1. Caracterização

1.1. Instituição de Ensino Superior:

Instituto Politécnico Do Cávado E Ave

1.1.a. Instituições de Ensino Superior (em associação) (artigo 41.º e seguintes do Decreto-Lei n.º 74/2006, de 24 de março, na redação dada pelo Decreto-Lei n.º 65/2018, de 16 de agosto e aditada pelo Decreto-Lei n.º 27/2021, de 16 de abril):

[sem resposta]

1.1.b. Outras Instituições de Ensino Superior (estrangeiras, em associação) (artigo 41.º e seguintes do Decreto-Lei n.º 74/2006, de 24 de março, na redação dada pelo Decreto-Lei n.º 65/2018, de 16 de agosto e aditada pelo Decreto-Lei nº 27/2021, de 16 de abril):

[sem resposta]

1.1.c. Outras Instituições (em cooperação) (artigo 41.º e seguintes do Decreto-Lei n.º 74/2006, de 24 de março, na redação dada pelo Decreto-Lei n.º 65/2018, de 16 de agosto e aditada pelo Decreto-Lei nº 27/2021, de 16 de abril. Vide artigo 6.º do Decreto-Lei n.º 133/2019, de 3 de setembro, quando aplicável):

[sem resposta]

1.2. Unidade orgânica (faculdade, escola, instituto, etc.):

Escola Superior De Tecnologia

1.2.a. Identificação da(s) unidade(s) orgânica(s) da(s) entidade(s) parceira(s) (faculdade, escola, instituto, etc.) (proposta em associação). (Decreto-Lei n.º 74/2006, de 24 de março, na redacção conferida pelo Decreto-Lei n.º 65/2018, de 16 de agosto, alterado pelo Decreto-Lei nº 27/2021 de 16 de abril):

[sem resposta]

1.3. Designação do ciclo de estudos (PT):

Cibersegurança Aplicada

1.3. Designação do ciclo de estudos (EN):

Applied Cibersecurity

1.4. Grau (PT):

Mestre

1.4. Grau (EN):

Master

1.5. Área científica predominante do ciclo de estudos. (PT)

Engenharia Informática

1.5. Área científica predominante do ciclo de estudos. (EN)

Computer Engineering

1.6.1. Classificação CNAEF – primeira área fundamental

[0481] Ciências Informáticas - Informática - Ciências, Matemática e Informática

1.6.2. Classificação CNAEF – segunda área fundamental, se aplicável

[sem resposta]

1.6.3. Classificação CNAEF – terceira área fundamental, se aplicável

[sem resposta]

1.7. Número de créditos ECTS necessário à obtenção do grau. (PT)

60.0

1.8. Duração do ciclo de estudos.

1 ano

1.8.1. Outra

[sem resposta]

1.9. Número máximo de admissões proposto

30.0

1.10. Condições específicas de ingresso. (PT)

1) Titulares do grau de licenciado ou equivalente legal nas áreas de Tecnologias de Informação e áreas afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
2) Titulares de um grau académico superior estrangeiro nas áreas de Tecnologias de Informação e áreas afins que seja reconhecido como satisfazendo os objetivos do grau de licenciado pelo Conselho Técnico-Científico, nas mesmas áreas de 1) e afins, com experiência profissional, mínima de 5 anos, devidamente comprovada;
3) Detentores de currículo académico, científico ou profissional, cuja capacidade seja reconhecida pelo CTC da escola, nas áreas referidas em 1), com experiência profissional, mínima de 5 anos, devidamente comprovada;
Os candidatos serão avaliados e seriados considerando a sua formação curricular e a natureza e relevância da sua experiência profissional, sendo privilegiados profissionais, executivos, quadros e dirigentes que pretendam estruturar conhecimento e o aplicar em Cibersegurança.

1.10. Condições específicas de ingresso. (EN)

1) Holders of a bachelor's degree or legal equivalent in the areas of Computer Engineering and related areas, with at least 5 years' professional experience duly proven;
2) Holders of a foreign higher academic degree that is recognized as meeting the objectives of the Bachelor's degree by the Scientific-Technical Council, in the same areas as 1) and with at least 5 years' professional experience duly proven;
3) Holders of an academic, scientific or professional curriculum, whose capacity is recognized by the Scientific- Technical Council of the School, in the areas referred to in 1), with at least 5 years' professional experience duly proven.
Candidates will be evaluated and graded considering their curriculum background and the nature and relevance of their professional experience, with professionals, executives, staff and managers with or without training in management who wish to structure knowledge and applying it in Cybersecurity.

1.11. Modalidade do ensino

Presencial

1.11.1 Regime de funcionamento, se presencial

Pós-laboral

1.11.1.a Se outro, especifique. (PT)

[sem resposta]

1.11.1.a Se outro, especifique. (EN)

[sem resposta]

1.12. Local onde o ciclo de estudos será ministrado (se aplicável). (PT)

Campus do IPCA - Barcelos

1.12. Local onde o ciclo de estudos será ministrado (se aplicável). (EN)

Campus do IPCA - Barcelos

1.13. Regulamento de creditação de formação académica e de experiência profissional, publicado em Diário da República

1.13._Despacho-n.º9030_2020_RA_IPCA-40-45_compressed.pdf

1.14. Observações. (PT)

O artigo 18 do Decreto-Lei no 65/2018 apresenta a possibilidade de criação de ciclos de estudo (CE) conducentes ao grau de mestre com 60 créditos, com duração normal de dois semestres curriculares e vocacionado para a promoção da aprendizagem ao longo da vida. No sentido de dar continuidade à estratégia de oferta formativa diferenciada pela EST/IPCA, foi realizada uma análise prospetiva de áreas inovadoras com potencial para criação dos referidos mestrados, tendo sido identificada a área da cibersegurança.
Assim, após a identificação da área em questão, e atendendo aos Protocolo de Cooperação com algumas empresas da área da cibersegurança, foi identificada a possibilidade de preparação de um ciclo de estudos que irá permitir: a integração dos estudantes em empresas da área da cibersegurança, o desenvolvimento/aprofundamento de competências técnicas relevantes para o mercado de trabalho e a promoção da aprendizagem ao longo da vida.
Nesse sentido, parece existir enquadramento suficiente para propor a criação de um novo mestrado na Escola Superior de Tecnologia, na área científica da Engenharia Informática, com um foco específico na Cibersegurança.

1.14. Observações. (EN)

Article 18 of Decree-Law No. 65/2018 presents the possibility of creating study cycles (EC) leading to the degree of master with 60 credits, with a normal duration of two curricular semesters and aimed at the promotion of lifelong learning. In order to give continuity to the strategy of differentiated training offer by EST/IPCA, a prospective analysis of innovative areas with potential for the creation of the referred masters was carried out, and the area of cybersecurity was identified.
Thus, after the identification of the area in question, and taking into account the Cooperation Protocols with some companies in the area of cybersecurity, the possibility was identified to prepare a study cycle that will allow: the integration of students in companies in the area of cybersecurity, the development/deepening of technical skills relevant to the labour market and the promotion of lifelong learning.
In that sense, there seems to be enough framework to propose the creation of a new master's degree in the School of Technology, in the scientific area of Computer Engineering, with a specific focus on Cybersecurity.

2. Formalização do Pedido

Mapa I - Conselho Pedagógico da Escola Superior de Tecnologia

Órgão ouvido:

Conselho Pedagógico da Escola Superior de Tecnologia

Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada:

Extrato ponto 9 Ata 13 2022-11-11_signed.pdf

Mapa I - Conselho Técnico-Científico da Escola Superior de Tecnologia

Órgão ouvido:

Conselho Técnico-Científico da Escola Superior de Tecnologia

Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada:

Extrato Minuta Acta_CTC_11_11_2022_signed_signed.pdf

Mapa I - Conselho Académico do Instituto Politécnico do Cávado e do Ave

Órgão ouvido:

Conselho Académico do Instituto Politécnico do Cávado e do Ave

Cópia de ata (ou extrato de ata) ou deliberação deste órgão assinada e datada:

Extrato_Acta nu?mero 33_CA_2022 (14-11) (002)_assinado.pdf

3. Âmbito e Objetivos

3.1. Objetivos gerais definidos para o ciclo de estudos (PT)

O Mestrado em Cibersegurança Aplicada tem por objetivo complementar a formação adquirida num primeiro ciclo de estudos em Engenharia Informática e áreas afins, aliada a uma sólida experiência profissional comprovada, de pelo menos cinco anos, na área do ciclo de estudos.
Visa transmitir aos estudantes um leque de competências que lhes permitam organizar, implementar, coordenar e controlar um sistema informático com características de segurança, numa organização.

A sólida formação adquirida nos domínios referidos faz do Mestre em Cibersegurança Aplicada um agente de inovação e mudança cultural e tecnológica na empresa. Este profissional sistematiza soluções, planeia e gere ações que visam aproveitar as oportunidades e prevenir as ameaças que rodeiam a empresa, de modo a garantir a segurança dos sistemas informáticos, a segurança da informação e a continuidade da operação dos sistemas de informação.

3.1. Objetivos gerais definidos para o ciclo de estudos (EN)

The Master in Applied Cybersecurity aims to complement the training acquired in a first cycle of studies in Computer Engineering and related areas, combined with a solid proven professional experience of at least five years in the area of the study cycle.
It aims to provide students with a range of competences that will enable them to organise, implement, coordinate, and control a computer system with security features in an organisation.
The solid training acquired in the mentioned domains makes the Master in Applied Cybersecurity an agent of innovation and cultural and technological change in the company. This professional systematises solutions, plans and manages actions aimed at seizing opportunities and preventing threats that surround the company, in order to guarantee the security of the computer systems, the security of the information and the continuity of the operation of the information systems.

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

Os Conhecimentos a serem adquiridos são:
- Principais normas no âmbito da Cibersegurança;
- Várias técnicas de inteligência artificial;
- Algoritmos criptográficos e técnicas a adotar em diversos cenários; - Legislação atual aplicável;
- Principais falhas de segurança.
As Competências a serem adquiridas são:
- Resolver problemas que envolvem questões legais de cibersegurança;
- Realizar um levantamento forense de um sistema informático para sua análise posterior;
- Delinear uma estratégia para a Cibersegurança, realçando a visão, a missão e os objetivos, e garantindo o alinhamento com o plano estratégico da organização;
- Monitorizar e avaliar a eficiência dos controlos de Cibersegurança adotados por uma organização, com o objetivo de garantir que estes proporcionam o nível de segurança desejado;
- Utilizar aplicações para prevenir intrusões nos sistemas, e verificar a sua integridade;
- Identificar vulnerabilidades nas redes e sistemas informáticos;

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

Students are intended to learn:
- Main standards in the field of Cybersecurity;
- Various techniques of artificial intelligence used in the field of Cybersecurity;
- Cryptographic algorithms and techniques to be adopted in various scenarios such as software developments, systems administration and computer networks;
- Current legislation applicable;
- Main security flaws in application development.
Students should also acquire the following competencies:
- Solve problems involving cybersecurity legal issues;
- Carry out a forensic survey of a computer system for its subsequent analysis;
- Outline a strategy for Cybersecurity, highlighting the vision, mission and objectives, and ensuring alignment with the strategic plan of the organisation;
- Monitor and evaluate the efficiency of the Cybersecurity controls;
- Use applications to prevent intrusions into systems, and verify their integrity;
- Identify vulnerabilities in networks and computer systems;

3.3. Justificar a adequação do objeto e objetivos do ciclo de estudos à modalidade do ensino e, quando aplicável, à percentagem das componentes não presencial e presencial, bem como a sua articulação. (PT)

Este novo ciclo de estudos é proposto na modalidade de ensino presencial, em regime de funcionamento pós-laboral. Sendo o objeto desta proposta a Cibersegurança Aplicada, esta tira proveito do ensino presencial em laboratório para a aplicação prática das competências descritas no ponto anterior, de modo a permitir aos estudantes explorarem todo o potencial do acesso aos equipamentos disponíveis e de poderem experimentar de um modo prático os desafios que irão encontrar num sistema de informação real em produção.

3.3. Justificar a adequação do objeto e objetivos do ciclo de estudos à modalidade do ensino e, quando aplicável, à percentagem das componentes não presencial e presencial, bem como a sua articulação. (EN)

This new study cycle is proposed in the face-to-face teaching modality, in an after-working hours regime. Being Applied Cybersecurity the object of this proposal, it will take advantage of face-to-face teaching in a laboratory facility for the practical application of the competences described in the previous point, in order to allow students to explore all the potential of the access to the available equipment and to be able to experience in a practical way the challenges that they will find in a real information system in production.

3.4. Justificar a 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. (PT)

O IPCA é uma Instituição de Ensino Superior Público, em crescimento sustentado, com intervenção nas áreas das tecnologias, das ciências empresariais, do design e do turismo, tendo como missão contribuir para o desenvolvimento da sociedade, estimular a criação cultural, a investigação e pesquisa aplicadas, e fomentar o pensamento reflexivo e humanista. De acordo com a sua Missão, e no sentido de uma resposta adequada a contextos de mudança e espaços de gestão de dinâmicas locais e globais de desenvolvimento e inovação, aproveitando as oportunidades e minimizando as ameaças, o Instituto assume como fundamentais os seguintes valores: Ética; Excelência; Ensino Inclusivo, Inovador e Flexível; Transferência e Valorização do Conhecimento; Competitividade e o Empreendedorismo. Entre os desafios e objetivos traçados na Estratégia Portugal 2030 destacam-se o aumento do número de alunos no ensino superior, com especial enfoque nas áreas STEAM e na área de competências digitais, o aumento da participação da população adulta ao longo da vida ensino superior e programas de requalificação e requalificação. Assim, enquanto agente do sistema científico e de ensino superior, o IPCA está empenhado em contribuir para o crescimento das qualificações em Portugal, em particular contribuir para a implementação das reformas e investimentos propostos pelo PRR, dando continuidade à implementação das redes europeias e para reforçar a articulação entre as instituições de ensino e formação, as instituições científicas e os locais, regionais e empregadores nacionais. A proposta de mestrado profissionalizante em Cibersegurança Aplicada enquadra-se:

- no Plano Estratégico do IPCA 2021-2025, em concreto no objetivo estratégico OE7 - Formação de cidadãos socialmente responsáveis, para garantir uma oferta formativa de qualidade e adequada às expectativas do mercado de trabalho;

- nos objetivos do PRR ao nível do programa "Impulso Adulto"; no sentido de apoiar a conversão e atualização de competências de adultos ativos, através de formação superior em áreas STEAM;

- na estratégia da Instituição em oferecer um novo ciclo de estudos de mestrado decorrente do reconhecimento e acreditação externa da qualidade dos seus cursos de licenciatura, nomeadamente do curso de Licenciatura em Engenharia de Sistemas Informáticos e da crescente exigência do mercado ao nível da oferta formativa de 2.o ciclo;

- no envolvimento do IPCA com o tecido empresarial da sua região de intervenção, que se manifesta disponível para esta intervenção;

- na oportunidade que este mestrado profissionalizante representa para a melhoria da qualificação do corpo docente da Escola Superior de Tecnologia, com o consequente aumento do pessoal docente na área da Informática, em particular na Cibersegurança. Por último importa referir o reconhecimento do centro de investigação 2Ai (Applied Artificial Intelligence Laboratory) pela FCT.

3.4. Justificar a 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. (EN)

IPCA is a Public Higher Education Institution, in sustained growth, with intervention in the areas of technology, business sciences, design and tourism, with the mission of contributing to the development of society, stimulating cultural creation, investigation and research applied, and foster reflective and humanistic thinking. In accordance with its Mission, and to respond to changing contexts and spaces for managing local and global dynamics of development and innovation, taking advantage of opportunities and minimising threats, the Institute assumes the following values as fundamental: Ethics; Excellence; Inclusive, Innovative and Flexible Teaching; Knowledge Transfer and Valorisation; Competitiveness and Entrepreneurship.

Among the challenges and objectives outlined in the Portugal 2030 Strategy, we highlight the increase in the number of students in higher education, with a special focus on the STEAM areas and in the area of digital skills, the increase in the participation of the adult population in higher education and requalification programs. Thus, as an agent of the scientific and higher education system, the IPCA is committed to contributing to the growth of qualifications in Portugal, in particular contributing to the implementation of the reforms and investments proposed by the PRR, continuing the implementation of European networks and strengthening the articulation between education and training institutions, scientific institutions and local, regional and national employers.

The proposal for a professional master's degree in Applied Cybersecurity fits:

- in the IPCA Strategic Plan 2021-2025, specifically in the strategic objective OE7 - Training of socially responsible citizens, to guarantee a training offer of quality and adequate to the expectations of the labor market;

- on the objectives of the PRR at the level of the "Impulso Jovem" program; in order to support the conversion and updating of skills of active adults, through higher education in STEAM areas;

- in the Institution's strategy of offering a new cycle of master's studies resulting from the external recognition and accreditation of the quality of its degree courses, namely the Degree course in Informatics Engineering and the growing demand of the market in terms of the training offer of 2nd cycle;

- in the involvement of IPCA with the business fabric of its region of intervention, which manifests itself available for this intervention;

- in the opportunity that this professional master's degree represents for the improvement of the qualification of the teaching staff of the School of Technology, with the consequent increase in the teaching staff in the field of Informatics, namely Cybersecurity.

Finally, it is important to mention the recognition of the 2Ai (Applied Artificial Intelligence Laboratory) research center by FCT.

4. Desenvolvimento curricular

4.1. Estrutura Curricular

Mapa II - Percurso geral

4.1.1. Ramos, variantes, áreas de especialização, especialidades ou outras formas de organização em que o ciclo de estudos se estrutura (a preencher apenas quando aplicável)* (PT):
Percurso geral

4.1.1. Ramos, variantes, áreas de especialização, especialidades ou outras formas de organização em que o ciclo de estudos se estrutura (a preencher apenas quando aplicável)* (EN):
Main Track

4.1.2. Áreas científicas e créditos necessários à obtenção do grau

Área Científica	Sigla	ECTS	ECTS Minímos
Arquitectura de Computadores e Sistemas Distribuídos e Cibersegurança	ACSDC	45.0	
Ciências da Computação	CC	3.0	
Ciências Jurídico-Fundamentais	CJF	0.0	3.0
Sistemas de Informação e Inteligência Artificial	SIIA	9.0	3.0
Total: 4		Total: 57.0	Total: 6.0

4.1.3. Observações (PT)

4.1.3. Observações (EN)

4.2. Unidades Curriculares

Mapa III - Auditoria Informática

4.2.1. Designação da unidade curricular (PT):
Auditoria Informática

4.2.1. Designação da unidade curricular (EN):
Computer Auditing

4.2.2. Sigla da área científica em que se insere (PT):
SIIA

4.2.2. Sigla da área científica em que se insere (EN):
IS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - T-10.0; TP-10.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Paulo Teixeira - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Como principais objetivos da unidade curricular estão a passagem do conhecimento prático sobre técnicas e teorias de Auditoria Informática com especial foco na auditoria da segurança de sistemas e redes de comunicações tecnológicas.
No final da unidade os alunos deverão perceber os desafios e conseguir efetuar auditorias e relatórios de elevada complexidade sobre os mais variados sistemas de informação.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
As main objectives of the curricular unit are the passage of practical knowledge about techniques and theories of Computer Auditing with a special focus on auditing the security of systems and technological communications networks.
At the end of the unit students should understand the challenges and be able to carry out highly complex audits and reports on the most varied information systems.

