NCE/18/1800154 — Apresentação do pedido - Novo ciclo de estudos

1. Caracterização geral do ciclo de estudos

1.1. Instituição de Ensino Superior:
Instituto Politécnico De Viana Do Castelo

1.1.a. Outra(s) Instituição(ões) de Ensino Superior (proposta em associação):

1.2. Unidade orgânica (faculdade, escola, instituto, etc.):
Escola Superior De Tecnologia E Gestão De Viana Do Castelo

1.2.a. Outra(s) unidade(s) orgânica(s) (faculdade, escola, instituto, etc.) (proposta em associação):

1.3. Designação do ciclo de estudos:
Cibersegurança

1.3. Study programme:
Cybersecurity

1.4. Grau:
Mestre

1.5. Área científica predominante do ciclo de estudos:
Ciência de Computadores

1.5. Main scientific area of the study programme:
Computer Science

1.6.1 Classificação CNAEF – primeira área fundamental, de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF-3 dígitos):
481

1.6.2 Classificação CNAEF – segunda área fundamental, de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF-3 dígitos), se aplicável:
523

1.6.3 Classificação CNAEF – terceira área fundamental, de acordo com a Portaria n.º 256/2005, de 16 de Março (CNAEF-3 dígitos), se aplicável:
<sem resposta>

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

1.8. Duração do ciclo de estudos (art.º 3 DL n.º 74/2006, de 24 de março, com a redação do DL n.º 63/2016 de 13 de setembro):
4 semestres

1.8. Duration of the study programme (article 3, DL no. 74/2006, March 24th, as written in the DL no. 63/2016, of September 13th):
4 semesters

1.9. Número máximo de admissões:
30

1.10. Condições específicas de ingresso.
O acesso ao Mestrado em Cibersegurança está condicionado a:
- Detentores de curso superior de 1º ciclo (licenciatura) na área da Engenharia Informática ou Eletrotécnica, Ciências Informáticas/Computação ou áreas afins tais como informática, telecomunicações, redes de computadores ou de comunicação, sistemas, tecnologias de Informação, eletrónica ou multimédia;
- Detentores de um currículo académico, científico ou profissional, que seja reconhecido pela Comissão Técnico-Científica como atestando capacidade para realização deste ciclo de estudos;
- Titulares de um grau académico superior estrangeiro conferido na sequência de um 1º ciclo de estudos organizados de acordo com os princípios do Processo de Bolonha por um Estado aderente a este processo ou cujo grau académico superior estrangeiro que seja reconhecido como satisfazendo os objectivos do grau de licenciado pela Comissão Técnico-Científica;

1.10. Specific entry requirements.
The requirements to access the Master in Cyber Security are the following:
- Holders of a graduation in the area of Informatics or Electrotechnical Engineering, Computer Science / Computing or related areas such as Informatics, Telecommunications, Computer or communication Networks, Information Systems and Technologies, Electronics or Multimedia;
- Holders of an academic, scientific or professional curriculum that is recognized by the Technical-Scientific Committee as attesting capacity to carry out this cycle of studies;
- Holders of a foreign higher academic degree awarded following a first cycle of studies organized according to the principles of the Bologna Process by a State adhering to this process or whose foreign higher academic degree is recognized as meeting the objectives of a graduation by the Technical-Scientific Committee;

1.11. Regime de funcionamento.
Pós Laboral

1.11.1. Se outro, especifique:
<sem resposta>

1.11.1. If other, specify:
<no answer>

1.12. Local onde o ciclo de estudos será ministrado:
Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Viana do Castelo
Avenida do Atlântico, n.º 644
4900-348 Viana do Castelo

1.12. Premises where the study programme will be lectured:
Escola Superior de Tecnologia e Gestão
Instituto Politécnico de Viana do Castelo
Avenida do Atlântico, n.º 644
4900-348 Viana do Castelo

1.13. Regulamento de creditação de formação académica e de experiência profissional (PDF, máx. 500kB):
1.13._Desp 4872 2016 Revisao Reg Creditacao Competencias.pdf
1.14. Observações:
Nada a assinalar.

1.14. Observations:
Nothing to report.

2. Formalização do Pedido

Mapa I - Direção da ESTG - UO

2.1.1. Órgão ouvido:
Direção da ESTG - UO

2.1.2. Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada (PDF, máx. 100kB):
2.1.2._Parecer-Direção.pdf

Mapa I - Conselho Técnico-Científico

2.1.1. Órgão ouvido:
Conselho Técnico-Científico

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

Mapa I - Presidência IPVC

2.1.1. Órgão ouvido:
Presidência IPVC

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

Mapa I - Área Científica de Electrotecnia e Informática

2.1.1. Órgão ouvido:
Área Científica de Electrotecnia e Informática

2.1.2. Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada (PDF, máx. 100kB):
2.1.2._PARECER-ACEI.pdf

Mapa I - Conselho Pedagógico

2.1.1. Órgão ouvido:
Conselho Pedagógico

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

Mapa I - Empresa - WaveCom

2.1.1. Órgão ouvido:
Empresa - WaveCom

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

Mapa I - Empresa - Guiatel

2.1.1. Órgão ouvido:
Empresa - Guiatel

2.1.2. Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada (PDF, máx. 100kB):
2.1.2._Parecer-Guiatel.pdf

Mapa I - Empresa - Wemake

2.1.1. Órgão ouvido:
Empresa - Wemake

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

2.1.2._parecer-wemake.pdf

3. Âmbito e objetivos do ciclo de estudos. Adequação ao projeto educativo, científico e cultural da instituição

3.1. Objetivos gerais definidos para o ciclo de estudos:

O Mestrado em Cibersegurança visa a formação avançada de profissionais e investigadores na área da segurança de redes, sistemas e informação. Neste ciclo de estudos pretende-se dotar os estudantes de conhecimentos técnicos na área da cibersegurança nos domínios da prevenção, deteção, mitigação e análise forense de ataques informáticos e de competências para a gestão de segurança das redes, sistemas e informação, e realização de auditorias de segurança informática.

O ciclos de estudos permite correlacionar os diversos aspetos técnicos, científicos e sociais da cibersegurança, possibilitando que os estudantes desenvolvam e definam soluções eficazes e sustentáveis para os diversos riscos e ciberameaças. Desta forma, contribui-se assim para o desenvolvimento de estratégias sustentáveis de defesa digital e para a segurança das organizações e dos cidadãos.

3.1. The study programme's generic objectives:

The Master in Cybersecurity aims at the advanced training of professionals and researchers in the area of network, systems and information security. This study programme aims to provide students with technical knowledge in the area of cybersecurity in the domains of prevention, detection, mitigation and forensic analysis of computer attacks and skills for the management of network, systems and information security, and conducting audits of systems security.

This study programme allow to correlate the multiple technical, scientific and social aspects of cybersecurity, enabling students to develop and define effective and sustainable solutions to the various security risks and cyber threats. In this way, it contributes to the development of sustainable digital defense strategies and to the security of organizations and citizens.

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

Conhecimentos:
- Dominar técnicas de segurança no software, sistemas, redes e informação
- Conhecer técnicas administração segura de sistemas e redes
- Conhecer a regulamentação na área da privacidade e proteção de dados pessoais ou sensíveis
- Conhecer os principais avanços na área da segurança de redes, sistemas e informação
Aptidões:
- Saber projetar, implementar e gerir os mecanismos de segurança de acordo com a análise de risco
- Saber implementar mecanismos para a segurança das redes, sistemas e da informação
- Saber compreender e resolver problemas relacionados com a prevenção e mitigação de ataques informáticos
Competências:
- Conceber e administrar sistemas e redes num contexto de cenários com ciberameaças
- Realizar auditorias de segurança de informação
- Recomendar soluções tecnológicas para a salvaguarda de dados sensíveis consoante o enquadramento legal aplicável
- Comunicar e interagir com equipas de trabalho e especificar soluções para os desafios encontrados

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

Knowledges:
- Mastering security techniques in software, systems, networks and information
- Know the techniques of safe administration of systems and networks
- Know the rules in the area of privacy and protection of personal or sensitive data
- Know the main advances in the area of the security of networks, systems and information
Skills:
- Know how to design, implement and manage security mechanisms according to the risk analysis
- Know how to implement mechanisms for the security of networks, systems and information
- Understand and solve problems related to the prevention and mitigation of computer attacks
Competences:
- Design and manage systems and networks in a context of cyber-threatened scenarios
- Conduct information security audits
- Recommend technological solutions to protect sensitive data according to the applicable legal framework.
- Communicate and interact with work teams specifying solutions to the challenges encountered

3.3. Inserção do ciclo de estudos na estratégia institucional de oferta formativa, face à missão institucional e, designadamente, ao projeto educativo, científico e cultural da instituição:

O IPVC promove a formação integral dos seus estudantes ao longo da vida, combinando ensino com investigação, numa atitude pró-ativa de permanente inovação, cooperação e compromisso, centrado no desenvolvimento da região e do país, e na internacionalização. Desde a sua génese, o IPVC é uma instituição empenhada na internacionalização através da partilha de conhecimento, pela investigação e formação, mobilidade, sendo reconhecida na cooperação internacional, em particular com a Comunidade dos Países de Língua Portuguesa.
A oferta formativa do IPVC pretende ser diversificada, inovadora, profissionalizante, global e versátil, em plena articulação com a investigação aplicada e em permanente compromisso com a região e o país. Em particular, este CE vem preencher uma lacuna nesta área de formação e assim permitir um maior ajustamento do projeto educativo e científico do IPVC aos desígnios da região em que se insere. Neste contexto, é de assinalar que este mestrado será uma potencial aposta para os estudantes já licenciados que pretendam seguir a área da cibersegurança, uma vez que não existe esta oferta similar (do mesmo grau académico) num raio de 80km. Além disso, este ciclo de estudos é direcionado para o desenvolvimento do tecido empresarial da região através da consciencialização e formação avançada nas mais variadas áreas incluídas na cibersegurança que servem de base à atividade económica dos atuais agentes produtivos da região.
Do ponto de vista da dinâmica interna da oferta formativa do IPVC, é de notar que a aposta nesta área de formação por parte do IPVC tomou forma há alguns anos pela inclusão de algumas unidades curriculares de segurança de redes e sistemas em algumas licenciaturas e, neste momento, os estudantes destes cursos já mostram interesse em prosseguir estudos nesta área.
Além disso, nos últimos dois anos letivos, foi realizada uma parceria com o Instituto Politécnico de Leiria, a Procuradoria Geral da República e com a Polícia Judiciária para a realização de duas edições de uma Pós-graduação em Informática de Segurança e Computação Forense. Estas parcerias estratégicas e a formação de pós-graduação nesta área da cibersegurança, permitiram realizar vários projetos de fim de curso cujos resultados foram aplicados diretamente pelas empresas, submeter várias publicações para conferências nacionais e internacionais com peer-review e realizar 3 seminários de Cibersegurança e Cibercrime (dois deles em 2017 e um deles em 2018) com mais de 200 participantes cada, contando com oradores de elevado prestígio na área e participação de entidades como o Centro Nacional de Cibersegurança, a Polícia Judiciária, a PT, Multicert, Farfetch, Pplware, etc. Além disso, em 2017 foram formadas 3 academias profissionais (Academia Cisco, RedHat e Palo Alto Networks) que permite oferecer aos estudantes percursos de certificação profissional na área da segurança de redes e sistemas e permite aos docentes a atualização contínua das suas competências.

3.3. Insertion of the study programme in the institutional educational offer strategy, in light of the mission of the institution and its educational, scientific and cultural project:

The IPVC promotes the integral formation of its students throughout life, combining teaching with investigation, in a proactive attitude of permanent innovation, cooperation and commitment, centered in the development of the region and the country, and in the internationalization. Since the beginning, the IPVC is an institution committed to internationalization through knowledge sharing, research and training, mobility, and is recognized in international cooperation, in particular with the "Comunidade dos Países de Língua Portuguesa".
The graduations offered by IPVC aim to be diversified, innovative, professional, global and versatile, in full articulation with applied research and in permanent commitment to the region and the country. In particular, this study programme (SP) will fill a gap in this area of training and thus allow a greater adjustment of the educational and scientific project of IPVC to the purposes of the region in which it is located. In this context, this master's degree will be a potential option for students who are already graduated and want to follow the area of cybersecurity, since there is no similar offer (of the same academic degree) within a 80km radius. In addition, this SP is directed to the development of the business fabric of the region through awareness and advanced training in the most varied areas included in the cybersecurity that serve as a basis for the economic activity of the region's current productive agents.
From the point of view of the internal dynamics of the IPVC training offer, it should be noted that the IPVC's commitment to this area of formation has taken shape some years ago by the inclusion of some curricular units of network and system security in some degree programs and, at this moment, their students already show interest in continuing studies in this area.
In addition, in the last two academic years, a partnership was established with the Leiria Polytechnic Institute, the Attorney General's Office and the Polícia Judiciária to offer two editions of a Postgraduate Computer Science in Security and Computer Forensics. These strategic partnerships and postgraduate training in this area of cybersecurity allowed several end-of-course projects to be implemented directly by companies, allowed several publications to national and international conferences with peer-review, the realization of 3 seminars of Cybersecurity and Cybercrime (two of them in 2017 and one in 2018) with more than 200 participants each, counting on speakers of high prestige in the area and participation of entities such as the National Center for Cybersecurity, the Judiciary Police, PT, Multicert, Farfetch, Pplware , etc. In addition, in 2017, 3 professional academies (Cisco Academy, RedHat and Palo Alto Networks) were formed to provide students with professional certification courses in the area of network and systems security and allow teachers to continuously update their skills.

4. Desenvolvimento curricular

4.1. Ramos, opções, perfis, maior/menor ou outras formas de organização em que o ciclo de estudos se

estrutura (a preencher apenas quando aplicável)

4.1. Ramos, opções, perfis, maior/menor ou outras formas de organização em que o ciclo de estudos se estrutura (a preencher apenas quando aplicável) / Branches, options, profiles, major/minor or other forms of organisation (if applicable)

Ramos, opções, perfis, maior/menor ou outras formas de organização em que o ciclo de estudos se estrutura:	Branches, options, profiles, major/minor or other forms of organisation:
Plano de estudos sem ramos ou opções	Study plan without branches or options

4.2. Estrutura curricular (a repetir para cada um dos percursos alternativos)

Mapa II - Não aplicável

4.2.1. Ramo, opção, perfil, maior/menor ou outra (se aplicável):
Não aplicável

4.2.1. Branch, option, profile, major/minor or other (if applicable):
Not applicable

4.2.2. Áreas científicas e créditos necessários à obtenção do grau / Scientific areas and credits necessary for awarding the degree

Área Científica / Scientific Area	Sigla / Acronym	ECTS Obrigatórios / Mandatory ECTS	ECTS Minímos optativos* / Minimum Optional ECTS*	Observações / Observations
Ciência de Computadores e Telecomunicações / Computer Science and Telecommunications	CCT/CST	120	0	
(1 Item)		**120**	**0**	

4.3 Plano de estudos

Mapa III - Não aplicável - Ano 1 / Semestre 1

4.3.1. Ramo, opção, perfil, maior/menor ou outra (se aplicável):
Não aplicável

4.3.1. Branch, option, profile, major/minor or other (if applicable):
Not applicable

4.3.2. Ano/semestre/trimestre curricular:
Ano 1 / Semestre 1

4.3.3 Plano de Estudos / Study plan

Unidade Curricular / Curricular Unit	Área Científica / Scientific Area (1)	Duração / Duration (2)	Horas Trabalho / Working Hours (3)	Horas Contacto / Contact Hours (4)	ECTS	Observações / Observations (5)
Criptografia Aplicada / Applied Cryptography	CCT/CST	Semestral	135	TP-16; PL-16	5	
Segurança de Redes e Sistemas / Networks and Systems Security	CCT/CST	Semestral	135	TP-16; PL-16	5	
Gestão da Segurança da Informação / Information Security Management	CCT/CST	Semestral	135	TP-32	5	
Segurança no Software / Software Security	CCT/CST	Semestral	135	TP-16; PL-16	5	

Segurança de Sistemas Ciberfísicos / Cyber-Physical Systems Security	CCT/CST	Semestral	108	TP-16; PL-8	4
Estratégias de Defesa na Administração de Sistemas / Defense Strategies in Systems Administration	CCT/CST	Semestral	162	TP-16; PL-24	6

(6 Items)

Mapa III - Não aplicável - Ano 1 / Semestre 2

4.3.1. Ramo, opção, perfil, maior/menor ou outra (se aplicável):
Não aplicável

4.3.1. Branch, option, profile, major/minor or other (if applicable):
Not applicable

4.3.2. Ano/semestre/trimestre curricular:
Ano 1 / Semestre 2

4.3.3 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)
Hacking Ético / Ethical Hacking	CCT/CST	Semestral	162	TP-20; PL-28	6	
Privacidade e Proteção de Dados / Privacy and Data Protection	CCT/CST	Semestral	81	TP-16	3	
Engenharia Social / Social Enginneering	CCT/CST	Semestral	81	TP-8; PL-8	3	
Gestão de Identidade Digital / Digital Identity Management	CCT/CST	Semestral	81	TP-8; PL-8	3	
Análise de Dados e CiberInteligência / CyberIntelligence and Data Analytics	CCT/CST	Semestral	135	TP-16; PL-16	5	
Auditoria e Conformidade em Cibersegurança / Cybersecurity Audit and Compliance	CCT/CST	Semestral	108	TP-16; PL-8	4	
Cibercrime e Análise Forense Digital / Cybercrime and Digital Forensics Analysis	CCT/CST	Semestral	162	TP-24; PL-16	6	

(7 Items)

Mapa III - Não aplicável - Ano 2 / Semestre 1

4.3.1. Ramo, opção, perfil, maior/menor ou outra (se aplicável):
Não aplicável

4.3.1. Branch, option, profile, major/minor or other (if applicable):
Not applicable

4.3.2. Ano/semestre/trimestre curricular:
Ano 2 / Semestre 1

4.3.3 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)

Metodologias de Investigação e Gestão de Projetos / Research Methodologies and Project Management	CCT/CST	Semestral	81	TP-8; PL-8	3

(1 Item)

Mapa III - Não aplicável - Ano 2 / Anual

4.3.1. Ramo, opção, perfil, maior/menor ou outra (se aplicável):
Não aplicável

4.3.1. Branch, option, profile, major/minor or other (if applicable):
Not applicable

4.3.2. Ano/semestre/trimestre curricular:
Ano 2 / Anual

4.3.3 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)
Dissertação/Projeto/Estágio / Dissertation/Project/Internship	CCT/CST	Anual	1539	OT-40	57	

(1 Item)

4.4. Unidades Curriculares

Mapa IV - Criptografia Aplicada

4.4.1.1. Designação da unidade curricular:
Criptografia Aplicada

4.4.1.1. Title of curricular unit:
Applied Cryptography

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
135

4.4.1.4. Horas de trabalho:
103

4.4.1.5. Horas de contacto:
32

4.4.1.6. ECTS:
5

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:

<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Luís Barreto; TP-16; PL-16

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Com esta UC espera-se os alunos estejam preparados para:
A. Poderem escolher que algoritmos e técnicas utilizar, seja ao nível de utilizadores, programadores ou administradores de redes e sistemas.
B. Analisar, modificar, escolher e implementar os protocolos necessários para a uma aplicação prática.
C. Implementar os algoritmos criptográficos dados.
D. Implementar ataques aos mesmos algoritmos e protocolos
E. Familiaridade com desafios científicos em segurança da informação.
F. Saber aplicar provas de segurança e capacidade de pensar abstratamente sobre problemas de segurança da informação.
G. Entender a utilização e a operação de uma variedade de mecanismos de controle de acesso e autenticação de usuários.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
With this course students are expected to be prepared to:
A. Choose which algorithms and techniques to use, regarding being level of users, programmers or network and system administrators.
B. Analyze, modify, choose and implement the necessary protocols for a practical application.
C. Implement the data cryptographic algorithms.
D. Implement attacks against the same algorithms and protocols.
E. Be conscious of the scientific challenges in information security.
F. Know how to apply security evidence and ability to think abstractly about information security issues.
G. Understand the use and operation of a variety of user access and authentication control mechanisms.

