis and pattern recognition
6. Security reports and alerts (dashboards)
7. Open-source SIEM systems (OSSEC, OSSIM, Graylog, …)
8. Test scenarios
9. SIEM systems and Big Data
10. Security Analytics

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

1. Gestão de eventos de segurança (C1, C2, C7)
2. Arquitetura dos sistemas SIEM (C2, C3, C7)
3. Recolha de dados de eventos de segurança (logs) (C3, C4, C5, C7)
4. Processamento de dados (C3, C4, C5, C7)
5. Análise de dados e identificação de padrões em tempo-real (C3, C4, C5, C7)
6. Relatórios de segurança e alertas (dashboards) (C3, C4, C5, C7)
7. Sistemas SIEM open-source (OSSEC, OSSIM, Graylog, …) (C5, C6, C7)
8. Cenários de testes reais (C4, C6, C8)
9. Sistemas SIEM em ambientes Big Data (C1, C2, C7)
10. Analítica de segurança (C1, C7)

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

1. Management of security events (C1, C2, C7)
2. Architecture of SIEM systems (C2, C3, C7)
3. Collection of security event data (logs) (C3, C4, C5, C7)
4. Data processing (C3, C4, C5, C7)
5. Real-time data analysis and pattern recognition (C3, C4, C5, C7)
6. Security reports and alerts (dashboards) (C3, C4, C5, C7)
7. Open-source SIEM systems (OSSEC, OSSIM, Graylog, …) (C5, C6, C7)
8. Test scenarios (C4, C6, C8)

9. SIEM systems and Big Data (C1, C2, C7)
10. Security Analytics (C1, C7)

3.3.7. Metodologias de ensino (avaliação incluída):
Ensino Presencial
Teórico-Prático (TP): exposição e compreensão dos conteúdos programáticos com casos práticos.

Aprendizagem Autónoma
Estudo: Leitura de apontamentos da unidade curricular e bibliografia.
Projeto: Realização de um projeto em equipa por forma a promover a organização do trabalho e o desenvolvimento de capacidades de autonomia, iniciativa e análise crítica.

Avaliação
Avaliação Periódica
Prova Escrita (PE)
Projeto
Classificação Final: CF = 50%PE + 50%Projeto

Avaliação Final
Prova Escrita (PE)
Classificação Final: CF = 100%PE

3.3.7. Teaching methodologies (including assessment):
Contact Teaching
Theoretical and Practical (TP): exposition and understanding of the theoretical concepts based on case studies.

Autonomous Learning
Study: Reading notes and recommended books.
Project: Development of a team project in order to promote planning and organization and also to develop autonomous ability, initiative and critical analysis.

Assessment
Periodic Evaluation
Written Test (WT)
Project
Final Grade: FG = 50%WT + 50%Project

Final Evaluation
Written Test (WT)
Final Grade: FG = 100%WT

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Ensino Presencial
Teórico-prático: C1, C2, C3, C4, C5, C6

Aprendizagem Autónoma
Estudo autónomo: C1, C2, C3, C7
Projeto: C4, C6, C8, C9

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

Contact Teaching
Theoretical and practical: C1, C2, C3, C4, C5, C6

Autonomous Learning
Study: C1, C2, C3, C7
Project: C4, C6, C8, C9

3.3.9. Bibliografia principal:

- David R. Miller et al., Security Information and Event Management (SIEM) Implementation, ISBN-13: 978-0071701099, 2010
- Anton A. Chuvakin and Kevin J. Schmidt, Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, ISBN-13: 978-1597496353, 2012
- Michael S. Collins, Network Security Through Data Analysis: Building Situational Awareness, ISBN-13: 978-1449357900, 2014
- Jay Jacobs and Bob Rudis, Data-Driven Security: Analysis, Visualization and Dashboards, ISBN-13: 978-1118793725, 2014
- Mark Talabis et al, Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data, ISBN-13: 978-0128002070, 2014
- Kelly M. Kavanagh, Oliver Rochford, Magic Quadrant for Security Information and Event Management, Gartner, 2015
- SIEM OSSEC, http://ossec.github.io/, setembro 2016
- SIEM OSSIM, https://www.alienvault.com/products/ossim, setembro 2016
- SIEM Graylog, https://www.graylog.org/, setembro 2016

Mapa IV - Tratamento de Incidentes Informáticos

3.3.1. Unidade curricular:
Tratamento de Incidentes Informáticos

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Carlos Manuel da Silva Rabadão

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
C1.Compreender o processo de resposta a incidentes
C2.Construir e prover uma equipa de "incident response" (IR) para o sucesso
C3.Melhorar uma infraestrutura ou organização, no sentido de facilitar o processo de IR
C4.Liderar uma investigação ou reparação de IR
C5.Recolher e tratar evidências
C6.Analisar evidências nos sistemas operativos
C7.Resolver brechas e incidentes detetados
C8.Capacidade para escrever de forma adequada relatórios de IR
C9.Capacidade para pesquisar informação em diferentes meios e formatos e de proceder à sua utilização de forma eficaz
C10.Capacidade de desenvolver cenários práticos IR
C11.Capacidade de realizar projetos em equipa

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

C1.Understand the Incident Response (IR) process
C2.Build and equip an IR team for success
C3.Enhance an infrastructure or organization to facilitate the IR process
C4.Lead an investigation or remediation effort
C5.Collect and handle evidences
C6.Analyse of OS evidences
C7.Remediate detected breaches and incidents
C8.Write IR reports
C9.Research information in different sources and formats and it effective application
C10.Development of practical scenarios of IR
C11.Ability to carry out projects in teams

3.3.5. Conteúdos programáticos:
1. Violação de dados e de respostas a incidentes
2. Planeamento e desenvolvimento do processo de resposta a incidentes de segurança informática
3. Deteção e caracterização de incidentes
4. Recolha e preservação da informação
5. Análise dos dados: metodologias e investigação
6. Definição e aplicação de medidas corretivas

3.3.5. Syllabus:
1. Data breaches and incident response fundamentals
2. Planning and development of computer security incident response process
3. Incident detection and characterization
4. Collection and preservation of information
5. Data analysis: methodologies and investigation
6. Remediation

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
1. Violação de dados e de respostas a incidentes (C1)
2. Planeamento e desenvolvimento do processo de resposta a incidentes de segurança informática (C2, C3, C4)
3. Deteção e caracterização de incidentes (C3, C4, C8, C10, C11)
4. Recolha e preservação da informação (C4,C5, C8, C10, C11)
5. Análise dos dados: metodologias e investigação (C4,C6, C8, C10, C11)
6. Definição e aplicação de medidas corretivas (C4, C7, C8, C10, C11)

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
1. Data breaches and incident response fundamentals (C1)
2. Planning and development of computer security incident response process (C2, C3, C4)
3. Incident detection and characterization (C3, C4, C8, C10, C11)
4. Collection and preservation of information (C4, C5, C8, C10, C11)
5. Data analysis: methodologies and investigation (C4, C6, C8, C10, C11)
6. Remediation (C4, C7, C8, C10, C11)

3.3.7. Metodologias de ensino (avaliação incluída):
Presencial
Teórico-Prático (TP): exposição e compreensão dos conteúdos programáticos relacionados com os capítulos 1 a 6, e sua consolidação com discussão de casos práticos.

Autónoma
Estudo autónomo: Leitura de materiais da unidade curricular e bibliografia.
Projeto: Realização de um projeto em equipa por forma a promover a organização do trabalho e o desenvolvimento de capacidades de autonomia, iniciativa e análise crítica.

3.3.7. Teaching methodologies (including assessment):
Contact teaching
Theoretical/practical (TP): Teacher presentation of the syllabus relating to chapters 1 to 6 and its assimilation by the students. Consolidation of theoretical knowledge thought out the discussion of practical cases.

Autonomous learning
Autonomous study: reading of course materials and recommended bibliography.
Project implementation in order to promote the organization of team work and the development of autonomy, initiative and critical analysis skills.