4.2.11. Conteúdos programáticos (PT):
1. Introdução à auditoria informática. 2. Controlos Internos: a) Etapas da auditoria; b) Ferramentas de auditoria; c) Técnicas de Auditoria e Avaliação de Software de Auditoria. 3. Relatório e Matrizes.

4.2.11. Conteúdos programáticos (EN):
1. Introduction to computer auditing; 2. Internal controls: a) Audit steps; b) Auditing tools; c) Audit Techniques and Audit Software Evaluation. 3. Report and Matrices.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos estão organizados de forma integrada, visando permitir a análise de perspetivas pertinentes para a Auditoria Informática. Parte-se de aspetos gerais da auditoria (1.) para o estudo das metodologias de controlos internos (2.) e uma análise aprofundada da metodologia de reporting (3.). No conjunto, pretende promover-se a aquisição de conhecimentos científicos e práticos para o desenvolvimento de competências profissionais.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The contents are organized in an integrated way, aiming to allow the analysis of pertinent perspectives for Computer Audit. It starts with general aspects of the audit (1.) for the study of internal control methodologies (2.) and an in-depth analysis of the reporting methodology (3.) As a whole, the intention is to promote the acquisition of scientific and practical knowledge for the development of professional skills.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

O desenvolvimento dos conteúdos será realizado com base numa abordagem teórica e teórico-empírica, construindo um quadro de referência de base, quer através de exposição quer de trabalhos de pesquisa e síntese. Estas abordagens serão complementadas, numa perspetiva de aplicação, com a análise de casos e a resolução de problemas. O desenvolvimento de competências será potenciado por estratégias de simulação.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

The development of the contents will be carried out based on a theoretical and theoretical-empirical approach, building a basic frame of reference, either through exposure, or through research and synthesis works. These approaches will be complemented, from an application perspective, with case analysis and problem solving. The development of skills will be enhanced by simulation strategies.

4.2.14. Avaliação (PT):
A avaliação será feita através de um exame teórico/prático (100%)

4.2.14. Avaliação (EN):
The evaluation will be made through an theoretical-practical exam (100%)

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
As metodologias de ensino e de aprendizagem visam o desenvolvimento integrado nos estudantes dos conhecimentos referidos nos conteúdos programáticos e a concretização dos objetivos e competências estabelecidos. A diversidade de conteúdos propostas tem por objetivo potenciar abordagem complexa da auditoria informática. Os métodos e estratégias propostos pretendem desenvolver nos alunos conhecimentos, compreensão e competências ao nível da aplicação.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
The development of the contents will be carried out based on a theoretical and theoretical-empirical approach, building a basic frame of reference, either through exposure, or through research and synthesis works. These approaches will be complemented, from an application perspective, with case analysis and problem solving. The development of skills will be enhanced by simulation strategies.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
James A. Hall (2016) Information Technology Auditing (ISBN: 978-113-394-988-6).
Peter H. Gregory (2019) CISA Certified Information Systems Auditor All-in-One Exam Guide, 4Th Edition (ISBN:978-125- 958-416-9).
Martin Weiss, Michael Solomon (2021) Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance) (978-1284090703).
Cees van der Wens (2019) SO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses (ISBN: 978-109-854-768-4).

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
James A. Hall (2016) Information Technology Auditing (ISBN: 978-113-394-988-6).
Peter H. Gregory (2019) CISA Certified Information Systems Auditor All-in-One Exam Guide, 4Th Edition (ISBN:978-125- 958-416-9).
Martin Weiss, Michael Solomon (2021) Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance) (978-1284090703).
Cees van der Wens (2019) SO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses (ISBN: 978-109-854-768-4).

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Criptografia Aplicada à Cibersegurança

4.2.1. Designação da unidade curricular (PT):
Criptografia Aplicada à Cibersegurança

4.2.1. Designação da unidade curricular (EN):
Cryptography Applied to Cybersecurity

4.2.2. Sigla da área científica em que se insere (PT):
ACSDC

4.2.2. Sigla da área científica em que se insere (EN):
CADS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - T-10.0; TP-10.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Óscar Ribeiro - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A Unidade Curricular tem como objetivo possibilitar aos alunos adquirir conhecimentos relativamente à seleção e aplicação dos sistemas criptográficos, estudando e entendendo a forma de implementar de uma variedade de mecanismos de cifra e autenticação.
No fim da Unidade Curricular os alunos devem ser capazes de: Selecionar algoritmos e técnicas a adotar em diversos cenários como o desenvolvimentos de software e a administração de sistemas e redes informáticas; Compreender os algoritmos de cifra na vertente científica e aplicada em ambientes de segurança da informação; Entender a utilização e a operação de uma variedade de mecanismos de controle de acesso e autenticação; Analisar, modificar, selecionar e implementar os protocolos necessários em cenários reais; Implementar os algoritmos criptográficos estudados; Aplicar técnicas de criptoanálise.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
The Curricular Unit aims to provide students with knowledge for the selection and application of cryptographic systems, studying and understanding how to implement a variety of mechanisms of encryption and authentication.
At the end of the unit students must be able to: Select algorithms and techniques to be adopted in different scenarios such as software development, systems administration and computer networks; Understand the encryption algorithms in the scientific and applied fields in information security environments; Understand the use and operation of a variety of access control and authentication mechanisms; Analyze, modify, select and implement the necessary protocols in real scenarios; Implement the studied cryptographic algorithms; Apply cryptanalysis techniques.

4.2.11. Conteúdos programáticos (PT):
1. Fundamentos de Segurança e Criptografia. 2. Criptografia Simétrica. 3. Cifras de Blocos e de Fluxo. 4. Criptografia Assimétrica. 5. Funções Hash e Autenticação. 6. Infraestruturas de Chave Pública. 7. Aplicações de diversas técnicas criptográficas.

4.2.11. Conteúdos programáticos (EN):
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. Cryptography Applications.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Para que os alunos sejam capazes de selecionar e aplicar sistemas criptográficos têm que dominar as seguintes temáticas: Estudar os fundamentos de Segurança e Criptografia, Criptografia Simétrica, Cifras de Blocos e de Fluxo, Criptografia Assimétrica, Funções Hash e Autenticação, Infraestruturas de Chave Pública e aplicar diversas técnicas criptográficas. Todos estes tópicos estão incluídos no conteúdo programático.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

For students to be able to select and apply cryptographic systems, they must master the following themes: Study the Fundamentals of Security and Encryption, Symmetric Encryption, Block and Flow Ciphers, Asymmetric Cryptography, Hash functions, Message Authentication, Public Key Infrastructures and Cryptography Applications. All of these topics are included in the syllabus.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

No decorrer das Aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão desenvolvidos trabalhos práticos com o objetivo de consolidar e demonstrar a aplicação prática dos conceitos teóricos abordados.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

In the theoretical-practical classes the program will be presented in the form of notes or slides. In practical classes, practical work will be developed in order to consolidate and demonstrate the practical application of the theoretical concepts covered.

4.2.14. Avaliação (PT):

A Avaliação contínua da unidade curricular é obtida pela média da componente teórica e componente prática com a seguinte ponderação: 50% Trabalhos práticos 50% Teste de Avaliação. Se o aluno não obtiver aproveitamento na avaliação contínua, poderá realizar um exame global no final do período letivo.

4.2.14. Avaliação (EN):

The continuous assessment of the course is obtained by the average of the theoretical and practical components with the following weighting: 50% Practical work 50% Test. If the student does not pass on the continuous assessment, the student may take a global exam at the end of the term.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):

Após a apresentação teórica dos conceitos fundamentais da criptografia nas aulas teórico-práticas, os mesmos serão aplicados nas aulas práticas, permitindo assim uma aprendizagem sustentada e aplicada à realidade, com o uso de diversas técnicas criptográficas.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):

After the theoretical presentation of the fundamental concepts of cryptography in the theoretical-practical classes, students will apply these concepts in the practical classes, allowing a sustained learning applied to reality, with the use of various cryptographic techniques.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):

Stallings, W. (2017). Cryptography and network security: Principles and practice. Boston: Pearson Prentice Hall. Jonathan Katz and Yehuda Lindell. (2019). Introduction to Modern Cryptography, Third Edition (3rd ed.). Chapman& Hall/CRC.
Zúquete.A. (2018). Segurança em Redes Informáticas - 5a edição. Editora FCA.
Goldreich, O. (2007). Foundations of cryptography. Cambridge: Cambridge Univ. Press.
Rass, S., & Slamanig, D. (2014). Cryptography for security and privacy in cloud computing. Boston: Artech House.

4.2.16. Bibliografia de consulta/existência obrigatória (EN):

Stallings, W. (2017). Cryptography and network security: Principles and practice. Boston: Pearson Prentice Hall. Jonathan Katz and Yehuda Lindell. (2019). Introduction to Modern Cryptography, Third Edition (3rd ed.). Chapman& Hall/CRC.
Zúquete.A. (2018). Segurança em Redes Informáticas - 5a edição. Editora FCA.
Goldreich, O. (2007). Foundations of cryptography. Cambridge: Cambridge Univ. Press.
Rass, S., & Slamanig, D. (2014). Cryptography for security and privacy in cloud computing. Boston: Artech House.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Desenvolvimento de Software Seguro

4.2.1. Designação da unidade curricular (PT):

Desenvolvimento de Software Seguro

4.2.1. Designação da unidade curricular (EN):

Secure Software Development

4.2.2. Sigla da área científica em que se insere (PT):
CC

4.2.2. Sigla da área científica em que se insere (EN):
CC

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - TP-20.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• *João Carlos Silva - 20.0h*

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Esta unidade curricular tem como principal objetivo familiarizar os alunos com os conceitos de modelos de arquitetura e desenvolvimento de software, fundamentos de segurança no desenvolvimento de aplicações, identificação de requisitos e vulnerabilidades, bem como de técnicas, metodologias e boas práticas para uma programação segura e confiável através da implementação e monitorização de controlos de segurança.
Os alunos que concluam com sucesso esta unidade curricular deverão ser capazes de: Compreender a importância do uso de boas práticas de desenvolvimento e arquitetura de software, para a construção de aplicações seguras; Identificar e escolher qual o modelo de desenvolvimento a utilizar consoante a tipologia do projeto; Saber distinguir requisitos funcionais e não funcionais, com especial enfoco na área da segurança; Conhecer guidelines para a identificação de vulnerabilidades; Conhecer em detalhe os standards de autenticação e identificação OAuth2 e OpenId Connect.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
This curricular unit has as main objective the familiarisation of students with the concepts of architecture models and software development, security fundamentals in application's development, identification of requirements and vulnerabilities, as well as techniques, methodologies and good practices for safe and secure programming, through the implementation and monitoring of security controls.
Students who successfully complete this course should be able to: Understand the importance of applying good practices in software development and architecture for building secure applications; Identify and choose which development model to use depending on the type of project; Know how to distinguish functional and non-functional requirements, with a special focus on security; Know guidelines for the identification of vulnerabilities; Know in detail the OAuth2 and OpenId Connect authentication and identification standards.

4.2.11. Conteúdos programáticos (PT):
1. Modelos de desenvolvimento de software: a) Waterfall; b) V; c) ncremental; d) RAD; e) Agile (SCRUM); f) Iterative; g) Spiral; h) Prototype. 2. Arquiteturas de Software: a) Layered pattern; b) Client-server pattern; c) Master-slave pattern; d) Broker pattern; e) Peer-to-peer pattern; f) Event-bus pattern; g) Model-View-Controller pattern. 3. Identificação de Requisitos e Vulnerabilidades: a) Exploração das guidelines presentes no IEEE Standard 830-1998. 4. Implementação e monitorização de controlos de segurança: a) Protocolo OAuth 2.0, com os Grant Types: Authorization Code, Client Credentials e Refresh Token; b) OpenIDConnect.

4.2.11. Conteúdos programáticos (EN):

1. Software development models: a) Waterfall; b) V; c) Incremental; d) RAD; e) Agile (SCRUM); f) Iterative; g) Spiral; h) Prototype. 2. Software Architectures: a) Layered pattern; b) Client-server pattern; c) Master-slave pattern; d) Broker pattern; e) Peer-to-peer pattern; f) Event-bus pattern; g) Model-View-Controller pattern. 3. Identification of Requirements and Vulnerabilities: a) Exploitation of the guidelines present in the IEEE Standard 830-1998. 4. Implementation and monitoring of security controls: a) OAuth 2.0 Protocol, with the Grant Types: Authorization Code, Client Credentials e Refresh Token; b) OpenIDConnect.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos programáticos desta UC abordam os principais temas na vasta área do desenvolvimento de software seguro. Estes conceitos permitem a compreensão dos principais vetores de atuação da área de desenvolvimento de software seguro, alavancando a capacidade dos discentes na identificação ativa de eventuais vulnerabilidades e na construção de um processo, adequado ao tipo de projeto e aplicação a ser desenvolvida, que permita o desenvolvimento de aplicações seguras.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The syllabus contents of this UC address the main themes in the vast area of secure software development. These concepts allow the understanding of the main vectors of study in the area of secure software development, leveraging the ability of students to actively identify possible vulnerabilities and to build a process, appropriate to the type of project and application to be developed, that allows them to develop secure applications.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

No âmbito da Unidade Curricular serão utilizadas as seguintes metodologias de ensino e aprendizagem: Exposição teórica e teórico-prática da matéria nas aulas; Demonstração prática dos conceitos e realização de exercícios durante as aulas. Debate dos temas abordados nas aulas e esclarecimento de dúvidas. Estímulo à participação, interação e dinâmica de grupo. Avaliação formativa adequada à aquisição de conhecimentos e competências. Realização de um trabalho prático para a aplicação dos conhecimentos e competências.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

Within the Curricular Unit, the following teaching and learning methodologies will be used: Theoretical and theoretical- practical exposition of the subject in class; Practical demonstration of concepts and exercises during classes. Debate on the topics covered in class and clarify doubts. Stimulating participation, interaction and group dynamics. Formative assessment suitable for the acquisition of knowledge and skills. Practical work for the application of knowledge and skills.

4.2.14. Avaliação (PT):

Para a avaliação contínua, serão realizados um trabalho prático (75%) e um teste de avaliação escrito (25%). Nas épocas de Recurso e Especial, a avaliação consiste nas mesmas componentes da época de avaliação contínua, com a exceção do trabalho prático que só pode ser entregue na época de avaliação contínua (cuja nota de avaliação será mantida para as restantes épocas).

4.2.14. Avaliação (EN):

The methodology used to evaluate students will consist in one written test (25%) and a practical assignment (75%), to be made during the lecture period. If a student fails to approve at the test, it will be given additional chances at the respective periods. It will not be allowed to deliver more than one practical assignment.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):

Tendo em conta os objectivos descritos para esta unidade curricular, a metodologia de ensino baseada em aulas teórico-práticas revela-se a mais adequada, com realização de um trabalho prático, em grupo, para aplicação dos conhecimentos e competências adquiridos em grupo, dos temas abordados nas aulas, com o inerente estímulo à participação, interação e dinâmica de grupo.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):

Bearing in mind the objectives described for this curricular unit, the teaching methodology based on theoretical- practical classes proves to be the most appropriate, with practical work to apply the knowledge and skills acquired in groups, of the topics covered in the classes, with the inherent stimulus to participation, interaction and group dynamics.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):

Miguel Pupo Correia, Paulo Jorge Sousa (2017) Segurança no Software, FCA.
Michael Howard, Steve Lipner (2006) The Security Development Lifecycle, Microsoft Press.
Ryan Boyd (2012) Getting Started with OAuth 2.0: Programming Clients for Secure Web API Authorization and Authentication, O'Reilly Media.
Andrew Stellman, Jennifer Greene (2013)Learning Agile: Understanding Scrum, XP, Lean, and Kanban. Theodor Richardson, Charles N Thies (2013) Secure Software Design, Jones & Bartlett Learning.
Ted Harrington (2020) Hackable: How to Do Application Security Right Kindle Edition. Lioncrest Publishing

4.2.16. Bibliografia de consulta/existência obrigatória (EN):

Miguel Pupo Correia, Paulo Jorge Sousa (2017) Segurança no Software, FCA.
Michael Howard, Steve Lipner (2006) The Security Development Lifecycle, Microsoft Press.
Ryan Boyd (2012) Getting Started with OAuth 2.0: Programming Clients for Secure Web API Authorization and Authentication, O'Reilly Media.
Andrew Stellman, Jennifer Greene (2013)Learning Agile: Understanding Scrum, XP, Lean, and Kanban. Theodor Richardson, Charles N Thies (2013) Secure Software Design, Jones & Bartlett Learning.
Ted Harrington (2020) Hackable: How to Do Application Security Right Kindle Edition. Lioncrest Publishing

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Direito e Ética na Cibersegurança

4.2.1. Designação da unidade curricular (PT):

Direito e Ética na Cibersegurança

4.2.1. Designação da unidade curricular (EN):

Law and Ethics in Cybersecurity

4.2.2. Sigla da área científica em que se insere (PT):

CJF

4.2.2. Sigla da área científica em que se insere (EN):

L

4.2.3. Duração (anual, semestral ou trimestral) (PT):

Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):

Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):

75.0

4.2.5. Horas de contacto:

Presencial (P) - T-20.0

4.2.6. % Horas de contacto a distância:

0.00%

4.2.7. Créditos ECTS:

3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:

• Gonçalo Nicolau cerqueira Sopas de Melo Bandeira - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
No final da unidade os alunos deverão ser capazes de: Identificar e distinguir diversos direitos e deveres na cibersegurança com ética; Compreender o lugar sistemático dos direitos e deveres na cibersegurança com ética e compreender o lugar sistemático dos direitos e deveres processuais neste contexto; Conhecer e compreender os princípios fundamentais de ordenação do domínio da cibersegurança com ética; Compreender as diferenças entre o mundo do direito substantivo e adjectivo na cibersegurança com ética através da compreensão do direito material, adjetivo e sancionatório que vivem dentro deles; Identificar o papel da jurisprudência e da doutrina na disciplina do direito da cibersegurança com ética; Desenvolver a capacidade de análise e de síntese; Aplicar os conhecimentos e competências adquiridos na resolução de casos complexos; Resolver problemas nesta área; Adquirir os conhecimentos e competências essenciais na área do direito da cibersegurança com ética em sentido amplo.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
At the end of the unit students should be able to: Identify and distinguish different rights and duties in cybersecurity with ethics; Understand the systematic place of rights and duties in cybersecurity with ethics and understand the systematic place of procedural rights and duties in the context of cybersecurity with ethics; Know and understand the fundamental principles of ordering the domain of cybersecurity with ethics; Understand the differences between the world of substantive law and adjective law in cybersecurity with ethics through the understanding of material, adjective and sanctioning laws that live within them; Identify the role of jurisprudence and doctrine in the discipline of cybersecurity law with ethics; Develop the capacity for analysis and synthesis; Apply the knowledge and skills acquired in solving complex cases; Solve problems in the area; Acquire essential knowledge and skills in the area of cybersecurity law with ethics in a broad sense.