4.4.5. Conteúdos programáticos:
1- Fundamentos de Segurança e Criptografia
2- Criptografia Simétrica
3- Cifras de Blocos e de Fluxo
4- Criptografia Assimétrica
5- Funções Hash function, Autenticação de Mensagem
6- Infraestruturas de Chave Pública
7- Criptografia para reforço da privacidade
8- Criptografia na Cloud
9- Aplicações da Criptografia

4.4.5. Syllabus:

1- Fundamentals of Security and Encryption
2- Symmetric Encryption
3- Block and Flow Ciphers
4- Asymmetric Cryptography
5- Hash functions, Message Authentication
6- Public Key Infrastructures
7- Privacy-enhancement Encryption
8- Cloud cryptography
9- Cryptography Applications

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Os seguintes conteúdos programáticos são mapeados com os seguintes objetivos da aprendizagem:
(Conteúdos: Objetivos)
1, 2, 3, 4: A, B, C, D, E,F, G

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
The following syllabus are mapped with the following learning objectives:

(Contents: Objectives)
1, 2, 3, 4: A, B, C, D, E, F, G

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.5*CT +0.5*CP*
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by the average of a theoretical component (TC) and a practical component (PC) with the following weighting:
*CG = 0.5 * TC + 0.5 * PC*
CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
O perfil de formação dos futuros Mestres por este Ciclo de Estudos conduzirá a profissionais qualificados, detentores de conhecimentos, capacidades e competências na sua área de formação. Nesse sentido, e com vista à operacionalização dos objetivos da Unidade Curricular em referência, as metodologias adotadas, baseadas em aulas teóricas e práticas, articuladas com práticas interrogativas apelam a participação dos alunos (de forma escrita e orais), individualmente ou em grupo, permitindo aos alunos adquirir conhecimentos relacionados com a aplicação da Criptografia e do conhecimento das suas teorias fundamentais, que permitem uma a seleção dos melhores modelos e comportamentos em termos de criptografia. Por outro lado, com a resolução de casos práticos, permite aos alunos adquirir conhecimentos relacionados com a implementação e conhecimento de novas técnicas no âmbito da criptografia aplicada.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The profile of future graduates of this cycle of studies will lead to qualified professionals, holders of knowledge, skills and competences in their area of formation. In this sense, and with a view to the operationalization of the objectives of the Curricular Unit in question, the methodologies adopted, based on theoretical and practical classes, articulated with interrogative practices call for the participation of the students (written and oral), individually or in groups, allowing students to acquire knowledge related to the application of Cryptography and the knowledge of their fundamental theories, which allow a selection of the best models and behaviors in terms of cryptography. On the other hand, the resolution of practical cases allows students to acquire knowledge related to the implementation and knowledge of new technical notions in the scope of applied cryptography.

4.4.9. Bibliografia de consulta/existência obrigatória:
[1] Oded Goldreich; Foundations of cryptography , Cambridge university press
[2] William Stallings; Cryptography and Network Security: Principles and Practice (7th Edition)
[3] M. Bellare and S. Goldwasser ; Lecture Notes on Cryptography
[4] Mihir Bellare and Phillip Rogaway ; Introduction to Modern Cry ptography
[5] André Zúquete; Segurança em Redes Informáticas, Editora FCA

Mapa IV - Segurança de Redes e Sistemas

4.4.1.1. Designação da unidade curricular:
Segurança de Redes e Sistemas

4.4.1.1. Title of curricular unit:
Networks and Systems Security

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
135

4.4.1.4. Horas de trabalho:
103

4.4.1.5. Horas de contacto:
32

4.4.1.6. ECTS:
5

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Pinto; TP-16; PL-16

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Conhecimentos:
A- domínio das ferramentas de Autenticação e controlo de acesso
B- domínio dos protolocos de segurança e serviços em redes IP
C- conhecer o funcionamento fundamental de sistemas de firewall
D- conhecer os diferentes tipos de segurança em meios wireless

Aptidões e competências:
E-Desenho, implementação e ensaio experimental de protocolos e serviços de segurança para redes e sistemas de computadores.
F- Implementação de propriedades de segurança para sistemas e aplicações na Internet
G- Implementação de sistemas seguros em redes wireless

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
Knowledge:
A- domain of Authentication and access control tools
B- domain of security protocols and services over IP networks
C- know the fundamental operation of firewall systems
D- know the different types of security in wireless media

Skills and competences:
E-Design, implementation and experimental testing of protocols and security services for computer networks and systems.
F- Implementation of security properties for systems and applications on the Internet
G- Implementation of secure systems in wireless networks

4.4.5. Conteúdos programáticos:
1 - Autenticação e Controlo de acesso
2 - Protocolos de segurança e serviços de segurança em Redes IP

3 - Vulnerabilidades em Redes e Sistemas
4 - Funcionamento de Firewalls
5 - Segurança em Redes Wireless

4.4.5. Syllabus:
1 - Authentication and Access Control
2 - Security protocols and security services in IP networks
3 - Vulnerabilities in Networks and Systems
4 - Firewalls Operation
5 - Security in Wireless Networks

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Do ponto de vista dos objetivos definidos, o objetivo A é garantido com recurso aos conteúdos 1,2,3,4 e 5. Os objetivo B e C são garantidos pelo conteúdo programático 2. O objetivo D é garantido pelo conteúdo 3 e 4. O objetivo E é garantido pelos conteúdos 3,4 e 5. Os objetivos F e G são garantidos pelos conteúdos 3, 4 e 5.

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
From the point of view of the defined objectives, objective A is guaranteed using content 1,2,3,4 and 5. Objectives B and C are guaranteed by the programmatic content 2. Objective D is guaranteed by content 3 and 4. Objective E is guaranteed by contents 3,4 and 5. Objectives F and G are guaranteed by contents 3, 4 and 5.

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demonstrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
CG = 0.5*CT +0.5*CP
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignments will be accomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by the average of a theoretical component (TC) and a practical component (PC) with the following weighting:
CG = 0.5 * TC + 0.5 * PC
PC: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
TC - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
O perfil de formação dos futuros Mestres por este Ciclo de Estudos conduzirá a profissionais qualificados, detentores de conhecimentos, capacidades e competências na sua área de formação. Nesse sentido, e com vista à operacionalização dos objetivos da Unidade Curricular em referência, as metodologias adotadas, baseadas em aulas teóricas e práticas, articuladas com práticas interrogativas apelam a participação dos alunos (de forma escrita e orais), individualmente ou em grupo, permitindo aos alunos adquirir conhecimentos relacionados com a aplicação da segurança em redes e sistemas e do conhecimento das suas teorias fundamentais, que permitem uma a seleção dos melhores modelos e comportamentos em termos de segurança dos dados e o desenho, implementação e ensaio experimental de protocolos e serviços de segurança para redes de computadores e sistemas.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The training profile of future Masters by this Cycle of Studies will lead to qualified professionals, holders of knowledge, skills and competences in their area of formation. In this sense, and with a view to the operationalization of the objectives of the Curricular Unit in question, the methodologies adopted, based on theoretical and practical classes, articulated with interrogative practices call for the participation of the students (written and oral), individually or in

groups, allowing to students to acquire knowledge related to the application of security in networks and systems and the knowledge of their fundamental theories that allow the selection of the best models and behaviors in terms of data security and the design, implementation and experimental testing of protocols and security in computer networks and systems.

4.4.9. Bibliografia de consulta/existência obrigatória:

- Stallings, W. (2017). Network security essentials: Applications and Standards (7th ed.). Harlow, England: Pearson.
- Stallings, W., & Brown, L. (2017). Computer Security: Principles and Practice, Global Edition (4th ed.). Harlow, England: Pearson.
- Gollmann, D. (2011). Computer Security (3rd ed.). Wiley & Sons.

Mapa IV - Gestão da Segurança da Informação

4.4.1.1. Designação da unidade curricular:
Gestão da Segurança da Informação

4.4.1.1. Title of curricular unit:
Information Security Management

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
135

4.4.1.4. Horas de trabalho:
103

4.4.1.5. Horas de contacto:
32

4.4.1.6. ECTS:
5

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Teresa Susana Mendes Pereira Bernardino; TP-32;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta unidade curricular tem por objetivo apresentar a abordagem à Segurança da Informação como um processo de gestão usando, como base principal, a norma ISO/IEC 27001. No final da UC, o aluno deve ser capaz de:
1. Delinear uma estratégia para a Cibersegurança, realçando a visão, a missão e os objetivos, e garantindo o alinhamento com o plano estratégico da organização.
2. Identificar requisitos de segurança específicos dos Sistemas de Informação organizacionais, em todas as fases do seu ciclo de vida.
3. Realizar uma avaliação de risco e delinear os controlos de segurança para mitigar os riscos identificados.
4. Desenvolver políticas de segurança, programas, e guias de implementação, de acordo com normas reconhecidas.
5. Monitorizar e avaliar a eficiência dos controlos de Cibersegurança adotados por uma organização, com o objetivo de garantir que eles proporcionam o nível de segurança desejado.

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

cybersecurity, highlighting vision, mission and objectives, and ensuring alignment with the organization's strategic plan. 2. Identify specific security requirements of Organizational Information Systems at all stages of their life cycle. 3. Conduct a risk assessment and outline security controls to mitigate identified risks. 4. Develop security policies, programs, and implementation guides in accordance with recognized standards. 5. Monitor and evaluate the effectiveness of cybersecurity controls adopted by an organization, to ensure that they provide the desired level of security.

4.4.5. Conteúdos programáticos:

C1 - Conceitos e definições
Segurança da Informação (confidencialidade, integridade e disponibilidade)
Recursos e tipos de recursos (Informação, físicos e software)
Valor e criticidade dos recursos críticos organizacionais
Ameaças e tipo de ameaças (acidentais vs. Deliberadas; internas vs. Externas)
Vulnerabilidades e as suas categorias (fraquezas no SW, HW, físicas, pessoas e procedimentos)
Conceito de politicas de segurança da informação
Identidade, autenticação e privacidade
Conceito de SGSI

C2 - Normas e standards de segurança
A família de normas ISO 27000
NIST SP800

C3 - Gestão do Risco
Modelos de gestão de risco
Processo da gestão do risco
Tratamento do risco
Objetivo dos controlos
Avaliação quantitativa/qualitativa do impacto
Quantificação do valor dos recursos organizacionais

C4 - Políticas e controlos de segurança
Controlo de acessos dos utilizadores
Formação e sensibilização
Controlos de segurança técnicos
Monitorização
Auditoria

4.4.5. Syllabus:

C1 - Concepts and Definitions
Information security (confidentiality, integrity, availability)
Asset, asset types (information, physical, software), asset value.
Threats and type of threats (accidental vs. deliberate; internal vs. external)
Vulnerabilities and their categorization (flaws in SW, HW, physical, people and procedures)
Information security policy concepts
The types, uses and purposes of controls
Identity, authentication and privacy
ISMS concept.

C2 - Security Standards
ISO 27000
NIST SP800

C3 - Risk Management
Risk Management models
Risk management process
Controls objectives
Impact assessment (qualitative/quantitative)
Identifying and accounting for the value of information assets

C4 - Policy and security controls
User access controls
Training and awareness
Technical security controls
Monitoring

Audit

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
O primeiro módulo introduz conceitos e definições utilizados no contexto da cibersegurança com ênfase nas ameaças, vulnerabilidades, recursos criticos da organização, bem como o impacto da eventual ocorrência de um incidente. Estes conteúdos alinham com as competências 1. e 2.

No segundo e terceiro modulos são abordados os sistemas de gestão de segurança. A gestão neste domínio assenta num modelo de Análise de Risco, e é suportada por políticas e controlos de segurança que devem ser adequados aos objetivos da organização e dos recursos que pretende proteger. Estes conteúdos alinham com as competências 2., 3., 4. e parcialmente,1.

O quarto módulo apresenta uma síntese das politicas e controlos de segurança a serem implementados tendo em conta a avaliação de risco realizada. É colocada ênfase na medição da eficiência desses controlos no contexto da Política de Segurança. Estes conteúdos alinham com as competências 3., 4. e 5.

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
The first module introduces concepts and definitions used in the context of cybersecurity with an emphasis on threats, vulnerabilities, critical resources of the organization as well as the impact of the eventual occurrence of an incident. These contents align with skills 1 and 2.

In the second and third modules are addressed the safety management systems. Management in this domain is based on a Risk Analysis model and is supported by security policies and controls that must be appropriate to the organization's objectives and the resources it intends to protect. These contents align with competencies 2., 3., 4. and partially, 1.

The fourth module presents a summary of the policies and safety controls to be implemented taking into account the risk assessment carried out. Emphasis is placed on measuring the effectiveness of such controls in the context of the Security Policy. These contents align with competencies 3., 4. and 5.

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas o programa será apresentado sob a forma de notas ou slides e serão realizados trabalhos para consolidar e demonstrar a aplicação dos conceitos abordados.

A Classificação Global (GC) desta unidade curricular é obtida através de uma componente teórica (CT) e uma participação nas atividades propostas pelas turmas (PA) com a seguinte ponderação:
CG = 0,5 * CT + 0,5 * PA
PA: Realização de atividades propostas. Para aprovação, é necessário ter um mínimo de 8 valores no PA.
CT - Obtido através de um teste ou exame no final do prazo. Para aprovação, é necessário ter uma pontuação mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the classes the program will be presented in the form of notes or slides and work will be done to consolidate and demonstrate the application of the concepts discussed.

The Global Classification (GC) of this curricular unit is obtained through a theoretical component (TC) and a participation in the Proposed Activities (PA) within the classes with the following weighting:
CG = 0.5 * TC + 0.5 * PA
PA: Proposed activities. For approval, it is necessary to have a minimum of 8 values in the AP.
CT - Obtained through a test or examination at the end of the term. For approval, it is necessary to have a minimum score of 8 values in the TC.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Nas aulas teóricas, e em complemento ao método expositivo dos conteúdos programáticos com projecção de elementos
exemplificadores, será ainda adoptada uma complementação ao mesmo através do método activo/demonstrativo.
Nas aulas práticas será adoptado um método totalmente activo, através da disponibilização de diversas fichas de exercícios que
permitirão ao estudante aplicar, na prática, os conhecimentos adquiridos nas aulas teóricas. Estas fichas incluirão sempre uma
pequena descrição dos objectivos a atingir, da matéria que se pretende abordar, exemplos e exercícios, dispostos em crecendo de
dificuldade, a resolver autonomamente ou em grupo pelo estudante, devidamente acompanhados pelo docente.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
In the lectures, and in addition to the expositive method of the syllabus with projection of sample elements, it will be adopted the active / demonstrative method. In practical classes it will be adopted a fully active method, by providing various forms of assignments that will allow students to apply in practice the knowledge acquired in lectures. These assignments will always include a brief description of the objectives to be achieved, the matter that is intended to address, examples and exercises, arranged in increase of difficulty to be solved independently or in groups by the student, duly accompanied by the teacher.

4.4.9. Bibliografia de consulta/existência obrigatória:
- Bishop, M., 2004. Introduction to Computer Security. 2nd ed. Addison-Wesley Professional.
- Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", Fourth Edition, Prentice Hall PTR, 2007.
- Saydjari, O. S. 2004. Cyber defense: art to science. Commun. ACM 47, 3 (Mar. 2004), 52-57. DOI= http://doi.acm.org /10.1145/971617.971645
- Santos, H.D., "A norma das normas em Segurança da Informação," Publicação da Associação Portuguesa para a Qualidade, vol. XXXV, pp. 11-19, Primavera, 2006.
- Vacca, John R., ed. Managing information security. Elsevier, 2013.