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Ensino Presencial
Teórico-prático: C1, C2, C3, C4, C5, C6, C7
Aprendizagem Autónoma
Estudo autónomo: C1, C2, C3, C4, C5, C6, C7
Projeto: C3, C7, C8, C9, C10, C11

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
Contact teaching
Theoretical/practical (TP): C1, C2, C3, C4, C5, C6, C7
Autonomous learning
Autonomous study: C1, C2, C3, C4, C5, C6, C7
Project: C3, C7, C8, C9, C10, C11

3.3.9. Bibliografia principal:
NIST Special Publication 800-61 - Rev.2. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone. NIST, 2012. http://dx.doi.org/10.6028/NIST.SP.800-61r2

NIST Special Publication 800-83 - Rev.1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. Murugiah Souppaya; Karen Scarfone. NIST, 2013. http://dx.doi.org/10.6028/NIST.SP.800-83r1

A step-by-step approach on how to set up a CSIRT. Henk Bronk, Marco Thorbruegge and Mehis Hakkaja. ENISA, 2006.
Incident response and computer forensics, 2nd edition, Jason T. Luttgens and Matthew Pepe. Mc Graw Hill Education, 3th edition, 2014. ISBN: 978-0-07-179868-6

Crafting the InfoSec Playbook: Security monitoring and incident response master plan, 1st edition. Jeff Bollinger, Brandon Enright & Matthew Valites. O'Reilly, 2015. ISBN: 978-1-491-94940-5

Mapa IV - Análise Forense Digital II

3.3.1. Unidade curricular:
Análise Forense Digital II

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

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta unidade curricular tem cariz laboratorial com o objetivo aplicar as técnicas, metodologias e ferramentas associados à análise forense de provas digitais em vários cenários práticos, nomeadamente computadores pessoais e dispositivos móveis. Os estudantes irão aplicar os conhecimentos adquiridos através da realização de vários trabalhos práticos.

Após a conclusão desta Unidade Curricular, o estudante deverá ser capaz de:
1- Recolher dados em suportes de armazenamento, redes de dados e memória volátil
2- Obter provas digitais nos backups em sistemas operativos pessoais
3- Obter evidencias digitais nas redes de dados
4- Obter provas digitais em sistemas operativos móveis
5- Criar e usar hashsets
6- Criar mapas de geolocalização
7- Correlacionar eventos provenientes de diversos meios ou dispositivos
8- Comunicar e reportar resultados de análise forense

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This course is laboratory-oriented in order to apply the techniques, methodologies and tools associated with the forensic analysis of digital evidences in a number of practical scenarios, including personal computers and mobile devices. Students will apply the knowledge acquired by developing several projects.

Upon completion of this course, the student will be able to:
1- Collect data on storage media, networks and volatile memory
2- Obtain digital evidence from backups on personal operating systems
3- Obtain digital evidence from data networks
4- Obtain digital evidence from mobile operating systems
5- Create and use hashsets
6- Create geolocation maps
7- Correlate events from several media or devices
8- Communicate and elaborate digital forensics reports

3.3.5. Conteúdos programáticos:
1. Partições, volumes e sistemas de ficheiros usados nos dispositivos móveis

2. Análise de redes de dados
endereços MAC, IPv4 e IPv6
geolocalização de IPs
2.1 Procedimentos
estudo da rede e recolha de tráfego
Filtros de pacotes
análise de logs
2.2 Limitações
segmentação, cifra, temporalidade e localização

anonimização de tráfego

3. Backups dos dispositivos móveis
3.1 Conceitos gerais
SO pessoais
Ficheiros plist
técnicas anti forense
Serviços de cloud

4. SO móveis
4.1 Procedimentos gerais
Aquisição de dados
Cartões SIM e de memória
4.2 Android
estruturas de dados
modelo segurança
4.3 iOS
estruturas de dados
modelo segurança
4.4 Windows Phone
estruturas de dados
modelo segurança

5. Casos de estudo
relatório forense digital

3.3.5. Syllabus:

1. Partitions, volumes and file systems on mobile devices

2. Computer networks analysis
MAC, IPv4 and IPv6 addresses
IPs geolocalization
2.1 Procedures
Network traffic collection and analysis
Packet filters
Logs analysis
2.2 Limitations
Segmentation, encryption, temporality and location
Traffic anonymisation

3. Backups from mobile devices
3.1 General concepts
Personal OS
Plist files
Anti-forensic techniques
Cloud services

4. Mobile OS
4.1 General concepts
Memory and SIM cards

4.2 Android
File system and data structures
Security model
4.3 iOS
File system and data structures
Security model
4.4 Windows Phone
File system and data structures
Security model

5. Study case
Digital forensics report

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Os tópico 1 a 4 visam dotar os estudantes de competências relacionadas com a recolha e obtenção de dados e de provas (objetivos de aprendizagem 1 a 6). Os objetivos de aprendizagem 2 a 4 são depois reforçados pelos tópicos 2 a 4. No tópico 4 detalham-se as particularidades dos principais SO móveis (objetivo de aprendizagem 4). Por último, o tópico 5, surge como a componente agregadora de competências que visa solidificar o objetivo de aprendizagem 8.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
Topics 1 to 4 aim to provide students with skills to collect and gather digital evidences (learning objectives 1 to 6). Learning objectives from 2 to 4 will be acquired by students in topics from 2 to 4. On topic 4 the peculiarities of the main mobile OS are detailed (learning objective 4). Finally, topic 5 arises as a skill aggregation component to empower and solidify the learning objective 8.

3.3.7. Metodologias de ensino (avaliação incluída):
A metodologia a adotar para a generalidade das aulas Teóricas será o método expositivo. Nas aulas Práticas será aplicado o método ativo onde os alunos desenvolverão guiões de exercícios, bem como um trabalho prático.

A avaliação dos estudantes será através de 1 teste escrito (tópico 1) e 1 trabalho prático de onde resultará um relatório (tópicos 2, 3 e 4) e por fim a apresentação e discussão do trabalho prático (tópico 5).

Nota final = 35% Teste escrito + 50% Trabalho prático + 15% Apresentação

3.3.7. Teaching methodologies (including assessment):
The methodology to adopt for most of the Theoretical classes is the expository method. In practical classes will be applied the active method, where students will develop exercises guidelines as well as a team project.

Students will be evaluated through one individual written tests (for topic 1) and 1 team project (for topics 2, 3 and 4) and, finally, the presentation and discussion of the project (topic 5).

Final grade = 35% Written test + 50% Team Project + 15% Presentation of a digital forensics report

3.3.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
As metodologias de ensino estão em coerência com os objetivos da unidade curricular dado que:
1) Os métodos de ensino utilizados, ajustam-se à natureza dos conteúdos programáticos e dos objetivos a atingir em cada sessão. A realização de exposições sobre as diferentes matérias (demonstração e discussão), quer por parte do docente, quer dos estudantes, conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos.

2) Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC.
O regime de avaliação foi concebido para avaliar a extensão e o nível de aquisição das competências a desenvolver.

3.3.8. Evidence of the teaching methodologies coherence with the curricular unit's intended learning outcomes:
The teaching methodologies are consistent with the objectives of the course given that:
1) The used teaching methods adjust to the nature of the syllabus and objectives to achieve in each session. The lectures on different topics (demonstration and discussion), either by the teacher or by students, is combined with the defined evaluation methodology to achieve the learning objectives;
2) Complementary skills such as teamwork, written and verbal communication will also be explored in the context of this course;
The evaluation process was designed to assess the extent and level of acquired and developed skills.

3.3.9. Bibliografia principal:
- R. Tamma and D. Tindall, Learning Android Forensics. Packt Publishing - ebooks Account, 2015.
- M. Epifani and P. Stirparo, Learning iOS Forensics. Packt Publishing - ebooks Account, 2015.
- Brett Shavers, Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects, 1st edition. Waltham, MA: Syngress, 2013.