4.2.11. Conteúdos programáticos (PT):
1. A Cibersegurança e o Cibercrime na Sociedade em Rede; 2. O Direito da Cibersegurança; 3. O Direito do Cibercrime; 4.Propriedade intelectual da informação no contexto digital (mensagens eletrónicas, redes sociais, informação pessoal armazenada na nuvem - Cloud, entre outros); 5. Privacidade; 6. Responsabilidade civil dos provedores de Internet e das empresas responsáveis pelas plataformas utilizadas na proteção da informação pessoal; 7. Jurisdição na internet: tribunal competente, lei aplicável e meios alternativos de resolução de litígios; 8. Comércio eletrónico.

4.2.11. Conteúdos programáticos (EN):
1. Cybersecurity and Cybercrime in the Networked Society; 2. The Law of Cybersecurity; 3. The Law of Cybercrime; 4. Intellectual property of information in the digital context (electronic messages, social networks, personal information stored in the Cloud, among others); 5. Privacy; 6. Civil liability of Internet providers and companies responsible for the platforms used to protect personal information; 7. Internet jurisdiction: competent court, applicable law and alternative means of dispute resolution; 8. E-commerce.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

O programa busca abarcar as disciplinas jurídicas positivadas, sejam nacionais, europeias ou internacionais, no contexto da cibersegurança com ética e do cibercrime, por forma a colocar os fundamentos para um eficiente desempenho profissional avançado dos alunos com a formação.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The program seeks to cover the legal disciplines approved, whether national, European or international, in the context of cybersecurity with ethics and cybercrime, in order to lay the foundations for an efficient advanced professional performance of students with training.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

No âmbito da Unidade Curricular serão utilizadas as seguintes metodologias de ensino e aprendizagem: Aulas teóricas, com exposição teórico-problemática dos conteúdos programáticos da disciplina, estimulando o espírito crítico dos discentes; Aulas práticas ("casos-de-estudo"), com discussão e resolução de casos práticos versando a matéria expendida nas partes mais teóricas.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

In the scope of the Curricular Unit the following methodologies of education and learning will be used: Theoretical lessons, with a theoretician-problematic exposition of the contents of programs of disciplines, stimulating the critical spirit of the learning; Practical lessons ("case-studies"), with the discussion and resolution of practical cases dealing with the matter expended in the more theoretical parts.

4.2.14. Avaliação (PT):
A avaliação será feita através da elaboração de um trabalho escrito individual sobre um dos temas constantes de lista a fornecer no âmbito do Direito e Ética na Cibersegurança, tendo em consideração uma perspetiva, direta ou indireta, de Cibersegurança e Informática Forense, e respectiva apresentação oral em data a combinar. Valoração total da nota final: entrega de Trabalho escrito e defesa oral: 90%; assiduidade e atenção nas aulas e participação construtiva: 10%.

4.2.14. Avaliação (EN):
The evaluation will be made through the elaboration of an individual written work on one of the topics on the list to be provided in the scope of Law and Ethics in Cybersecurity, taking into account a direct or indirect perspective of Cybersecurity and Forensic Informatics, and respective oral presentation on a date to be agreed. Total valuation of the final grade: delivery of written work and oral defense: 90%; attendance and attention in class and constructive participation: 10%.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
O método adotado justifica-se pela garantia de um primeiro contacto com os conteúdos programáticos da UC, mediado pelo docente responsável. A análise de casos e resolução de exercícios em aula permitirá a sedimentação de conhecimentos e, ao mesmo tempo, o desenvolvimento da capacidade de análise e espírito crítico, com vista à aquisição de competências de trabalho autónomo, resultantes dos objetivos supramencionados.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
The method adopted is justified to ensure a first contact with the syllabus of the curricular unit, mediated by the teacher. Case analysis and problem-solving in the classroom will allow the consolidation of knowledge and at the same time, the development of capacity for analysis and critical thinking in order to acquire skills to work autonomously, resulting from the above objectives.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
AA.VV.(1999 e 2012), Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, II e III, Art.s 202o A 307o, Dirigido por Jorge de Figueiredo Dias, Coimbra Editora, Coimbra.
Bandeira, Gonçalo S. de Melo (2011 e 2016), in «Abuso de Informação, Manipulação do Mercado e Responsabilidade Penal das 'Pessoas Colectivas' § 'Tipos Cumulativos' e Bens Jurídicos Colectivos na 'Globalização' ", Publicação Revista e Ampliada com Texto Extra, Editora Juruá, 5a Edição, Lisboa.
Bandeira, Gonçalo S. de Melo (2019), Lições de Direito e Ética na Cibersegurança, Pós-Graduação em Cibersegurança e Informática Forense, Escola Superior de Tecnologia, Instituto Politécnico do Cávado e do Ave, Minho, Barcelos.
Gouveia, Jorge Bacelar (2018), Direito da Segurança -Cidadania, Soberania e Cosmopolitismo. Coimbra: Almedina.
Meulen, Nicole van der; JO, Eun A. & SOESANTO, Stefan (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. RAND Europe / Parlamento Europe

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
AA.VV.(1999 e 2012), Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, II e III, Art.s 202o A 307o, Dirigido por Jorge de Figueiredo Dias, Coimbra Editora, Coimbra.
Bandeira, Gonçalo S. de Melo (2011 e 2016), in «Abuso de Informação, Manipulação do Mercado e Responsabilidade Penal das 'Pessoas Colectivas' § 'Tipos Cumulativos' e Bens Jurídicos Colectivos na 'Globalização' ", Publicação Revista e Ampliada com Texto Extra, Editora Juruá, 5a Edição, Lisboa.
Bandeira, Gonçalo S. de Melo (2019), Lições de Direito e Ética na Cibersegurança, Pós-Graduação em Cibersegurança e Informática Forense, Escola Superior de Tecnologia, Instituto Politécnico do Cávado e do Ave, Minho,
Barcelos. Gouveia, Jorge Bacelar (2018), Direito da Segurança -Cidadania, Soberania e Cosmopolitismo. Coimbra: Almedina.
Meulen, Nicole van der; JO, Eun A. & SOESANTO, Stefan (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. RAND Europe / Parlamento Europeu

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Estágio / Projeto

4.2.1. Designação da unidade curricular (PT):
Estágio / Projeto

4.2.1. Designação da unidade curricular (EN):
Internship / Project

4.2.2. Sigla da área científica em que se insere (PT):
ACSDC

4.2.2. Sigla da área científica em que se insere (EN):
CADS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
750.0

4.2.5. Horas de contacto:
Presencial (P) - OT-30.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
30.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Patrícia Leite - 30.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Trabalho autónomo do aluno em contexto empresarial (no caso de estágio), ou em contexto de desenvolvimento de projeto de investigação (projeto).

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
Autonomous work of the student in the company context (in the case of internship), or in the context of the development of a research project (project).

4.2.11. Conteúdos programáticos (PT):
Unidade curricular sem conteúdos programáticos específicos.

4.2.11. Conteúdos programáticos (EN):
Curricular unit without specific syllabus

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos programáticos irão depender do trabalho em que o aluno estiver integrado.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The syllabus will depend on the work in which the student is integrated.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

Nesta unidade curricular os estudantes irão aplicar os seus conhecimentos e competências na resolução de problemas num contexto empresarial (estágio) ou num projeto aplicado.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

In this curricular unit, students will apply their knowledge and competences in the resolution of problems in an enterprise context (internship) or in an applied project.

4.2.14. Avaliação (PT):
A avaliação do estágio/projeto será realizado de acordo com regulamento próprio da escola.

4.2.14. Avaliação (EN):
The evaluation of the internship/project will be carried out according to the school's own regulations.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
Considerando o objetivo de trabalho autónomo, é esperado que o aluno seja capaz de desenvolver o seu trabalho com orientação do seu supervisor.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
Considering the objective of autonomous work, it is expected that the student will be able to develop his work with guidance from his supervisor.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
Toda a bibliografia relacionada nas restantes unidades curriculares do curso.

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
All the related bibliography from the other curricular units.

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Inteligência Artificial aplicada à Cibersegurança

4.2.1. Designação da unidade curricular (PT):
Inteligência Artificial aplicada à Cibersegurança

4.2.1. Designação da unidade curricular (EN):
Artificial Intelligence applied to Cybersecurity

4.2.2. Sigla da área científica em que se insere (PT):
SIIA

4.2.2. Sigla da área científica em que se insere (EN):
IS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - T-10.0; TP-10.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Joaquim Gonçalves - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Como principais objetivos da unidade curricular estão a passagem do conhecimento prático sobre técnicas e teorias de Inteligência Artificial Aplicada à Cibersegurança Informática com especial foco na nas técnicas de Machine Learing de padrões e Deep Learning. No final da unidade os alunos deverão perceber os desafios e conseguir efetuar análises e definição de algoritmos que permitam às técnicas de AI potenciar resultados de elevada complexidade na cibersegurança.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
As main objectives of the curricular unit are the passage of practical knowledge about techniques and theories of Artificial Intelligence Applied to Computer Cybersecurity with a special focus on the Machine Learning techniques of patterns and Deep Learning.
At the end of the unit, students should understand the challenges and be able to carry out analysis and define algorithms that allow AI techniques to enhance highly complex results in cybersecurity.

4.2.11. Conteúdos programáticos (PT):
1. Introdução à IA: a) Noções Básicas; b) Métodos de Pesquisa. 2. Métodos de Pesquisa: a) Redes Bayesianas; b) Aprendizagem Máquina; c) Redes Neuronais. 3. Soluções de Segurança IA.

4.2.11. Conteúdos programáticos (EN):
1. Introduction to AI: a) Basic notions; b) Research Methods. 2. Research Methods: a) Bayesian networks; b) Machine Learning; c) Neural Networks. 3. IA Security Solutions.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos estão organizados de forma integrada, visando permitir a análise de perspetivas pertinentes para o uso da Inteligência Artificial na Cibersegurança. Parte-se de aspetos gerais de AI (1.), para o estudo dos métodos de pesquisa (2.) e uma análise aprofundada de Soluções de Segurança IA (3.). No conjunto, pretende promover-se a aquisição de conhecimentos científicos e práticos para o desenvolvimento de competências profissionais.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The contents are organized in an integrated way, aiming to allow the analysis of relevant perspectives for Artificial Intelligence in Cybersecurity. It starts with general aspects of AI (1.), for the study of research methods (2.) and an in- depth analysis of AI Security Solutions (3.). As a whole, the intention is to promote the acquisition of scientific and practical knowledge for the development of professional skills.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

O desenvolvimento dos conteúdos será realizado com base numa abordagem teórica e teórico-empírica, construindo um quadro de referência de base, quer através de exposição, quer de trabalhos de pesquisa e síntese. Estas abordagens serão complementadas, numa perspetiva de aplicação, com a análise de casos e a resolução de problemas. O desenvolvimento de competências será potenciado por estratégias de simulação.
A avaliação será feita através da entrega, apresentação e defesa de um paper científico com qualidade de apresentação numa conferência. (Avaliação a 100%)

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

The development of the contents will be carried out based on a theoretical and theoretical-empirical approach, building a basic frame of reference, either through exposure, or through research and synthesis works. These approaches will be complemented, from an application perspective, with case analysis and problem solving. The development of skills will be enhanced by simulation strategies.

4.2.14. Avaliação (PT):
A avaliação será feita através da entrega, apresentação e defesa de um artigo científico com qualidade de apresentação numa conferência. (Avaliação a 100%)

4.2.14. Avaliação (EN):
The evaluation will be made through the delivery, presentation and defense of a scientific paper with presentation quality in a conference. (100% evaluation)

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
As metodologias de ensino e de aprendizagem visam o desenvolvimento integrado nos estudantes dos conhecimentos referidos nos conteúdos programáticos e a concretização dos objetivos e competências estabelecidos. A diversidade de conteúdos propostas tem por objetivo potenciar abordagem complexa em sistemas inteligentes no campo da segurança da informação. Os métodos e estratégias propostos pretendem desenvolver nos alunos conhecimentos, compreensão e competências ao nível da aplicação.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
Teaching and learning methodologies aim at the integrated development in students of the knowledge referred to in the syllabus and the achievement of established objectives and competencies. The proposed diversity of content aims to enhance a complex approach in intelligent systems in the field of information security. The proposed methods and strategies aim to develop students' knowledge, understanding and skills at the application level.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
Cylance Data Team (2017) Introduction to Artificial Intelligence for Security Professionals (ASIN: B07654CFFQ). Alessandro Parisi (2019) Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies (ISBN: 978-178-980-402-7).
Xingming Sun (2020) Artificial Intelligence and Security (ISBN: 978-303-024-267-1).

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
Cylance Data Team (2017) Introduction to Artificial Intelligence for Security Professionals (ASIN: B07654CFFQ). Alessandro Parisi (2019) Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies (ISBN: 978-178-980-402-7).
Xingming Sun (2020) Artificial Intelligence and Security (ISBN: 978-303-024-267-1).

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Laboratório de Análise Forense

4.2.1. Designação da unidade curricular (PT):
Laboratório de Análise Forense

4.2.1. Designação da unidade curricular (EN):
Forensic Analysis Laboratory

4.2.2. Sigla da área científica em que se insere (PT):
ACSDC

4.2.2. Sigla da área científica em que se insere (EN):
CADS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - PL-20.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Nuno Ricardo Mateus Coelho - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Dotar os discentes de competências para proceder à seleção, registo, recolha, análise, interpretação e apresentação de prova digital.
No final da Unidade Curricular os alunos devem compreender: Funcionamento da Polícia Judiciária e seu enquadramento no âmbito das investigações de cibercriminalidade ou criminalidade praticada com o recurso a meio informático (de forma genérica); Hardware e software utilizado na prática de análise forense; Identificação de equipamentos passíveis de recolha de prova digital; Técnicas de identificação e de recolha de prova digital; Técnicas de análise de suporte digital; Técnicas de recuperação de dados; Técnicas contra-forenses.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
Provide students with the skills to select, register, collect, analyze, interpret and present digital evidence.
At the end of the Unit students should understand: Operation of the Portuguese Criminal Police and its framework in the context of investigations of cybercrime or crime committed with the use of computer (in general means); Hardware and software used in the practice of forensic analysis; Identification of equipment passible to collect digital evidence; Digital proof identification and collection techniques; Digital support analysis techniques; Data recovery techniques; Counter-forensic techniques.

4.2.11. Conteúdos programáticos (PT):
1. Polícia Judiciária e o cibercrime; 2. Estrutura de laboratório de análise forense; 3. Análise forense, vista por um perito; 4. Esterilização de dispositivos; 5. Cálculo de 'hashing'; 6. Criação e cópia de imagens forenses; 7. Gestão de imagens e extracção de informação; 8. 'First-Responder': a) Informação do sistema; b) Pesquisas. 9. Recuperação de ficheiros; 10. 'Data Carving'; 11. Memória RAM; 12. 'Browser Cache' & 'Other Data'; 13. 'Registry'; 14. Encriptação; 15. Medidas AntiForenses; 16. Introdução a 'Mobile Forensics'.

4.2.11. Conteúdos programáticos (EN):
1. Portuguese Criminal Police and cybercrime; 2. Forensic analysis laboratory structure; 3. Forensic analysis, seen by an expert; 4. Sterilization of devices; 5. Hashing calculation; 6. Creation and copying of forensic images; 7. Image management and information extraction; 8. 'First-Responder': a) System information; b) Research. 9. File recovery; 10. 'Data Carving'; 11. RAM Memory; 12. 'Browser Cache' & 'Other Data'; 13. 'Registry'; 14. Encryption; 15. Anti-Forensic Measures; 16. Introduction to 'Mobile Forensics'.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

A conjugação de uma vertente teórica, inicial, com uma vertente teórico-prática, posterior, dos conteúdos a lecionar possibilitará conduzir o estudante pelo processo gradual de assimilação das matérias, levando-o a facilmente percepcionar quer os conceitos, quer a forma de atingir os objectivos da análise forense, facto que será demonstrado com a realização de um trabalho final.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The combination of an initial theoretical component with a later theoretical-practical component of the contents, will make it possible to lead the student through the gradual process of assimilation of the materials, leading him to easily perceive both the concepts and the way to achieve the objectives of forensic analysis, a fact that will be demonstrated by the realisation of a final work.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

Apresentação inicial teórica de conceitos básicos e métodos genéricos, mas essenciais para a execução da função. Aprofundamento gradual de conceitos, conjugando-os com a apresentação de ferramentas aplicáveis e a realização de exercícios práticos que permitam a consolidação da matéria e que possibilitarão o posterior desenvolvimento dos conhecimentos em cada subtema.
Culminar com a realização do trabalho prático final, onde são demonstrados os conhecimentos adquiridos, conjugados com a apresentação dos resultados.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

Theoretical presentation initially of basic concepts and generic methods, but essential for the execution of the function.
Gradual deepening of concepts, combining them with the presentation of applicable tools and the realisation of practical exercises that allow the consolidation of the matter and that will enable the further development of knowledge in each sub-theme.
Culminate with the realisation of the final practical work, where the acquired knowledge is demonstrated, combined with the presentation of the results.

4.2.14. Avaliação (PT):
A avaliação consiste na entrega, apresentação e defesa de trabalho prático final (100%).

4.2.14. Avaliação (EN):
The evaluation will be made through the delivery, presentation and defense of final practical work (100%).