Mapa IV - Segurança no Software

4.4.1.1. Designação da unidade curricular:
Segurança no Software

4.4.1.1. Title of curricular unit:
Software Security

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
135

4.4.1.4. Horas de trabalho:
103

4.4.1.5. Horas de contacto:
32

4.4.1.6. ECTS:
5

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Miguel Simões Pinto Carneiro; TP-16;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Sara Paiva; PL-16;

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Com esta unidade curricular pretende-se alargar as competências associadas à segurança no desenvolvimento de

software, sensibilizando os alunos para a importância do potencial impacto a considerar nas várias fases existentes durante o processo de desenvolvimento de software, independentemente da metodologia de projetos aplicada.
Assim, o aluno deverá ser capaz de:
1 - Ser autónomo no desenho de um modelo de análise de ameaças num cenário de caso
2 - Identificar, enumerar e priorizar, com sucesso, as potenciais vulnerabilidades sob um hipotético ponto de vista de um hacker
3 - Ser eficaz na identificação de pontos de entrada (entry points) aquando da programação de software reconhecendo habitualmente as entradas mais desejadas e facilitadoras do ponto de vista de um atacante.
4 - Conhecer as principais considerações OWASP (Open Web Application Security Project) no desenvolvimento de aplicações seguras.
5 - Programar uma aplicação com as técnicas de segurança aprendidas

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This curricular unit aims to broaden the skills associated with security in software development where the students should focus the importance of the potential impact to be considered in the many phases that exist during the software development process, regardless of the applied project methodology.
At the end of this unit the students should be able to:
1 - Design a threat analysis model in a case scenario
2 - Identify, enumerate and prioritize, successfully, potential vulnerabilities under a hypothetical point of view of an hacker
3 - When programming an software aplication it should be able to Identify entry points recognizing the most desired and facilitating entries from an attacker's point of view.
4 - Apply OWASP (Open Web Application Security Project) considerations in the development of secure applications.
5 - Program an software application with learned techniques that are secure related

4.4.5. Conteúdos programáticos:
1 - CONCEITOS
1.1 vulnerabilidades
1.2 ataques
1.3 confiabilidade vs. segurança
2 - MODELOS DE ANÁLISE DE AMEAÇAS
3 - SEGURANÇA E DESENVOLVIMENTO DE SOFTWARE
3.1 processos de desenvolvimento de software seguro
3.1.1 modelo cascata e modelo espiral
3.1.2 microsoft security development lifecycle
3.1.3 segurança no desenvolvimento ágil
3.1.4 verificação e validação – norma IEEE 1012-2012
3.1.5 building security in maturity model
3.1.6 segurança aplicacional – norma ISO/IEC 27034
3.2 segurança durante o projeto
3.2.1 segurança nas linguagens de programação
3.2.2 sandboxes
4. VULNERABILIDADES
4.1 Buffers overflow
4.2 Race conditions
4.3 Validação de entradas
4.4 Ficheiros de inclusão local/remota
5. APLICAÇÕES WEB
5.1 top 10 OWASP
5.2 Análise de vulnerabilidades e mitigação
6. APLICAÇÕES MÓVEIS
6.1 top 10 de vulnerabilidades em aplicações móveis
6.2 Técnicas de análise de vulnerabilidades e de mitigação
6.3 Conceção de uma aplicação segura
7. AUDITORIA E TESTES DE SEGURANÇA AO SOFTWARE

4.4.5. Syllabus:
1 - CONCEPTS
1.1 vulnerabilities
1.2 attacks
1.3 reliability vs. safety
2 - THREAT ANALYSIS MODELS
3 - SOFTWARE SECURITY AND DEVELOPMENT
3.1 Secure Software Development Processes
3.1.1 cascade model and spiral model

3.1.2 microsoft security development lifecycle
3.1.3 security in agile development
3.1.4 verification and validation - IEEE 1012-2012 standard
3.1.5 building security in maturity model
3.1.6 application security - ISO / IEC 27034
3.2 security by design
3.2.1 programming languages security concepts
3.2.2 sandboxes
4. VULNERABILITIES
4.1 Buffers overflow
4.2 Race conditions
4.3 Entries validations
4.4 Local / Remote File Inclusions
5. WEB APPLICATIONS
5.1 top 10 OWASP
5.2 Vulnerability and mitigation analysis
6. MOBILE APPLICATIONS
6.1 top 10 vulnerabilities in mobile applications
6.2 Vulnerability and mitigation analysis techniques
6.3 Designing an secure application
7. SOFTWARE AUDIT AND SECURITY TESTS

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
1 - Ser autónomo no desenho de um modelo de análise de ameaças num cenário de caso: 1+2
2 - Identificar, enumerar e priorizar, com sucesso, as potenciais vulnerabilidades sob um hipotético ponto de vista de um hacker 1+2+3
3 - Ser eficaz na identificação de pontos de entrada (entry points) aquando da programação de software reconhecendo habitualmente as entradas mais desejadas e facilitadoras do ponto de vista de um atacante.1+3+4
4 - Conhecer as principais considerações OWASP (Open Web Application Security Project) no desenvolvimento de aplicações seguras: 1+2+3+4+5+6
5 - Programar uma aplicação com as técnicas de segurnça aprendidas: 6+7

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
1 - Design a threat analysis model in a case scenario: 1+2
2 - Identify, enumerate and prioritize, successfully, potential vulnerabilities under a hypothetical point of view of an hacker: 1+2+3
3 - When programming an software aplication it should be able to Identify entry points recognizing the most desired and facilitating entries from an attacker's point of view: 1+3+4
4 - Apply OWASP (Open Web Application Security Project) considerations in the development of secure applications: 1+2+3+4+5+6
5 - Program an software application with learned techniques that are secure related: 6+7

4.4.7. Metodologias de ensino (avaliação incluída):
As aulas incluem sessões teóricas, discussões dirigidas e sessões de carácter prático com demonstração de casos temáticos relacionados com situações ocorridas quando a segurança no software não é considerada.
– Nas sessões teóricas será utilizado o método expositivo.
– As discussões dirigidas serão orientadas para o estudo de casos.
– As sessões de carácter prático incluem a resolução de casos práticos destinados a permitir validar as competências adquiridas.

Avaliação contínua:
- Teste escrito (40%)
- Trabalhos práticos (60%)
Exame final: Exame teórico-prático (100%)

4.4.7. Teaching methodologies (including students' assessment):
This curricular unit include theoretical sessions, guided discussions and practical sessions for demonstration of thematic cases related to situations that occurred when security in the software is not considered.
– In theoretical sessions we'll use the expository method.
– Targeted discussions will focus on case studies.
– Practical sessions include the resolution of practical cases to enable the skills acquired to be validated.

Continuous evaluation:
- Written test (40%)

- Practical work (60%)
Final exam: Theoretical-practical exam (100%)

4.4.8. 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 uma vez que:
1) Os métodos de ensino utilizados ajustam-se à natureza dos conteúdos programáticos e aos objetivos a atingir em cada sessão.
A realização de exposições sobre as diferentes matérias conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos
2) As metodologias de ensino adotadas procuram potenciar a participação ativa dos alunos e a transmissão metódica e rigorosa dos diferentes saberes
3) Competências complementares como sejam o trabalho em equipa, comunicação escrita e verbal serão também exploradas no âmbito desta unidade curricular.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
Teaching methodologies are compliance with the objectives of this curricular unit because:
1) Teaching methods used fit the nature of the syllabus and objectives to be achieved in each session.
The presentation of expositions on the different subjects is conjugated with the methodology of evaluation established, thus allowing to reach the objectives defined
2) Teaching methodologies adopted seek to foster the active participation of the students and the methodical and rigorous transmission of different knowledge
3) Complementary skills such as teamwork, written and verbal communication will also be explored within this curricular unit.

4.4.9. Bibliografia de consulta/existência obrigatória:
Correia, M. Sousa, P. (2017) Segurança no Software. 2ª Ed. Lisboa, Portugal: FCA.
OWASP. (2017). Open Web Application Security Project. Retrieved from: https://www.owasp.org/index.php/Main_Page

Mapa IV - Segurança de Sistemas Ciberfísicos

4.4.1.1. Designação da unidade curricular:
Segurança de Sistemas Ciberfísicos

4.4.1.1. Title of curricular unit:
Cyber-Physical Systems Security

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
108

4.4.1.4. Horas de trabalho:
84

4.4.1.5. Horas de contacto:
24

4.4.1.6. ECTS:
4

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):

Sérgio Lopes; TP-16; PL-8;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Com esta unidade curricular pretende-se alargar as competências associadas à segurança no desenvolvimento de software, sensibilizando os alunos para a importância do potencial impacto a considerar nas várias fases existentes durante o processo de desenvolvimento de software, independentemente da metodologia de projetos aplicada.
Assim, o aluno deverá ser capaz de:
1 - Ser autónomo no desenho de um modelo de análise de ameaças num cenário de caso
2 - Identificar, enumerar e priorizar, com sucesso, as potenciais vulnerabilidades sob um hipotético ponto de vista de um hacker
3 - Ser eficaz na identificação de pontos de entrada (entry points) aquando da programação de software reconhecendo habitualmente as entradas mais desejadas e facilitadoras do ponto de vista de um atacante.
4 - Conhecer as principais considerações OWASP (Open Web Application Security Project) no desenvolvimento de aplicações seguras.
5 - Programar uma aplicação com as técnicas de segurnça aprendidas

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This curricular unit aims to broaden the skills associated with security in software development where the students should focus the importance of the potential impact to be considered in the many phases that exist during the software development process, regardless of the applied project methodology.
At the end of this unit the students should be able to:
1 - Design a threat analysis model in a case scenario
2 - Identify, enumerate and prioritize, successfully, potential vulnerabilities under a hypothetical point of view of an hacker
3 - When programming an software aplication it should be able to Identify entry points recognizing the most desired and facilitating entries from an attacker's point of view.
4 - Apply OWASP (Open Web Application Security Project) considerations in the development of secure applications.
5 - Program an software application with learned techniques that are secure related

4.4.5. Conteúdos programáticos:
1 - CONCEITOS
1.1 vulnerabilidades
1.2 ataques
1.3 confiabilidade vs. segurança
2 - MODELOS DE ANÁLISE DE AMEAÇAS
3 - SEGURANÇA E DESENVOLVIMENTO DE SOFTWARE
3.1 processos de desenvolvimento de software seguro
3.1.1 modelo cascata e modelo espiral
3.1.2 microsoft security development lifecycle
3.1.3 segurança no desenvolvimento ágil
3.1.4 verificação e validação – norma IEEE 1012-2012
3.1.5 building security in maturity model
3.1.6 segurança aplicacional – norma ISO/IEC 27034
3.2 segurança durante o projeto
3.2.1 segurança nas linguagens de programação
3.2.2 sandboxes
4. VULNERABILIDADES
4.1 Buffers overflow
4.2 Race conditions
4.3 Validação de entradas
4.4 Ficheiros de inclusão local/remota
5. APLICAÇÕES WEB
5.1 top 10 OWASP
5.2 Análise de vulnerabilidades e mitigação
6. APLICAÇÕES MÓVEIS
6.1 top 10 de vulnerabilidades em aplicações móveis
6.2 Técnicas de análise de vulnerabilidades e de mitigação
6.3 Conceção de uma aplicação segura
7. AUDITORIA E TESTES DE SEGURANÇA AO SOFTWARE

4.4.5. Syllabus:
1 - CONCEPTS

1.1 vulnerabilities
1.2 attacks
1.3 reliability vs. safety
2 - THREAT ANALYSIS MODELS
3 - SOFTWARE SECURITY AND DEVELOPMENT
3.1 Secure Software Development Processes
3.1.1 cascade model and spiral model
3.1.2 microsoft security development lifecycle
3.1.3 security in agile development
3.1.4 verification and validation - IEEE 1012-2012 standard
3.1.5 building security in maturity model
3.1.6 application security - ISO / IEC 27034
3.2 security by design
3.2.1 programming languages security concepts
3.2.2 sandboxes
4. VULNERABILITIES
4.1 Buffers overflow
4.2 Race conditions
4.3 Entries validations
4.4 Local / Remote File Inclusions
5. WEB APPLICATIONS
5.1 top 10 OWASP
5.2 Vulnerability and mitigation analysis
6. MOBILE APPLICATIONS
6.1 top 10 vulnerabilities in mobile applications
6.2 Vulnerability and mitigation analysis techniques
6.3 Designing an secure application
7. SOFTWARE AUDIT AND SECURITY TESTS

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
1 - Ser autónomo no desenho de um modelo de análise de ameaças num cenário de caso: 1+2
2 - Identificar, enumerar e priorizar, com sucesso, as potenciais vulnerabilidades sob um hipotético ponto de vista de um hacker 1+2+3
3 - Ser eficaz na identificação de pontos de entrada (entry points) aquando da programação de software reconhecendo habitualmente as entradas mais desejadas e facilitadoras do ponto de vista de um atacante.1+3+4
4 - Conhecer as principais considerações OWASP (Open Web Application Security Project) no desenvolvimento de aplicações seguras: 1+2+3+4+5+6
5 - Programar uma aplicação com as técnicas de segurnça aprendidas: 6+7

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
1 - Design a threat analysis model in a case scenario: 1+2
2 - Identify, enumerate and prioritize, successfully, potential vulnerabilities under a hypothetical point of view of an hacker: 1+2+3
3 - When programming an software aplication it should be able to Identify entry points recognizing the most desired and facilitating entries from an attacker's point of view: 1+3+4
4 - Apply OWASP (Open Web Application Security Project) considerations in the development of secure applications: 1+2+3+4+5+6
5 - Program an software application with learned techniques that are secure related: 6+7

4.4.7. Metodologias de ensino (avaliação incluída):
As aulas incluem sessões teóricas, discussões dirigidas e sessões de carácter prático com demonstração de casos temáticos relacionados com situações ocorridas quando a segurança no software não é considerada.
– Nas sessões teóricas será utilizado o método expositivo.
– As discussões dirigidas serão orientadas para o estudo de casos.
– As sessões de carácter prático incluem a resolução de casos práticos destinados a permitir validar as competências adquiridas.

Avaliação contínua:
- Teste escrito (40%)
- Trabalhos práticos (60%)
Exame final: Exame teórico-prático (100%)

4.4.7. Teaching methodologies (including students' assessment):
This curricular unit include theoretical sessions, guided discussions and practical sessions for demonstration of

thematic cases related to situations that occurred when security in the software is not considered.
– In theoretical sessions we'll use the expository method.
– Targeted discussions will focus on case studies.
– Practical sessions include the resolution of practical cases to enable the skills acquired to be validated.

Continuous evaluation:
- Written test (40%)
- Practical work (60%)
Final exam: Theoretical-practical exam (100%)

4.4.8. 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 uma vez que:
1) Os métodos de ensino utilizados ajustam-se à natureza dos conteúdos programáticos e aos objetivos a atingir em cada sessão.
A realização de exposições sobre as diferentes matérias conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos
2) As metodologias de ensino adotadas procuram potenciar a participação ativa dos alunos e a transmissão metódica e rigorosa dos diferentes saberes
3) Competências complementares como sejam o trabalho em equipa, comunicação escrita e verbal serão também exploradas no âmbito desta unidade curricular.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
Teaching methodologies are compliance with the objectives of this curricular unit because:
1) Teaching methods used fit the nature of the syllabus and objectives to be achieved in each session.
The presentation of expositions on the different subjects is conjugated with the methodology of evaluation established, thus allowing to reach the objectives defined
2) Teaching methodologies adopted seek to foster the active participation of the students and the methodical and rigorous transmission of different knowledge
3) Complementary skills such as teamwork, written and verbal communication will also be explored within this curricular unit.

4.4.9. Bibliografia de consulta/existência obrigatória:
Correia, M. Sousa, P. (2017) Segurança no Software. 2ª Ed. Lisboa, Portugal: FCA.
OWASP. (2017). Open Web Application Security Project. Retrieved from: https://www.owasp.org/index.php/Main_Page

Mapa IV - Estratégias de Defesa na Administração de Sistemas

4.4.1.1. Designação da unidade curricular:
Estratégias de Defesa na Administração de Sistemas

4.4.1.1. Title of curricular unit:
Defense Strategies in Systems Administration

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
162

4.4.1.4. Horas de trabalho:
122

4.4.1.5. Horas de contacto:
40

4.4.1.6. ECTS:
6

4.4.1.7. Observações:

<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Silvestre Malta; TP-16; PL-24

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta UC pretende que os alunos aprendam técnicas de administração de sistemas que potenciem mais segurança, prevenindo e impedindo que invasores obtenham acesso indevido aos sistemas.
Os alunos irão aprender a melhorar estratégias de defesa aprimorando políticas de segurança, fortalecendo a rede, implementando sensores ativos e aproveitando a inteligência contra ameaças.
Os objetivos:
O1 - Utilização de várias técnicas para impedir que intrusos acedam a dados confidenciais
O2 - Impedir a instalação de malware e respetivas técnicas de deteção
O3 - Evitar que utilizadores do sistema acedam a dados aos quais não estão autorizados
O4 - Técnicas de verificação rápida na deteção serviços de rede maliciosos indevidamente instalados
O5 - Aprender técnicas de segurança transversais a vários sistemas operativos.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This subject is intended for students to learn system administration techniques that enhance security by preventing and preventing intruders from gaining undue access to systems.
Students will learn how to improve defense strategies by improving security policies, strengthening the network, deploying active sensors, and leveraging intelligence against threats.
The goals:
O1 - Use of various techniques to prevent intruders from accessing sensitive data
O2 - Prevent the installation of malware and its detection techniques
O3 - Prevent system users from accessing data they are not authorized to
O4 - Rapid scanning techniques in detecting malicious network services improperly installed
O5 - Learn security techniques across multiple operating systems.

4.4.5. Conteúdos programáticos:
C1 - Fundamentos da administração de sistemas

C2 - Técnicas seguras em ambientes virtuais.

C3 - Proteção de contas
Implementação e técnicas avançadas.

C4 – Implementação e Configuração Avançada de Firewalls e IDS
Estratégias de configuração em diversas plataformas.

C5 – Encriptação e hardening
Configuração em ficheiros, diretório e partições.

C6 – Controlo de acesso discricionário
Configuração e implementacão de ACL's

C7 – Auditoria
Sistemas de auditoria em sistemas físicos, passwords, filesystems e software instalado

C8 – Processo de resposta a incidentes
Criação de processos tipo pré-incidentes, durante e pós-incidentes
Ferramentas e tecnologias associadas, SIEM, SOC

C9 - Exploração de técnicas de defesa a ataques a infraestruturas

4.4.5. Syllabus:
C1 - Fundamentals of System Administration

C2 - Secure techniques in virtual environments.

C3 - Account Protection
implementation and advanced techniques.

C4 - Firewalls and IDS Advanced Implementation and Configuration
Configuration strategies across platforms.

C5 - Encryption and hardening
Configuration in files, directory and partitions.

C6 - Discretionary access control
Configuration and implementation of ACL's

C7 - Audit
Audit systems in physical systems, passwords, filesystems and installed software

C8 - Incident response process
Creation of pre-incident, during and post-incident processes
Related tools and technologies, SIEM, SOC

C9 - Exploitation of defense techniques to attacks on infrastructures

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
O1 - Utilização de várias técnicas para impedir que intrusos acedam a dados confidenciais (C2, C3, C4, C5, C6 e C9)
O2 - Impedir a instalação de malware e respetivas técnicas de deteção (C4, C6 e C7)
O3 - Evitar que utilizadores do sistema acedam a dados aos quais não estão autorizados (C3 e C6)
O4 - Técnicas de verificação rápida na deteção serviços de rede maliciosos indevidamente instalados (C7 e C8)
O5 - Aprender técnicas de segurança transversais a vários sistemas operativos. (C8 e C9)

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
O1 - Use of various techniques to prevent intruders from accessing confidential data (C2, C3, C4, C5, C6 and C9)
O2 - Prevent the installation of malware and its detection techniques (C4, C6 and C7)
O3 - Prevent system users from accessing data to which they are not authorized (C3 and C6)
O4 - Rapid scanning techniques in detecting improperly installed malicious network services (C7 and C8)
O5 - Learn security techniques across multiple operating systems. (C8 and C9)

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
CG = 0.5*CT +0.5*CP
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by the average of a theoretical component (TC) and a practical component (PC) with the following weighting:
CG = 0.5 * TC + 0.5 * PC
CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

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

As metodologias de ensino são coerentes com os objetivos da unidade curricular dado que:

1) a exposição teórica de conceitos e fundamentos permite preparar a realização, por parte dos alunos, de pequenos trabalhos práticos. A exposição da matéria, conjuntamente com os materiais previamente disponibilizados, permitirão aos alunos assimilarem as matérias e realizar o teste teórico da componente teórica da Unidade Curricular.

2) a elaboração de pequenos trabalhos práticos permitirá aos alunos assimilar os conceitos teóricos permitindo igualmente simular em laboratório a administração de sistemas.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The teaching methodologies are coherent with the curricular unit goals as:

1)The theoretical exposition of concepts allows the realization of small practical work by the students.
The exposure of the subject, together with the materials previously available, enable students to assimilate the materials and conduct the written test of the theoretical component of the curricular unit.