Mapa IV - Projeto de Segurança II

3.3.1. Unidade curricular:
Projeto de Segurança II

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

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
<sem resposta>

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
C1 - Desenvolver e implementar um trabalho prático que integre os tópicos abordados nas UC do 2ºsemestre.
C2 - Produzir documentação técnica sobre as decisões tomadas no decorrer do trabalho e sobre os resultados obtidos.
C3 - Produzir um relatório com a proposta de tese a realizar durante os 3º e 4º semestres do curso.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
C1 - To deploy and develop a lab project which should include the set of topics studied in the 2nd semester.
C2 - To produce technical documentation related with the decisions made under the development of the work and also about the results obtained.
C3 - To produce a thesis proposal of the research or internship to be developed in the 3rd and 4th semester of the course.

3.3.5. Conteúdos programáticos:
Os estudantes realizarão um trabalho prático de entre uma lista de trabalhos propostos pelos docentes do curso. O trabalho deverá conter um levantamento do estado da arte numa determinada área, bem como uma demonstração prática de um conceito, uma aplicação ou uma tecnologia.

3.3.5. Syllabus:

Students will develop a lab project among a list of works proposed by the professors. The work should have the state of the art in the area, as well as a demonstration of a pilot application or technology.

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

A diversidade de unidades curriculares lecionadas implicará necessariamente trabalhos práticos multidisciplinares e adequados à área de interesse de cada aluno
A organização das UC implicará que a realização deste projeto preceda o início da realização da dissertação/estágio/projeto do curso de mestrado. O resultado final desta UC será a apresentação de resultados preliminares e do estado da arte do trabalho que o aluno pretende desenvolver no âmbito da dissertação/estágio/projeto.

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

Diversity of the course units previously lectured will promote the setup of multidisciplinary and in line with students' research interests and expectations. This course unit appears before the beginning of dissertation/internship/project and its main achievement is the presentation, by the student, of the state of the art and preliminary results of the work he/she aims to develop in dissertation/internship/project.

3.3.7. Metodologias de ensino (avaliação incluída):

Acompanhamento individual dos estudantes no planeamento do trabalho, na recolha e análise da informação relevante, na execução do trabalho e no desenvolvimento de capacidade crítica.
Desenvolvimento de trabalho autónomo do estudante em laboratório de investigação.

Avaliação:
- Relatório sobre o trabalho de pesquisa e desenvolvimento - 75%
- Apresentação - 25%

3.3.7. Teaching methodologies (including assessment):

Supervision of individual students in planning the work, collecting and analysing relevant information, in performing the work and in developing of critical skills.
Development of independent work and on-site research lab training.

Assessment:
- R&D report - 75%
- Oral presentation - 25%

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

As metodologias de ensino usadas que contribuem para as competências gerais estabelecidas para a UC baseiam-se na orientação tutorial em ambiente académico e de investigação.

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

The teaching methods contribute to the general skills set for the subject and are based on academic and research supervision.

3.3.9. Bibliografia principal:

Bigliografia a ser definida e indicada para cada projeto.
Bibliography to be defined for each project.

Mapa IV - Projeto

3.3.1. Unidade curricular:

Projeto

3.3.2. Docente responsável (preencher o nome completo) e respetivas horas de contacto na unidade curricular:
Mário João Gonçalves Antunes, 10h

3.3.3. Outros docentes e respetivas horas de contacto na unidade curricular:
Carlos Manuel Silva Rabadão, 10h
Patrício Rodrigues Domingues, 10h
Miguel Monteiro Sousa Frade, 10h
Paulo Manuel Gonçalves Oliveira Valente da Cruz, 10h
Maria Beatriz Guerra Piedade, 10h

3.3.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
C1. Capacidade de sintetizar, otimizar e propor soluções inovadoras para problemas e situações novas, relacionadas com as várias áreas de interesse no âmbito da cibersegurança e da computação forense.
C2. Capacidade de conceber e demonstrar soluções inovadoras no âmbito das áreas de interesse do curso.
C3. Capacidade para integrar os conhecimentos adquiridos, lidar com questões complexas, desenvolver soluções ou emitir juízos em situações de informação limitada ou incompleta, incluindo reflexões sobre as implicações e responsabilidades éticas e sociais que resultem dessas soluções e desses juízos ou os condicionem;
C4. Capacidade de identificar as necessidades inerentes à concretização de um determinado projeto, planear atividades no espaço e no tempo e verificar a execução dos objetivos;
C5. Capacidade de apresentar e justificar as suas opções quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
C1. Ability to synthesize, optimize and propose implementable solutions to problems in new and unfamiliar situations, related to the various areas of interest in Computer Engineering - Mobile Computing.
C2. Ability to design, implement and maintain solutions within the Engineering Computing - Mobile Computing area;
C3. Ability to integrate knowledge, handle complexity, develop solutions and make judgements in situations of limited or incomplete information, including reflections on the implications, ethical and social responsibilities resulting from those solutions or judgements;
C4. Ability to identify requirements, need resources and plan activities to achieve successfully tasks and research objectives;
C5. Ability to present and justify technical, organisational and scientific decisions to either specialists or non-specialists in a clear and unambiguous way.

3.3.5. Conteúdos programáticos:
Os estudantes desenvolverão um trabalho original nas áreas de cibersegurança e/ou computação forense.
O trabalho, cujo plano deverá ser aprovado pelo órgão científico estatutariamente competente, será maioritariamente realizado em ambiente académco e de investigação.

3.3.5. Syllabus:
Students will develop an original work in cybersecurity and/or digital forensics.
The work plan shall be approved by the school scientific body and shall be mostly done in academic and research environment.

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
A diversidade de unidades curriculares, constituindo um perfil curricular adequado à área de interesse de cada aluno, permite adquirir conhecimentos e capacidade de compreensão de forma a constituir uma base para desenvolvimentos originais na unidade curricular de dissertação/projeto.
A organização das unidades curriculares, assente na realização de trabalhos pelos alunos fora das aulas, assim como a realização de um trabalho de projeto de grande dimensão, permite que os alunos adquiram a capacidade para integrar conhecimentos.
A escrita e apresentação pública dos trabalhos realizados no âmbito das unidades curriculares, e principalmente a dissertação resultante da unidade curricular de

dissertação/projeto e a sua apresentação tem como objetivo garantir que os alunos sejam capazes de comunicar as conclusões e os conhecimentos e raciocínios a elas subjacentes quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

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

The diversity of course units, constituting a curriculum appropriate to the profile area of interest of each student, allows the ability to acquire knowledge and understanding to form a basis for original developments in the course of the research project
The conception of modules, based on the performance of work by students outside the classroom as well as carrying out a project work of large dimensions, allows students to acquire the ability to integrate knowledge.
The writing and public presentation of work carried out within the courses and the dissertation mainly resulting from the project and its presentation is designed to ensure that students are able to communicate the conclusions and the knowledge and reasoning underlying them either to experts or non-experts in a clear and unambiguous way.

3.3.7. Metodologias de ensino (avaliação incluída):

Acompanhamento individual dos estudantes no planeamento do trabalho, na recolha e análise da informação relevante, na execução do trabalho e no desenvolvimento de capacidade crítica, por um docente doutorado.
Desenvolvimento de trabalho autónomo do estudante em laboratório de investigação.
A dissertação/projeto implica a elaboração de um relatório final, objeto de apreciação e discussão pública por um júri nomeado pelo órgão legal e estatutariamente competente, de acordo com o regulamento do Instituto Politécnico de Leiria.

3.3.7. Teaching methodologies (including assessment):

Supervision of individual students in planning the work, collecting and analysing relevant information, in performing the work and in developing of critical skills , by a Ph.D member of staff.
Development of independent work and on-site research lab training. The dissertation/project involves the preparation of a final report, subject to public discussion and consideration by a jury, according to Instituto Politécnico de Leiria regulation.

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

As metodologias de ensino usadas que contribuem para as competências gerais estabelecidas para a UC passam pela orientação tutorial em ambiente académico e de investigação.

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

The teaching methods contribute to the general skills set for the subject and are based on academic and research supervision at Instituto Politécnico de Leiria.

3.3.9. Bibliografia principal:

Bibliografia a definir pelos supervisores.