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
A aplicação das metodologias de aprendizagem acima indicadas possibilitará ao discente atravessar todo o processo utilizado na área forense digital, adquirindo e consolidando os conhecimentos de forma progressiva e orientada por módulos, o que facilitará o cumprimento das metas a que se propõe a unidade curricular.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
The application of the learning methodologies indicated above will allow the student to go through the entire process used in the digital forensic area, acquiring and consolidating knowledge progressively and guided by modules, which will facilitate the achievement of the goals proposed by the curricular unit.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
Chauhan, Sudhanshu; Panda, Nutan Kumar. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. USA: Syngress, 2015.
Shaaban, Ayman; Sapronov, Konstantin. Pratical Windows Forensics. UK: Packt Publishing, 2016.
William Oettinger (2020) Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence. Packt Publishing
https://www.policiajudiciaria.pt/

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
Chauhan, Sudhanshu; Panda, Nutan Kumar. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. USA: Syngress, 2015.
Shaaban, Ayman; Sapronov, Konstantin. Pratical Windows Forensics. UK: Packt Publishing, 2016.
William Oettinger (2020) Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence. Packt Publishing
https://www.policiajudiciaria.pt/

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Laboratório de Testes de Intrusão

4.2.1. Designação da unidade curricular (PT):
Laboratório de Testes de Intrusão

4.2.1. Designação da unidade curricular (EN):
Intrusion Testing Laboratory

4.2.2. Sigla da área científica em que se insere (PT):
ACSDC

4.2.2. Sigla da área científica em que se insere (EN):
CADS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.2.5. Horas de contacto:
Presencial (P) - PL-20.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Nuno Alberto Ferreira Lopes - 20.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Como principais objetivos da unidade curricular estão a passagem do conhecimento prático sobre sistemas, técnicas e teorias de testes de segurança e intrusão de sistemas e redes de comunicações tecnológicas.
No final da unidade, os alunos deverão perceber os desafios e conseguir efetuar ataques, invasões e explorações de vulnerabilidades em sistemas de informação como meio de antecipação desses mesmos ataques. Deverão ainda conseguir criar programas que permitam extração de informação.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
As main objectives of the curricular unit are the passage of practical knowledge about systems, techniques and theories of tests of security and intrusion of systems and networks of technological communications.
At the end of the unit, students should understand the challenges and be able to carry out attacks, invasions and exploits of vulnerabilities in information systems as a means of anticipating these same attacks. They should also be able to create programs that allow information to be extracted.

4.2.11. Conteúdos programáticos (PT):
1. Introdução ao Hacking Ético; 2. Enumeração e Reconhecimento; 3. Análise a redes; 4. Enumeração; 5. Análise de vulnerabilidade; 6. invasão de Sistema; 7. Ameaças de malware; 8. Snifing; 9. Engenharia Social; 10. Negação de serviço; 11. Rapto de Sessão; 12. Evasão de IDS, firewalls e Honeypots; 13. Invasão servidores web; 14. Hacking de aplicativos da web; 15. Injeção de SQL; 16. Hacking de redes sem fio; 17. Hacking de plataformas móveis; 18. Hacking de IoT; 19. Computação em nuvem; 20. Criptografia.

4.2.11. Conteúdos programáticos (EN):

1. Introduction to Ethical Hacking; 2. Enumeration and Recognition; 3. Network analysis; 4. Enumeration; 5. Vulnerability analysis; 6. System invasion; 7. Malware threats; 8. Snifing; 9. Social Engineering; 10. Denial of service; 11. Session Abduction; 12. Evasion of IDS, firewalls and Honeypots; 13. Hacking of web servers; 14. Hacking of web applications; 15. SQL injection; 16. Hacking of wireless networks; 17. Hacking of mobile platforms; 18. IoT hacking; 19. Cloud computing; 20. Encryption.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos estão organizados de forma integrada, visando permitir a análise de perspecivas pertinentes para a intervenção educativa. Parte-se de aspetos gerais de Pentesting (1.) para o estudo das metodologias de Pentesting (2.) e uma análise aprofundada das formas e meios de ultrapassar a segurança ativa de rede (3.). No conjunto, pretende promover-se a aquisição de conhecimentos científicos e práticos para o desenvolvimento de competências profissionais.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The contents are organized in an integrated way, aiming to allow the analysis of relevant perspectives for educational intervention. It starts with general aspects of Pentesting (1.) for the study of Pentesting methodologies (2.) and an in- depth analysis of the ways and means of overcoming active network security (3.). As a whole, the intention is to promote the acquisition of scientific and practical knowledge for the development of professional skills.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

O desenvolvimento dos conteúdos será realizado com base numa abordagem teórica e teórico-empírica, construindo um quadro de referência de base, quer através de exposição, quer de trabalhos de pesquisa e síntese. Estas abordagens serão complementadas, numa perspetiva de aplicação, com a análise de casos e a resolução de problemas. O desenvolvimento de competências será potenciado por estratégias de simulação.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

The development of the contents will be carried out based on a theoretical and theoretical-empirical approach, building a basic frame of reference, either through exposure, or through research and synthesis works. These approaches will be complemented, from an application perspective, with case analysis and problem solving. The development of skills will be enhanced by simulation strategies.

4.2.14. Avaliação (PT):

A avaliação consiste na entrega, apresentação e defesa de trabalho prático final (100%).

4.2.14. Avaliação (EN):

The evaluation will be made through the delivery, presentation and defense of final practical work (100%).

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):

As metodologias de ensino e de aprendizagem visam o desenvolvimento integrado nos estudantes dos conhecimentos referidos nos conteúdos programáticos e a concretização dos objetivos e competências estabelecidos. A diversidade de conteúdos propostos tem por objetivo potenciar uma abordagem complexa da segurança em redes informáticas e dos testes de intrusão às mesmas. Os métodos e estratégias propostos pretendem desenvolver nos alunos conhecimentos, compreensão e competências ao nível da aplicação.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):

Teaching and learning methodologies aim at the integrated development in students of the knowledge referred to in the syllabus and the achievement of established objectives and competencies. The diversity of content proposed aims to enhance a complex approach to security in computer networks and intrusion tests. The proposed methods and strategies aim to develop students' knowledge, understanding and skills at the application level.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):

Georgia Weidman (2014)Penetration Testing: A Hands-On Introduction to Hacking - Paperback (ISBN:978-159-327-564- 8).
George Sammons (2017) Kali Linux 2: Penetration testing for beginners (ISBN: 978-198-130-367-0).
Ric Messier (2021) CEH Certified Ethical Hacker John Wiley & Sons Inc (ISBN: 9781119800286).

4.2.16. Bibliografia de consulta/existência obrigatória (EN):

Georgia Weidman (2014)Penetration Testing: A Hands-On Introduction to Hacking - Paperback (ISBN:978-159-327-564- 8).
George Sammons (2017) Kali Linux 2: Penetration testing for beginners (ISBN: 978-198-130-367-0).
Ric Messier (2021) CEH Certified Ethical Hacker John Wiley & Sons Inc (ISBN: 9781119800286).

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Segurança da Informação em Organizações

4.2.1. Designação da unidade curricular (PT):
Segurança da Informação em Organizações

4.2.1. Designação da unidade curricular (EN):
Information Security in Organisations

4.2.2. Sigla da área científica em que se insere (PT):
SIIA

4.2.2. Sigla da área científica em que se insere (EN):
IS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
150.0

4.2.5. Horas de contacto:
Presencial (P) - T-30.0; TP-30.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Luís Ferreira - 60.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A UC apresenta os princípios no âmbito da gestão da segurança da Informação em Organizações. São introduzidos os procedimentos para a gestão do risco, as boas práticas de segurança e os controlos de segurança a adoptar, baseadas na família de normas da ISO/IEC 27000 e do NIST.
Os estudantes devem obter competências como: Desenvolver políticas de segurança, programas, e guias de implementação, de acordo com normas reconhecidas; 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; Delinear uma estratégia para a Cibersegurança, realçando a visão, a missão e os objetivos, e garantindo o alinhamento com o plano estratégico da organização; Identificar requisitos de segurança específicos dos Sistemas de Informação organizacionais, em todas as fases do seu ciclo; Realizar uma avaliação de risco e delinear os controlos de segurança para mitigar os riscos identificados.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):

The course presents the principles in the scope of information security management for organizations. Risk management' procedures are introduced as well as the main good practices and security controls based on the ISO/IEC 27000 and based on NIST.
Students should gain skills like: Develop security policies, programs, and implementation guides, in accordance with recognized standards; Monitor and evaluate the efficiency of cybersecurity controls adopted by an organization, with the aim of ensuring that they provide the desired level of security; Outline a strategy for cybersecurity, highlighting the vision, mission and objectives, and ensuring alignment with the organization's strategic plan; Identify specific security requirements for organizational Information Systems, at all stages of their cycle; Conduct a risk assessment and outline security controls to mitigate the identified risks.

4.2.11. Conteúdos programáticos (PT):

1. Conceitos e definições: a) Segurança da Informação (confidencialidade, integridade e disponibilidade); b) Recursos e tipos de recursos (Informação, físicos e software); c) Valor e criticidade dos recursos críticos organizacionais; d) Ameaças e tipo de ameaças (acidentais vs. deliberadas; internas vs. externas); e) Vulnerabilidades e as suas categorias (fraquezas no SW, HW, físicas, pessoas e procedimentos); f) Conceito de politicas de segurança da informação. 2. Conceito de SGSI. 3. Normas e standards de segurança: a) A família de normas ISO/IEC 27000; b) NIST. 4. Gestão do Risco: a) Modelos de gestão de risco; b) Processo da gestão do risco; c) Tratamento do risco; d) Objetivo dos controlos; e) Avaliação quantitativa/qualitativa do impacto; f) Quantificação do valor dos recursos organizacionais. 5. Políticas e controlos de segurança: a) Controlo de acessos dos utilizadores; b) Formação e sensibilização; c) Controlos de segurança técnicos; d) Monitorização; e) Auditoria.

4.2.11. Conteúdos programáticos (EN):

1. Concepts and Definitions: a) Information security (confidentiality, integrity, availability); b) Asset, asset types (information, physical, software), asset value; c) Threats and type of threats (accidental vs. deliberate; internal vs. external); d) Vulnerabilities and their categorization (flaws in SW, HW, physical, people and procedures); e) Information security policy concepts; f) The types, uses and purposes of controls. 2. ISMS concept. 3. Security Standards: a) ISO/IEC 27000; b) NIST. 4. Risk Management: a) Risk Management models; b) Risk management process; c) Controls objectives; d) Impact assessment (qualitative/quantitative); e) Identifying and accounting for the value of information assets. 5. Policy and security controls: a) User access controls; b) Training and awareness; c) Technical security controls; d) Monitoring; e) Audit.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

O primeiro módulo introduz conceitos e definições utilizados no contexto da cibersegurança com ênfase nas ameaças, vulnerabilidades, recursos críticos 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 módulos 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 políticas 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.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

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.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

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. Serão criados grupos para uma dinamização ágil sobre as atividades a realizar juntamente com a visualização e discussão de videos ilucidativos de boas práticas.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

In classes, the program will be presented using the active method in the form of notes or slides and work will be carried out to consolidate and demonstrate the application of the concepts covered. Groups will be created for an agile dynamization on the activities to be carried out together with the visualization and discussion of illustrative videos of good practices.

4.2.14. Avaliação (PT):
*A Classificação Global (GC) desta unidade curricular é obtida através da realização de trabalhos teórico-práticos (80%) e de um teste individual escrito (TI) (20%): CG = 0,8 * TP + 0,2 * TI. De referir que a avaliação dos trabalhos teórico-práticos contempla uma componente individual (40%) e uma componente de grupo (40%).*
Avaliação em exame: CG é obtida através da realização de um teste escrito teórico-prático, mantendo a nota dos trabalhos teórico-práticos. As percentagens mantêm-se.

4.2.14. Avaliação (EN):
*The Global Classification (GC) of this curricular unit is obtained through theoretical- practical works (80%) and an individual written test (IT) (20%): GC = 0,8 * TP + 0,2 * IT. The evaluation of the theoretical-practical work includes an individual component (40%) and a group component (40%).*
Assessment on exam period: GC is obtained through a written theoretical and practical test, keeping the mark of the theoretical and practical work. The percentages are maintained.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):
Nas aulas teóricas, e em complemento ao método expositivo dos conteúdos programáticos com projeção de elementos exemplificadores, será ainda adoptada uma complementação ao mesmo através do método ativo/demonstrativo. Nas aulas práticas será adoptado um método totalmente ativo, através da disponibilização de diversos exercícios que permitirão ao estudante aplicar, na prática, os conhecimentos adquiridos nas aulas teóricas. Estes exercícios incluirão sempre uma pequena descrição dos objetivos a atingir, da matéria que se pretende abordar, dispostos em crescendo de dificuldade, a resolver autonomamente ou em grupo pelo estudante, devidamente acompanhados pelo docente.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
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.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
ISO/IEC 27001:2013.
NIST Cybersecurity Framework 1.1, 2018.
Bishop, M., 2018. Introduction to Computer Security, Art and Science. Pearson Education. Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", 5th Edition, Prentice Hall, 2021. 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
Vacca, John R., ed. Managing information security. Elsevier, 2013.

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
ISO/IEC 27001:2013.
NIST Cybersecurity Framework 1.1, 2018.
Bishop, M., 2018. Introduction to Computer Security, Art and Science. Pearson Education. Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", 5th Edition, Prentice Hall, 2021. 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
Vacca, John R., ed. Managing information security. Elsevier, 2013.

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Segurança nas Redes e Administração de Sistemas

4.2.1. Designação da unidade curricular (PT):
Segurança nas Redes e Administração de Sistemas

4.2.1. Designação da unidade curricular (EN):
Network Security and Systems Administration

4.2.2. Sigla da área científica em que se insere (PT):
ACSDC

4.2.2. Sigla da área científica em que se insere (EN):
CADS

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.2.4. Horas de trabalho (número total de horas de trabalho):
150.0

4.2.5. Horas de contacto:
Presencial (P) - T-20.0; TP-40.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Sandro Carvalho - 60.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
[sem resposta]

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
Um dos principais objetivos da unidade curricular é a passagem do conhecimento teórico-prático sobre sistemas, técnicas e teorias de segurança de equipamentos e procedimentos para segurança de redes e comunicações tecnológicas. Além disso, outro objetivo principal é familiarizar os alunos com as ferramentas que existem de modo a conseguir-se assegurar os sistemas e evitar ataques/mitigá-los o mais rapidamente possível. A demonstração prática dos conceitos utilizará o sistema operativo Linux.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
One of the main objectives of the course are the transfer of theoretical and practical knowledge about systems, techniques and theories of equipment security and procedures for the security of networks and technological communications.
In addition, other main objectives are to familiarize students with the tools that exist in order to be able to secure the systems and avoid attacks/mitigate them as soon as possible. The practical demonstration of the concepts will use the Linux operating system.

4.2.11. Conteúdos programáticos (PT):
1 - Segurança em Redes Informáticas - Vulnerabilidade, ataques, riscos e defesas: a) Políticas vs Mecanismos de Segurança; b) Criptografia e Criptoanálise; c) Gestão de chaves públicas; d) Correio eletrónico seguro; e) PGP. 2 - Protocolos AAA. 3 - Firewall em redes e web context: a) IDS, IPD, HIDS, DL; b) VP, SSH, SSL, IPSEC, PPTP, L2TP; c) OpenVPN; d) PPP sobre SSL e SSH. 4. Assegurar um Sistema operativo: a) Instalação de um sistema operativo CentOS; b) Atualizar um Sistema Operativo e ferramentas; c) Permissões; d) Métodos de autenticação; e) Firewall (breve descrição do firewalld); f) Logging. 5. Monitorização: a) Configuração de snmp; b) Instalação de um servidor de monitorização; c) Plugins de monitorização. 6. Backups: a) Instalação de um servidor de backups. 7. Segurança em Serviços: a) Instalação de servidores web; b) Instalação de servidores de base de dados. 8. Verificadores de Integridade do sistema.

4.2.11. Conteúdos programáticos (EN):

1 - Computer Network Security - Vulnerability, attacks, risks and defenses: a) Policies vs Security Mechanisms; b) Cryptography & Cryptoanalysis; c) Public key management; d) Secure email; e) PGP. 2 - AAA protocols. 3 - Firewall in networks and web context: a) IDS, IPD, HIDS, DL; b) VP, SSH, SSL, IPSEC, PPTP, L2TP; c) OpenVPN; d) PPP over SSL and SSH. 4. Ensuring an Operating System: a) Installing a CentOS operating system; b) Update an Operating System and tools; c) Permissions; d) Authentication methods; e) Firewall (brief description of the firewalld); f) Logging. 5. Monitoring: a) Snmp configuration; b) Installation of a monitoring server; c) Monitoring plugins. 6. Backups: a) Installing a backup server. 7. Service Security: a) Installation of web servers; b) Installation of database servers. 8. System Health Checkers.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (PT):

Os conteúdos estão organizados de forma integrada, visando permitir a análise de perspetivas pertinentes para a intervenção educativa. Parte-se de aspetos gerais da Segurança em Redes Informáticas (1.) para o estudo de protocolos AAA (2.) e uma análise profunda dos sistemas e tecnologias de ativos de rede que promovem a segurança, proteção de sistemas informáticos (3.). Posteriormente são abordados os conteúdos programáticos referentes à Administração de Sistemas (4. a 8.), abordando os principais conceitos na área de segurança de sistemas operativos linux. Estes conceitos permitem a compreensão das principais características de funcionamento dos sistemas, de modo a poderem ser usados mais eficazmente, que são igualmente objetivos fulcrais da UC.
No conjunto, pretende promover-se a aquisição de conhecimentos científicos e o desenvolvimento de competências profissionais nestas áreas.

4.2.12. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular. (EN):

The contents are organized in an integrated way, aiming to allow the analysis of relevant perspectives for educational intervention. It starts from general aspects of Security in Computer Networks (1.) for the study of AAA protocols (2.) and an in-depth analysis of systems and technologies of network assets that promote security, protection of computer systems (3.).
Later, the programmatic contents related to Systems Administration are discussed (4. to 8.), addressing the main concepts in the area of security of linux operating systems. These concepts allow the understanding of the main operating characteristics of the systems, so that they can be used more effectively, which are this course objectives. As a whole, the aim is to promote the acquisition of scientific knowledge and the development of professional skills.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (PT):

No âmbito da Unidade Curricular serão utilizadas as seguintes metodologias de ensino e aprendizagem: Exposição teórica e teórico-prática da matéria nas aulas; Demonstração prática dos conceitos e realização de fichas práticas durante as aulas; Debate dos temas abordados nas aulas e esclarecimento de duvidas; Estímulo à participação, interação e dinâmica de grupo; Realização de trabalhos práticos para a aplicação dos conhecimentos e competências.

4.2.13. Metodologias de ensino e de aprendizagem específicas da unidade curricular articuladas com o modelo pedagógico. (EN):

Within this course, the following teaching and learning methodologies will be used: Theoretical and theoretical- practical exposition of the material in class; Practical demonstration of concepts and practice sheets during classes; Debate of the topics covered in class and clarification of doubts; Stimulating participation, interaction and group dynamics; Practical exercises to apply the knowledge and skills.

4.2.14. Avaliação (PT):

A avaliação será feita através da entrega, apresentação e defesa de três trabalhos práticos (20% + 40% + 40%).

4.2.14. Avaliação (EN):

The evaluation will be made through the delivery, presentation and defense of three practical assignments (20% + 40% + 40%).

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (PT):

Tendo em conta os objetivos descritos para esta unidade curricular, a metodologia de ensino baseada em aulas teórico-práticas revela-se a mais adequada, com realização de trabalhos práticos para aplicação dos conhecimentos e competências adquiridos e debate, em grupo, dos temas abordados nas aulas, com o inerente estímulo à participação, interação e dinâmica de grupo.