2) the development of small practical work will allow students to assimilate the theoretical concepts allowing also to simulate in the laboratory the system administration.

4.4.9. Bibliografia de consulta/existência obrigatória:
[1] Donald Tevault; Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats; Packt
[2] Yuri Diogenes, Erdal Ozkaya; Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics; Packt
[3] Lee Brotherston, Amanda Berlin ; Defensive Security Handbook: Best Practices for Securing Infrastructure; O´Reilly
[4] Richard Bejtlich; The Practice of Network Security Monitoring: Understanding Incident Detection and Response; No Statch Press

Mapa IV - Hacking Ético

4.4.1.1. Designação da unidade curricular:
Hacking Ético

4.4.1.1. Title of curricular unit:
Ethical Hacking

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
162

4.4.1.4. Horas de trabalho:
114

4.4.1.5. Horas de contacto:
48

4.4.1.6. ECTS:
6

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):

António Pinto; TP-20

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Carlos Antunes; PL-28

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
O1.Conhecimento das restrições éticas e legais associadas aos testes de penetração e ethical hacking
O2.Domínio das etapas de desenvolvimento de testes de penetração e apresentação de resultados
O3.Identificação de aplicações/tráfego malicioso na rede
O4.Implementação de aplicações úteis na exploração de falhas
O5.Identificar ameaças e selecionar as medidas para impedir acesso físico a equipamentos e a mitigar ataques de engenharia social
O6.Aplicar as medidas corretivas adequadas à mitigação de falhas de segurança
O7.Identificar e resolver problemas nas aplicações e serviços web
O8.Determinar falhas de segurança em redes móveis, e para implementar soluções de segurança das comunicações
O9. Reforçar as competetências relacionadas com sistemas de IDS/IPS
O10. Reforçar as capacidades dos serviços de autenticação e controlo de acesso
O11. Identificar vulnerabilidades de dispositivos móveis e aplicação de medidas preventivas
O12. Avaliar o risco da utilização de aplicações móveis

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
O1.Ethical policies and legality of activities involving a penetration test
O2.Domain of the stages of penetration tests and final reporting results
O3.Identify the type of applications/malicious traffic, determine vulnerabilities in services and elect the most appropriate exploits
O4.Implement small applications useful in fault operation
O5.Identify threats and select measures to prevent physical access and social engineering attacks
O6.Apply appropriate corrective measures to mitigate security breaches
O7.Identify and solve problems in web applications/services
O8.Determine security flaws in mobile networks and to implementation of mitigation technics
O9.Strengthen the skills of planning and implementation of detection systems / prevent attacks O10.Strengthen planning capabilities and implementation of authentication, access control and traffic analysis O11.Identify vulnerabilities of mobile devices and apply preventive measures
O12.Assess the risk of using mobile applications

4.4.5. Conteúdos programáticos:
C1. Introdução aos conceitos do Ethical hacking
C2. Tipos de ameaças e ataques a redes cabladas e sem fio
C3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN)
C4. Fragilidades protocolares dos s istemas de comunicações móveis
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio
C6. Metodologias para testes de penetração
C7. Caracterização e implementação de ataques contra redes e sistemas móveis
C8. Planeamento de soluções de comunicação segura em redes e sistemas móveis
C9. Identificação e deteção de vulnerabilidades nos sistemas móveis
C10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis

4.4.5. Syllabus:
C1. Ethical hacking concepts
C2. Types of threats and attacks on wired and wireless networks
C3. Protocols and security algorithms in 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN) C4. Protocol weaknesses of mobile communication systems
C5. Confidentiality, privacy and availability technologies in wireless networks
C6. Methodologies for the penetration tests
C7. Characterization and implementation of attacks against networks and mobile systems
C8. Planning of secure communication solutions in mobile networks and systems
C9. Identification and detection of vulnerabilities in mobile systems
C10. Implementation mechanisms and security systems for wireless networks and mobile devices

4.4.6. 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 cabladas e sem fio (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 móveis (O4)
C5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio (O11)
C6. Metodologias para testes de penetração (O7, O8)C7. Caracterização e implementação de ataques contra redes e sistemas móveis (O11)
C8. Planeamento de soluções de comunicação segura em redes e sistemas móveis (O10, 012)
C9. Identificação e deteção de vulnerabilidades nos sistemas móveis (O11)
C10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis (O9)

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
C1. Introduction to the concepts of Ethical hacking (O1, O2)
C2. Types of threats and attacks on wired and wireless networks (O3, O5)
C3. Protocols and security algorithms in 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN) (O5, O6)
C4. protocol weaknesses of mobile communication systems (O4)
C5. confidentiality of technology, privacy and availability in wireless networks (O11)
C6. Methodologies for the penetration tests (O7, O8)
C7. Characterization and implementation of attacks against networks and mobile systems (O11)
C8. Planning of secure communication solutions in mobile networks and systems (O10, O12)
C9. Identification and detection of vulnerabilities in mobile systems (O11)
C10. Implementation mechanisms and security systems for wireless networks and mobile devices (O9)

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.5*CT +0.5*CP*
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by means of a theoretical component (TC) and a practical component (PC) with the following weighting:
*CG = 0.5 * TC + 0.5 * PC*
CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. 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, com vista a 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 componete 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 de exploração de vulnerabilidades adequados, d) realização de testes de penetração, e) mitigação de falhas detetadas e e) escrita de relatório e e) apresentação e defesa do projeto realizado, permitem desenvolver nos estudantes os objetivos (O4, O5, O6, O7, O8, O9, O10, O11, O12)

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The methodology of theoretical and practical teaching is based on the transmission of knowledge about offensive

security for assessment and mitigation of vulnerabilities in ubiquitous systems, networks and applications, in order to give an overview of the exploration and mitigation of failures, taking into account the legal and ethical constraints of activities involving a penetration test. It allows us to develop students skills (O1, O2, O3).

The methodology used in the lab component focuses initially on consolidation of the knowledge acquired in the prevoius component through the implementation of laboratory works (O1, O2, O3) and, at a later stage, in the implemetation of a practical project that includes the following phases: a) study of the proposed scenario, b) identification of flaws and vulnerabilities of the scenario, c) selection of the appropriate exploit mechanisms, d) conducting penetration testing e) mitigation of the detected vulnerabilities e) writing report e) presentation and defense of the implemented project, allowing the students to develop the skills (O4, O5, O6, O7, O8, O9, O10, O11, O12).

4.4.9. Bibliografia de consulta/existência obrigatória:

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
The Hacker Playbook 2: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1512214567; CreateSpace
Independent Publishing Platform, 2015.

Mapa IV - Privacidade e Proteção de Dados

4.4.1.1. Designação da unidade curricular:
Privacidade e Proteção de Dados

4.4.1.1. Title of curricular unit:
Privacy and Data Protection

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
81

4.4.1.4. Horas de trabalho:
65

4.4.1.5. Horas de contacto:
16

4.4.1.6. ECTS:
3

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Carneiro; TP-16

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Nesta unidade curricular pretende-se sensibilizar os alunos para a importância relacionada com a privacidade e

proteção de dados na esfera digital, potenciando os conhecimentos necessários para garantir a segurança de dados das infraestruturas e aplicações ao longo do seu ciclo de vida.
Sendo uma exigência legal, os alunos irão rever as recomendações legais impostas no ambito do Regulamento Geral de Proteção de Dados (RGPD).
No final desta unidade curricular, o aluno deverá:
1 - Sensibilizar e estar consciente da importância da privacidade e proteção de dados pessoais em todo o espectro digital da cadeia de negócio.
2 - Recomendar tecnologia que garanta a segurança adequada ao cumprimento da conformidade legal aplicável aos vários tipos de dados.
3 - Reconhecer potencialidades e limitações da tecnologia a desenvolver e implementar num programa de privacidade para conduzir à avaliação dos dados.
4 - Efetivar um plano de resposta a incidentes de segurança dos dados.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This curricular unit aims to equip students with the importance related to privacy and data protection in the digital sphere, enhancing the knowledge necessary to ensure data security of infrastructures and applications throughout their life cycle.
As a legal requirement, students will review the recommendations imposed by General Data Protection Regulation (GDPR).
At the end of this curricular unit, the student should:
1 - Raise awareness of the importance of privacy and protection of personal data across the digital spectrum of the business chain.
2 - Recommend technology that ensures adequate security compliance with legal compliance applicable to many data types.
3 - Recognize potentialities and limitations of the technology to be developed and implemented in a privacy program to lead to the evaluation of the data.
4 - Implement a plan to respond to data security incidents. (data breach).

4.4.5. Conteúdos programáticos:
1 INTRODUÇÃO
Cenários críticos para a proteção de dados
Proteção de dados em tecnologias emergentes
Recolha e transferência de informação

2 AVALIAÇÃO DE DADOS, SISTEMAS E PROCESSOS
Mapeamento e classificação de dados em sistemas de informação organizacionais.
Estratégias de computação na nuvem.
Padrões tecnológicos para a salvaguarda da informação (datacenters, acesso físicos, destruição e higienização de dados, dispositivos forenses).
Diligências devidas e avaliação de risco tecnológico nas fusões, aquisições e alienações

3 PROTEÇÃO E PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO
Proteção de dados na internet das coisas
Privacidade por design e por omissão

4 MÉTRICAS
Custos dos controles técnicos
Custo da retenção de dados
Técnicas para reduzir indicadores sobre incidentes

5 RESPOSTA A INCIDENTES
Processamento de formulários no acesso, reparação, correção e gestão da integridade de dados
A conformidade legal na resposta digital
Efetivar um plano de resposta a incidentes de violação de dados

4.4.5. Syllabus:
1. INTRO
Scenarios for critical data protection
Emerging technologies and data protection
Collection and transfer of information

2 DATA EVALUATION, SYSTEMS AND PROCESSES
Mapping and classification of data types at enterprise information systems.
Cloud Computing Strategies.
Technological standards for safeguarding information (datacenters, physical access, data destruction and sanitization,

forensic devices).
Due diligence and technological risk assessment in mergers, acquisitions and divestitures

3 INFORMATION SECURITY PROTECTION AND PRACTICES
Data protection on IoT
Privacy by design and Privacy by default

4 METRICS
Costs of technical controls
Cost of data retention
Techniques to minimize incident indicators

5 INCIDENT RESPONSES
Processing forms to access, repair, fix, and manage data integrity
Legal compliance for an digital response
Effective response plan for data breach incidents

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
1 - Sensibilizar e estar consciente da importância da privacidade e proteção de dados pessoais em todo o espectro digital da cadeia de negócio: 1+2
2 - Recomendar tecnologia que garanta a segurança adequada ao cumprimento da conformidade legal aplicável aos vários tipos de dados: 1+2+3
3 - Reconhecer potencialidades e limitações da tecnologia a desenvolver e implementar num programa de privacidade para conduzir à avaliação dos dados: 1+2+3+4
4 - Efetivar um plano de resposta a incidentes de segurança dos dados: 5

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
1 - Raise awareness of the importance of privacy and protection of personal data across the digital spectrum of the business chain: 1+2
2 - Recommend technology that ensures adequate security compliance with legal compliance applicable to many data types: 1+2+3
3 - Recognize potentialities and limitations of the technology to be developed and implemented in a privacy program to lead to the evaluation of the data: 1+2+3+4
4 - Implement a plan to respond to data security incidents. (data breach): 5

4.4.7. Metodologias de ensino (avaliação incluída):
As aulas incluem sessões teóricas, discussões dirigidas e sessões de carácter prático com demonstração de casos temáticos.
– Nas sessões teóricas será utilizado o método expositivo.
– As discussões dirigidas serão orientadas para o estudo de casos.
– As sessões de carácter prático incluem a resolução de casos práticos destinados a permitir validar as competências adquiridas.

Avaliação contínua:
- Teste escrito (100%)
Exame final: Exame teórico-prático (100%)

4.4.7. Teaching methodologies (including students' assessment):
This curricular unit include theoretical sessions, guided discussions and practical sessions for demonstration of thematic cases.
– In theoretical sessions we'll use the expository method.
– Targeted discussions will focus on case studies.
– Practical sessions include the resolution of practical cases to enable the skills acquired to be validated.

Continuous evaluation:
- Written test (100%)
Final exam: Theoretical-practical exam (100%)

4.4.8. 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 uma vez que:
1) Os métodos de ensino utilizados ajustam-se à natureza dos conteúdos programáticos e aos objetivos a atingir em cada sessão.
A realização de exposições sobre as diferentes matérias conjuga-se com a metodologia de avaliação estabelecida,

permitindo assim atingir os objetivos definidos
2) As metodologias de ensino adotadas procuram potenciar a participação ativa dos alunos e a transmissão metódica e rigorosa dos diferentes saberes
3) Competências complementares como sejam o trabalho em equipa, comunicação escrita e verbal serão também exploradas no âmbito desta unidade curricular.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
Teaching methodologies are compliance with the objectives of this curricular unit because:
1) Teaching methods used fit the nature of the syllabus and objectives to be achieved in each session.
The presentation of expositions on the different subjects is conjugated with the methodology of evaluation established, thus allowing to reach the objectives defined
2) Teaching methodologies adopted seek to foster the active participation of the students and the methodical and rigorous transmission of different knowledge
3) Complementary skills such as teamwork, written and verbal communication will also be explored within this curricular unit.

4.4.9. Bibliografia de consulta/existência obrigatória:
Leenes,R. , van Brakel,R. , Gutwirth,S. , Hert, P. (2018). Data Protection and Privacy: The Internet of Bodies. United Kingdom: Hart Publishing.
Stalla-Bourdillon, S., Phillips, J., & Ryan, M. D. (2014). Privacy vs security. (Springer Briefs in Cybersecurity). London, GB: Springer.

Mapa IV - Engenharia Social

4.4.1.1. Designação da unidade curricular:
Engenharia Social

4.4.1.1. Title of curricular unit:
Social Enginneering

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
81

4.4.1.4. Horas de trabalho:
65

4.4.1.5. Horas de contacto:
16

4.4.1.6. ECTS:
3

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Pinto; TP-8

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Pedro Carneiro; TP-8

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

Os estudantes nesta UC deverão:

A - Conhecer as diferentes técnicas básicas de Engenharia Social

B - Dominar a utilização de Ferramentas de Engenharia Social

C - Conhecer as diferentes técnicas avançadas de Engenharia Social

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

Students in this subject should:

A - Know the different basic techniques of Social Engineering

B - Mastering the use of Social Engineering Tools

C - Know the different advanced techniques of Social Engineering

4.4.5. Conteúdos programáticos:

1. Visão Geral

2. Técnicas de Influência

3. Ferramentas de Engenharia Social

4. Open Source Intelligence (OSINT)

5. Tornar-se outra pessoa

6. Conhecer o inimigo

7. Mind Tricks

8. Elicitação

9. Hacking não técnico

10. O "Lockpicker" mentiroso

11. Ultrapassando Sistemas Físicos

12. Engenharia Social Reversa

4.4.5. Syllabus:

1. Overview

2. Influence Techniques

3. Develop Your Tools

4. Open Source Intelligence (OSINT)

5. Becoming Another Person

6. Know Your Enemy

7. Mind Tricks

8. Elicitation

9. Non-Tech Hacking

10. The Lying Lockpicker

11. Getting Past Physical Systems

12. Reverse Social Engineering

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

Aos estudantes desta UC:

- Os tópicos 1 e 2 permitem atingir o objetivo A

- Os tópicos 3 e 4 permitem atingir o objetivo B

- Os tópicos 5 a 12 permitem atingir o objetivo C

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

To students for this subject:

- Topics 1 and 2 allow to achieve objective A

- Topics 3 and 4 allow to reach objective B

- Topics 5 to 12 allow to achieve objective C

4.4.7. Metodologias de ensino (avaliação incluída):

Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:

CG = 0.6*CT +0.4*CP

CP: Avaliação contínua obtida através da realização de trabalhos práticos, respectivos relatórios e ainda a avaliação do desempenho nos trabalhos em laboratório. Para aprovação à UC é necessário nota mínima de 8 valores na CP.

CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é

necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by means of a theoretical component (TC) and a practical component (PC) with the following weighting:
CG = 0.6 * TC + 0.4 * PC
CP: Continuous evaluation obtained through the accomplishment of practical works, respective reports and also the evaluation of the performance in the lab work. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. 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 aos objetivos a atingir em cada sessão.
2) As metodologias de ensino utilizadas procuram potenciar a participação ativa dos discentes e a transmissão metódica e rigorosa dos diferentes saberes
3) Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The teaching methodologies are in line with the objectives of this subject given that:
1) The teaching methods used are appropriate to the nature of the syllabus and the objectives to be achieved in each session.
2) The teaching methodologies used seek to foster the active participation of the students and the methodical and rigorous transmission of different knowledge
3) Complementary skills such as teamwork, written and verbal communication will also be explored within the scope of this subject.

4.4.9. Bibliografia de consulta/existência obrigatória:
- Christopher Hadnagy. 2018. Social Engineering: The Science of Human Hacking. John Wiley & Sons. ISBN 978-1-119-43338-5.
- Kevin D. Mitnick and William L. Simon. 2005. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. John Wiley & Sons, Inc., New York, NY, USA.
- Kevin D. Mitnick and William L. Simon. 2003. The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons, Inc., New York, NY, USA.