Mapa IV - Dissertação

3.3.1. Unidade curricular:

Dissertação

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

Mário João Gonçalves Antunes, 10h

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

Carlos Manuel Silva Rabadão, 10h
Patrício Rodrigues Domingues, 10h
Miguel Monteiro Sousa Frade, 10h
Paulo Manuel Gonçalves Oliveira Valente da Cruz, 10h
Maria Beatriz Guerra Piedade, 10h

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

C1. Capacidade de sintetizar, otimizar e propor soluções inovadoras para problemas e situações novas, relacionadas com as várias áreas de interesse no âmbito da cibersegurança e da computação forense.
C2. Capacidade de conceber e demonstrar soluções inovadoras no âmbito das áreas de interesse do curso.
C3. Capacidade para integrar os conhecimentos adquiridos, lidar com questões complexas, desenvolver soluções ou emitir juízos em situações de informação limitada ou incompleta, incluindo reflexões sobre as implicações e responsabilidades éticas e sociais que resultem dessas soluções e desses juízos ou os condicionem;
C4. Capacidade de identificar as necessidades inerentes à concretização de um determinado projeto, planear atividades no espaço e no tempo e verificar a execução dos objetivos;
C5. Capacidade de apresentar e justificar as suas opções quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

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

C1. Ability to synthesize, optimize and propose implementable solutions to problems in new and unfamiliar situations, related to the various areas of interest in Computer Engineering - Mobile Computing.
C2. Ability to design, implement and maintain solutions within the Engineering Computing - Mobile Computing area;
C3. Ability to integrate knowledge, handle complexity, develop solutions and make judgements in situations of limited or incomplete information, including reflections on the implications, ethical and social responsibilities resulting from those solutions or judgements;
C4. Ability to identify requirements, need resources and plan activities to achieve successfully tasks and research objectives;
C5. Ability to present and justify technical, organisational and scientific decisions to either specialists or non-specialists in a clear and unambiguous way.

3.3.5. Conteúdos programáticos:

Os estudantes desenvolverão um trabalho original nas áreas de cibersegurança e/ou computação forense.
O trabalho, cujo plano deverá ser aprovado pelo órgão científico estatutariamente competente, será maioritariamente realizado em ambiente académico e de investigação.

3.3.5. Syllabus:

Students will develop an original work in cybersecurity and/or digital forensics.
The work plan shall be approved by the school scientific body and shall be mostly done in academic and research environment.

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

A diversidade de unidades curriculares, constituindo um perfil curricular adequado à área de interesse de cada aluno, permite adquirir conhecimentos e capacidade de compreensão de forma a constituir uma base para desenvolvimentos originais na unidade curricular de dissertação/projeto.
A organização das unidades curriculares, assente na realização de trabalhos pelos alunos fora das aulas, assim como a realização de um trabalho de projeto de grande dimensão, permite que os alunos adquiram a capacidade para integrar conhecimentos.
A escrita e apresentação pública dos trabalhos realizados no âmbito das unidades curriculares, e principalmente a dissertação resultante da unidade curricular de dissertação/projeto e a sua apresentação tem como objetivo garantir que os alunos sejam capazes de comunicar as conclusões e os conhecimentos e raciocínios a elas subjacentes quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

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

The diversity of course units, constituting a curriculum appropriate to the profile area of interest of each student, allows the ability to acquire knowledge and understanding to form a basis for original developments in the course of the research project
The conception of modules, based on the performance of work by students outside the classroom as well as carrying out a project work of large dimensions, allows students to acquire the ability to integrate knowledge.

The writing and public presentation of work carried out within the courses and the dissertation mainly resulting from the project and its presentation is designed to ensure that students are able to communicate the conclusions and the knowledge and reasoning underlying them either to experts or non-experts in a clear and unambiguous way.

3.3.7. Metodologias de ensino (avaliação incluída):

Acompanhamento individual dos estudantes no planeamento do trabalho, na recolha e análise da informação relevante, na execução do trabalho e no desenvolvimento de capacidade crítica, por um docente doutorado.
Desenvolvimento de trabalho autónomo do estudante em laboratório de investigação.
A dissertação/projeto implica a elaboração de um relatório final, objeto de apreciação e discussão pública por um júri nomeado pelo órgão legal e estatutariamente competente, de acordo com o regulamento do Instituto Politécnico de Leiria.

3.3.7. Teaching methodologies (including assessment):

Supervision of individual students in planning the work, collecting and analysing relevant information, in performing the work and in developing of critical skills , by a Ph.D member of staff.
Development of independent work and on-site research lab training. The dissertation/project involves the preparation of a final report, subject to public discussion and consideration by a jury, according to Instituto Politécnico de Leiria regulation

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

As metodologias de ensino usadas que contribuem para as competências gerais estabelecidas para a UC passam pela orientação tutorial em ambiente académico e de investigação.

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

The teaching methods contribute to the general skills set for the subject and are based on academic and research supervision at Instituto Politécnico de Leiria.

3.3.9. Bibliografia principal:

Bibliografia a definir pelos supervisores.

Mapa IV - Estágio

3.3.1. Unidade curricular:

Estágio

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

Mário Joao Gonçalves Antunes, 10h

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

Carlos Manuel Silva Rabadão, 10h
Patrício Rodrigues Domingues, 10h
Miguel Monteiro Sousa Frade, 10h
Paulo Manuel Gonçalves Oliveira Valente da Cruz, 10h
Maria Beatriz Guerra Piedade, 10h

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

C1. Capacidade de sintetizar, otimizar e propor soluções inovadoras para problemas e situações novas, relacionadas com as várias áreas de interesse no âmbito da cibersegurança e da computação forense.
C2. Capacidade de conceber e demonstrar soluções inovadoras no âmbito das áreas de interesse do curso.
C3. Capacidade para integrar os conhecimentos adquiridos, lidar com questões complexas, desenvolver soluções ou emitir juízos em situações de informação limitada ou incompleta, incluindo reflexões sobre as implicações e responsabilidades éticas e sociais que resultem dessas soluções e desses juízos ou os condicionem;
C4. Capacidade de identificar as necessidades inerentes à concretização de um determinado projeto, planear atividades no espaço e no tempo e verificar a execução dos objetivos;
C5. Capacidade de apresentar e justificar as suas opções quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

3.3.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
C1. Ability to synthesize, optimize and propose implementable solutions to problems in new and unfamiliar situations, related to the various areas of interest in Computer Engineering - Mobile Computing.
C2. Ability to design, implement and maintain solutions within the Engineering Computing - Mobile Computing area;
C3. Ability to integrate knowledge, handle complexity, develop solutions and make judgements in situations of limited or incomplete information, including reflections on the implications, ethical and social responsibilities resulting from those solutions or judgements;
C4. Ability to identify requirements, need resources and plan activities to achieve successfully tasks and research objectives;
C5. Ability to present and justify technical, organisational and scientific decisions to either specialists or non-specialists in a clear and unambiguous way.

3.3.5. Conteúdos programáticos:
Os estudantes desenvolverão um trabalho original nas áreas de cibersegurança e/ou computação forense.
O trabalho, cujo plano deverá ser aprovado pelo órgão científico estatutariamente competente, será maioritariamente realizado em ambiente académco e de investigação.

3.3.5. Syllabus:
Students will develop an original work in cybersecurity and/or digital forensics.
The work plan shall be approved by the school scientific body and shall be mostly done in academic and research environment.

3.3.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
A diversidade de unidades curriculares, constituindo um perfil curricular adequado à área de interesse de cada aluno, permite adquirir conhecimentos e capacidade de compreensão de forma a constituir uma base para desenvolvimentos originais na unidade curricular de dissertação/projeto.
A organização das unidades curriculares, assente na realização de trabalhos pelos alunos fora das aulas, assim como a realização de um trabalho de projeto de grande dimensão, permite que os alunos adquiram a capacidade para integrar conhecimentos.
A escrita e apresentação pública dos trabalhos realizados no âmbito das unidades curriculares, e principalmente a dissertação resultante da unidade curricular de dissertação/projeto e a sua apresentação tem como objetivo garantir que os alunos sejam capazes de comunicar as conclusões e os conhecimentos e raciocínios a elas subjacentes quer a especialistas quer a não especialistas de uma forma clara e sem ambiguidades.