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):

Having regard to the objectives outlined for this curricular unit, the teaching methodology based on practical classes is the most appropriate, including practical assignments and group discussion with encouragement for participation, interaction and group dynamic.

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
Sagar Rahalkar, Sairam Jetty (2019) Securing Network Infrastructure (ISBN: 978-183-864-230-3).
André Zuquete (2013) Segurança em Redes Informáticas (ISBN: 978-972-722-767-9).
Edmundo Monteiro, Fernando Boavida (2011) Engenharia de Redes Informáticas (ISBN: 978-972-722-694-8). Jorge Granjal (2017) Segurança Prática em Sistemas e Redes com Linux (ISBN: 978-972-722-865-2).
https://www.zabbix.com/documentation/1.8/manual/quickstart
https://icinga.com/docs/icinga-2/latest/
https://icinga.com/docs/icinga-director/latest/doc/02-Installation/ https://www.fail2ban.org/wiki/index.php/Main_Page
http://rkhunter.sourceforge.net/
https://github.com/gentilkiwi/mimikatz/wiki https://projects.theforeman.org/projects/katello/wiki/Pulp_3_Integration
https://www.zabbix.com/documentation/1.8/manual/quickstart
https://icinga.com/docs/icinga-2/latest/
https://icinga.com/docs/icinga-director/latest/doc/02-Installation/ https://www.fail2ban.org/wiki/index.php/Main_Page

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
Sagar Rahalkar, Sairam Jetty (2019) Securing Network Infrastructure (ISBN: 978-183-864-230-3).
André Zuquete (2013) Segurança em Redes Informáticas (ISBN: 978-972-722-767-9).
Edmundo Monteiro, Fernando Boavida (2011) Engenharia de Redes Informáticas (ISBN: 978-972-722-694-8). Jorge Granjal (2017) Segurança Prática em Sistemas e Redes com Linux (ISBN: 978-972-722-865-2).
https://www.zabbix.com/documentation/1.8/manual/quickstart
https://icinga.com/docs/icinga-2/latest/
https://icinga.com/docs/icinga-director/latest/doc/02-Installation/ https://www.fail2ban.org/wiki/index.php/Main_Page
http://rkhunter.sourceforge.net/
https://github.com/gentilkiwi/mimikatz/wiki https://projects.theforeman.org/projects/katello/wiki/Pulp_3_Integration
https://www.zabbix.com/documentation/1.8/manual/quickstart
https://icinga.com/docs/icinga-2/latest/
https://icinga.com/docs/icinga-director/latest/doc/02-Installation/ https://www.fail2ban.org/wiki/index.php/Main_Page

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

4.3. Unidades Curriculares (opções)

Mapa IV - Opção I

4.3.1. Designação da unidade curricular (PT):
Opção I

4.3.1. Designação da unidade curricular (EN):
Option I

4.3.2. Sigla da área científica em que se insere (PT):
CJF:SIIA

4.3.2. Sigla da área científica em que se insere (EN):
IS:L

4.3.3. Duração (anual, semestral ou trimestral) (PT):
Semestral

4.3.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual

4.3.4. Horas de trabalho (número total de horas de trabalho):
75.0

4.3.5. Horas de contacto:
Presencial (P) - T-10.0; TP-10.0

4.3.6. % Horas de contacto a distância:
0.00%

4.3.7. Créditos ECTS:
3.0

4.3.8. Unidades Curriculares filhas:
- *Auditoria Informática - 3.0 ECTS*
- *Direito e Ética na Cibersegurança - 3.0 ECTS*

4.3.9. Observações (PT):
[sem resposta]

4.3.9. Observações (EN):
[sem resposta]

4.4. Plano de Estudos

Mapa V - Percurso geral - 1

4.4.1. Ramos, variantes, áreas de especialização, especialidades ou outras formas de organização em que o ciclo de estudos se estrutura (a preencher apenas quando aplicável)* (PT):
Percurso geral

4.4.1. Ramos, variantes, áreas de especialização, especialidades ou outras formas de organização em que o ciclo de estudos se estrutura (a preencher apenas quando aplicável)* (EN):
Main Track

4.4.2. Ano curricular:

1

4.4.3. Plano de Estudos

Unidade Curricular	Área Científica	Duração	Horas Trabalho	Horas Contacto	% HC a distância	Tipo	Opcional	ECTS
Criptografia Aplicada à Cibersegurança	ACSDC	Semestral 1ºS	75.0	P: T-10.0; TP-10.0	0.00%		Não	3.0
Desenvolvimento de Software Seguro	CC	Semestral 1ºS	75.0	P: TP-20.0	0.00%		Não	3.0
Inteligência Artificial aplicada à Cibersegurança	SIIA	Semestral 1ºS	75.0	P: T-10.0; TP-10.0	0.00%		Não	3.0
Laboratório de Análise Forense	ACSDC	Semestral 1ºS	75.0	P: PL-20.0	0.00%		Não	3.0
Laboratório de Testes de Intrusão	ACSDC	Semestral 1ºS	75.0	P: PL-20.0	0.00%		Não	3.0
Opção I	CJF:SIIA	Semestral 1ºS	75.0	P: T-10.0; TP-10.0	0.00%	UC de Opção	Não	3.0
Segurança da Informação em Organizações	SIIA	Semestral 1ºS	150.0	P: T-30.0; TP-30.0	0.00%		Não	6.0

Segurança nas Redes e Administração de Sistemas	ACSDC	Semestral 1ºS	150.0	P: T-20.0; TP-40.0	0.00%		Não	6.0
Estágio / Projeto	ACSDC	Semestral 2ºS	750.0	P: OT-30.0	0.00%		Não	30.0
Total: 9								

4.5. Metodologias e Fundamentação

4.5.1.1. Justificar o desenho curricular. (PT)

A estrutura curricular deste curso está orientada em três linhas curriculares que se caracterizam do seguinte modo.

A primeira linha curricular é composta pelas UCs em "Criptografia Aplicada à Cibersegurança" e pelo "Desenvolvimento de código seguro", que fazem um enquadramento na área da criptografia, que serve como base à segurança informática, assim como na área de engenharia de software, que engloba técnicas de desenvolvimento de software que são transversais a todas as soluções informáticas.

A segunda linha curricular engloba as UCs de "Segurança nas Redes e Administração e Sistemas", "Laboratório de Testes de Intrusão", "Laboratório de Análise Forense", e finalmente "Inteligência Artificial aplicada à Cibersegurança". Estas UCs irão criar a estrutura base de conhecimentos e competências para o domínio da cibersegurança aplicada, introduzindo os conceitos teóricos e posteriormente as ferramentas práticas de segurança informática. Termina com a utilização de Inteligência Artificial para o aumento do desempenho das ferramentas.

Finalmente, a terceira linha curricular é composta pelas UCs de "Segurança da Informação nas Organizações", "Auditoria Informática" e "Direito e Ética na Cibersegurança". Esta linha aborda a integração da cibersegurança nas organizações, através do estudo de métodos para a combinação das técnicas de segurança abordadas na linha anterior e as organizações compostas pelas pessoas (o factor humano no sistema). Complementa-se com auditorias informáticas e o estudo do comportamento humano nas organizações do ponto de vista do direito e da ética.

4.5.1.1. Justificar o desenho curricular. (EN)

The curricular structure of this course is oriented in three curricular lines that are characterised as follows.

The first curricular line is composed of the Curricular Units in "Cryptography Applied to Cybersecurity" and "Development of safe code", which make a framework in the area of cryptography, that serves as basis to computer security, as well as in the area of software engineering, which includes software development techniques that are transversal to all computer solutions.

The second curricular line includes the CUs of "Network Security and System Administration", "Intrusion Testing Lab", "Forensic Analysis Lab", and finally "Artificial Intelligence applied to Cybersecurity". These CUs will create the knowledge and skills base structure for the domain of applied cybersecurity, introducing the theoretical concepts and later the practical tools for cybersecurity. It ends with the use of Artificial Intelligence to increase the performance of the tools.

Finally, the third curricular line is composed of the CUs of "Information Security in Organisations", "Computer Auditing" and "Law and Ethics in Cybersecurity". This line addresses the integration of cybersecurity in organisations, by studying methods for combining the security techniques addressed in the previous line and the organisations composed by people (the human factor in the system). It is complemented with computer audits and the study of human behaviour in organisations from the point of view of law and ethics.

4.5.1.2. Percentagem de créditos ECTS de unidades curriculares lecionadas predominantemente a distância.

0.0

4.5.2.1.1. Modelo pedagógico que constitui o referencial para a organização do processo de ensino e aprendizagem das unidades curriculares (PT)

A abordagem pedagógica adotada tem como eixos principais: o contacto direto e de proximidade entre docentes e estudantes; a aplicação do conhecimento para a solução de problemas práticos; a colaboração entre pares e com as entidades parceiras. Considerando o foco na aprendizagem e desenvolvimento de competências orientadas para a prática, tendo por base um sólido conhecimento teórico, são privilegiadas estratégias de aprendizagem ativa, designadamente: estudo de casos aplicados à segurança informática; experimentação em contexto de laboratório. Pretende-se, desta forma, a aplicação dos conceitos teóricos em casos práticos, quer com suporte teórico-prático nos temas mais conceptuais, quer pela experimentação mais prática dos conceitos abordados em laboratórios.
Esta abordagem assenta num regime presencial, tendo os docentes como principal responsabilidade o

acompanhamento dos estudantes no desenvolvimento das tarefas práticas e na construção de conhecimento. Pretende-se uma relação pedagógica de proximidade que conduza à obtenção de resultados de aprendizagem significativos, nomeadamente através de um uso efectivo e substantivo das ferramentas de segurança disponíveis.
Subjacente a este modelo está o propósito institucional de formar pessoas capazes de promover o desenvolvimento económico e social da região do Cávado e do Ave, em que o IPCA se insere. Neste sentido, estão previstas atividades individuais e colaborativas, tendo em vista aprendizagens tanto de um ponto de vista cognitivo, como socio-emocional. Nesta perspetiva, a colaboração entre pares e a parceria com entidades parceiras assumem especial importância. Assim, no âmbito das diferentes UCs, nuns casos de forma isolada, noutros em cooperação entre si e/ou com entidades parceiras, serão adotadas estratégias de aprendizagem baseadas em problemas concretos, incluindo os de natureza multidisciplinar e transversal. Neste caso, destacam-se as metodologias adotadas nas UCs de Segurança da Informação em Organizações, Laboratórios de Testes de Intrusão e naturalmente a UC de projeto/estágio.
No que diz respeito à avaliação, o plano de estudos combina modalidades de avaliação formativa e sumativa, designadamente avaliação contínua, em que o estudante deverá realizar trabalhos individuais, trabalhos de grupo e provas de avaliação. O acompanhamento aos estudantes e a avaliação terão ainda como suporte a plataforma Moodle, ambiente virtual de aprendizagem adotado a nível institucional para contacto remoto, disponibilização de documentação e suporte digital à avaliação.

4.5.2.1.1. Modelo pedagógico que constitui o referencial para a organização do processo de ensino e aprendizagem das unidades curriculares (EN)

The main axes of the adopted pedagogical approach are: direct and close contact between teachers and students; application of knowledge to solve practical problems; collaboration among peers and with partner entities.
Considering the focus on learning and developing practice-oriented skills, based on a solid theoretical knowledge, active learning strategies are privileged, namely: case studies applied to computer security; laboratory experimentation. The aim is to apply theoretical concepts in practical cases, either with theoretical-practical support in the more conceptual topics, or through more practical experimentation of the concepts addressed in laboratories.
This approach is based on the student active participation in the classroom, having the teachers as their main responsibility the follow-up of the students in the development of the practical tasks and in the construction of knowledge. A close pedagogical relationship is intended to lead to the achievement of significant learning results, namely through an effective and substantive use of the available cybersecurity tools.
Underlying this model is the institutional purpose of training people who are able to promote the economic and social development of the region of Cávado and Ave, where IPCA is inserted. In this sense, individual and collaborative activities are foreseen, aiming at learning both from a cognitive and socio-emotional point of view. In this perspective, the collaboration among peers and the partnership with partner entities assume special importance. Thus, within the different CUs, in some cases in an isolated way, in others in cooperation with each other and/or with partner entities, learning strategies based on concrete problems will be adopted, including those of a multidisciplinary and transversal nature. In this case, the methodologies adopted in the UCs of Information Security in Organisations, Intrusion Testing Labs and naturally the Project/Internship UC stand out.
As far as assessment is concerned, the study plan combines formative and summative assessment modalities, namely continuous assessment, in which the student must carry out individual works, group works and assessment tests. Student monitoring and assessment will also be supported by the Moodle platform, a virtual learning environment adopted at institutional level for remote contact, provision of documentation and digital support for assessment.

4.5.2.1.2. Anexos do modelo pedagógico

[sem resposta]

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

As metodologias de ensino e aprendizagem são definidas de acordo com as especificidades de cada par UC/Ciclo de Estudos, com contributos do responsável pela UC, do coordenador da área disciplinar e do diretor de curso. As metodologias adotadas são transmitidas aos estudantes no início do semestre, via plataforma de e-learning (Moodle), através da "Ficha da UC". Esta ficha é validada pelo coordenador da área disciplinar e pelo diretor de departamento. A opinião dos estudantes é recolhida no final de cada semestre, através do Questionário de Avaliação Pedagógica - QAPa, em tópicos como: "Valorização da participação dos estudantes nas atividades de aprendizagem"; "Adequação das estratégias e metodologias de ensino/aprendizagem adotadas ao programa da UC", e "Capacidade de estimular a motivação e interesse nos estudantes". Os dados obtidos são analisados pelo responsável da UC, pelo coordenador da área disciplinar em que a UC se insere, e pelo diretor de curso.

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

Learning and teaching methodologies are defined according to the specificities of each pair UC/Cycle of Studies, with contributions from the Teacher responsible for the UC, the coordinator of the disciplinary area and the course director. The methodologies adopted are made available to students at the beginning of the semester, via e-learning platform (Moodle), through the "UC's File". This document is validated by the disciplinary area's coordinator and by the department director.
The students' opinion is collected at the end of each semester, through the Pedagogical Evaluation Questionnaire - QAPa, on topics such as: "Valuing student participation in learning activities"; "Adequacy of teaching/learning strategies and methodologies adopted for UC programs" and "Ability to stimulate student motivation and interest".

The data obtained are analysed by the Teacher responsible for the UC, and by the coordinator of the disciplinary area.

4.5.2.1.4. Identificação das formas de garantia da justeza, fiabilidade e acessibilidade das metodologias e dos processos de avaliação (PT)

No início de cada UC, o docente irá explicar em detalhe a metodologia de avaliação aos estudantes. Essa metodologia fica registada na ficha da UC, a qual é validada pelo responsável da área disciplinar e pelo diretor de departamento. Relativamente ao processo de avaliação, este pode consistir em diferentes elementos, nomeadamente testes escritos, testes práticos, avaliações orais e avaliações práticas, quer individualmente quer em grupo. Todos os testes (escritos e práticos) correspondem a exames realizados em papel ou formato digital, sendo estes corrigidos pelo docente responsável. Todas as avaliações realizadas através de processos orais ou práticas deverão ser quantificadas num conjunto de parâmetros previamente definidos e apresentados aos estudantes. Todos os estudantes têm direito a solicitar a análise de todos os elementos de avaliação. Caso o assim entenda, o aluno pode solicitar que o seu trabalho seja reavaliado por um segundo docente.

4.5.2.1.4. Identificação das formas de garantia da justeza, fiabilidade e acessibilidade das metodologias e dos processos de avaliação (EN)

At the beginning of each Curricular Unit, the lecturer will explain in detail the assessment methodology to students. This methodology is registered in the curricular unit sheet, which is validated by the head of the disciplinary area and the department director. Regarding the assessment process, it can consist of different elements, namely written tests, practical tests, oral assessments and practical assessments, either individually or in group. All tests (written and practical) correspond to exams conducted on paper or in digital format, which are corrected by the teacher in charge. All assessments carried out through oral or practical processes must be quantified in a set of parameters previously defined and presented to the students. All students have the right to request the analysis of all assessment elements. If he/she so wishes, the student may request that his/her work be re-evaluated by a second teacher.

4.5.2.1.5. Formas de garantia de que a avaliação da aprendizagem dos estudantes será feita em função dos objetivos de aprendizagem da unidade curricular (PT)

As metodologias de avaliação foram selecionadas de modo que os objetivos das unidades curriculares possam ser atingidos, tal como se pode constatar nas fichas das diversas unidades curriculares do ciclo de estudos. Tendo em consideração as recomendações do processo de Bolonha, e com o objetivo de melhorar o sucesso escolar dos estudantes, tem sido privilegiada a avaliação periódica (contínua) nos ciclos de estudos existentes na EST. Com este tipo de avaliação pretende-se que os estudantes desenvolvam um trabalho continuado ao longo do semestre. As metodologias de avaliação integram, frequentemente, diversas componentes de avaliação. Este tipo de sistemas de avaliação permite avaliar não só o domínio dos conteúdos programáticos expostos nas aulas, bem como a aquisição de competências por parte dos estudantes no empreendimento de trabalhos práticos e projetos a nível individual e em grupo.

4.5.2.1.5. Formas de garantia de que a avaliação da aprendizagem dos estudantes será feita em função dos objetivos de aprendizagem da unidade curricular (EN)

The evaluation methodologies have been selected so that the goals of the curricular units can be reached, as can be seen in the curricula of the various curricular units of the study cycle. Considering the recommendation of the Bologna Process, and in order to improve student's achievement, periodic (or continuous) assessment in EST's study cycles has been encouraged. With this type of evaluation, it is intended that the students develop a continuous work throughout the semester. Evaluation methodologies often include several evaluation components (e.g. written tests on content, written reports and oral presentations). This type of evaluation system allows assessing the apprehension, not only of the curricular contents of the curricular unit exposed in class, but also the acquisition of competences by the students in the undertaking of practical assignments and projects made at the individual or group level.

4.5.2.1.6. Demonstração da existência de mecanismos de acompanhamento do percurso e do sucesso académico dos estudantes (PT)

Desde 2020, o IPCA criou um gabinete para promover o sucesso académico e combater o insucesso e abandono escolares, o GAPSA – Gabinete para a Promoção do Sucesso Académico. Este Gabinete tem por missão construir conhecimento acerca das características dos estudantes e dos seus percursos de formação, apoiar no desenvolvimento de formas de vida académica adequadas ao desenvolvimento integral do estudante, bem como no desenho de medidas de apoio que atendam de forma qualificada às suas necessidades.

O GAPSA desenvolve a sua atividade em estreita articulação os demais serviços, escolas e agentes responsáveis pela gestão pedagógica do IPCA e encontra-se integrado no Observatório para a Promoção do Sucesso Académico e o Combate ao Abandono (OPAS), o qual visa a implementação de um conjunto de aplicações informáticas baseadas em inteligência artificial para prever comportamentos indicadores de abandono/promoção escolar.