Mapa IV - Gestão de Identidade Digital

4.4.1.1. Designação da unidade curricular:
Gestão de Identidade Digital

4.4.1.1. Title of curricular unit:
Digital Identity Management

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
81

4.4.1.4. Horas de trabalho:
65

4.4.1.5. Horas de contacto:

16

4.4.1.6. ECTS:
3

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
António Pinto; TP-8; PL-8;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Gerais:
1. Distinguir uma identidade físicas de uma identidade digital;
2. Compreender a problemática da identidade no mundo digital, da sua gestão e do seu relacionamento com a identidade física;
3. Identificar as principais características e requisitos dos diversos tipos de aplicações de gestão de identidades e do seu
relacionamento com a gestão de controle de acessos.
Específicos:
4. Especificar soluções que permitam um controle de acessos físico e lógico granular a informação, sistemas, dispositivos e
instalações;
5. Identificar serviços de gestão de identidades (e.g. SSO, LDAP, AD);
6. Compreender e diferenciar sistemas de autenticação single-fator e multi-fator (e.g. fatores de autenticação, força, biometria);
7. Registrar e identificar usos de identidade;
8. Identificar serviços de gestão de identidades federada (e.g. SAML, OpenID);

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
General:
1. Distinguish a physical identity from a digital identity;
2. Understand the problem of identity in the digital world, its management and its relationship with physical identity;
3. Identify the key characteristics and requirements of the various types of identity management applications and their relationship with access control management.
Specific:
4. Specify solutions that allow a granular physical and logical accessl to the information, systems, devices and installations;
5. Identify identity management services (e.g. SSO, LDAP, AD);
6. Understand and differentiate single-factor and multi-factor authentication systems (e.g., authentication, strength, biometrics);
7. Register and identify uses of identity;
8. Identify federated identity management services (eg SAML, OpenID);

4.4.5. Conteúdos programáticos:
1. Controlo do acesso físico e lógico aos ativos
2. Gestão da identificação e da autenticação de pessoas e dispositivos
3. Serviços de identidade on-premise
4. Serviços de identidade na nuvem
5 Gestão da identidade e do seu ciclo de vida

4.4.5. Syllabus:
1. Control physical and logical access to assets
2. Identification management and authentication of persons and devices
3. On-premise identity services

4. Cloud identity services
5 Identity Management and its Life Cycle

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Gerais:
1. Distinguir uma identidade físicas de uma identidade digital (C2);
2. Compreender a problemática da identidade no mundo digital, da sua gestão e do seu relacionamento com a identidade física (C1 e C2);
3. Identificar as principais características e requisitos dos diversos tipos de aplicações de gestão de identidades e do seu
relacionamento com a gestão de controle de acessos. (C2, C3, C4 e C5)
Específicos:
4. Especificar soluções que permitam um controle de acessos físico e lógico granular a informação, sistemas, dispositivos e
instalações; (C1 e C2)
5. Identificar serviços de gestão de identidades (e.g. SSO, LDAP, AD); (C1 e C2)
6. Compreender e diferenciar sistemas de autenticação single-fator e multi-fator (e.g. fatores de autenticação, força, biometria); (C3, C4 e C5)
7. Registrar e identificar usos de identidade; (C5)
8. Identificar serviços de gestão de identidades federada (e.g. SAML, OpenID); (C3, C4 e C5)

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
General:
1. Distinguish a physical identity from a digital identity; (C2)
2. Understand the problem of identity in the digital world, its management and its relationship with physical identity; (C1 and C2)
3. Identify the key characteristics and requirements of the various types of identity management applications and their relationship with access control management.
Specific: (C2,C3,C4 and C5)
4. Specify solutions that allow a granular physical and logical accessl to the information, systems, devices and installations; (C1 and C2)
5. Identify identity management services (e.g. SSO, LDAP, AD); (C1 and C2)
6. Understand and differentiate single-factor and multi-factor authentication systems (e.g., authentication, strength, biometrics); (C3, C4 and C5)
7. Register and identify uses of identity; (C5)
8. Identify federated identity management services (eg SAML, OpenID); (C3, C4 and C5)

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.5*CT +0.5*CP*
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by average of a theoretical component (TC) and a practical component (PC) with the following weighting:
*CG = 0.5 * TC + 0.5 * PC*
CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Nas aulas teóricas, e em complemento ao método expositivo dos conteúdos programáticos com projecção de

elementos
exemplificadores, será ainda adoptada uma complementação ao mesmo através do método activo/demonstrativo. Nas aulas práticas será adoptado um método totalmente activo, através da disponibilização de diversas fichas de exercícios que permitirão ao estudante aplicar, na prática, os conhecimentos adquiridos nas aulas teóricas. Estas fichas incluirão sempre uma pequena descrição dos objectivos a atingir, da matéria que se pretende abordar, exemplos e exercícios, dispostos em crescendo de dificuldade, a resolver autonomamente ou em grupo pelo estudante, devidamente acompanhados pelo docente.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
In the lectures, and in addition to the expositive method of the syllabus with projection of sample elements, it will be adopted the active / demonstrative method.
In practical classes it will be adopted a fully active method, by providing various forms of assignments that will allow students to
apply in practice the knowledge acquired in lectures. These assignments will always include a brief description of the objectives to be achieved, the matter that is intended to address, examples and exercises, arranged in increase of difficulty to be solved
independently or in groups by the student, duly accompanied by the teacher.

4.4.9. Bibliografia de consulta/existência obrigatória:
Identity Management: A Primer 1st Edition by Graham Williamson (Author); David Yip (Author); Ilan Sharoni (Author); Kent Spaulding (Author) - ISBN-13: 978-1583470930, ISBN-10: 158347093X (2009)
CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 7th Edition by James M. Stewart (Author); Mike Chapple (Author); Darril Gibson (Author) - ISBN-13: 978-1119042716, ISBN-10: 1119042712 (2015)
Mechanics of User Identification and Authentication: Fundamentals of Identity Management 1st Edition by Dobromir Todorov (Author) - ISBN-13: 978-1420052190, ISBN-10: 1420052195 (2014)

Mapa IV - Análise de Dados e Ciberinteligência

4.4.1.1. Designação da unidade curricular:
Análise de Dados e Ciberinteligência

4.4.1.1. Title of curricular unit:
Data Analytics and Cyber Intelligence

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
135

4.4.1.4. Horas de trabalho:
103

4.4.1.5. Horas de contacto:
32

4.4.1.6. ECTS:
5

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
João Paulo Magalhães; TP-16; PL-16;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Considerando o crescimento e sofisticação das ciber ameaças, esta unidade curricular contribui para uma melhor compreensão do problema e das melhores práticas a adotar em apoio aos objetivos estratégicos, operacionais e táticos das organizações.

No final da UC, o estudante deve ser capaz de:
1. Compreender as ameaças e as motivações por detrás destas;
2. Reconhecer diferentes tipos de ciber ameaças;
3. Compreender a diferença entre dados, informação e inteligência ao nível das ciber ameaças;
4. Compreender o processo de aquisição, análise de dados e apresentação de indicadores de compromisso relacionados com ciber ameaças;
5. Identificar e sugerir ferramentas e fontes de inteligência adequados à organização;
6. Auxiliar as organizações na avaliação do seu conhecimento situacional sobre ciber ameaças;
7. Desenhar, gerir ou apoiar a implementação e manutenção de um programa de cyber intelligence e cyber awareness.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
Considering the growth and sophistication of cyber threats, this curricular unit contributes to a better understanding of the problem and to the knowledge of the best practices to adopt in supporting the strategic, operational and tactical objectives of organisations.

At the end of this curricular unit, the student should be able to:
1. Understand the cyber threats and the motivations behind these;
2. Recognise different types of cyber threats;
3. Understand the difference between data, information and intelligence;
4. Understand the process of data acquisition, data analysis and data presentation;
5. Identify and suggest tools and sources of intelligence according to the organisation needs;
6. Support organisations in assessing their situational awareness on cyber threats;
7. Design, manage or support the implementation of cyber intelligence and awareness programs.

4.4.5. Conteúdos programáticos:
1. CiberAmeaças
- Tipos de ameaças
- Motivações
- O negócio de ameaças
- Use / mostrar casos

2. Inteligência Cibernética
- O ciclo de inteligência (sigint, osint, humint, imint, geoint, masint)
- Tipos de inteligência (estratégica, operacional, tática)
- Detalhe de ataques cibernéticos
- Negação e decepção
- Incorporando o ciclo de vida da inteligência no fluxo de trabalho em segurança

3. Coleta de Dados e Análise de Dados para Cyber Intelligence
- Plataformas Threat Intelligence
- Princípios da análise de dados
- Coleta de dados
- Análise e apresentação de dados

4. Partilha de inteligência
- Plataformas Threat Intelligence
- Comunidades (CERTs, CSIRTs, ISACs, ...)
- Esforços de interoperabilidade (openIOC, CyBox, STIX, TAXII, ...)

4.4.5. Syllabus:
1. Cyber threats
- Types of threats
- Motivations
- The threats business
- Use/show cases

2. Cyber Intelligence
- The intelligence cycle (sigint, osint, humint, imint, geoint, masint)
- Types of intelligence (strategic, operational, tactical)
- Approaching cyber-attacks
- Denial and deception
- Incorporating the intelligence lifecycle into security workflow

3. Data Gathering and Data Analytics for Cyber Intelligence
- Threat Intelligence Platforms
- Principles of Data Analytics
- Data gathering
- Data analysis and presentation

4. Intelligence sharing
- Threat Intelligence Platforms
- Communities (CERTs, CSIRTs, ISACs, ...)
- Interoperability efforts (openIOC, CyBox, STIX, TAXII, ...)

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Os tópicos 1, 2 e 6 têm por objetivo dotar os alunos de conhecimentos sobre as ciber ameaças, as motivações por detrás das mesmas, a forma como são levadas a cabo e qual o papel da cyber intelligence no âmbito das ameaças. Estes tópicos contribuem para os objetivos 1, 2, 3 e 6.

Os tópicos 3, 4, 5 e 6 focam o desenho de programas cyber intelligence, dando a conhecer: as limitações das soluções tradicionais; os procedimentos de obtenção de dados sobre ciber ameaças; as soluções existentes no mercado segmentadas de acordo com os diferentes tipos de necessidades de informação situacional; as técnicas e ferramentas de análise de dados; as dinâmicas entre as comunidades que tratam estes assuntos. Estes tópicos estão alinhados com os objetivos 4, 5 e 6.

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
Topics 1, 2 and 6 are planned to provide students with knowledge about cyber threats, the motivations behind them, the way they are carried out and the role of cyber intelligence to handle with them. These topics contribute to the learning goals 1, 2, 3 and 6.

The topics 3, 4, 5 and 6 focus on the design of cyber intelligence programs, addressing topics such as: the limitations of traditional solutions; the data collection procedures on cyber threats; the existing solutions in the market according to the different cyber intelligence needs; the techniques and data analysis tools; the information sharing and combined efforts to address these issues. These topics are aligned with the learning goals 4, 5 and 6.

4.4.7. Metodologias de ensino (avaliação incluída):
Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demontrar a aplicação dos conceitos abordados.

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
CG = 0.5*CT +0.5*CP
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respectivos relatórios. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignements will be acomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by means of a theoretical component (TC) and a practical component (PC) with the following weighting:
CG = 0.5 * TC + 0.5 * PC
CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. 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 (palestra, discussão dirigida, execução), quer por parte do docente, quer dos estudantes, conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos.

2) As metodologias de ensino utilizadas procuram, sempre que possível, potenciar a participação ativa dos discentes. 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.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
The teaching methodologies are consistent with the objectives of the course as:
1) The teaching methods used are in line with the program and the objectives to achieve in each session. The different subjects introduced by means of lectures, directed discussions, execution of practical assignments is combined with the evaluation, allowing assessing the achievement of the learning goals.

2) The teaching methods used seek, as often as possible, to enhance the active participation of the students. Complementary skills such as teamwork, written and verbal communication will also be explored within the UC.

The evaluation process is designed to assess the extent and the level of competencies to acquire during the course.

4.4.9. Bibliografia de consulta/existência obrigatória:
[1] Building an Intelligence-Led Security Program, Allan Liska, ISBN: 9780128021453, Syngress Media, U.S., 2014
[2] Data-Driven Security: Analysis, Visualization and Dashboard, Jay Jacobs and Bob Rudis, ISBN: 978-1118793725, Wiley, 2014
[3] How to Define and Build an Effective Cyber Threat Intelligence Capability, Henry Dalziel, ISBN: 978-0128027301, Syngress, 2014

Mapa IV - Auditoria e Conformidade em Cibersegurança

4.4.1.1. Designação da unidade curricular:
Auditoria e Conformidade em Cibersegurança

4.4.1.1. Title of curricular unit:
Cybersecurity Audit and Compliance

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
108

4.4.1.4. Horas de trabalho:
84

4.4.1.5. Horas de contacto:
24

4.4.1.6. ECTS:
4

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:

<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Teresa Pereira; TP-24;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Pedro Carneiro; PL-8

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta UC aborda os princípios e abordagens metodológicas de auditoria dos sistemas de informação que permitem garantir a conformidade de um SGSI com as leis e disposições regulamentares exigidas, no contexto da norma de segurança da ISO/IEC 27001.
No final desta UC o aluno deverá ser capaz de cumprir os seguintes objetivos de aprendizagem:
1. Explicar o uso de standards numa auditoria e verificar a conformidade do SGSI.
2. Desenvolver, implementar e executar uma estratégia de auditoria ao SGSI
3. Descrever os componentes e os requisitos básicos necessários num plano de auditoria.
4. Descrever os parâmetros necessários para conduzir e relatar uma auditoria.
5. Avaliar o desenho, implementação e monitorização dos controles de segurança implementados e verificar se garantem a proteção dos ativos de informação da organização.
6. Realizar uma analise critica de situações legais e éticas, examinar a sua possível resolução e recomendar um conjunto de ações.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This course covers the principles, the approaches and the methodology in auditing information systems to ensure the processes and the procedures are in compliance with pertinent laws and regulatory provisions especially in the context of information security standard ISO/IEC 27001.
The successful student will fulfil the following learning objectives:
1. Describe the role of ISMS compliance with the security standard ISO/IEC 27001.
2. Explain the use of standards and frameworks in a compliance audit of an ISMS.
3. Develop, implement and execute an ISMS audit strategy in compliance with the standard ISO/IEC 27001
4. Describe the components and basic requirements for creating an audit plan.
5. Describe the diferent parameters required to conduct and report on IT
audit for organizational compliance
6. Critically analyze legal and ethical situations, examine their possible resolution and recommend a justifiable course of actions.

4.4.5. Conteúdos programáticos:
Módulo 1 (Conceitos e definições)
1. Modelo PDCA e sua aplicação num SGSI
2. Normas e diretrizes para auditoria de um SGSI (por exemplo, ISACA, COBIT, ITIL)
Módulo 2 (Processo de auditoria)
1. Compreender o negócio da organização
2. O ciclo de vida da auditoria do SGSI
3. Responsabilidade, autoridade e responsabilidade do auditor do SGSI
4. Código de ética profissional, leis e regulamentação
Módulo 3 (Processo de Risco de Auditoria)
1. Elementos de uma análise de risco
2. Auditoria baseada na análise do risco e métodos de avaliação de risco
Módulo 4 (Planeamento e Gestão de Auditorias)
1. Desenvolvimento do plano de auditoria
2. Classificação de auditorias e âmbito
3. Missão da auditoria
Módulo 5 (Evidência de Auditoria)
1. Procedimento de recolha de evidências de auditoria
2. Conformidade
Módulo 6 (Relatório de Auditoria)
1. Elaboração do relatório executivo e os resultados
2. Comunicação dos resultados da auditoria

4.4.5. Syllabus:
Module 1 (Concepts and definitions)
1. PDCA model and its application in an ISMS
2. Standards and guidelines for ISMS auditing (e.g. ISACA, COBIT, ITIL)

Module 2 (Audit Process)
1. Understanding the organization's business
2. The ISMS audit life-cycle
3. The ISMS auditor responsability, authority and accountability
4. Code of professional ethics, laws and regulations
Module 3 (Audit Risk Process)
1. Elements of a risk analysis
2. Risk-based auditing and risk assessment methods
Module 4 (Audit Planning and Management)
1. Developing the audit plan
2. Classification and scope audits
3. Audit mission
Module 5 (Audit Evidence)
1. Audit evidence procedures
2. Compliance
Module 6 (Audit Reporting)
1. Audit reporting techniques
2. Writting the executive summary and findings
Communicate the auditing results

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
O objetivo desta unidade curricular é expor aos alunos os conceitos, estratégias e melhores práticas de auditoria e controle do SGSI.Os conteúdos programáticos são desenvolvidos de acordo com a evolução do conhecimento necessária para acompanhar o objectivo referido anteriormente.
No primeiro módulo, os alunos adquirirão o conhecimento sobre os conceitos e objetivos de um SGSI, bem como obterão conhecimento dos atuais padrões, estruturas e diretrizes de auditoria reconhecidas. Estes conteúdos estão alinhados com as competências 1. e 2.Nos módulos seguintes, é desenvolvido um conjunto de tarefas para capacitar os alunos a adquirir competências e habilidades para planejar e executar auditorias a organizações que implementaram um SGSI e verificar se estão em conformidade com as leis, regulamentos e com o padrão de segurança ISO / IEC. 27001. Estes conteúdos estão alinhados com as competências 3., 4., 5., 6. e 7.

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
The purpose of this course is to expose to the students the concepts, strategies and best practices in ISMS audit and control.
In the first module students will acquire the knowledge regarding the concepts and goals of an ISMS as well as get knowledge of the current recognized audit standards, frameworks and guidelines. These contents are aligned with the competences 1., and 2.
In the following modules, it is developed a set of tasks to enable students to acquire competences and skills to plan and execute audits to organizations which implemented an ISMS and verify if they are in compliance with the laws, regulations and the security standard ISO/IEC 27001. These contents are aligned with the competences 3., 4., 5., 6., and 7.

4.4.7. Metodologias de ensino (avaliação incluída):
As aulas incluem sessões teóricas. Nas sessões teóricas será utilizado essencialmente o método expositivo e demonstrações. As discussões dirigidas serão orientadas para o estudo de casos. As sessões de carácter prático incluem a utilização de ferramentas (treino) e a resolução de exercícios destinados a validar as competências adquiridas.
A maioria das atividades a desenvolver pelos alunos são supervisionadas. Não obstante, em alguns tópicos onde existem questões em aberto, as atividades de ensino procurarão estimular a criatividade e autonomia do aluno. Estas tarefes assentarão predominantemente na leitura de artigos científicos e relatórios técnicos, complementada com produção de trabalhos de síntese.
A avaliação dos alunos é contínua, sendo a classificação final obtida com base em:
(a) Participação nas atividades da UC (discussões dirigidas e apresentações) (10%);
(b) Elaboração de um artigo de natureza científica (40%);
(c) Trabalhos de grupo (50%).

4.4.7. Teaching methodologies (including students' assessment):
In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignments will be accomplished in order to consolidate and demonstrate the application of the concepts addressed.

The Global Classification (GC) of this curricular unit is obtained by means of a theoretical component (TC), a practical component (PC) and a participation on classes proposed activities (PA) with the following weighting:
CG = 0.4 * TC + 0.5 * PC + 0,1 * PA

CP: Continuous evaluation obtained through the accomplishment of practical works and respective reports. For approval it is necessary to have a minimum of 8 values in the CP.
CT - Obtained through a test or exam at the end of the term. For approval it is necessary to have a minimum score of 8 values in the TC.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Esta unidade curricular promove o desenvolvimento de dois tipos de competências: análise das questões associadas ao planeamento de auditorias aos SGSI, bem como a sua evolução; e na simulação prática de auditorias, com ênfase na medição da sua eficiência, no contexto dos objetivos de negócio da organização. A importância relativa desses dois tipos de competências está patente no peso atribuído às atividades de avaliação relacionadas. A utilização das ferramentas é avaliada através da execução de trabalhos práticos, incidindo essencialmente na perspetiva da auditoria aos SGSI e visando o controlo da eficiência das Políticas de Segurança implementadas. A execução dos trabalhos práticos deverá ocupar os alunos em sensivelmente metade do tempo.
A capacidade de análise e de discussão, centrada sobretudo na estratégia, na identificação de requisitos no planeamento e execução de uma auditoria, é avaliada através da apresentação, em aula e em grupo, de simulação prática de uma auditoria a um processo do SGSI e da elaboração do respective relatório da auditoria.
O relatório requer aos alunos a identificação do processo do SGSI auditado, com a posterior análise e formulação de argumentos relacionados com a simulação da auditoria. A correção técnica e a criatividade são também parâmetros de avaliação. Os critérios usados destinam-se a avaliar o nível de compreensão da temática relacionada com a auditoria dos SGSI, assim como a sua capacidade para discutir aspetos evolutivos da temática.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
This course promotes the development of two types of competences: analysis of the issues associated with the planning the ISMS' audits, and their evolvement; and the practical simulation of audits, with emphasis on measuring their efficiency, in the context of the organization's business objectives. The relative importance of these two types of competencies is evident in the weight attached to related assessment activities. The use of the tools is evaluated through the execution of practical work, focusing essentially on the audit perspective to the ISMS and aiming to control the efficiency of the Security Policies implemented. Practical assignments should cover students in roughly half the time.The ability to analyze and discuss, focusing mainly on strategy, identifying requirements in the planning and execution of an audit, is evaluated through the presentation, in class and in group, of practical simulation of an audit to an ISMS process and the audit report.The report requires students to identify the audited ISMS process, with subsequent analysis and formulation of arguments related to audit simulation. Technical correction and creativity are also evaluation parameters. The criteria used are intended to assess the level of understanding of the issue related to the ISMS audit, as well as its ability to discuss the evolutionary aspects of the ISMS.