3.3.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
The diversity of course units, constituting a curriculum appropriate to the profile area of interest of each student, allows the ability to acquire knowledge and understanding to form a basis for original developments in the course of the research project
The conception of modules, based on the performance of work by students outside the classroom as well as carrying out a project work of large dimensions, allows students to acquire the ability to integrate knowledge.
The writing and public presentation of work carried out within the courses and the dissertation mainly resulting from the project and its presentation is designed to ensure that students are able to communicate the conclusions and the knowledge and reasoning underlying them either to experts or non-experts in a clear and unambiguous way.

3.3.7. Metodologias de ensino (avaliação incluída):
Acompanhamento individual dos estudantes no planeamento do trabalho, na recolha e análise da informação relevante, na execução do trabalho e no desenvolvimento de capacidade crítica, por um docente doutorado.
Desenvolvimento de trabalho autónomo do estudante em laboratório de investigação.

A dissertação/projeto implica a elaboração de um relatório final, objeto de apreciação e discussão pública por um júri nomeado pelo órgão legal e estatutariamente competente, de acordo com o regulamento do Instituto Politécnico de Leiria.

3.3.7. Teaching methodologies (including assessment):

Supervision of individual students in planning the work, collecting and analysing relevant information, in performing the work and in developing of critical skills , by a Ph.D member of staff.
Development of independent work and on-site research lab training. The dissertation/project involves the preparation of a final report, subject to public discussion and consideration by a jury, according to Instituto Politécnico de Leiria regulation.

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

As metodologias de ensino usadas que contribuem para as competências gerais estabelecidas para a UC passam pela orientação tutorial em ambiente académico e de investigação.

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

The teaching methods contribute to the general skills set for the subject and are based on academic and research supervision at Instituto Politécnico de Leiria.

3.3.9. Bibliografia principal:

Bibliografia a definir pelos supervisores.

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

4.1 Descrição e fundamentação dos recursos docentes do ciclo de estudos

4.1.2 Equipa docente do ciclo de estudos

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

Nome / Name	Grau / Degree	Área científica / Scientific Area	Regime de tempo / Employment link	Informação/ Information
Mário João Gonçalves Antunes	Doutor	Ciência de Computadores	100	Ficha submetida
Carlos Manuel da Silva Rabadão	Doutor	Engenharia Informática	100	Ficha submetida
Patrício Rodrigues Domingues	Doutor	Engenharia Informática	100	Ficha submetida
Miguel Monteiro Sousa Frade	Doutor	Engenharia Informática	100	Ficha submetida
Carlos Manuel Gonçalves Antunes	Mestre	Engenharia Informática	100	Ficha submetida
Maria Beatriz Guerra Piedade	Doutor	Tecnologias e Sistemas de Informação	100	Ficha submetida
José Vítor Martins Ramos	Mestre	Engenharia Informática - Sistemas e Tecnologias de Informação	100	Ficha submetida
Paulo Manuel Gonçalves Oliveira Valente da Cruz	Licenciado	Engenharia Electrotécnica	50	Ficha submetida
(8 Items)			**750**	

<sem resposta>

4.2. Dados percentuais dos recursos docentes do ciclo de estudos

4.2.1.Corpo docente próprio do ciclo de estudos

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

Corpo docente próprio / Full time teaching staff	ETI / FTE	Percentagem* / Percentage*
Nº de docentes do ciclo de estudos em tempo integral na instituição / No. of full time teachers:	7.5	100

4.2.2.Corpo docente do ciclo de estudos academicamente qualificado

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

Corpo docente academicamente qualificado / Academically qualified teaching staff	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos com o grau de doutor (ETI) / Teaching staff with a PhD (FTE):	5	66.7

4.2.3.Corpo docente do ciclo de estudos especializado

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

Corpo docente especializado / Specialized teaching staff	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos com o grau de doutor especializados nas áreas fundamentais do ciclo de estudos (ETI) / Teaching staff with a PhD, specialized in the main areas of the study programme (FTE):	5	66.7
Especialistas, não doutorados, de reconhecida experiência e competência profissional nas áreas fundamentais do ciclo de estudos (ETI) / Specialists, without a PhD, of recognized professional experience and competence, in the main areas of the study programme (FTE):	1	13.3

4.2.4.Estabilidade do corpo docente e dinâmica de formação

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

Estabilidade e dinâmica de formação / Stability and tranning dynamics	ETI / FTE	Percentagem* / Percentage*
Docentes do ciclo de estudos em tempo integral com uma ligação à instituição por um período superior a três anos / Full time teaching staff with a link to the institution for a period over three years:	7	93.3
Docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (ETI) / Teaching staff registered in a doctoral programme for more than one year (FTE):	2	26.7

4.3. Procedimento de avaliação do desempenho

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

De acordo com o Decreto-Lei n.º 207/2009 (Estatuto da Carreira do Pessoal Docente do Ensino Superior Politécnico), de 31 de Agosto, foi instituída a avaliação de desempenho do pessoal docente das instituições de ensino superior. O regulamento de avaliação do desempenho dos docentes do Instituto Politécnico de Leiria foi publicado em D.R. (Despacho nº 11288/2013, nº 167, Série II, de 30 de agosto de 2013). Nos termos do disposto no art.º 35A do ECPDESP são objeto de avaliação todas as atividades previstas no referido Estatuto, considerando as vertentes técnico-científica (30 pontos), a vertente pedagógica (50 pontos) e a vertente organizacional (20 pontos).
Para além da avaliação institucional, no âmbito do curso são realizados questionários semestrais junto dos alunos e docentes a fim de averiguar a qualidade pedagógica do curso bem como a satisfação dos envolvidos e recolher sugestões de melhoria.

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

According to Decree-Law No. 207/2009 (Career Statute of Teaching Staff in Higher Polytechnic) in August 31 was established the performance evaluation of teaching staff in higher education institutions. The performance assessment regulation of Polytechnic Institute of Leiria was published in DR (Order No. 11288/2013, No. 167, Series II, of 30 August 2013). In accordance with art. º 35A of ESPDEP are objects of assessment all activities envisaged in the Statute, considering the technical and scientific aspects (30 points), the pedagogic aspects (50 points) and organizational aspects (20 points).
Apart from institutional assessment, within the course are conducted questionnaires each semester among students and teachers in order to ascertain the pedagogic quality of the course as well as the satisfaction of those involved and to collect suggestions for improvement.

5. Descrição e fundamentação de outros recursos humanos e materiais

5.1. Pessoal não docente afeto ao ciclo de estudos:

Os colaboradores não docentes envolvidos na lecionação distribuem-se por diversos serviços que se caracterizam pela realização de tarefas técnicas ou administrativas. Ao nível das tarefas técnicas relevamos a atualização e manutenção dos equipamentos laboratoriais, o apoio às aulas práticas de laboratório, a atualização de software nos laboratórios de aplicações informáticas e a manutenção de plataformas de gestão de conteúdos de gestão pedagógica e de e-learning. As tarefas administrativas consistem essencialmente na elaboração de horários e marcação de salas paras as aulas e avaliações, na criação e no lançamento de pautas, no registo de faltas dos estudantes e no acompanhamento de estágios e de estudantes em programas de mobilidade.
No âmbito destas intervenções estão afetos cerca de 30 colaboradores em regime de contrato de trabalho em funções públicas e destes, 3 estão afetos ao Departamento de Eng. Informática com o objetivo principal de manutenção dos laboratórios e de software.

5.1. Non teaching staff allocated to the study programme:

There are 30 members of the non-academic staff, of which 3 are exclusively assigned to the Department of Computer Engineering with the main goal of laboratory and software maintenance. This staff supports academic activities, distributed through different services, which are responsible for technical and/or administrative tasks. The main technical tasks of these offices include maintaining and updating the laboratories' equipment, supporting laboratory classes, updating software in computer sciences laboratories, and maintaining pedagogical management and e-learning content management systems. Administrative tasks consist mainly in scheduling classes, booking classrooms for classes and exams, creating students' grades lists and making them public, keeping a record of student's attendance, as well as supporting students' internships and mobility programmes.