4.5.2.1.6. Demonstração da existência de mecanismos de acompanhamento do percurso e do sucesso académico dos estudantes. (EN)

Since 2020, IPCA has created an office to promote academic success and combat failure and dropout, the GAPSA - Office for the Promotion of Academic Success. The mission of this Office is to build knowledge about the characteristics of students and their training paths, to support the development of forms of academic life that are appropriate to the full development of students, as well as to design support measures that meet their needs in a qualified way.

GAPSA develops its activity in close articulation with other services, schools and agents responsible for the pedagogical management of the IPCA and is integrated in the Observatory for the Promotion of Academic Success and the Fight against Drop-outs (OPAS), which aims at the implementation of a set of computer applications based on artificial intelligence to predict behaviours that indicate drop-out/promotion.

4.5.2.1.7. Metodologias de ensino previstas com vista a facilitar a participação dos estudantes em atividades científicas (quando aplicável) (PT)

As metodologias de ensino das unidades curriculares presentes no ciclo de estudos orientam os estudantes a desenvolverem atividades científicas aplicadas, quer pelos temas científicos de ponta abordados em muitas das unidades curriculares, quer por se tratar de um nível académico (Mestrado) que requer e exige fundamentação e aplicação científica.
A unidade curricular de Projeto inclui a abordagem de conteúdos de métodos de trabalho de projeto e métodos de investigação para habilitar os estudantes para o exercício de investigação orientada à engenharia e recorrer. A elaboração de trabalhos como componente de avaliação em várias unidades curriculares permite o desenvolvimento de práticas de investigação e a aquisição dos instrumentos para a realização de trabalhos onde se encontra presente a componente científica.

4.5.2.1.7. Metodologias de ensino previstas com vista a facilitar a participação dos estudantes em atividades científicas (quando aplicável) (EN)

The teaching methodologies of the curricular units guide the students to develop applied scientific activities, because of the cutting-edge scientific topics addressed in many of the curricular units and the academic level (Masters) that requires and demands scientific basis and application.
The Project curricular unit includes working methods and research methods to enable students to carry out research oriented to engineering and resource. The elaboration of works as an assessment component in several curricular units allows the development of research practices and the acquisition of the instruments to carry out work where the scientific component is present.

4.5.2.2.1. Fundamentação do número total de créditos ECTS e da duração do ciclo de estudos (PT)

A distribuição dos ECTS foi definida nos termos da legislação em vigor. Ponderou-se a unidade curricular enquanto medida do trabalho sob todas as suas formas (sessões de ensino de natureza coletiva, tutorial, estágios, projetos). Nesta distribuição, foi considerado a duração normal do curso, o número de semestres letivos e os requisitos para que o curso fosse conducente ao grau de mestre no ensino politécnico, tendo-se estabelecido um total de 60 ECTS distribuídos por 2 semestres. Nesta lógica, fez-se coincidir o trabalho dos estudantes em ECTS do curso com outros cursos congéneres, nacionais e internacionais.

4.5.2.2.1. Fundamentação do número total de créditos ECTS e da duração do ciclo de estudos (EN)

The distribution of ECTS was defined under the terms of the legislation in force. The curricular unit was planned as a measure of the work in all its forms (teaching sessions of collective nature, tutorial, internships, projects). In this distribution, the normal duration of the course, the number of teaching semesters and the requirements for the course to lead to the degree of master in polytechnic education were considered, having been established a total of 60 ECTS distributed by 2 semesters. In this logic, the students' work in ECTS was made to coincide with other similar national and international courses.

4.5.2.2.2. Forma de verificação de que a carga média de trabalho que será necessária aos estudantes corresponde ao estimado em créditos ECTS (PT)

A metodologia de aprendizagem e de avaliação às diferentes unidades curriculares contempla, diferenciadamente, componentes de realização de trabalhos individuais e em grupo, a leitura de textos recomendados, a preparação e apresentação de relatórios ou a resolução de casos de estudo ou exercícios práticos, além da necessidade de estudo para os momentos de avaliação individual (avaliação contínua/testes e exames). Neste sentido, a verificação da adequação da carga média de trabalho por unidade curricular é feita inicialmente, ao elaborar a ficha da unidade curricular. Tendo em consideração o estudo e os trabalhos que os estudantes são incentivados a realizar para cada unidade curricular, considerou-se que o tempo médio de trabalho necessário é de 26,6 horas de trabalho por unidade de ECTS.

4.5.2.2.2. Forma de verificação de que a carga média de trabalho que será necessária aos estudantes corresponde ao estimado em créditos ECTS. (EN)

The learning and assessment methodology for the different curricular units includes, in a different way, individual and group work components, reading recommended texts, preparing and presenting reports or solving case studies or practical exercises, as well as the need to study for individual assessment moments (tests and exams). In this sense, the verification of the adequacy of the average workload per curricular unit is done initially, when preparing the certificate of the curricular unit. Considering the study and the work that students are encouraged to perform for each course unit, it was considered that the average work time required is 26,6 hours of work per unit of ECTS.

4.5.2.2.3. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de créditos ECTS das unidades curriculares (PT)

A forma como os docentes foram consultados sobre a metodologia de cálculo do número de créditos ECTS das unidades curriculares do ciclo de estudos englobou, como se estabelece nos regulamentos da Escola Superior
de Tecnologia, reuniões efetuadas por todos os órgãos e que principiaram em reuniões de área Disciplinar, seguidas de reuniões de Departamento e posterior aprovação pela Direção da Escola que as submete ao Conselho

Pedagógico e ao Conselho Técnico-Científico.

4.5.2.2.3. Forma como os docentes foram consultados sobre a metodologia de cálculo do número de créditos ECTS das unidades curriculares (EN)

As established in the School of Technology's regulations, the way in which the teaching staff was consulted about the methodology for calculating the number of ECTS credits of the study cycle's course units involved meetings held by all the bodies, beginning with meetings of the disciplinary area, followed by Departmental meetings and then approved by the School's Director, who submits them to the Pedagogical Council and the Scientific-Technical Council.

4.5.2.3. Observações (PT)

Não aplicável.

4.5.2.3. Observações (EN)

Not applicable.

5. Pessoal Docente

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

• *Nuno Alberto Ferreira Lopes*

5.2. Pessoal docente do ciclo de estudos

Nome	Categoria	Grau	Vínculo	Especialista	Regime de	Informação
Nuno Alberto Ferreira Lopes	Professor Adjunto ou equivalente	Doutor Informática	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
João Carlos Silva	Professor Adjunto ou equivalente	Doutor Informática	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Paulo Teixeira	Professor Adjunto ou equivalente	Mestre Sistemas e Tecnologias da Informação	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Gonçalo Nicolau cerqueira Sopas de Melo Bandeira	Professor Adjunto ou equivalente	Doutor Ciências Jurídico-Criminais Direito Público	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Patrícia Leite	Equiparado a Professor Adjunto ou equivalente	Doutor Ciências da Informação	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID

Nome	Categoria	Grau	Vínculo	Especialista	Regime de	Informação
Joaquim Gonçalves	Professor Adjunto ou equivalente	Doutor Ciências da Informação - Tecnologias da Informação	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Luís Ferreira	Professor Adjunto ou equivalente	Doutor Engenharia Industrial e Sistemas	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Nuno Ricardo Mateus Coelho	Professor Adjunto ou equivalente	Doutor Informática	Outro vínculo		15	Ficha Submetida CienciaVitae OrcID
Óscar Ribeiro	Equiparado a Professor Adjunto ou equivalente	Doutor Engenharia Informática	Outro vínculo		100	Ficha Submetida CienciaVitae OrcID
Sandro Carvalho	Assistente convidado ou equivalente	Doutor Engenharia Eletrotécnica e de Computadores	Outro vínculo		55	Ficha Submetida OrcID
					Total: 870	

5.2.1. Ficha curricular do docente

5.2.1.1. Dados Pessoais - Nuno Alberto Ferreira Lopes

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Informática

Área científica deste grau académico (EN)

Informatics

Ano em que foi obtido este grau académico

2009

Instituição que conferiu este grau académico

Universidade do Minho

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

B51B-E448-2C8E

Orcid

0000-0001-8897-5061

5.2.1.2. Filiação Unidades de Investigação - Nuno Alberto Ferreira Lopes

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	

5.2.1.3. Outros graus académicos ou títulos - Nuno Alberto Ferreira Lopes

Ano	Grau ou Título	Área	Instituição	Classificação
2002	Licenciatura em Engenharia de Sistemas Informáticos	Informática	Universidade do Minho	16 valores

5.2.1.4. Formação pedagógica - Nuno Alberto Ferreira Lopes

Formação pedagógica relevante para a docência
Como promover o pensamento crítico e criativo usando o método cooperativo Jigsaw e os mapas de conceitos - Jornadas Interinstitucionais de Desenvolvimento Pedagógico
A aprendizagem invertida (flipped learning) e o ensino misto (b-learning) - Jornadas Interinstitucionais de Desenvolvimento Pedagógico
O Design thinking como metodologia transversal em Project based learning - Jornadas Interinstitucionais de Desenvolvimento Pedagógico
Cibersegurança e Gestão de Crises no ciberespaço, curso V, Instituto Nacional da Defesa (IDN), Abril 2018.

5.2.1.5. Distribuição do serviço docente - Nuno Alberto Ferreira Lopes

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Sistemas Operativos	Licenciatura em Engenharia Sistemas Informáticos	60.0	30.0	30.0						
Arquitectura de Computadores e Sistemas Operativos	Licenciatura em Engenharia Informática Médica	60.0		60.0						
Inteligência Artificial na Cibersegurança	Mestrado em Inteligência Artificial Aplicada	30.0		24.0					6.0	
Redes de Computadores	Licenciatura em Engenharia Informática Médica	60.0		60.0						
Redes de Computadores e Sistemas Distribuídos	Licenciatura em Engenharia Eletrotécnica e de Computadores	60.0	40.0		20.0					
Computação de Alto Desempenho	Mestrado em Engenharia Informática	30.0		30.0						
Comunicações de Dados	Licenciatura em Engenharia Informática Médica	60.0	30.0	30.0						

5.2.1.1. Dados Pessoais - João Carlos Silva

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Informática

Área científica deste grau académico (EN)

Informatic

Ano em que foi obtido este grau académico

2010

Instituição que conferiu este grau académico

Universidade do Minho

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

E012-820F-D378

Orcid

0000-0002-4575-0142

5.2.1.2. Filiação Unidades de Investigação - João Carlos Silva

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	Institucional

5.2.1.3. Outros graus académicos ou títulos - João Carlos Silva

Ano	Grau ou Título	Área	Instituição	Classificação
2010	Doutoramento	Informática	Universidade do Minho	Aprovado

5.2.1.4. Formação pedagógica - João Carlos Silva

Formação pedagógica relevante para a docência
Coordenador da Área Disciplinar de Ciências e Tecnologias de Programação
Diretor do curso de Mestrado em Engenharia Informática de 2019 até 2022
Diretor do Departamento de Tecnologias da Computação e Informação
Formação sobre a utilização de câmara e smartboard em sala de aula

5.2.1.5. Distribuição do serviço docente - João Carlos Silva

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Estruturas de Dados Avançadas	Licenciatura em Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Programação Imperativa	Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)	60.0	30.0	30.0						
Estruturas de Dados Avançadas	Licenciatura em Engenharia Eletrotécnica e Computadores	60.0	30.0	30.0						
Plano de Dissertação/Projeto/Estágio	Mestrado em Engenharia Informática	15.0			15.0					
Dissertação/Projeto/Estágio	Mestrado em Engenharia Informática	30.0			30.0					
Programação	Licenciatura em Engenharia e Gestão Industrial	60.0		60.0						
Estruturas de Dados Avançadas	Licenciatura em Engenharia em Informática Médica	60.0		30.0	30.0					

5.2.1.1. Dados Pessoais - Paulo Teixeira

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Sistemas e Tecnologias da Informação

Área científica deste grau académico (EN)

Information Systems and Technologies

Ano em que foi obtido este grau académico

2005

Instituição que conferiu este grau académico

Universidade de Aveiro

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

7D1E-9358-81B8

Orcid

0000-0002-7596-9735

5.2.1.2. Filiação Unidades de Investigação - Paulo Teixeira

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial e Ciência de Computadores (UACC)	Excelente	Universidade do Porto (UP)	

5.2.1.3. Outros graus académicos ou títulos - Paulo Teixeira

Ano	Grau ou Título	Área	Instituição	Classificação
2005	Mestre	Sistemas e Tecnologias de Informação	Universidade de Aveiro	14
1999	Licenciatura	Sistemas e Tecnologias de Informação	Universidade Fernando Pessoa	15 (20)

5.2.1.4. Formação pedagógica - Paulo Teixeira

Formação pedagógica relevante para a docência
Curso de Formação Pedagógica de Formadores do Sistema de Aprendizagem
Certificado de aptidão pedagógica
Várias formações e certificações no âmbito da pedagogia
Concepção e Desenvolvimento de Conteúdos para e-Learning

5.2.1.5. Distribuição do serviço docente - Paulo Teixeira

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Métodos de Investigação em Engenharia Informática	Mestrado em Engenharia Informática	30.0		30.0						
Sistemas de Armazenamento de Dados	Engenharia de Desenvolvimento de Jogos Digitais	60.0		60.0						
Sistemas de Informação para a Qualidade, Ambiente e Segurança	Mestrado em Sistemas Integrados de Gestão para a Qualidade Ambiente e Segurança	60.0		40.0	20.0					
Governação Digital	Gestão Pública	30.0	15.0	15.0						
Armazenamento e Acesso a Dados	Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Cibersegurança	Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Armazenamento e Acesso a Dados	Engenharia e Gestão Industrial	60.0		60.0						

5.2.1.1. Dados Pessoais - Gonçalo Nicolau cerqueira Sopas de Melo Bandeira

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Ciências Jurídico-Criminais Direito Público

Área científica deste grau académico (EN)

Legal and Criminal Sciences Public Law

Ano em que foi obtido este grau académico

2009

Instituição que conferiu este grau académico

Faculdade de Direito da Universidade de Coimbra

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

DA19-3665-82E1

Orcid

0000-0001-8859-4023

5.2.1.2. Filiação Unidades de Investigação - Gonçalo Nicolau cerqueira Sopas de Melo Bandeira

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Centro de Investigação em Justiça e Governação (JusGov)	Muito Bom	Universidade do Minho (UM)	

5.2.1.3. Outros graus académicos ou títulos - Gonçalo Nicolau cerqueira Sopas de Melo Bandeira

Ano	Grau ou Título	Área	Instituição	Classificação
2014	Pós-Doutoramento em Direitos Humanos-Responsabilidade Financeira	Direitos Humanos - Direito Público	Jus Gentium Conimbrigae - Faculdade de Direito da Universidade de Coimbra	Aprovado
2009	Doutoramento em Ciências Jurídico-Criminais-Direito Público	Direito	Faculdade de Direito da Universidade de Coimbra	Aprovado por Unanimidade com Distinção
2003	Mestrado em Ciências Jurídico-Criminais-Direito Público	Direito	Faculdade de Direito da Universidade Católica Portuguesa	17 Valores ou Muito Bom (0-20)
2000	Curso de Especialização em Ciências Jurídico-Criminais-Direito Público	Direito Público	Faculdade de Direito da Universidade Católica Portuguesa	16 Valores

5.2.1.4. Formação pedagógica - Gonçalo Nicolau cerqueira Sopas de Melo Bandeira

Formação pedagógica relevante para a docência
Informática para as Ciências e Engenharias, Faculdade de Ciências da Universidade Nova de Lisboa, 70 horas

5.2.1.5. Distribuição do serviço docente - Gonçalo Nicolau cerqueira Sopas de Melo Bandeira

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Direito e Processo Penal, Regime Diurno	Solicitadoria, Estudos Legais	60.0	45.0	15.0						
Direito e Processo Penal, Regime Nocturno	Solicitadoria, Estudos Legais	60.0	45.0	15.0						
Direitos Fundamentais, Regime Diurno	Fiscalidade	60.0	0.0	60.0						
Infracções Tributárias	Mestrado em Fiscalidade	16.0	0.0	16.0						
Direito das Sociedades e dos Valores Mobiliários	Mestrado em Auditoria	12.0	0.0	12.0						
Direito e Processo Penal e das Contraordenações, Regime Diurno	Solicitadoria, Estudos Legais	60.0	45.0	15.0						
Direito e Processo Penal e das Contraordenações, Regime Nocturno	Solicitadoria, Estudos Legais	60.0	45.0	15.0						
Direito Tecnodigital, Regime Diurno	Engenharia e Desenvolvimento de Jogos Digitais	30.0		30.0						

5.2.1.1. Dados Pessoais - Patrícia Leite

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Equiparado a Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Ciências da Informação

Área científica deste grau académico (EN)

Information Science

Ano em que foi obtido este grau académico

2015

Instituição que conferiu este grau académico

Universidade Fernando Pessoa

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

2D17-B7C4-7A84

Orcid

0000-0002-6678-3912

5.2.1.2. Filiação Unidades de Investigação - Patrícia Leite

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	
Laboratório de Inteligência Artificial e Ciência de Computadores (UACC)	Excelente	Universidade do Porto (UP)	

5.2.1.3. Outros graus académicos ou títulos - Patrícia Leite

Ano	Grau ou Título	Área	Instituição	Classificação
2005	Sistemas de Informação	Sistemas de Informação	Universidade do Minho	muito bom

5.2.1.4. Formação pedagógica - Patrícia Leite

Formação pedagógica relevante para a docência
Projetos baseados na aprendizagem - duas fases de formação, na primeira foi apresentada e discutida uma primeira versão dos learning outcomes do curso, da estrutura curricular, e posteriormente dos conteúdos programáticos e na segunda preparado todo o arranque para ser implementado nos cursos.
50+10 concept - a pedagogical framework for the development of future skills across IPCA - Polytechnic Institute of Cávado and Ave's educational offer. This framework was designed to address the challenge of integrating transversal competences with knowledge and disciplinary expertise, in Higher Education courses. It offers an integrated approach that aims to respond to the needs of students, teachers, employers, hence society at large, incorporating student-centered teaching and learning strategies, pedagogical development, transferable competences and university-community-industry-society partnerships, capable of delivering social transformations.