4.4.9. Bibliografia de consulta/existência obrigatória:
- Richard E. Cascarino, "Auditor's Guide to Information Systems Auditing" Wiley. ISBN 0470009896. 2007.

- Weiss, Martin, and Michael G. Solomon Sudbury, 2010. Auditing IT Infrastructures for Compliance, 1st ed., MA: Jones & Bartlett, 2010.

Mapa IV - Cibercrime e Análise Forense Digital

4.4.1.1. Designação da unidade curricular:
Cibercrime e Análise Forense Digital

4.4.1.1. Title of curricular unit:
Cybercrime and Digital Forensics Analysis

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
162

4.4.1.4. Horas de trabalho:
122

4.4.1.5. Horas de contacto:
40

4.4.1.6. ECTS:
6

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Baltazar Rodrigues; TP-24; PL-16;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
<sem resposta>

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Os estudantes no final desta unidade curricular deverão ficar aptos a identificar, preservar e recolher prova digital contida em computadores, bem como em fontes abertas na Internet, respeitando o normativo legal, as normas e procedimentos instituídos e as regras de boas práticas Internacionais, assim como devem ficar aptos a analisar e demonstrar por relatório a prova digital recolhida.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
Students at the end of this curricular unit should be able to identify, preserve and collect digital evidence contained in computers, as well as in open sources on the Internet, respecting the legal norms, established norms and procedures and the rules of good international practice, as well as should be able to analyze and demonstrate the digital evidence collected by report.

4.4.5. Conteúdos programáticos:
1. Introdução à investigação forense digital
1.1 Método científico
1.2 Privacidade e ética

2. Obtenção de evidências
2.1 Procedimentos de 1ª intervenção e recolha de equipamentos
2.2 Enumerar Fontes de evidências
2.3 Suportes de armazenamento

3. Análise forenses

4. Documentação e comunicação (Reporting escrito)

4.4.5. Syllabus:
1. Introduction to digital forensics
1.1 Scientific method
1.2 Privacy and ethics

2. Obtaining Evidence
2.1 Procedures for first intervention and collection of equipment
2.2 List sources of evidence
2.3 Storage media

3. Forensic analysis

4. Documentation and communication (Reporting written)

4.4.6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular:
Para cada objectivo definido, são apresentados os conteúdos que para ele contribuem:
- Compreender as funcionalidades e funcionamento das ferramentas gratuitas de índole forense.
Conteúdos que contribuem para este objetivo: Todos.
- Compreender os métodos, procedimentos e boas práticas aplicadas na computação forense.

Conteúdos que contribuem para este objetivo: Conceito de Informática Forense e Metodologias.
- Compreender os preceitos deontológicos, na utilização das ferramentas de computação forense e na elaboração de relatórios de demonstração probatória.
Conteúdos que contribuem para este objetivo: Elaboração de Relatório; Ética e harmonização.
Aplicar os conhecimentos adquiridos na resolução prática de exercícios práticos de recuperação de dados e de recuperação de informação em espaços não alocados; ou através da resolução de exercícios práticos para recuperação de informação oculta em dados comuns.
Conteúdos que contribuem para este objetivo: Todos

4.4.6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes:
For each defined objective, the contents that contribute to it are presented:
- Understand the functionalities and operation of free forensic tools.
Content that contributes to this objective: All.
- Understand the methods, procedures and good practices applied in forensic computing.
Contents that contribute to this objective: Introduction.
- Understand deontological precepts, the use of forensic computing tools and the preparation of probative demonstration reports.
Content contributing to this objective: Reporting; Ethics and harmonization.
Apply the knowledge acquired in the practical resolution of practical exercises of data recovery and retrieval of information in unallocated spaces; or through the resolution of practical exercises for retrieving information hidden in common data.
Content that contributes to this goal: All

4.4.7. Metodologias de ensino (avaliação incluída):
Aulas Teórico-Práticas (TP) - Exposição participativa e discussão dos conceitos previstos no conteúdo programático, acompanhada pela análise de exemplos. Resolução de exercícios práticos de identificação, preservação, recolha, validação e análise de informação relevante probatória.
Avaliação : 100% Teste de consolidação de conhecimentos on-line, com questões de verdadeiro ou falso e múltipla resposta.

4.4.7. Teaching methodologies (including students' assessment):
Theoretical-practical classes (TP) - Participatory exhibition and discussion of the concepts provided in the programmatic content, accompanied by the analysis of examples. Resolution of practical exercises of identification, preservation, collection, validation and analysis of relevant probative information.
Assessment: 100% Test of consolidation of knowledge online, with questions of true or false and multiple answer.

4.4.8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular:
Compreender as funcionalidades e funcionamento das ferramentas gratuitas de índole forense.
Compreender os métodos, procedimentos e boas práticas aplicadas na computação forense.
Compreender os preceitos deontológicos, na utilização das ferramentas de computação forense e na elaboração de relatórios de demonstração probatória.
Adquirir a capacidade de recolher e validar informação relevante de fontes abertas, com recurso a ferramentas gratuitas.
Aplicar os conhecimentos adquiridos na resolução prática de exercícios simples de recolha de informação relevante em fontes abertas na Internet, com recurso a ferramentas gratuitas; na resolução de exercícios práticos de recuperação de dados e de recuperação de informação em espaços não alocados; ou através da resolução de exercícios práticos para recuperação de informação oculta em dados comuns.
São trabalhados através das atividades:
- Exposição participativa e discussão dos conceitos previstos no conteúdo programático, acompanhada pela análise de exemplos e resolução de exercícios práticos.
- Resolução de exercícios práticos aplicando os conhecimentos adquiridos nas aulas.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:
Understand the features and functionality of free forensic tools.
Understand the methods, procedures, and best practices applied in forensic computing.
Understand the deontological precepts, the use of forensic computer tools and the preparation of probative demonstration reports.
Acquire the ability to collect and validate relevant information from open sources, using free tools.
Apply the knowledge acquired in the practical resolution of simple exercises to collect relevant information in open sources on the Internet, using free tools; in the resolution of practical exercises of data recovery and retrieval of information in unallocated spaces; or through the resolution of practical exercises for retrieving information hidden in common data.
They are worked through activities:
- Participatory presentation and discussion of the concepts provided in the programmatic content, accompanied by the

analysis of examples and resolution of practical exercises.
- Resolution of practical exercises applying the knowledge acquired in class.

4.4.9. Bibliografia de consulta/existência obrigatória:
Bibliografia Principal:
Fichas de estudo disponibilizadas na plataforma moodle.
Bibliografia Complementar:
Manuais e fichas de exercícios práticos disponibilizados nas sessões de contacto.
Introdução à Cibersegurança; Mário Antunes e Baltazar Rodrigues, ISBN: 978-972-722-861-4; FCA, Lisboa, 2018

Mapa IV - Metodologias de Investigação

4.4.1.1. Designação da unidade curricular:
Metodologias de Investigação

4.4.1.1. Title of curricular unit:
Research Methodologies

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
81

4.4.1.4. Horas de trabalho:
65

4.4.1.5. Horas de contacto:
16

4.4.1.6. ECTS:
3

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Pinto; TP-8;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Luís Barreto; PL-8;

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Esta unidade curricular tem como objetivos aprofundar as metodologias de investigação que possam ajudar a adquirir conhecimentos para a realização da dissertação de mestrado, entre outros projetos e trabalhos científicos.
Abrange as práticas de redação e apresentação de artigos científicos, a avaliação de contribuições científicas assim como todos os aspectos profissionais relacionados com pesquisa e desenvolvimento.

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
This curricular unit aims to deepen the research methodologies that can help to acquire knowledge for the accomplishment of the dissertation, among other projects and scientific works.
It covers practicals of scientific article writing and presenting, the evaluation of scientific contributions related with professional aspects of research and development .

4.4.5. Conteúdos programáticos:

C1 - Métodos e técnicas em projectos de investigação
C2 - Métodos sistemáticos de pesquisa de informação científica
C3 - Concepção e realização de trabalhos para publicação
C4 - Tutoriais sobre realização de trabalhos de investigação
C5 - Concepção, elaboração e defesa do projecto de dissertação

4.4.5. Syllabus:

C1 - Methods and techniques in research projects
C2 - Systematic methods of scientific information search
C3 - Design and execution of publications
C4 - Tutorials about execution of researh works
C5 - Design, preparation and defense of the dissertation report

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

O principal objetivo desta unidade curricular é estudar as metodologias de investigação que possam ajudar os estudantes a adquirir conhecimentos para a realização da dissertação de mestrado.
Os conteúdos programáticos propostos asseguram o desenvolvimento dessas competências, assim como da escrita de artigos e outros conteúdos científicos.

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

The main objective of this subject is to study the research methodologies that can help the students to acquire knowledge in order to acomplish their master dissertation.
The proposed program contents ensure the development of these skills, as well as writing articles and other scientific content.

4.4.7. Metodologias de ensino (avaliação incluída):

Exposição de Conceitos. Pesquisa de artigos científicos. Exposição e análise de casos práticos.
A avaliação desta UC incide sobre os trabalhos realizados nos casos práticos abordados.

4.4.7. Teaching methodologies (including students' assessment):

Exposure Concepts. Research scientific articles.Analysis of practical cases.
The evaluation of this subject is focused on the work done in the practical cases addressed.

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

A prossecução dos objetivos propostos passa, quer pela abordagem teórica aos principais conceitos de Metodologias de Investigação, quer pela aplicação prática, com recurso a exemplos e à realização de pesquisa de artigos científicos, teses e dissertações.
Os principais objetivos da presente Unidade Curricular passam por compreender as metodologias de investigação, bem como a sua contextualização para uma boa execução da dissertação.
Pretende-se dar a conhecer a realidade da diversidade das Metodologias de Investigação, bem como os critérios e os constrangimentos com que o investigador se debate.
Neste sentido é feita uma pesquisa de artigos científicos, teses e dissertações, o que permite a discussão de opções e perguntas entre os vários alunos, criando assim um efeito de sinergia que promova a aprendizagem em grupo.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:

The pursuit of the proposed objectives passes, either by theoretical approach to the main concepts of research methodologies, or by practical application, using examples and conducting research papers, theses and dissertations.The main objectives of this course unit is to understand the research methodologies as well as their context for a adequately perform the dissertation.
It is intended to make known the reality of the diversity of research methodologies, and the criteria and constraints that the researcher debate. In this sense a search is performed of scientific papers, theses and dissertations which allows the discussion of options and questions among several students, thus creating a synergistic effect that promotes group learning

4.4.9. Bibliografia de consulta/existência obrigatória:

Maria José Sousa, Cristina Sales Batista - Como fazer teses, dissertações e relatórios segundo Bolonha. Lidel 2011;
Luis Adriano Oliveira - Dissertação e Tese em Ciência e Tecnologia segundo Bolonha. Guia de Boas práticas - Lidel 2011.
Umberto Eco - Como se faz uma tese em ciências humanas. Editora Presença. 6ª ed. 1995;

Mapa IV - Dissertação/Projeto/Estágio

4.4.1.1. Designação da unidade curricular:
Dissertação/Projeto/Estágio

4.4.1.1. Title of curricular unit:
Dissertation/Project/Internship

4.4.1.2. Sigla da área científica em que se insere:
CCT/CST

4.4.1.3. Duração:
1539

4.4.1.4. Horas de trabalho:
1499

4.4.1.5. Horas de contacto:
40

4.4.1.6. ECTS:
57

4.4.1.7. Observações:
<sem resposta>

4.4.1.7. Observations:
<no answer>

4.4.2. Docente responsável e respetiva carga letiva na Unidade Curricular (preencher o nome completo):
Pedro Pinto; TP-7;

4.4.3. Outros docentes e respetivas cargas letivas na unidade curricular:
Luís Barreto; PL-7;
Teresa Pereira; PL-7;
Pedro Carneiro; PL-7;
Sara Paiva; PL-6;
Sérgio Lopes; PL-6;

4.4.4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):
Dado o cariz da área cientifica em que se enquadra o ciclo de estudos, é apropriado proporcionar aos alunos mais do que que uma opção podendo adequar a UC ao melhor perfil de cada um. A disciplina proporcionará a integração dos conhecimentos adquiridos ao longo do CE e a transição, em alguns casos de consolidação, para o mercado de trabalho. Os trabalhos podem assumir 3 formatos: dissertação de cariz académico, estágio de cariz empresarial (adequados aos alunos sem experiência na área), projeto integrado num contexto empresarial. Em qualquer dos casos os alunos deverão conduzir um projeto que contemple não só a aplicação dos conceitos adquiridos durante a sua formação, mas também a integração de novas técnicas e de saberes, de modo a realizar um trabalho inovador. Os regulamentos de funcionamento e avaliação encontram-se disponibilizados em www.ipvc.pt

4.4.4. Intended learning outcomes (knowledge, skills and competences to be developed by the students):
Given the nature of the scientific area that represents the cycle of studies (CS), it is appropriate to provide students with more than an option that can tailor the curricular unit (CU) to the best profile of each one. The CU will provide the integration of the knowledge acquired throughout the CS and the transition, in some cases of consolidation, to the labor market. The students can choose 3 formats: academic dissertation, business internship (suitable for students with no experience in the area), integrated project in a business context. In any case, students should conduct a project that contemplates not only the application of the concepts acquired during their training, but also the integration of new techniques and knowledge, in order to carry out innovative work. The operating and evaluation regulations are available at www.ipvc.pt.

4.4.5. Conteúdos programáticos:

Variável consoante a temática da dissertação/projeto/estágio mas que contemple na sua maioria os conteúdos aprendidos durante o desenvolvimento do ciclo de estudos e com a a integração de novas técnicas e de saberes

4.4.5. Syllabus:

Variable depending on the theme of the dissertation / project / internship but that contemplates mostly the contents learned during the development of the cycle of studies and with the integration of new techniques and knowledge.

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

N/A

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

N/A

4.4.7. Metodologias de ensino (avaliação incluída):

Orientação tutorial. Após a conclusão do trabalho segue-se a discussão em júri de três membros.

4.4.7. Teaching methodologies (including students' assessment):

Tutorial guidance. After the conclusion of the work , the jury discussion of three members follows.

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

Variável dependendo do tipo de trabalho a realizar.

4.4.8. Evidence of the coherence between the teaching methodologies and the intended learning outcomes:

Variable accordingly to the work to be developed.

4.4.9. Bibliografia de consulta/existência obrigatória:

Variável.

4.5. Metodologias de ensino e aprendizagem

4.5.1. Adequação das metodologias de ensino e aprendizagem aos objetivos de aprendizagem (conhecimentos, aptidões e competências) definidos para o ciclo de estudos:

As metodologias adotadas podem ser resumidas da seguinte forma: todas as unidades curriculares assumem horas de aulas teórico-práticas (TP), Práticas Laboratoriais (PL) ou de Orientação Tutorial (OT). As aulas TP de exposição permitirão abordar devidamente as matérias e conceitos avançados na área da segurança informática e também explorar os detalhes da regulamentação e legislação aplicável nesta área da cibersegurança. As aulas PL permitem treinar os procedimentos para que os estudantes possam depois saber avaliar os cenários e aplicar os mecanismos de segurança de redes e sistemas adequados ao risco assumido. Também poderão treinar como resolver problemas relacionados com a prevenção e mitigação de ataques informáticos.

A última unidade curricular tem uma tipologia diferente de OT que permite designar um tutor para cada aluno que fará o acompanhamento dos trabalhos da dissertação/projeto/estágio desde o início até ao seu final.

4.5.1. Evidence of the teaching and learning methodologies coherence with the intended learning outcomes of the study programme:

The methodologies adopted can be summarized as follows: all curricular units assume hours of theoretical-practical classes (TP), Laboratory Practices (PL) or Tutorial Guidance (OT). The TP exposition classes will allow to duly address the advanced subjects and concepts in the area of computer security and also explore the details of the regulations and legislation applicable in this area of cybersecurity. The PL classes allow you to train the procedures so that the students can then know how to evaluate the scenarios and apply the security mechanisms of networks and systems appropriate to the risk assumed. They will also be able to train how to solve problems related to the prevention and mitigation of computer attacks.

The last unit has a different typology of OT that allows to designate a tutor for each student who will follow the work of the dissertation / project / stage from the beginning to the end.

4.5.2. Forma de verificação de que a carga média de trabalho que será necessária aos estudantes corresponde ao estimado em ECTS:

Este CE será concluído após a obtenção de 120 ECTS e 4 semestres e então, serão tomadas as seguintes formas de

verificação:
1. Após o termo do mestrado (2 anos), é verificada a adequação dos créditos por aferição do workload, por recurso a inquérito a docentes e discentes.
2. Considera-se como tempo de trabalho anual dos alunos 1620 horas a realizar em 40 semanas:
a) No primeiro ano, cada semestre tem 30 ECTS, correspondendo a 810 horas de trabalho, distribuído por 20 semanas. 1 ECTS corresponde a 810/30 = 27h de trabalho do estudante.
b) O segundo ano contém duas UCs, sendo uma anual com 57 ECTS e uma semestral com 3 ECTS, totalizando 60 ECTS correspondendo cada semestre a 810 horas de trabalho, distribuído por 20 semanas.
3. Adota-se um calendário escolar, semestral, com 20 semanas/semestre, sendo 16 semanas de contacto e 4 semanas para preparação de avaliações, finalização de trabalhos e relatórios, preparação de apresentações orais, seminários, etc.