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

1 laboratório específico de cibersegurança e informática forense
1 Biblioteca (3.500m2)
43 Salas de aula com equipamento audiovisual
7 Anfiteatros
2 Laboratórios de informática com software Multimédia (Laboratório de Aplicações Informáticas I, Laboratório de Desenvolvimento de Aplicações)
2 Laboratórios de Comunicações (Laboratório de Comunicações Avançadas; Laboratório de Redes e Sistemas de Comunicação)
8 Laboratórios de informática generalistas (Laboratório de Base de Dados, Laboratório de Sistemas de Informação, Laboratório de Sistemas Operativos, Laboratório de Aplicações Informáticas II - VI)
1 Laboratório de Ensino (outros)

2 Laboratórios de Investigação
1 Sala de Apoio
2 Salas de informática
4 Reprografias
155 Gabinetes docentes
2 Salas de Projeto
2 Auditórios
2 Salas de Formação

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

1 specific lab for cybersecurity and digital forensics
1 Library (3.500m2)
43 classrooms with audiovisual equipment
7 amphitheatres
2 Computer labs with Multimedia software (Laboratory of Computer Applications I, Application Development Laboratory)
2 Communications Laboratories (Laboratory of Advanced Communications, Laboratory of Networking and Communication Systems)
8 Generalists computer labs (Laboratory Database, Laboratory Information Systems, Operating Systems Laboratory, Laboratory for Computer Applications II - VI)
1 Teaching Laboratory (other)
2 Research Laboratories
1 Room Support
2 Rooms computer
4 print shops
155 teachers Offices
2 Project Rooms
2 Auditoriums
2 Training Rooms

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

- Laboratório de Comunicações Avançadas
- Laboratório Redes e Serviços de Comunicação
- Laboratório de Desenvolvimento de aplicações
- Laboratório Base de Dados
- Laboratório Sistemas de Informação
- Laboratório SO
- Laboratórios de Aplicações Informáticas (LAI I - LAI V)
- Sala de Projecto Informático
- 7 Smartphones (Android ou iOS)
- 10 Tablets (Android ou iOS)
- Placas gráficas Nvidia GTX 480-16
- Laboratório de cibersegurança e informática forense com os seguintes equipamentos:
Computadores dedicados para análise forense
Rede local separada do resto da instituição
NAS para armazenamento de backups
Bloqueadores de escrita: SATA e USB
Adaptadores para interfaces de discos
XRY Office Version (leitor de cartões SIM, cartões SIM para clonagem de ICCID e IMSI, cabos variados, hub USB para aquisição simultânea de 3 dispositivos, bolsa de Faraday)
Telefones e discos rígidos para testes
Software diverso (FTK imager, Autopsy, ...)

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

- Laboratory of Advanced Communications
- Laboratory Advanced Networking
- Laboratory of Applications development
- Laboratory of Databases
- Laboratory Operating Systems
- Laboratory of Computer Applications (LAI I - V LAI)
- Computers Room for Project
- 7 Smartphone (Android or iOS)
- 10 Tablets (Android or iOS)
- Graphics Card Nvidia GTX 480-16
- Cybersecurity and Digital Forensics Lab, with the following equipments:
Dedicated computers for digital forensics
Dedicated local area network
NAS for storage and backups
Write blocker: SATA e USB
Adapters for disks interfaces
XRY Office Version (SIM card reader, SIM cards to clone ICCID and IMSI, assorted cables, hub USB, Faraday bag)
Phones and HDD and hard disk drives for testing
Digital forensics software, mainly FTK imager, Autopsy.

6. Atividades de formação e investigação

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

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

Centro de Investigação / Research Centre	Classificação (FCT) / Mark (FCT)	IES / Institution	Observações / Observations
Centro de Investigação em Informática e Comunicações	Fair	Instituto Politécnico de Leiria	
INstituto de Engenharia de Sistemas e Computadores - Tecnologia e Ciência (INESC-TEC) - CRACS	Excellent	Universidade do Porto	
Center for Informatics and Systems (CISUC)	Very Good	Universidade de Coimbra	
Instituto de Telecomunicações (IT)	Excellent	Instituto Politécnico de Leiria	

Perguntas 6.2 e 6.3

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

http://a3es.pt/si/iportal.php/cv/scientific-publication/formId/c9eeaade-b49b-9090-6c21-57d020d804a3

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

1) Polícia Judiciária, Laboratório de Polícia Científica (LPC)
2) Escola da Polícia Judiciária
3) Procuradoria Geral da República - Gabinete de Cibercrime
4) NERLEI - Associação Empresarial da Região de Leiria

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

1) Scientific Police Laboratory – Judiciary Police
2) School of Judiciary Police
3) Attorney General's Office - Cybercrime Office
4) NERLEI - Entrepreneurial Association of the Leiria Region

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

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

- Pós-graduação em Informática de Segurança e Computação Forense (Despacho n.º 4564/2012), realizada em parceria com a Polícia Judiciária e a Escola da Polícia Judiciária. Conta já com três edições, abrangendo profissionais da PJ e da PGR, bem como profissionais da TI a exercer funções no mercado de trabalho na área de segurança informática e administração de sistemas.
- Procuradoria Geral da República - Gabinete de Cibercrime - elaboração de relatórios periciais de informática forense, realizados no Laboratório de Cibersegurança e Informática Forense (LabCIF)
- Formação técnica a profissionais da PJ, através da parceria com a Escola da PJ.
- Workshop inserido nas atividades da PG em Informática de Segurança e Computação Forense, com a participação de vários oradores e entidades de reconhecido mérito na cibersegurança e computação forense.

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

- Postgraduation on Cybersecurity and Digital Forensics (Despacho n.º 4564/2012), in a partnership with Portuguese Judiciary Police (PJ) and its school (EPJ). It has now three editions, with both PJ and PGR's computers technicians and also IT professionals working in computers security and systems and network administration.
- Procuradoria Geral da República - Cybercrime Office - preparation of expert reports of digital forensics performed on Cybersecurity Laboratory and Forensic Computing (LabCIF)
- Technical courses to IT professionals at PJ, through the partnership with EPJ.
- Workshop in the scope of postgraduation activities, that had the participation of several individuals and activities of recognized merit on cybersecurity and digital forensics.

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

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

Neste ciclo de estudos não é possível fazer uma avaliação com outros ciclos congéneres, na medida em que não existe, tanto quanto é do nosso conhecimento, um que contemple simultaneamente as duas áreas principais de formação: cibersegurança e informática forense.
Acresce ainda que previsivelmente os alunos que ingressarão neste ciclo de estudos se encontram no mercado de trabalho.

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

In this study programme it is not possible to evaluate with other counterparts cycles, to the extent that there is, to the best of our knowledge, no one that simultaneously incorporates the two main fields: cybersecurity and digital forensics.
Furthermore, predictably students who will enter this course are in the labor market.

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

8.2. Evaluation of the capability to attract students based on access data (DGES):
Not applicable

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

8.3. List of eventual partnerships with other institutions in the region teaching similar study programmes:
Not applicable

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

9.1. Fundamentação do número total de créditos ECTS e da duração do ciclo de estudos, com base no determinado nos artigos 8.º ou 9.º (1.º ciclo), 18.º (2.º ciclo), 19.º (mestrado integrado) e 31.º (3.º ciclo) do Decreto-Lei n.º 74/2006, de 24 de Março:
O curso de mestrado em Cibersegurança e Computação Forense está organizado em 4 semestres curriculares de trabalho totalizando 120 ECTS, estando de acordo com o definido no nº.1 do artigo 18º e o n.º1 do artigo 20 do decreto lei 74/2006 na redação última que lhe foi conferida pelo decreto lei 115/2013, de 7 de agosto. A parte letiva está concentrada nos dois
primeiros semestres e corresponde a 60 ECTS (50% do total dos créditos do ciclo de estudos - cumpre a alínea a do n.º1 do artigo 20 do decreto lei 74/2006), distribuídos por 11 unidades curriculares. Nos 3º e 4º semestres os alunos têm a opção de elaborar uma dissertação de natureza científica, desenvolver um trabalho de projeto ou efetuar um estágio de natureza profissional objeto de relatório final, correspondente a 50 ECTS (50% do total dos créditos do ciclo de estudos - cumpre a alínea b do n.º1 do artigo 20 do decreto lei 74/2006).