5.2.1.5. Distribuição do serviço docente - Patrícia Leite

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Gestão de Sistemas de Informação	Licenciatura em Engenharia Informática Médica	30.0		30.0						
Tecnologias de Informação para a Gestão	Licenciatura em Gestão de Empresas	60.0		60.0						
Projecto Multimodal	Mestrado em Engenharia Informática	30.0		0.0	30.0					
Projecto Aplicado	Licenciatura em Engenharia e Sistemas Informáticos	60.0			60.0					
Análise Projecto de Sistemas	Licenciatura em Engenharia Informática Médica	60.0		45.0	15.0					
Programação Web	Licenciatura em Engenharia Informática Médica	60.0		30.0	30.0					

5.2.1.1. Dados Pessoais - Joaquim Gonçalves

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Ciências da Informação - Tecnologias da Informação

Área científica deste grau académico (EN)

Data Science - Information Technology

Ano em que foi obtido este grau académico

2012

Instituição que conferiu este grau académico

Universidade Fernando Pessoa

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

131B-C03E-3354

Orcid

0000-0003-2219-1816

5.2.1.2. Filiação Unidades de Investigação - Joaquim Gonçalves

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial e Ciência de Computadores (UACC)	Excelente	Universidade do Porto (UP)	Institucional
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	Institucional

5.2.1.3. Outros graus académicos ou títulos - Joaquim Gonçalves

Ano	Grau ou Título	Área	Instituição	Classificação
1990	Licenciatura em Matemáticas Aplicadas	461	Universidade Lusíada	14
1994	Mestrado em Engenharia Electrotécnica e de Computadores - Perfil Ssitemas	481	Faculdade de Engenharia da Universidade do Porto	Muito bom

5.2.1.4. Formação pedagógica - Joaquim Gonçalves

Formação pedagógica relevante para a docência
Scrum Master
Curso de ITIL
Demola

5.2.1.5. Distribuição do serviço docente - Joaquim Gonçalves

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Armazenamento e Acesso a Dados	Lic Engenharia Informática Médica	60.0		60.0						
Inteligência Artificial	Lic. Engenharia Informática Médica	60.0		60.0						
Inteligência Artificial	Lic Engenharia de Sistemas Informáticos	60.0	20.0	40.0						
Inteligência Artificial Aplicada	Mestrado em Engenharia Informática	30.0		30.0						
Inteligência artificial aplicada à indústria	Mestrado em Engenharia e Gestão Industrial	30.0		30.0						
Aprendizagem Computacional	Mestrado em Inteligência Artificial Aplicada	30.0		24.0					6.0	
Armazenamento e Acesso a dados	Lic Engenharia Electrotécnica e de Computadores	60.0	30.0	30.0						
Programação de Bases de Dados	Lic Engenharia Informática Médica	60.0		60.0						

5.2.1.1. Dados Pessoais - Luís Ferreira

Vínculo com a IES

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018

Área científica deste grau académico (PT)

Engenharia Industrial e Sistemas

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2013

Instituição que conferiu este grau académico

Universifdade do Minho

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

AD10-8EAE-8EE2

Orcid

0000-0001-9635-5372

5.2.1.2. Filiação Unidades de Investigação - Luís Ferreira

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	

5.2.1.3. Outros graus académicos ou títulos - Luís Ferreira

5.2.1.4. Formação pedagógica - Luís Ferreira

Formação pedagógica relevante para a docência
1. PRACE Winter School 2019 - Introduction to Machine Learning for scientists, KU Leuven ICTS, Bruxelas, 4-8 março 2019.
2. Introduction to Quantum Computing, CESGA, Santiago de Compostela, Espanha, 1-5 abril 2019.
3. Cibersegurança e Gestão de Crises no Ciberespaço, curso V, Instituto Nacional da Defesa (IDN), 03-06 de abril e 4 de maio, 2018
4. Optimización y profiling de aplicaciones usando herramientas de Intel, Mobility Agreement - Staff Mobility For Training ERASMUS+, CESGA, Santiago de Compostela, Espanha, 5-7 junho de 2018.
5. GPU Hackthon “CESGAHACK 18”, Mobility Agreement - Staff Mobility For Training, ERASMUS+, CESGA, 5-9 março, Santiago de Compostela, Espanha, 5-9 março 2018
8. Processamiento de Dados con Python: Entornos y Aplicaciones, CESGA - Centro de Supercomputación de Galicia, Santiago de Compostela, Espanha, 16-18 junho 2015

5.2.1.5. Distribuição do serviço docente - Luís Ferreira

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Programação Imperativa	Engenharia Informática Médica	60.0	0.0	60.0						
Programação Orientada a Objetos	Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Integração de Sistemas de Informação	Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Projeto de Computação na Cloud	Mestrado em Engenharia Informática	30.0	30.0							
Estruturas de Dados Avançadas	Engenharia Sistemas Informáticos	60.0	30.0	30.0						
Estruturas de Dados Avançadas	Engenharia de Desenvolvimento de Jogos	60.0	30.0	30.0						

5.2.1.1. Dados Pessoais - Nuno Ricardo Mateus Coelho

Vínculo com a IES

Outro vínculo

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Outro vínculo

Área científica deste grau académico (PT)

Informática

Área científica deste grau académico (EN)

Computer Sciences

Ano em que foi obtido este grau académico

2020

Instituição que conferiu este grau académico

Universidade de Trás-os-Montes e Alto Douro

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

15

CienciaVitae

A514-DAF9-ECB2

Orcid

0000-0001-5517-9181

5.2.1.2. Filiação Unidades de Investigação - Nuno Ricardo Mateus Coelho

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
INESC TEC - INESC Tecnologia e Ciência (INESC TEC)	Muito Bom	Inesc Tec - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)	Institucional

5.2.1.3. Outros graus académicos ou títulos - Nuno Ricardo Mateus Coelho

Ano	Grau ou Título	Área	Instituição	Classificação
2015	Mestrado em Engenharia Informática	Engenharia Informática - Segurança Informática	ISEP Porto	16
2012	Licenciatura Engenharia Sistemas de Informação e Multimédia	Information Systems	Instituto Superior de Línguas e Administração	13

5.2.1.4. Formação pedagógica - Nuno Ricardo Mateus Coelho

Formação pedagógica relevante para a docência
Certificado de Competências Pedagógicas

5.2.1.5. Distribuição do serviço docente - Nuno Ricardo Mateus Coelho

5.2.1.1. Dados Pessoais - Óscar Ribeiro

Vínculo com a IES

Outro vínculo

Categoria

Equiparado a Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Outro vínculo

Área científica deste grau académico (PT)

Engenharia Informática

Área científica deste grau académico (EN)

Computer Science and engineering

Ano em que foi obtido este grau académico

2009

Instituição que conferiu este grau académico

Universidade do Minho

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

100

CienciaVitae

5C18-833A-8DF2

Orcid

0000-0002-7301-3211

5.2.1.2. Filiação Unidades de Investigação - Óscar Ribeiro

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	Institucional

5.2.1.3. Outros graus académicos ou títulos - Óscar Ribeiro

Ano	Grau ou Título	Área	Instituição	Classificação
2002	Licenciatura	Matemática e Ciências da Computação	Universidade do Minho	16
2005	Mestrado	Engenharia Informática	Universidade do Minho	muito bom

5.2.1.4. Formação pedagógica - Óscar Ribeiro

Formação pedagógica relevante para a docência
Formação de Metodologias de Ensino Inovadoras, 8 de abril
Formação Pauta de Avaliação Contínua, 23 de março

5.2.1.5. Distribuição do serviço docente - Óscar Ribeiro

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Labortatórios de Informática	Licenciatura em Engenharia de Sistemas Informáticos	60.0			60.0					
Labortatórios de Informática	Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)	60.0			60.0					
Programação Orientada a Objetos	Licenciatura Engenharia Eletrotécnica e de Computadores	60.0	30.0	30.0						
Integração de Sistemas de Informação	Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)	60.0	30.0	30.0						
Processamento de Linguagens	Licenciatura em Engenharia de Sistemas Informáticos	60.0	30.0	30.0						
Processamento de Linguagens	Licenciatura em Engenharia de Sistemas Informáticos (pós-laboral)	60.0	30.0	30.0						

5.2.1.1. Dados Pessoais - Sandro Carvalho

Vínculo com a IES

Outro vínculo

Categoria

Assistente convidado ou equivalente

Grau Associado

Sim

Grau

Outro vínculo

Área científica deste grau académico (PT)

Engenharia Eletrotécnica e de Computadores

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2015

Instituição que conferiu este grau académico

UTAD

Título de Especialista (Art. 3.º alínea g) do DL n.º 74/2006, de 24 de março na redação do DL n.º 65/2018, 16 de Agosto)

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

Regime de dedicação na instituição que submete a proposta (%)

55

CienciaVitae

-

Orcid

0000-0003-4470-4993

5.2.1.2. Filiação Unidades de Investigação - Sandro Carvalho

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	

5.2.1.3. Outros graus académicos ou títulos - Sandro Carvalho

Ano	Grau ou Título	Área	Instituição	Classificação
2008	Licenciatura	Engenharia Eletrotécnica e de Computadores	UTAD	16
2009	Mestrado	Engenharia Eletrotécnica e de Computadores	UTAD	17

5.2.1.4. Formação pedagógica - Sandro Carvalho

Formação pedagógica relevante para a docência
Certificado de Aptidão Pedagógica (CAP)

5.2.1.5. Distribuição do serviço docente - Sandro Carvalho

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Registo Clínico Eletrónico	Licenciatura em Engenharia Informática Médica	60.0	0.0	45.0	15.0					
Arquitetura de Dispositivos de Suporte a Jogos	Licenciatura em Engenharia e Desenvolvimento de Jogos Digitais	60.0	0.0	60.0	0.0					
Arquitetura de Computadores	Licenciatura em Engenharia de Sistemas Informáticos	60.0	30.0	30.0	0.0					
Arquitetura de Computadores - PL	Licenciatura em Engenharia de Sistemas Informáticos	60.0	30.0	30.0	0.0					

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

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

5.3.1.1. Número total de docentes.

10

5.3.1.2. Número total de ETI.

8.70

5.3.2. Corpo docente próprio – docentes do ciclo de estudos integrados na carreira docente ou de investigação (art.º 3 DL-74/2006, na redação fixada pelo DL-65/2018).*

Vínculo com a IES	**% em relação ao total de ETI**
Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018	80.46%
Investigador de Carreira (Art. 3º, alínea l) do DL-74/2006, na redação fixada pelo DL-65/2018	0.00%
Outro vínculo	19.54%

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

Corpo docente academicamente qualificado	**ETI**	**Percentagem***
Docentes do ciclo de estudos com o grau de doutor (ETI)	770	88.51%

5.3.4. Corpo docente especializado

Corpo docente especializado	**ETI**	**Percentagem***
Doutorados especializados na(s) área(s) fundamental(is) do CE (% total ETI)	5.15	59.20%
Não doutorados, especializados nas áreas fundamentais do CE (% total ETI)	1.0	11.49%

Não doutorados na(s) área(s) fundamental(is) do CE, com Título de Especialista (DL 206/2009) nesta(s) área(s)(% total ETI)	0.0	0.00%
% de docentes com título de especialista ou doutores especializados, na(s) área(s) fundamental(is) do ciclo de estudos (% total ETI)		70.69%

5.3.5. Corpo Docente integrado em Unidades de Investigação da Instituição, suas subsidiárias ou polos nela integrados (art.º 29.º DL-74/2006, na redação fixada pelo DL-65/2018)

Descrição	ETI	Percentagem*
Corpo Docente integrado em Unidades de Investigação da Instituição, suas subsidiárias ou polos nela integrados	3.15	36.21%

5.3.6. Estabilidade e dinâmica de formação do corpo docente.

Estabilidade e dinâmica de formação	ETI	Percentagem*
Docentes do ciclo de estudos de carreira com uma ligação à instituição por um período superior a três anos	7.0	80.46%
Docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (ETI)	1.0	11.49%

5.4. Desempenho do pessoal docente

5.3.1.1 Procedimento de avaliação do desempenho do pessoal docente e medidas conducentes à sua permanente atualização e desenvolvimento profissional (PT).

O Pessoal docente é avaliado pelo Regulamento consagrado no Despacho n.º 11965/2010, publicado em Diário da República, 2.ª série - N.º 142 - 23 de Julho de 2010, revisto e republicado conforme Declaração de Retificação Nº1312/2014 publicado no Diário da República, 2.ª série, N.º 246 de 22 de dezembro. Como principais indicadores da avaliação de desempenho do pessoal docente destacam-se: o cumprimento do serviço docente distribuído, a participação em atividades de gestão, órgãos e comissões da instituição, a investigação científica e a formação contínua. Na avaliação do desempenho do pessoal docente, também se releva o depoimento periódico dos estudantes sobre o ensino desenvolvido pelos seus professores. A instituição participa nas Jornadas Interinstitucionais para o Desenvolvimento Pedagógico para efeitos de atualização pedagógica e desenvolvimento profissional.

5.3.1.1 Procedimento de avaliação do desempenho do pessoal docente e medidas conducentes à sua permanente atualização e desenvolvimento profissional (EN).

The teaching staff is evaluated by the Regulation Order No. 11965/2010, published in "Diário da República", 2nd Series - No. 142 - July 23, 2010, revised and republished as the Declaration of Rectification No. 1312/2014 published in "Diário da República", 2nd series, No. 246 of 22. As key indicators of the performance evaluation of the teaching staff of IPCA we highlight the academic service distribution, the participation in management activities, councils and committees of the institution, scientific research and training. When accessing the performance of academic staff, the students' survey about teaching activities is also taken into account. The institution participates in the interinstitutional seminars for pedagogical development, for pedagogical updating and professional development purposes.

5.3.2.1. Observações (PT)

A equipa docente proposta para este ciclo de estudos é, praticamente na íntegra, doutorada na área fundamental de Informática, com currículo na área da cibersegurança e membro de vários centros de investigação nomeadamente: 2AI, Laboratório de Inteligência Artificial Aplicada, do Instituto Politécnico do Cávado e do Ave; LIACC- Laboratório de Inteligência Artificial e Ciência de Computadores, da Universidade do Porto; JusGov- Centre for Justice and Governance da Universidade do Minho; e LAPI2S- Laboratory of Privacy and Information Systems Security.
Algumas das publicações mais relevantes pela equipa são:
** Almeida, A., Mateus-Coelho, N., Lopes, N. (2021). Paranoid OS: Wearable Trackers. Advanced Research on Information Systems Security, Volume 1, No 1, pp 24-40.*
** Almeida, A., Mateus-Coelho, N., Lopes, N., Portela, I. (2022). Paranoid OS: Wearable Trackers. Proceedings of the International Conference on Industry Sciences and Computer Sciences Innovation. Procedia Computer Science.*
** Fernandes, R., Lopes, N., Gonçalves, J. (2022) Network Intrusion Detection Packet Classification with the HIKARI-2021 Dataset: a study on ML Algorithms. Proceedings of the 1st Workshop on Applications of Artificial Intelligence for Society, co-located with 10th International Symposium on Digital Forensics and Security. IEEE.*
** Vidal Carvalho, J.; Carvalho, S.; Rocha, A. (2020) European strategy and legislation for cybersecurity: implications for Portugal. Cluster Computing - The Journal of Networks, Software Tools and Applications. https://doi.org/10.1007/s10586-020-03052-y*

** Carvalho, S., Carvalho J.V., Casquilho, M., Silva J.C., Santos, G. (2022) The Use of ICT in Today's Society from the Perspective of Citizens and Businesses: Security risks and their influence on the quality of life of the Portuguese population. International Journal for Quality Research.*
** Mateus-Coelho, N., Cruz-Cunha, M., Ferreira, L. (2021) Security in Microservices Architectures. Procedia Computer Science, vol 181. Elsevier.*
** Mateus-Coelho, N., Cruz-Cunha, M. (2022) Serverless Service Architectures and Security Minimals. 10th International Symposium on Digital Forensics and Security. IEEE.*
** Alves, F., Mateus-Coelho, N., Cruz-Cunha, M. (2022) ChevroCrypto – Security & Cryptography Broker. 10th International Symposium on Digital Forensics and Security. IEEE.*
Para além das publicações, o corpo docente participa na coordenação do projeto de investigação "Cybers SeC IP - CYBERSecurity SciEntific Competences and Innovation Potential" (https://2ai.ipca.pt/cybers-sec-ip/), onde a aplicação de cibersegurança é essencial para garantir a segurança da informação.
Adicionalmente, os docentes Nuno Lopes e Joaquim Gonçalves realizaram o Workshop on Applications of Artificial Intelligence for Society, integrado na conferência International Symposium on Digital Forensics and Security. Finalmente o docente Nuno Coelho coordena a revista Advanced Research on Information Systems Security.

5.3.2.1. Observações (EN)

The faculty proposed for this study cycle is, practically in its entirety, PhDs in the fundamental area of Computer Science, with a curriculum in the area of cybersecurity and members of several research centres, namely: 2AI, Laboratory of Applied Artificial Intelligence of the Polytechnic Institute of Cávado and Ave; LIACC- Laboratory of Artificial Intelligence and Computer Science of the University of Porto; JusGov- Centre for Justice and Governance of the University of Minho; and LAPI2S- Laboratory of Privacy and Information Systems Security.
Some of the most relevant publications by the team are:
** Almeida, A., Mateus-Coelho, N., Lopes, N. (2021). Paranoid OS: Wearable Trackers. Advanced Research on Information Systems Security, Volume 1, No 1, pp 24-40.*
** Almeida, A., Mateus-Coelho, N., Lopes, N., Portela, I. (2022). Paranoid OS: Wearable Trackers. Proceedings of the International Conference on Industry Sciences and Computer Sciences Innovation. Procedia Computer Science.*
** Fernandes, R., Lopes, N., Gonçalves, J. (2022) Network Intrusion Detection Packet Classification with the HIKARI-2021 Dataset: a study on ML Algorithms. Proceedings of the 1st Workshop on Applications of Artificial Intelligence for Society, co-located with 10th International Symposium on Digital Forensics and Security. IEEE.*
** Vidal Carvalho, J.; Carvalho, S.; Rocha, A. (2020) European strategy and legislation for cybersecurity: implications for Portugal. Cluster Computing - The Journal of Networks, Software Tools and Applications. https://doi.org/10.1007/s10586-020-03052-y*
** Carvalho, S., Carvalho J.V., Casquilho, M., Silva J.C., Santos, G. (2022) The Use of ICT in Today's Society from the Perspective of Citizens and Businesses: Security risks and their influence on the quality of life of the Portuguese population. International Journal for Quality Research.*
** Mateus-Coelho, N., Cruz-Cunha, M., Ferreira, L. (2021) Security in Microservices Architectures. Procedia Computer Science, vol 181. Elsevier.*
** Mateus-Coelho, N., Cruz-Cunha, M. (2022) Serverless Service Architectures and Security Minimals. 10th International Symposium on Digital Forensics and Security. IEEE.*
** Alves, F., Mateus-Coelho, N., Cruz-Cunha, M. (2022) ChevroCrypto – Security & Cryptography Broker. 10th International Symposium on Digital Forensics and Security. IEEE.*
In addition to publications, the faculty participates in the coordination of the research project "Cybers SeC IP - CYBERSecurity SciEntific Competences and Innovation Potential" (https://2ai.ipca.pt/cybers-sec-ip/), where the application of cybersecurity is essential to ensure information security.
The professors Nuno Lopes e Joaquim Gonçalves organised the Workshop on Applications of Artificial Intelligence for Society, integrated into the International Symposium on Digital Forensics and Security. Finally, professor Nuno Coelho coordinates the Advanced Research on Information Systems Security international journal.