4.5.2. Means to verify that the required students' average workload corresponds the estimated in ECTS.:
This graduation will be completed after obtaining 120 ECTS and 4 semesters and then, the following forms of verification will be taken:
1. After the end of the master's degree (2 years), the appropriateness of the workload assessment is verified, by means of a survey of teachers and students.
2. The annual work time of students is 1620 hours in 40 weeks:
a) In the first year, each semester has 30 ECTS, corresponding to 810 hours of work, distributed over 20 weeks. 1 ECTS corresponds to 810/30 = 27 hours of student work.
b) The second year contains two PAs, one annual with 57 ECTS and one semester with 3 ECTS, totaling 60 ECTS each corresponding to 810 working hours, distributed over 20 weeks.
3. A semi-annual school calendar is adopted, with 20 weeks / semester, with 16 weeks of contact and 4 weeks for preparation of evaluations, completion of papers and reports, preparation of oral presentations, seminars, etc.

4.5.3. Formas de garantia de que a avaliação da aprendizagem dos estudantes será feita em função dos objetivos de aprendizagem da unidade curricular:
A definição dos métodos de avaliação estão alinhados com os objectivos de aprendizagem das UCs deste CE. A avaliação de cada UC é definida pelos docentes e validada pela coordenação de curso e é obtida utilizando diversos elementos como os resultados dos testes, a apresentação de trabalhos, apresentações públicas e exames, o desempenho e a participação dos estudantes nas aulas.

4.5.3. Means of ensuring that the students assessment methodologies are adequate to the intended learning outcomes:
The definition of the evaluation methods is aligned with the learning objectives of each curricular unit of this study programme. The evaluation of each curricular unit is defined by the teachers and validated by the course coordination and is obtained using various elements such as test results, presentation of assignments, public presentations and examinations, performance and student participation in classes.

4.5.4. Metodologias de ensino previstas com vista a facilitar a participação dos estudantes em atividades científicas (quando aplicável):
A unidade curricular de dissertação/projeto/estágio tem uma tipologia diferente de orientação tutorial em que o estudante com o auxílio do orientador irá escolher a modalidade pretendida. Em qualquer das modalidades o estudante terá que fazer um levantamento do estado da arte, explorar novo temas relacionados com a área da cibersegurança e propor avanços. Neste percurso, o estudante será incentivado a participar em eventos científicos como por exemplo realizar comunicações orais, publicar artigos em conferências e realizar workshops. Para que este processo possa ser facilitado é importante (1) a existência da UC de Metodologias de Investigação para acompanhar o estudante nas diferentes fases de trabalho, estabelecer os milestones e definir objetivos específicos para prosseguir com os trabalhos da dissertação/projeto/estágio e (2) que os estudantes sejam integrados numa estrutura de investigação, em particular, no centro de investigação do IPVC, o ARC4DigiT.

4.5.4. Teaching methodologies that promote the participation of students in scientific activities (as applicable):
The curricular unit of dissertation / project / internship has a different typology of tutorial orientation in which the student with the aid of the tutor will choose the desired modality. In any of the modalities the student will have to do a survey of the state of the art, explore new topics related to the area of cybersecurity and propose advances. In this course, the student will be encouraged to participate in scientific events such as oral communications, conference articles and workshops. In order for this process to be facilitated, it is important to (1) the existence of the UC of Research Methodologies to accompany the student in the different phases of work, establish the milestones and define specific objectives to proceed with dissertation / project / 2) that students could be integrated into a research structure, in particular at the IPVC Research Center, ARC4DigiT.

4.6. Fundamentação do número total de créditos ECTS do ciclo de estudos

4.6.1. 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 DL n.º 74/2006, de 24 de março:
O Mestrado em Cibersegurança será concluído após a obtenção de 120 ECTS distribuídos ao longo de 4 semestres letivos, de acordo com o estipulado no no 1 do artigo 18 do Dec. Lei 74/2006, de 24 de Março, alterado pelo Dec. Lei 107/2008, de 25 de Junho, que considera serem estes os créditos (entre 90 a 120ECTS) e a duração adequados a uma mestrado com os objetivos científico-pedagógicos propostos.

4.6.1. Justification of the total number of ECTS credits and of the duration of the study programme, based on articles 8 or 9 (1st cycle), 18 (2nd cycle), 19 (integrated master) and 31 (3rd cycle) of DL no. 74/2006, republished by DL no. 63/2016, of September 13th:
The Master in Cybersecurity will be concluded after obtaining 120 ECTS distributed over four academic semesters, according to what is stipulated in article 18, paragraph 1, of Dec. Law 74/2006, of March 24, modified by Dec. Law 107 / 2008, of 25 June, which considers these to be the credits (between 90 and 120 ECTS) and the duration appropriate to a master's degree with the proposed scientific-pedagogical objectives.

4.6.2. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de créditos ECTS das unidades curriculares:
Na presente proposta, não havendo histórico de lecionação e por não existirem inquéritos a docentes e alunos, fez-se uma estimativa de workload com base na tipologia de cada unidade curricular e respetivos conteúdos programáticos.

4.6.2. Process used to consult the teaching staff about the methodology for calculating the number of ECTS credits of the curricular units:
In the present proposal, there is no history of teaching and because there are no inquiries to teachers and students, an estimate of workload was made based on the typology of each curricular unit and its programmatic contents.

4.7. Observações

4.7. Observações:
<sem resposta>

4.7. Observations:
<no answer>

5. Corpo Docente

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

5.1. Docente(s) responsável(eis) pela coordenação da implementação do ciclo de estudos.
Pedro Filipe Cruz Pinto

5.3 Equipa docente do ciclo de estudos (preenchimento automático)

5.3. Equipa docente do ciclo de estudos / Study programme's teaching staff

Nome / Name	Categoria / Category	Grau / Degree	Especialista / Specialist	Área científica / Scientific Area	Regime de tempo / Employment regime	Informação/ Information
Pedro Filipe Cruz Pinto	Professor Adjunto ou equivalente	Doutor		Telecomunicações	100	Ficha submetida
Silvestre Lomba Malta	Assistente convidado ou equivalente	Mestre		Engenharia Informática - Ramo de Redes e Sistemas de Comunicação	50	Ficha submetida
Teresa Susana Mendes Pereira Bernardino	Professor Adjunto ou equivalente	Doutor		Tecnologias e Sistemas de Informação	100	Ficha submetida
Luís Manuel Cerqueira Barreto	Professor Adjunto ou equivalente	Doutor		Engenharia Eletrotécnica	100	Ficha submetida

Sérgio Ivan Fernandes Lopes	Professor Adjunto ou equivalente	Doutor		Engenharia Eletrotécnica	100	Ficha submetida
Pedro Miguel Simões Pinto Carneiro	Assistente convidado ou equivalente	Mestre	CTC da Instituição proponente	ENGENHARIA INFORMÁTICA	50	Ficha submetida
Sara Maria da Cruz Maia de Oliveira Paiva	Professor Adjunto ou equivalente	Doutor		Ciências Informáticas	100	Ficha submetida
António Alberto dos Santos Pinto	Professor Adjunto ou equivalente	Doutor		Engenharia Eletotécnica e Computadores	10	Ficha submetida
João Paulo Ferreira de Magalhães	Professor Adjunto ou equivalente	Doutor		Ciências e Tecnologias da Informação	10	Ficha submetida
Baltazar Manuel Proença Rodrigues	Professor Adjunto ou equivalente	Licenciado		Engenharia Informática	10	Ficha submetida
Carlos Manuel Gonçalves Antunes	Professor Adjunto ou equivalente	Mestre	Título de especialista (DL 206/2009)	Engenharia Informática	10	Ficha submetida
					640	

<sem resposta>

5.4. Dados quantitativos relativos à equipa docente do ciclo de estudos.

5.4.1. Total de docentes do ciclo de estudos (nº e ETI)

5.4.1.1. Número total de docentes.

11

5.4.1.2. Número total de ETI.

6.4

5.4.2. Corpo docente próprio - Docentes do ciclo de estudos em tempo integral

5.4.2. Corpo docente próprio – docentes do ciclo de estudos em tempo integral.* / "Full time teaching staff" – number of teaching staff with a full time link to the institution.*

Corpo docente próprio / Full time teaching staff	**Nº / No.**	**Percentagem / Percentage**
Nº de docentes do ciclo de estudos em tempo integral na instituição / No. of teaching staff with a full time link to the institution:	5	78.125

5.4.3. Corpo docente academicamente qualificado – docentes do ciclo de estudos com o grau de doutor

5.4.3. Corpo docente academicamente qualificado – docentes do ciclo de estudos com o grau de doutor* / "Academically qualified teaching staff" – staff holding a PhD*

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 holding a PhD (FTE):	5.2	81.25

5.4.4. Corpo docente do ciclo de estudos especializado

5.4.4. Corpo docente do ciclo de estudos especializado / "Specialised teaching staff" of the study programme.

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 holding a PhD and specialised in the fundamental areas of the study programme	5	78.125	6.4
Especialistas, não doutorados, de reconhecida experiência e competência profissional nas áreas fundamentais do ciclo de estudos (ETI) / Specialists not holding a PhD, with well recognised experience and professional capacity in the fundamental areas of the study programme	0.6	9.375	6.4

5.4.5. Estabilidade e dinâmica de formação do corpo docente.

5.4.5. Estabilidade e dinâmica de formação do corpo docente. / Stability and development dynamics of the teaching staff

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 / Teaching staff of the study programme with a full time link to the institution for over 3 years	5	78.125	6.4
Docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (ETI) / FTE number of teaching staff registered in PhD programmes for over one year	1	15.625	6.4

Pergunta 5.5. e 5.6.

5.5. Procedimento de avaliação do desempenho do pessoal docente e medidas conducentes à sua permanente atualização e desenvolvimento profissional.

O sistema de avaliação do desempenho do IPVC define mecanismos para identificar objetivos e avaliar regularmente o desempenho do pessoal docente. Existe uma plataforma de preenchimento usada pelos docentes e realizam-se inquéritos à qualidade do ensino, resultando um diagnóstico de necessidades de formação, sendo posteriormente debatido pelas direções, Áreas Científicas, Conselho Técnico-Científico e Conselho Pedagógico. Estas medidas permitem um estímulo aos docentes na procura e reforço de competências. Os docentes têm mostrado interesse em metodologias de aprendizagem baseada em problemas, Team-based learning, avaliação da aprendizagem e plataformas digitais. Relativamente ao corpo docente específico deste CE, a abertura em 2017 das academias Cisco Networking Academy, Red Hat Academy e Palo Alto Networks Cybersecurity Academy, tem potenciado aos docentes uma constante formação nestas áreas, permitindo a sua atualização regular e o seu desenvolvimento profissional.

5.5. Procedures for the assessment of the teaching staff performance and measures for their permanent updating and professional development.

The IPVC performance evaluation system defines mechanisms to identify objectives and regularly assess the performance of teaching staff. There is a platform used by teachers and surveys are carried out on the quality of teaching, resulting in a diagnosis of training needs, and subsequently debated by the Direction, Scientific Areas, Technical-Scientific Council and Pedagogical Council. These measures allow teachers to be encouraged to seek and reinforce their skills. Teachers have shown interest in problem-based learning methodologies, Team-based learning, assessment of learning and digital platforms. With respect to the specific teaching staff of this study programme, the implementation in 2017 of a set of academies, such as the Cisco Networking Academy, Red Hat Academy and Palo Alto Networks Cybersecurity Academy, has empowered teachers to constantly training in these areas, allowing for regular updating and professional development.

5.6. Observações:

<sem resposta>

5.6. Observations:

<no answer>

6. Pessoal Não Docente

6.1. Número e regime de tempo do pessoal não-docente afeto à lecionação do ciclo de estudos.

O número de pessoas não docentes nas áreas mais relevantes ao apoio do ciclo de estudos são:

Apoio aos Laboratórios - 3 funcionários (tempo inteiro)
Secretariado dos Conselhos Técnico-Científico e Pedagógico - 2 funcionário (tempo inteiro)
Biblioteca da ESTG - 3 funcionários (tempo inteiro)
Serviços Académicos - 4 funcionários (tempo inteiro)
Neste contexto, existem muitos outros serviços e unidades que por razões de pertinência não estão aqui colocados.

6.1. Number and work regime of the non-academic staff allocated to the study programme.
The number of non-teaching people in the areas most relevant to the support of the study cycle are:
Support to Laboratories - 3 employees (full time)
Secretariat of the Technical-Scientific and Pedagogical Councils - 2 official (full time)
ESTG Library - 3 employees (full time)
Academic Services - 4 employees (full time)
In this context, there are many other services and units that for reasons of relevance are not placed here.

6.2. Qualificação do pessoal não docente de apoio à lecionação do ciclo de estudos.
A maior parte do pessoal docente possui o 12º ano ou o grau de licenciado nas mais diversas áreas.

6.2. Qualification of the non-academic staff supporting the study programme.
Most of the teaching staff has a 12th grade or a bachelor's degree in several areas.

6.3. Procedimento de avaliação do pessoal não-docente e medidas conducentes à sua permanente atualização e desenvolvimento profissional.
Para avaliação do pessoal não docente referido, vários questionários são realizados ao longo do ano letivo. Os seus resultados são analisados e procedem-se às medidas corretivas que se mostrarem necessárias.

6.3. Assessment procedures of the non-academic staff and measures for its permanent updating and personal development
For the evaluation of the non-teaching staff referred to, several questionnaires are carried out throughout the school year. Their results are analyzed and corrective measures are taken as necessary.

7. Instalações e equipamentos

7.1. Instalações físicas afetas e/ou utilizadas pelo ciclo de estudos (espaços letivos, bibliotecas, laboratórios, salas de computadores, etc.):
A ESTG-IPVC dispõe dos seguintes recursos materiais, em termos de instalações, equipamentos e materiais didáticos:
- Salas de aulas para formação teórica e teórico-prática, com capacidades variáveis, devidamente equipadas com projetores de vídeo, slides, televisores, DVD e projetores multimédia (área com mais de 3000m2).
- Salas de informática equipadas com PC's e impressoras em rede.
- Laboratórios de aulas com equipamento diverso nas áreas de redes, telecomunicações e segurança, sistemas, eletrónica e microprocessadores, informática, química, física, materiais, entre outros.
- Biblioteca com 2200 m2 constituída por sala de leitura com três níveis, tipo anfiteatro, capacidade para 320 leitores, 2 salas de informática de acesso livre, salas de estudo, gabinete de línguas, videoteca, depósito e arquivo.
- Em toda a escola acesso livre à Internet sem fios – rede wireless.
- Espaços de apoio (área 420 m2).

7.1. Facilities used by the study programme (lecturing spaces, libraries, laboratories, computer rooms, ...):
The ESTG-IPVC has the following material resources in terms of facilities, equipment and materials:
- Classrooms for theoretical and theoretical and practical training, with multiple capacities, fully equipped with datashows, TV, DVD and multimedia projectors (area of over 3000m2).
- Computer rooms equipped with PCs and networked printers.
- Laboratories with diverse equipment in the areas of networking, telecommunications and security systems, electronics and microprocessors, computer science, chemistry, physics, materials, among others.
- Library with 2200 m2 consisting of a reading room with three levels, amphitheater, up to 320 students, 2 free access computer rooms, study rooms, office language, library, storage and archiving.
- Free access to wireless Internet - wireless network.
- Support spaces (area 420 m2).

7.2. Principais equipamentos e materiais afetos e/ou utilizados pelo ciclo de estudos (equipamentos didáticos e científicos, materiais e TIC):

Laboratório de redes, telecomunicações e segurança estão equipado com:
****PCs ASUS e Servidores Dell Poweredge***
****Switch's e Routers:***
-HP A5500 series
-HP A5800 series
-HP Procurve 350
-Cisco 1941
-Cisco ISR 4221
-Cisco Catalyst 2960
****Equip. Wireless:***
-HP Mobility Controller
-APs HP, Linksys, Cisco Aironet, Ubiquiti
-Power Injectors Cisco
****Equip. Segurança:***
-Security Gateways Juniper
-Firewalls Cisco ASA 5505
****Equip. de análise Forense:***
- XRY, Mobile Forensic Examiner
****Equip. Suporte:***
-UPS, cabos e acessórios, bastidores conetores, SFPs, Alicates, Testadores de Cabos, Cabo UTP, Painéis Transferência

Laboratórios genéricos de Informática, equipados com PCs ASUS e ecrãs LCD

Laboratório de Eletrónica e Microprocessadores, equipado com:
****Sistemas de Desenvolvimento, Analisadores e Programadores***
****Equip. análise e Kits: Osciloscópios digitais, geradores de sinal***

Laboratório de Fibra Ótica, equipado com:
****Equip. de corte e fusão de fibra***
****Analizadores de espectro e OTDR***

7.2. Main equipment or materials used by the study programme (didactic and scientific equipment, materials, and ICTs):
Laboratory of networks, telecommunications and security are equipped with:
****ASUS PCs and Dell Poweredge Servers***
****Switch's and Routers:***
-HP A5500 series
-HP A5800 series
-HP Procurve 350
-Cisco Routers 1941
-Cisco Routers ISR 4221
-Cisco Switch Catalyst 2960
****Wireless Equip.:***
-HP Mobility Controller
-AP's HP, Linksys, Cisco Aironet, Ubiquiti
-Cisco Power Injectors
****Security Equip.:***
-Juniper Security Gateway
-Cisco ASA 5505
****Forensic analysis Equip.:***
-XRY, Mobile Forensic Examiner
****Support Equip.:UPS, Cables & Accessories , Connector Racks, SFPs, Pliers, Network Cable Testers, UTP Cable, Transfer Panels***

Generic Computer Labs, equipped with ASUS PCs and LCD screens
Laboratory of Electronics and Microprocessors, equipped with:
****Development Systems, Analyzers & Programmers***
****Equip. analysis and Kits: Digital oscilloscopes, signal generators***
Laboratory of Fiber Optics, equipped with:
****Equip. of fiber cutting and melting***
****Spectrum Analyzers and OTDR***

8. Atividades de investigação e desenvolvimento e/ou de formação avançada e desenvolvimento profissional de alto nível.

8.1. Centro(s) de investigação, na área do ciclo de estudos, em que os docentes desenvolvem a sua atividade científica

8.1. 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 teaching staff develops its scientific activity

Centro de Investigação / Research Centre	Classificação (FCT) / Classification FCT	IES / HEI	N.º de docentes do CE integrados / Number of study programme teaching staff integrated	Observações / Observations
INESCTEC	Excelente	FEUP	3	
Arc4Digit	Não Disponível	ESTG-IPVC	6	
AtlanTIC	Não Aplicável	Universidade de Vigo	1	
Instituto de Telecomunicações	Muito Bom	Instituto de Telecomunicações	2	
CIICESI	Não Disponível	ESTG - IPP	1	

Pergunta 8.2. a 8.4.

8.2. Mapa-resumo de publicações científicas do corpo docente do ciclo de estudos, em revistas de circulação internacional com revisão por pares, livros ou capítulos de livro, relevantes para o ciclo de estudos, nos últimos 5 anos.
http://www.a3es.pt/si/iportal.php/cv/scientific-publication/formId/28f60cc3-ff12-15f4-ea62-5bbc9a9aaa1e
8.3. Mapa-resumo de atividades de desenvolvimento de natureza profissional de alto nível (atividades de desenvolvimento tecnológico, prestação de serviços ou formação avançada) ou estudos artísticos, relevantes para o ciclo de estudos:
http://www.a3es.pt/si/iportal.php/cv/high-level-activities/formId/28f60cc3-ff12-15f4-ea62-5bbc9a9aaa1e
8.4. Lista dos principais projetos e/ou parcerias nacionais e internacionais em que se integram as atividades científicas, tecnológicas, culturais e artísticas desenvolvidas na área do ciclo de estudos.