9.1. Justification of the total number of ECTS credits and of the duration of the study programme, based on articles no.8 or 9 (1st cycle), 18 (2nd cycle), 19 (integrated master) and 31 (3rd cycle) of Decreto-Lei no. 74/2006, March 24th:
The Master's degree in Cybersecurity and Digital Forensics is organized into 4 semesters of work totaling 120 ECTS, which is consistent with that defined in n.º 1 of article 18 and n. 1 of article 20 of Decree Law 74/2006 in the newsroom last that it conferred by Legislative Decree 115/2013 of 7 August. Curricular part is concentrated in the first two semesters and corresponds to 60 ECTS (50% of the total credits of the course - consistent with the n. 1 of article 20 of Decree Law 74/2006), spread over 10 curricular units . In the 3rd and 4th semesters students have the option of developing a scientific dissertation, develop a project work or carry out a professional traineeship object the final report, corresponding to 60 ECTS (50% of the total credits of the course - consistent with subparagraph b of n.º 1 of article 20 of decree law 74/2006).

9.2. Metodologia utilizada no cálculo dos créditos ECTS das unidades curriculares:
A atribuição dos créditos (European Credit Transfer System) foi realizada de acordo com o disposto do decretolei n.º42/2005 de 22 de fevereiro. Foi igualmente considerado o regulamento de aplicação de sistema de créditos curriculares aos cursos do IPLeiria (Regulamento n.º 16/2006; aprovado pelo Conselho Geral do IPL para dar cumprimento ao artigo 11.º do Decreto-Lei n.º 42/2005), no qual se estima que 1 unidade de crédito ECTS corresponde a 27 horas de trabalho total do aluno. Nestas horas incluem-se o trabalho individual e de grupo do aluno e o contacto direto com o professor dentro e fora de aula. Com base naquele parâmetro e tendo como objetivo que a estrutura curricular do mestrado seja equilibrada em termos de ECTS (6 ECTS - considerando que todas as unidades curriculares são igualmente relevantes para a formação), os docentes responsáveis das unidades curriculares definiram os conteúdos programáticos, a sua extensão e complexidade, tendo em conta os ECTS definidos.

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

The allocation of credits (European Credit Transfer System) was performed in accordance with the provisions of Legislative Decree n. º 42/2005 of 22 February. It was also considered the implementing regulation of the course credit system to courses IPLeiria (Regulations No. 16/2006; approved by the General Council of the Polytechnic Institute of Leiria, conform Art. 11 of Decree-Law No. 42/2005), which estimates that 1 unit ECTS credit corresponds to 27 hours of total work of the student. These hours include individual work and group and direct contact between the student and the teacher inside and outside of class. Based on that parameter and having as objective that the curriculum of the Master is balanced in terms of ECTS (6 ECTS - considering that all units are equally relevant to the training), the teachers in charge of curriculum units defined the syllabus and the its size and complexity, taking into account the ECTS defined.

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

Os ECTS foram atribuídos considerando que as unidades curriculares são igualmente relevantes na estrutura curricular do mestrado em cibersegurança e computação forense. Os docentes responsáveis pelos programas de cada unidade curricular, em colaboração com outros docentes das respetivas áreas científicas, definiram os conteúdos programáticos, a sua extensão e a complexidade de cada unidade curricular tendo em atenção as horas de trabalho totais previstas, correspondendo a 6 ECTS.

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

The ECTS were assigned considering that the curricular units are equally relevant to the curriculum of the Master in Cybersecurity and digital forensics. The teachers responsible for each course unit curricular, in collaboration with other teachers of the respective scientific areas, defined the syllabus, its length and complexity of each unit curricular taking into account the total expected hours of work, corresponding to 6 ECTS.

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

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

Em Portugal:
- Mestrado em Segurança Informática; Faculdade de Ciências, Universidade do Porto
- Mestrado em Segurança Informática; Faculdade de Ciências, Universidade de Lisboa
- Mestrado em Segurança de Informação e Direito no Ciberespaço; Instituto Superior Técnico, Universidade de Lisboa
- Mestrado em Engenharia de Segurança Informática; Instituto Politécnico de Beja

No espaço europeu:
- Master of Science in Computer Security; University of Liverpool, UK
- Master of Science in Network Security and Pen Testing; Middlesex University London, UK
- Master of Science in Information Security & Privacy; Cardiff University, UK
- Master of Science in Computer Security and Forensics; University of Bedfordshire, UK
- Master of Science in Digital Investigation & Forensic Computing; University College Dublin, UK

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

In Portugal:
- MSc in Computers Security; Faculty of Science, University of Porto
- MSc in Computers Security; Faculty of Science, University of Lisbon
- MSc in Information Security and Cyberspace Law; Instituto Superior Técnico, University of Lisbon
- MSc in Computers Security Engineering; Polytechnic Institute of Beja

In Europe:
- Master of Science in Computer Security; University of Liverpool, UK

- Master of Science in Network Security and Pen Testing; Middlesex University London, UK
- Master of Science in Information Security & Privacy; Cardiff University, UK
- Master of Science in Computer Security and Forensics; University of Bedfordshire, UK
- Master of Science in Digital Investigation & Forensic Computing; University College Dublin, UK

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

Os ciclos de estudo existentes em Portugal não contemplam de forma explícita as duas áreas oferecidas que o ciclo de estudo que se propõe: cibersegurança e informática forense. De uma forma geral, os ciclos de estudo abordam vários tópicos da segurança de informação, incluindo a criptografia, mas não contemplam as técnicas e metodologias usadas na análise forense de equipamentos digitais e na recuperação de dados. O ciclo de estudos que se propõe inclui as duas áreas, cibersegurança e análise forense digital, tornando-se assim, desse ponto de vista, uma oferta formativa diferenciadora no panorama de formação de 2ºciclo na área da segurança informática.

No espaço europeu é possível encontrar vários ciclos de estudo dedicados a ambas as áreas. O ciclo de estudos que se propõe está em linha com os congéneres europeus, quer ao nível da definição de competências, quer ao nível dos tópicos incluídos no plano de estudos, quer ainda na adoção das boas práticas em termos de metodologia de ensino.

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

Existing study programmes in Portugal do not address explicitly the two areas offered in the study programme that is proposed: cybersecurity and digital forensics. In general, the study programmes address various topics of information security, including cryptography, but do not include the techniques and methodologies used in digital forensic and further data recovery. The study programme that is proposed includes both areas, cybersecurity and digital forensics, thus making it from this point of view, a distinctive educational offer in the panorama of 2nd cycle of training in the field of computers security.

In Europe you can find various study programmes dedicated to both fields. The course that is proposed is in line with European counterparts, both in terms of skills development, both in terms of the topics included in the syllabus, as well as the adoption of good practice in terms of teaching methodology.

11. Estágios e/ou Formação em Serviço

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

Mapa VII - Protocolos de Cooperação

Mapa VII - Estágio optativo. Lista de eventuais entidades disponível em 11.2

11.1.1. Entidade onde os estudantes completam a sua formação:

Estágio optativo. Lista de eventuais entidades disponível em 11.2

11.1.2. Protocolo (PDF, máx. 150kB):

11.1.2._Minuta_Estagio_MCIF.pdf

Mapa VIII. Plano de distribuição dos estudantes

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

11.2._LISTA DE ESTAGIOS.pdf

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

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

A ESTG-Leiria dispõe de um Gabinete de Estágios e Acompanhamento Profissional (GEAP) cujos objetivos são desenvolver programas de estágios adequados à formação dos estudantes, dispor de contactos com entidades recetoras de estagiários e entidades empregadoras dos diversos ramos de atividade e contribuir para a integração dos estudantes no mercado de trabalho, servindo de elo de ligação entre a escola e o meio empresarial. Para além do supervisor da entidade recetora do estagiário, os estudantes de estágio têm um orientador, docente do ciclo de estudos, que acompanha e orienta o estudante na elaboração do relatório de estágio através de reuniões em sala de aula ou gabinete da instituição e mantém o contacto com a entidade recetora do estagiário, nomeadamente, através de visitas à instituição e video-conferência.