Em áreas próximas ao ciclo de estudos proposto existem as licenciaturas de Engenharia Informática, Engenharia de Redes e Sistemas de Computadores e a Engenharia de Computação Gráfica e Multimédia. Além destes, existe também a pós-graduação em Informática de Segurança e Computação Forense. Em todos os ciclos de estudos correntes há várias parcerias em curso, nomeadamente com:
- APNOR - Associação de Politécnicos do Norte
- Instituto Politécnico de Leiria
- Instituto Politécnico do Porto
- Polícia Judiciária
- Procuradoria Geral da República
- Várias empresas no setor da informática e telecomunicações (Atlanse, Ubiquity, Borgwarner, G9Telecom, Bosch, DSTelecom, etc)
Além destas, serão também fomentadas parcerias especificamente na área da cibersegurança entre o IPVC e a Universidade de Vlgo, Espanha

8.4. List of main projects and/or national and international partnerships underpinning the scientific, technologic, cultural and artistic activities developed in the area of the study programme.

In areas close to the proposed study programme there are the degrees of Informatics Engineering, Network Engineering and Computer Systems and Computer and Multimedia Computer Engineering. In addition to these, there is also a postgraduation in Computer Security and Computer Forensics. In all current study cycles there are several ongoing partnerships, including:
- APNOR - North Polytechnic Association
- Instituto Politécnico de Leiria
- Instituto Politécnico do Porto
- Judiciary Police
- Attorney General's Office
- Several companies in the IT and telecommunications sector (Atlanse, Ubiquity, Borgwarner, G9Telecom, Bosch, DSTelecom, etc.)
In addition to these, partnerships specifically in the area of cybersecurity between the IPVC and the University of Vlgo, Spain

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

9.1. Avaliação da empregabilidade dos graduados por ciclo de estudos similares com base em dados oficiais:
A nível nacional (continente) o nível de desemprego registado entre os detentores de um grau académico de nível, superior, em dezembro de 2017, situava-se, de acordo com as estatísticas do Instituto de Emprego e Formação Profissional, de 14,2%. Na região Norte (NUT II) o nível global de desemprego, em Dezembro de 2017 era de 41,9%. Na actividade económica de Informação e Comunicação em Dezembro de 2017, o desemprego era de 1,4%. Não foram encontradas estatísticas relativas aos cursos similares (de 2º ciclo) em bases de dados oficiais.

9.1. Evaluation of the employability of graduates by similar study programmes, based on official data:
At the national level, the level of unemployment among the holders of a higher academic level in December 2017 was 14.2%, according to statistics from the IEFP. In the North region (NUT II) the overall level of unemployment in December 2017 was 41.9%. In the economic activity of Information and Communication in December 2017, unemployment was 1.4%. No statistics were found for similar courses (of 2nd cycle) in official databases.

9.2. Avaliação da capacidade de atrair estudantes baseada nos dados de acesso (DGES):
No IPVC e em particular na sua Escola Superior de Tecnologia e Gestão temos 3 cursos de engenharia com estudantes interessados em seguir a área da Segurança Informática, são eles o curso de Engenharia de Redes e Sistemas de Computadores, o de Engenharia Informática e o Engenharia de Computação Gráfica e Multimédia. Segundo dados de acesso (DGES):
- Engenharia Informática: 46(2013); 36(2014); 60(2015); 61(2016); 56(2017)
- Engenharia de Computação Gráfica e Multimédia: 8(2013); 6(2014); 19(2015); 18(2016); 27(2017)
- Engenharia de Redes e Sistemas de Computadores: (não tem ainda dados disponíveis uma vez que é um curso recente, mas é um curso que é preenchido na totalidade das vagas: 30 por ano)
Dos dados acima, temos que aproximadamente 100 alunos terminam a sua licenciatura na instituição. Não obstante a captação de alunos externos, muitos destes alunos internos pretendem seguir estudos nesta área da cibersegurança e assim, é de esperar no CE proposto um número entre 15 a 30 alunos.

9.2. Evaluation of the capability to attract students based on access data (DGES):
In IPVC, in particular ESTG 3 engineering courses exist with students interested in the area of Computer Security, are they the course of Computer Networks and Systems Engineering, Informatics Engineering and Engineering of Computer Graphics and Multimedia. According to access data (DGES):
- Informatics Engineering: 46 (2013); 36 (2014); 60 (2015); 61 (2016); 56 (2017)
- Engineering of Computer Graphics and Multimedia: 8 (2013); 6 (2014); 19 (2015); 18 (2016); 27 (2017)
- Network and Computer Systems Engineering: (data is not yet available since it is a recent course, but it is a course that is filled in the total of the places: 30 per year)
From the above data, we have approximately 100 students finishing their degree at the institution. Notwithstanding the recruitment of external students, many of these internal students intend to follow studies in this area of cybersecurity and thus, it is expected a number between 15 to 30 students in the proposed CE.

9.3. Lista de eventuais parcerias com outras instituições da região que lecionam ciclos de estudos similares:
Na região, e num raio de 80km não existem cursos de 2º ciclo na área da cibersegurança e portanto não existem parcerias com instituições da região. No entanto, até ao momento foram realizadas com sucesso 2 edições da Pós-graduação em Informática de Segurança e Computação Forense, em parceria com o Instituto Politécnico de Leiria, com a Polícia Judiciária e com a Procuradoria Geral da República. Na conceção do plano curricular proposto, existe ainda uma colaboração de docentes do Instituto Politécnico do Porto (IPP). Por conseguinte, assim que o CE seja avaliado, estas parcerias com instituições de referência nesta área serão formalizadas, em particular uma parceria com o IPP e com a Polícia Judiciária.

9.3. List of eventual partnerships with other institutions in the region teaching similar study programmes:
n the region, and within a radius of 80km there are no 2nd cycle courses in the area of cybersecurity and therefore there are no partnerships with institutions in the region. However, two editions of the Computer Security and Computing Forensics Postgraduate Program have been successfully completed in partnership with the Leiria Polytechnic Institute, the Polícia Judiciária and the Attorney General's Office. In the design of the proposed curricular plan, there is also a collaboration of professors from the Polytechnic Institute of Porto (IPP). Therefore, once the study programme is evaluated, these partnerships with institutions of reference in this area will be formalized, in particular a partnership with the IPP and the Polícia Judiciária.

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:
Europeu de Ensino Superior com duração e estrutura semelhantes à proposta:

Existe, no espaço europeu de ensino superior, um número considerável de cursos de mestrado em Cibersegurança com duração e objetivos semelhantes aos que aqui se propõe.
Alguns exemplos de escolas de ensino superior que oferecem este curso são:
- Universidade de Liverpool (Inglaterra);
- Universidade de Swansea (País de Gales);
- Universidade de Wolverhampton (Inglaterra)
- Universidade de Rennes (França)
- Universidade de Twente (Holanda)
- Universidade de Turku (Finlandia)
- Universidade de Trento (Itália)

10.1. Examples of study programmes with similar duration and structure offered by reference institutions in the European Higher Education Area:
There is a considerable number of master's degrees in Cybersecurity in the European Higher Education schools with duration and objectives similar to those proposed here.
Some examples of European Higher Education schools are:
- University of Liverpool (England);
- University of Swansea (Wales);
- University of Wolverhampton (England)
- University of Rennes (France)
- University of Twente (Netherlands)
- University of Turku (Finland)
- University of Trento (Italy)

10.2. Comparação com objetivos de aprendizagem de ciclos de estudos análogos existentes em instituições de referência do Espaço Europeu de Ensino Superior:
Os objetivos de aprendizagem do mestrado em Cibersegurança são semelhantes aos dos cursos existentes nas escolas de referência europeias. A generalidade dos cursos referidos no ponto anterior, enfatizam qualificações especializadas na área da Cibersegurança, combinando as mesmas áreas transversais abordadas nesta proposta, estando o foco de especialização em:
- Segurança de Redes, Sistemas e Informação,
- Programação Segura,
- e na Regulamentação, Auditoria e Análise Forense,
combinando estes aspetos avançados de segurança na sua aplicação prática e nas suas implicações dentro de uma empresa.

10.2. Comparison with the intended learning outcomes of similar study programmes offered by reference institutions in the European Higher Education Area:
The learning objectives of Cybersecurity are similar to those of the isolated subjects in European reference schools. Most of the disciplines mentioned above emphasize the qualifications in the area of Cybersecurity, combining the cross-sectional areas addressed in this proposal, being the focus of specialization in:
- Network Security and Information Systems,
- Secure Programming,
- and in Regulation, Auditing and Forensic Analysis,
combining these security advanced aspects in practical application and in the security issues inside a company.

11. Estágios e/ou Formação em Serviço

11.1. e 11.2 Estágios e/ou Formação em Serviço

Mapa VII - Protocolos de Cooperação

Mapa VII - Protocolos de Cooperação

11.1.1. Entidade onde os estudantes completam a sua formação:
<sem resposta>

11.1.2. Protocolo (PDF, máx. 150kB):
<sem resposta>

11.2. Plano de distribuição dos estudantes

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

<sem resposta>

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

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

<sem resposta>

11.3. Institution's own resources to effectively follow its students during the in-service training periods:

<no answer>

11.4. Orientadores cooperantes

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

<sem resposta>

11.4.2. 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:

- Objetivos adequados à realidade do mercado e necessidades globais;
- Plano curricular orientado para a aplicação prática dos conhecimentos;
- Corpo docente diversificado e especializado com experiência área da Segurança Informática
- Experiência adquirida com a realização de duas edições da Pós-Graduação Cibersegurança e Informática Forense;
- Realização de várias edições de um seminário técnico-científico em Cibersegurança (http://www.ipvc.pt/estg-iii-seminario-ciberseguranca);
- Reputação bem estabelecida do IPVC, quer a jusante junto de potenciais formandos, quer a montante junto das empresas;
- A capacidade científica instalada do corpo docente, validada pelas publicações na área científica do CE;
- A qualidade e diversidade dos recursos existentes, incluindo instalações, equipamentos e serviços (Biblioteca, Laboratórios de Informática, Serviços de Ação Social);
- Existência de parcerias de colaboração com outras Instituições no âmbito de formações na mesma área (ex. parceria com a Polícia Judiciária, a Procuradoria Geral da República, IPL, e outras empresas da área);
- Alinhamento com segundos ciclos similares em universidades reconhecidas na Europa;
- Quadro de docentes único no IPVC, e não por Escola, o que permite uma maior flexibilidade na gestão do pessoal

docente.

12.1. Strengths:

- Objectives of the study programme appropriate to the reality of the market and global needs;
- Curricular plan oriented towards the practical application of knowledge;
- Diversified and specialized teaching staff with experience in the Computer Security area
- Experience gained with the realization of two editions of the post graduation of Cyber Security and Forensic Computer Science;
- Realization of several editions of a technical-scientific seminar in Cybersecurity (http://www.ipvc.pt/estg-iii-seminario-ciberseguranca);
- Well-established reputation of IPVC, both downstream of potential trainees and upstream to companies;
- The installed scientific capacity of the faculty, validated by the publications in the scientific area of the study programme;
- The quality and diversity of existing resources, including facilities, equipment and services (Library, Information Technology Laboratories, Social Action Services);
- Existence of partnerships with other Institutions in the area of training in the same area (eg partnership with the Policia Judiciária, the Attorney General's Office, IPL and other companies in the area);
- Alignment with similar second cycles at recognized universities in Europe;
- Single staff of teachers in the IPVC, not by School, which allows for greater flexibility in the management of teaching staff.

12.2. Pontos fracos:

- Poucas empresas especializadas neste domínio na Região (designadamente Consultoras de Segurança Informática);
- Ainda alguma falta de conhecimento do que é a CiberSegurança por parte de muitas das empresas da Região, nomeadamente das Pequenas e Médias Empresas;
- A existência de uma linha de Investigação no IPVC orientada para a área específica da CiberSegurança com a contribuição de vários docentes é relativamente recente (3~4 anos);
- Falta de docentes com o título de especialista na área.

12.2. Weaknesses:

- Few companies specialized in this field in the Region (namely Computer Security Consultants);
- Still some lack of knowledge of what is Cybersecurity by many of the companies in the Region, namely Small and Medium Enterprises;
- The existence of a line of Research in the IPVC oriented to the specific area of Cybersecurity with the contribution of several teachers is relatively recent (3 ~ 4 years);
- Lack of teachers with the title of specialist in the field.

12.3. Oportunidades:

- Oferta inovadora e diferenciada na área geográfica;
- Conhecimentos adquiridos no ciclo de estudos cada vez mais cruciais num mundo globalizado e da informação;
- Existência de uma nova Unidade de Investigação no IPVC, o ARC4DigIT, que é uma oportunidade de potenciar as competências I&D específicas do IPVC na área do CE;
- Necessidade, na região, de quadros de empresa capazes de inovar e de criar valor pela qualidade e pela diferença;
- Necessidade de requalificação profissional e valorização da aprendizagem ao longo da vida;
- A Cibersegurança está elencada como uma área estratégica no programa quadro Europeu Horizonte 2020;
- Proximidade ao mercado espanhol, sem oferta formativa nesta área;
- Reforço de parcerias/colaborações externas, e procura de novos parceiros no desenvolvimento de projetos técnicos e de investigação;
- Estabilização do corpo docente.

12.3. Opportunities:

- Innovative and differentiated offer in the geographical area;
- Knowledge acquired in the cycle of studies increasingly crucial in a globalized world and of information;
- Existence of a new IPVC Research Unit, ARC4DigIT, which is an opportunity to enhance IPVC specific R&D competences in the study programme area;
- The need, in the region, for companies capable of innovating and creating value through quality and difference;
- The need for professional retraining and lifelong learning;
- Cybersecurity is listed as a strategic area in the Horizon 2020 European Framework Program;
- Proximity to the Spanish market, without the training offer in this particular area;
- Strengthening of external partnerships/collaborations, and seeking new partners in the development of technical and research projects;
- Stabilization of the teaching staff.

12.4. Constrangimentos:

- Abertura em IES próximas de cursos de pós-gradução na mesma área de especialização;
- Ainda pouca valorização, sobretudo remuneratória, da formação pós-graduada pelas muitas entidades empregadoras;
- Incertezas nas perspetivas de evolução nas políticas de financiamento do sistema científico e tecnológico nacional;
- Reduzido apoio financeiro para a investigação dos docentes;
- Incumprimento do pagamento de propinas devido a dificuldades económicas dos estudantes.

12.4. Threats:

- Opening postgraduate courses in close IES in the same area of specialization;
- There is still little appreciation, especially for remuneration, of postgraduate training by many employers;
- Uncertainties in the evolution perspectives in the financing policies of the national scientific and technological system;
- Reduced financial support for teacher research;
- Failure to pay tuition fees due to students' financial difficulties.

12.5. Conclusões:

Em conclusão, no que respeita ao ambiente interno do IPVC estão reunidos os recursos humanos e materiais, bem como a rede de contactos e a construção de uma reputação positiva, junto das entidades públicas e privadas, para que o mestrado em cibersegurança possa funcionar com sucesso.
É ainda importante acrescentar que no âmbito do Plano Estratégico do IPVC (2015-2019), uma das atividades consideradas estratégicas e contempladas é o de incrementar a utilização das TIC, sendo por isso fundamental incluir nessa atividade todas as questões vinculadas com a segurança das redes, sistemas e dados.
É também importante referir, por outro lado, que está consagrada na Estratégia Nacional de Especialização Inteligente - Portugal 2020 (ENEI) como visão que Portugal deve consolidar ou fazer emergir a sua liderança na economia digital através da utilização e desenvolvimento das vantagens adquiridas em tecnologias de informação e de comunicação. Nesse sentido um dos temas identificados no ENEI é o Tecnologias de Informação e Comunicação, inserido no eixo temático 1 - TECNOLOGIAS TRANSVERSAIS E SUAS APLICAÇÕES, sendo um dos tópicos de desenvolvimento referidos a Cibersegurança, como forma de Promoção da Internet do Futuro, considera por isso o IPVC que a proposta deste Mestrado em Cibersegurança está perfeitamente enquadrada com a visão e a estratégia nacional 2020, constituindo-se também como um polo de potencial inovação nomeadamente na Competitividade e Tecnologia das TICE. Nesse mesmo sentido, mas englobada na Estratégia Regional de Especialização Inteligente (RIS3) - Norte 2020 a componente da Cibersegurança é referenciada como um elemento fundamental no Eixo Prioritário 9- Capacitação Institucional e TIC, estando, por isso, este novo CE inserido nos instrumentos para a concretização da visão da estratégia de desenvolvimento regional prevista no NORTE 2020: "A Região do Norte será, em 2020, capaz de gerar um nível de produção de bens e serviços transacionáveis que permita recuperar a trajetória de convergência a nível europeu, assegurando, de forma sustentável, acréscimos de rendimento e de emprego da sua população e promovendo, por essa via, a coesão económica, social e territorial."

12.5. Conclusions:

In conclusion, regarding to the internal environment of the IPVC, the human and material resources, as well as the network of contacts and the positive reputation, gathered from public and private entities, are met so that this masters in cybersecurity can successfully be implemented.
It is also important to add that within the scope of the Strategic Plan of the IPVC (2015-2019), one of the activities considered strategic and contemplated is to increase the use of ICT, and it is therefore fundamental to include in this activity all issues related to network security, systems and data.
It is also important to mention that it is enshrined in the National Strategy for Intelligent Specialization - Portugal 2020 (ENEI) as a vision that Portugal must consolidate or emerge its leadership in the digital economy through the use and development of the advantages acquired in technologies of information and communication. In this sense one of the themes identified in ENEI is Information and Communication Technologies, inserted in the thematic axis 1 - TRANSVERSE TECHNOLOGIES AND ITS APPLICATIONS, being one of the topics of development referred to Cybersecurity, as a way of promoting the Internet of the Future, considers therefore the IPVC that the proposal of this Masters in Cybersecurity is perfectly framed with the vision and national strategy 2020, constituting also as a pole of potential innovation namely in the Competitiveness and Technology of the TICE. In the same sense, but included in the Regional Strategy for Intelligent Specialization (RIS3) - North 2020, the Cybersecurity component is referred to as a fundamental element in Priority Axis 9 - Institutional Capacity Building and ICT, and this new study programme is therefore included in the instruments for the NORTE 2020 vision of the regional development strategy: "The Northern Region will be able, in 2020, to generate a level of production of tradable goods and services that will make it possible to recover the convergence trajectory at European level assuring the income and employment of its population and thereby promoting economic, social and territorial cohesion."