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

The ESTG-Leiria has an Office of Internships and Professional Monitoring (GEAP) whose goals are to develop internship programs appropriate to the education of students, make the contacts with entities that receive interns and employers of various industries and contribute to the integration students in the labor market, serving as a liaison between the school and the business. Apart from the supervisor of entity receiving intern, the internship students have a guider, teacher of the course, which accompanies and guides the student in preparing the report internship through meetings in the classroom or office of the institution and that maintains contact with the entity receiving intern, including through visits to the institution and video conferencing.

11.4. Orientadores cooperantes

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

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

11.4.1_11.4.1_Ata n58 CTC_Normas Supervisores de Estagio.pdf

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

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

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

<sem resposta>

12. Análise SWOT do ciclo de estudos

12.1. Pontos fortes:

1. Unidade orgânica com historial de formação na área das ciências informática
2. Existência de formação de 1º ciclo em Engenharia Informática
3. Experiência na lecionação de uma Pós-graduação em Informática de Segurança e Computação Forense
4. Existência de protocolos de cooperação com instituições de referência na áreas do curso (PJ e PGR)
5. Elaboração regular de peritagens forenses digitais
6. Corpo docente altamente qualificado com doutoramento e existência de especialistas, o que potencia a formação dos alunos e desenvolvimento de trabalhos de dissertação/projeto/estágio;
7. Integração de docentes em centros de investigação de referência;

8. Inexistente oferta formativa de 2ºciclo a nível nacional na área de informática forense
9. Laboratório com equipamento específico
10. Publicações científicas nos tópicos abordados no curso;
11. Participação no projecto Multinational Smart Defence Project on Cyber Defence Education & Training (MN CD E&T), da NATO e Academia Militar

12.1. Strengths:

1. Organic Unit has a long history on offering course on computers engineering
2. There exists a course of 1st cycle in Computers Engineering
3. Experience on a Post-graduation on cybersecurity and digital forensics
4. There exists solid cooperation protocols with important institutions in the topics covered in the course (PJ and PGR)
5. Elaboration of digital forensics reports
6. Professors are almost all PhD or specialists
7. Professors are integrated in research centers highly classified;
8. There is no master degree on digital forensics
9. There exists a dedicated lab with specific equipment for digital forensics.
10. Scientific publications in the topics covered in the course.
11. Participation in project Multinational Smart Defence Project on Cyber Defence Education & Training (MN CD E&T), by NATO and Academia Militar

12.2. Pontos fracos:

1. Alguns estudantes que estão atualmente no mercado de trabalho e que completaram os estudos há mais tempo, poderão não ter as competências nalguns tópicos de base do curso.

12.2. Weaknesses:

1. Those students that are now at labor market and finished their graduations some time ago, may not have the minimum skills in some fundamental topics of the course.

12.3. Oportunidades:

1. Parcerias fortes com empresas de referência na região onde os alunos poderão realizar os estágios, podendo assim contribuir para a melhoria das infraestruturas de TI e da implementação de políticas de segurança;
2. Curso com cariz muito prático com funcionamento modular e em regime pós-laboral, o que atrairá candidatos atualmente no mercado de trabalho
3. Tanto quanto é do nosso conhecimento, inexistência em outras IES portuguesas, de uma formação de 2ºciclo que contemple cumulativamente as duas áreas: cibersegurança e informática forense.
4. Crescente preocupação generalizada pela segurança da informação e das infraestruturas de TI.
5. Inexistência de empresas na área de computação forense instaladas na região de Leiria

12.3. Opportunities:

1. Strong partnerships with companies and institutions where students are able to develop their partnerships, as well to contribute for secure IT infrastructures and for the implementation of security policies.
2. Course is highly practical and hands-on, with a modular functioning and in part-time, which may attract candidates that are now working in IT industry.
3. To the best of our knowledge there is no similar 2nd cycle course in others portugues IES which includes both cybersecurity and digital forensics subjects.
4. Growing and generalized concern around information security and IT infraestructures.
5. There is no companies on digital forensics operating on Leiria region.

12.4. Constrangimentos:

1. A atual conjuntura pode dificultar a dispensa dos colaboradores para realizarem formação avançada

12.4. Threats:

1. Social and economics conjuncture may bring obstacles to the student's enrollment in a master course.

12.5. CONCLUSÕES:

O mestrado em cibersegurança e computação forense surge na sequência de um vasto conjunto de iniciativas bem sucedidas nesta área, levadas a cabo pela ESTG-Leiria, das quais destacamos: criação, organização e lecionação de um curso de pós-graduação em informática de segurança e computação forense; criação de um laboratório de informática forense para a realização de perícias a equipamentos digitais emanadas do gabinete de cibercrime da Procuradoria Geral da República, com o qual o IPLeiria tem um protocolo de cooperação; elaboração de cursos curtos de formação na Escola da PJ sobre tópicos relacionados com os temas abordados no curso proposto; envolvimento dos docentes na supervisão de estágios e dissertações de mestrado realizados na Polícia Judiciária.
Com este mestrado pretende-se dar seguimento a este trabalho, oferecendo uma formação de 2ºciclo que junta duas áreas complementares: a cibersegurança e a computação forense. Trata-se de um curso de formação avançada que terá um cariz prático e orientado para a resolução de problemas das organizações ao nível da proteção da infraestrutura de rede e análise forense dos seus equipamentos. O curso funcionará em regime pós-laboral, o que possibilitará a sua frequência por profissionais que se encontrem atualmente no mercado de trabalho. A sua organização modular possibilitará uma melhor articulação das matérias e dos trabalhos práticos que serão propostos. Em cada um dos dois semestres da parte letiva haverá uma UC de "projeto" onde serão realizados trabalhos práticos que integrarão as matérias abordadas nas restantes UCs de cada semestre.

Nas UC de estágio, projeto e dissertação pretendemos desenvolver procedimentos que potenciem a ligação com as empresas da região, nomeadamente na implementação de soluções de segurança na infraestrutura da rede e dos serviços.

O ciclo de estudos conta com recursos humanos docentes qualificados com o grau de doutor ou com o título de especialista, bem como com recursos materiais adequados ao seu funcionamento.

12.5. CONCLUSIONS:

2nd cycle master degree on cybersecurity and digital forensics is grounded in the sequence of a wide set of well succeeded initiatives in these fields, carried on by ESTG-Leiria, from which we highlight: setup, organization and lecture of a postgraduation course on cybersecurity and digital forensics; setup of a lab room fully dedicated to digital forensics to carry on digital forensics reports analysis, related to public processes emanated from Procuradoria Geral da República's cybercrime office, with which IPLeiria has a cooperation protocol; setup and lecture of short courses at Escola da PJ for technicians; teacher's involvement on supervision of internships, projects and dissertations carried on Portuguese Judiciary Police.
With this Master degree we aim to follow up the work done so far, by offering a 2nd cycle master course which joins two complementary areas: cybersecurity and digital forensics. It is an advanced course with a practical nature and mostly oriented to solve real problems in the network infrastructure and digital forensics of its electronic equipments.
Course will function with an after labour schedule, which gives a chance for IT professionals to attend it.
The general organization is based on modules which enables a better articulation of subjects and also the practical works that are proposed. In the first two semesters there will be a course unit for projects where students will do practical works with the subjects covered during each semester in the other unit courses.

In internship, project and dissertation we aim to develop procedures that may leverage the links with the companies of our region, namely in the implementation of solutions in their IT and services infrastructures.

The course also features highly qualified lecturers with PhD or "Título de Especialista", as well as the material resources adequate to the normal functioning.