6. Pessoal técnico, administrativo e de gestão

6.1. Número e regime de dedicação do pessoal técnico, administrativo e de gestão afeto à lecionação do ciclo de estudos. Apresentação da estrutura e organização da equipa que colaborará com os docentes do ciclo de estudos. (PT)

Para além da sua organização científico-pedagógica a EST dispõe de serviços administrativos que prestam o apoio necessário ao seu funcionamento global. Atualmente, dispõe de 1 Chefe de Divisão e 3 colaboradores administrativos, todos em regime de tempo integral, que desempenham tarefas de gestão e apoio ao funcionamento da oferta educativa da Escola, para além de outras atribuições (apoio na organização de eventos diversos, conferências, seminários, cursos breves e outras formações). Apoiam, ainda, o funcionamento da EST todos os funcionários dos restantes serviços do IPCA, nomeadamente, Divisão Académica e Serviços de Ação Social, Biblioteca, Divisão de Sistemas de Informação, Divisão Administrativa e Financeira, Divisão de recursos Humanos, Gabinete para a Avaliação e Qualidade, Gabinete de Relações Internacionais, entre outros. Nestes serviços, transversais ao funcionamento do IPCA, trabalham 52 funcionários em dedicação exclusiva.

6.1. Número e regime de dedicação do pessoal técnico, administrativo e de gestão afeto à lecionação do ciclo de estudos. Apresentação da estrutura e organização da equipa que colaborará com os docentes do ciclo de estudos. (EN)

In addition to its scientific-pedagogical organisation, EST has administrative services that provide the necessary support for its global operation. Currently, it has 1 Head of Division and 3 administrative employees, all on a full-time basis, who perform management tasks and support the operation of the School educational offer, in addition to other attributions (support in the organisation of various events, conferences, seminars, short courses and other training). Apart from these, all employees of the other services of IPCA support the operation of EST, including Academic and Social Services Division, Library, Information Systems Division, Administrative and Financial Division, Human Resources Division, Office for Evaluation and Quality, International Relations Office, among others,. In these services, work more 52 employees in full time.

6.2. Qualificação do pessoal técnico, administrativo e de gestão de apoio à lecionação do ciclo de estudos. (PT)

Dos 4 colaboradores dos Serviços Administrativos da Escola Superior de Tecnologia 2 possuem formação superior (licenciatura), nas áreas de Gestão Pública e Fiscalidade (e uma especialização em auditoria), e 2 colaboradores têm como habilitação o ensino secundário (12º ano). Relativamente aos restantes serviços, 46 funcionários possuem formação superior (incluindo mestres e um doutor) e os restantes o ensino secundário. O IPCA promove e apoia a formação contínua dos seus funcionários, criando condições para que possam progredir nos seus estudos e obter níveis mais elevados de qualificação.

6.2. Qualificação do pessoal técnico, administrativo e de gestão de apoio à lecionação do ciclo de estudos. (EN)

Of the 4 employees of the Administrative Services of the Escola Superior de Tecnologia, 2 have higher education(degree) in the areas of Public Management and Taxation (and a specialisation in auditing), and 2 employees have secondary education (high school diploma) as qualification. Regarding the remaining services, 46 employees have higher education (including masters and a PhD) and the remaining have secondary education. The IPCA promotes and supports the continuous training of its employees, providing conditions to progress in their studies and obtain higher levels of qualification.

6.3. Procedimento de avaliação do pessoal técnico, administrativo e de gestão e medidas conducentes à sua permanente atualização e desenvolvimento profissional. (PT)

Nos termos da lei, o pessoal não docente é avaliado de acordo com o SIADAP. O IPCA promove e apoia a formação contínua dos seus funcionários, criando condições para que possam progredir nos seus estudos e obter níveis mais elevados de qualificação.

6.3. Procedimento de avaliação do pessoal técnico, administrativo e de gestão e medidas conducentes à sua permanente atualização e desenvolvimento profissional. (EN)

Non-academic staff are assessed in accordance with SIADAP. IPCA promotes and supports the ongoing training of its employees, creating conditions for them to progress in their studies and achieve higher levels of qualification.

7. Instalações e equipamentos

7. 1. Instalações físicas afetas e/ou utilizadas pelo ciclo de estudos, se aplicável. (PT)

As instalações físicas da EST são recentes e modernas, com um conjunto de laboratórios e salas de aulas equipadas com diversos meios e recursos pedagógicos adequados e de suporte à realização de formação avançada ao nível de Mestrado.
Os laboratórios existentes abrangem um conjunto de domínios de conhecimento, a referir, o M-Factory Lab, o Laboratório Internet Of Things, o Laboratório Automação e Robótica, o Laboratório Redes, o Laboratório de Desenvolvimento de Jogos Digitais, o Laboratório de Eletrónica, o Laboratório de Ensaios e Caraterização e o Laboratório de Instrumentação Médica.Adicionalmente, existem 3 laboratórios associados ao centro de investigação da EST, designadoAppliedArtificialIntelligence(2Ai).
Além dos laboratórios que servem de espaços de utilização pedagógico, existem 7 salas de aulas, diversos gabinetes de docentes, 1 sala de computadores e 1 auditório. As salas de aulas estão equipadas com quadros interativos e videoprojectores.

7. 1. Instalações físicas afetas e/ou utilizadas pelo ciclo de estudos, se aplicável. (EN)

The physical facilities of the EST are recent and modern, with a set of laboratories and classrooms equipped with various material and teaching resources suitable for supporting the achievement of advanced training at the Master's level.
The existing laboratories cover a range of knowledge areas, namely the M-Factory Lab, the Internet of Things Lab, the Automation and Robotics Lab, the Networking Lab, the Digital Games Development Lab, the Electronics Lab, the Testing and Characterisation Lab and the Medical Instrumentation Lab. Additionally, there are 3 laboratories associated with the EST research center, named Applied Artificial Intelligence (2Ai).
Besides the laboratories that serve as teaching facilities, there are 7 classrooms, several teachers' offices, and 1 auditorium. The classrooms are equipped with smart boards and video projectors.

7. 2. Sistemas tecnológicos e recursos digitais de mediação afetos e/ou utilizados especificamente pelos estudantes do ciclo de estudos. (PT)

Para apoio à interação entre a instituição e os estudantes do ciclo de estudos, são disponibilizadas várias plataformas digitais:

1. Sistema de Gestão Académica (SIGES) para gestão pela instituição dos processos académicos como sendo:
- *a) definição de planos de estudo*
- *b) definição de calendário escolar e aulas/horários*
- *c) acesso a estatísticas*

2. Portal (netP@/SIGES) incluindo a gestão de processos e disponibilização de informação relativa a:
- *a) candidaturas*
- *b) inscrições (no ciclo de estudos e em exames)*
- *c) secretaria eletrónica (outras interações entre alunos e instituição)*
- *d) pagamentos de emolumentos*
- *e) comunicação de informação*
- *f) notas/pautas*
- *g) horários*

3. Learning Management System (Moodle) incluindo:
- *a) acesso a recursos pedagógicos*
- *b) assiduidade*
- *c) sistema de avaliação da qualidade do ensino*

4. Plataformas de produtividade digital incluindo:
- *a) Sistema de Email com listas de distribuição para difusão de informação mais geral*
- *b) Office 365 - Outlook, Word, Excel, PowerPoint, OneNote*
- *c) Microsoft 365 - OneDrive, SharePoint, Teams, Sway, Forms, Stream, Power Automate, e Power Apps*
- *d) Zoom (Colibri FCCN)*

5. Acesso Wifi à internet (eduroam)

6. Apoio técnico à utilização das plataformas e ao próprio equipamento informático dos alunos disponibilizado pela Divisão de Sistemas de Informação do IPCA

7. Sistemas de impressão disponibilizados aos alunos mediante carregamento de plafond

8. Plataforma SASocial para interação dos alunos com os Serviços de Ação Social do IPCA, incluindo serviços de:
- *a) alojamento em residências (em disponibilização)*
- *b) acesso a alojamento privado*
- *c) alimentação*
- *d) comunicação em circuito fechado de TVs instaladas nos campi*
- *e) acesso a serviço de bicicletas (U-Bike)*
- *f) gestão de bolsa de colaboradores*
- *g) marcações de atendimento presencial*
- *h) acesso a fundo de emergência*

7. 2. Sistemas tecnológicos e recursos digitais de mediação afetos e/ou utilizados especificamente pelos estudantes do ciclo de estudos. (EN)

To support the interaction between the institution and the students of the study cycle, several digital platforms are available:

1. Academic Management System (SIGES) for management by the institution of academic processes such as:
- *a) definition of study plans*
- *b) definition of school calendar and classes/timetables*
- *c) access to statistics*

2. Portal (netP@/SIGES) including the management of processes and availability of information regarding:
- *(a) applications*
- *b) registrations (in study cycle and examinations)*
- *c) e-secretariat (other interactions between students and institution)*
- *d) Emoluments payments*
- *e) Communication of information*
- *f) grades/logs*
- *g) timetable*

3. Learning Management System (Moodle) including:
- *(a) access to teaching resources*
- *b) attendance*
- *c) system for evaluating the quality of teaching*

4. Digital productivity platforms including:
- *(a) Email system with distribution lists for dissemination of more general information*
- *b) Office 365 - Outlook, Word, Excel, PowerPoint, OneNote*
- *c) Microsoft 365 - OneDrive, SharePoint, Teams, Sway, Forms, Stream, Power Automate, and Power Apps*
- *d) Zoom (Colibri FCCN)*

5. Wifi access to the internet (eduroam)

6. Technical support for the use of the platforms and the students' own computer equipment made available by the Information Systems Division of IPCA

7. Printing systems made available to the students by charging a plafond

8. SASocial platform for the interaction of the students with the Social Services of IPCA, including services of:
a) Accommodation in residences (in availability)
b) Access to private accommodation
c) food
d) closed circuit TV communication installed on the campi
e) access to bicycle service (U-Bike)
f) management of employees' stock exchanges
g) face-to-face service appointments
h) access to emergency fund

7. 3. Principais equipamentos e materiais afetos e/ou utilizados pelo ciclo de estudos. (PT)

Devido à sua transversalidade, o curso irá utilizar um conjunto diversos de equipamentos didáticos e pedagógicos existente em diversos laboratórios e nas salas de aula.
O Laboratório de Redes está equipado com material específico de comunicações de dados, para ensaiar a comunicação e a sua segurança entre dispositivos (fixos ou móveis) utilizando as mesmas tecnologias presentes na Internet. O Laboratório de Eletrónica possui bancadas de trabalho dotadas de equipamentos de suporte para a experimentação com redes de sensores e a segurança em sistemas embebidos. O Laboratório M-Factory Lab encontra- se equipado com equipamentos industriais de controlo numérico computorizado (acrómico em inglês CNC) de fresagem e torneamento. O Laboratório de Automação e Robótica tem um braço robótico, uma bancada de sistema pneumática e sistema modular de produção. Em termos de TIC's, ao nível físico, todos os espaços estão equipados com Internet e VOIP.

7. 3. Principais equipamentos e materiais afetos e/ou utilizados pelo ciclo de estudos. (EN)

Due to its transversality, the course will use a diverse set of didactic and pedagogical equipment existing in several laboratories and classrooms.
The Network Laboratory is equipped with specific data communications material, to test the communication and its security between devices (fixed or mobile) using the same technologies present in the Internet. The Electronics Lab has workbenches equipped with support equipment for experimentation with sensor networks and security in embedded systems. The M-Factory Lab is equipped with industrial computerised numerical control (CNC) milling and turning equipment. The Automation and Robotics Lab has a robotic arm, a pneumatic system bench and a modular production system. These previous labs will support the implementation of security in an Internet of Things (IOT) context.
In terms of ICT, at the physical level, all spaces are equipped with Internet and VOIP.

8. Atividades de investigação

8.1. Unidade(s) de investigação, no ramo de conhecimento ou especialidade do ciclo de estudos, em que os docentes desenvolvem a sua atividade científica.

Unidade de investigação	Classificação (FCT)	IES	Tipos de Unidade de Investigação	N.º de docentes do ciclo de estudos integrados
Centro de Investigação em Justiça e Governação (JusGov)	Muito Bom	Universidade do Minho (UM)		1
INESC TEC - INESC Tecnologia e Ciência (INESC TEC)	Muito Bom	Inesc Tec - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC)	Institucional	1
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)		4
Laboratório de Inteligência Artificial Aplicada (2Ai)	Muito Bom	Instituto Politécnico do Cávado e do Ave (IPCA)	Institucional	3

Unidade de investigação	Classificação (FCT)	IES	Tipos de Unidade de Investigação	N.º de docentes do ciclo de estudos integrados
Laboratório de Inteligência Artificial e Ciência de Computadores (UACC)	Excelente	Universidade do Porto (UP)		2
Laboratório de Inteligência Artificial e Ciência de Computadores (UACC)	Excelente	Universidade do Porto (UP)	Institucional	1

8.2. Lista dos principais projetos e/ou parcerias nacionais e internacionais (PT)

O IPCA integra a Universidade Europeia RUN-EU (Regional University Network), que envolve as seguintes instituições parceiras: Instituto Politécnico de Leiria, que coordena, Limerick Institute of Technology e Athlone Institute of Technology, agora unificadas na Technological University of the Shannon (Irlanda), Széchenyi István University (SZE) (Hungria), Häme University of Applied Sciences HAMK (Finlândia), NHL Stenden University of Applied Sciences (Holanda), e FH Vorarlberg University of Applied Sciences (Áustria). No âmbito desta parceria, está a ser desenvolvido em conjunto com os parceiros um Short Advanced Program (SAP) em Introdução à Cibersegurança, assim como um "joint degree program" de um mestrado em Cibersegurança, com base na Pós-graduação de Cibersegurança e Informática Forense do IPCA e no Master of Science in Computer Networks and Security da TUS Irlanda. Para além desta colaboração internacional, o IPCA também participa nos seguintes projetos de investigação na área da cibersegurança através do centro de investigação 2Ai: - Cybers SeC IP - Reforço de competências científicas e potencial de inovação em cibersegurança (NORTE-01-0145- FEDER-000044) – Projeto coordenado no 2AI pelo Professor Nuno Lopes, que irá assumir a responsabilidade desta proposta, em que o principal objetivo é reforçar as competências científicas e o potencial de inovação da região Norte, para enfrentar o desafio da cibersegurança, através do investimento num pequeno conjunto de tecnologias facilitadoras e de conhecimentos, num programa coerente organizado em duas linhas de investigação: uma relacionada com a conceção e proteção de sistemas digitais seguros, e uma segunda centrada na segurança e privacidade dos dados. - Sono ao Volante 2.0 - Sistema de informação para a previsão do sono ao volante e a deteção de distúrbio ou privação crónica do sono – o objetivo principal é o desenvolvimento de um primeiro protótipo de um sistema de informação integrado não intrusivo e de baixo-custo que permita a previsão do sono ao volante e a deteção de distúrbio ou privação crónica do sono. Este projeto tem uma componente crítica de cibersegurança que tem de ser implementada no sistema, considerando que manipula dados sensíveis e pessoais e que os transmite numa rede de dispositivos. Para além destes projetos, os docentes que compõem esta oferta formativa orientam regularmente dissertações de mestrado e estágios de licenciatura na área científica da Engenharia Informática, em concreto na área específica da cibersegurança, através de parcerias com empresas nacionais que operam nesta área. Por último, o IPCA irá assinar um protocolo de cooperação com o Centro Nacional de Cibersegurança (CNCS) para ser membro da C-Academy através do apoio à leccionação de cursos na área da cibersegurança. O docente responsável por este ciclo de estudos, Professor Nuno Lopes, será o responsável no IPCA por esta parceria.

8.2. Lista dos principais projetos e/ou parcerias nacionais e internacionais (EN)

IPCA is part of the European University RUN-EU (Regional University Network), which involves the following partner institutions: Instituto Politécnico de Leiria, which coordinates, Limerick Institute of Technology and Athlone Institute of Technology, now unified in the Technological University of the Shannon (Ireland), Széchenyi István University (SZE) (Hungary), Häme University of Applied Sciences HAMK (Finland), NHL Stenden University of Applied Sciences (Netherlands), and FH Vorarlberg University of Applied Sciences (Austria). Within the scope of this partnership, a Short Advanced Program (SAP) in Introduction to Cybersecurity is being developed together with the partners, as well as a joint degree program of a Master's degree in Cybersecurity, based on IPCA's Postgraduate Diploma in Cybersecurity and Computer Forensics and TUS Ireland's Master of Science in Computer Networks and Security. Besides this international collaboration, IPCA also participates in the following research projects in the area of cybersecurity through the research centre 2Ai: - Cybers SeC IP - Strengthening scientific skills and innovation potential in cybersecurity (NORTE-01-0145- FEDER-000044) - Project coordinated in 2AI by Professor Nuno Lopes, who will also take responsibility for this proposal, in which the main objective is to strengthen the scientific skills and innovation potential of the North region, to meet the challenge of cybersecurity, through investment in a small set of enabling technologies and knowledge, in a coherent programme organised into two lines of research: one related to the design and protection of secure digital systems, and a second focused on data security and privacy. - Sono ao Volante 2.0 - Information system for the prediction of sleep at the wheel and the detection of chronic sleep disorder or deprivation - the main goal is the development of a first prototype of an integrated non-intrusive and low-cost information system that allows the prediction of sleep at the wheel and the detection of chronic sleep disorder or deprivation. This project has a critical cybersecurity component that has to be implemented in the system, considering that it manipulates sensitive and personal data and transmits them in a network of devices. In addition to these projects, the teachers that make up this training offer regularly guide master's dissertations and undergraduate internships in the scientific area of Computer Engineering, specifically in the specific area of cybersecurity, through partnerships with national companies operating in this area. Finally, IPCA will sign a

cooperation agreement with the National Centre for Cybersecurity (CNCS) to become a member of the C-Academy by supporting the teaching of courses in the area of cybersecurity. The professor responsible for this study cycle, Professor Nuno Lopes, will be the responsible for the C-Academy in IPCA.

9. Política de proteção de dados

9.1. Política de proteção de dados (Regulamento (UE) n.º 679/2016, de 27 de abril transposto para a Lei n.º 58/2019, de 8 de agosto)

9.1 Protec?a?o Dados.pdf

10. Comparação com CE de referência

10.1. Exemplos de ciclos de estudos existentes em instituições de referência (PT)

Existem múltiplos cursos de mestrado na área da Cibersegurança. Entre outros referimos:
- Master of Science in Computer Networks and Security, Technological University of the Shannon, Ireland
- MSc Cybersecurity, Munster Technological University, Cork, Ireland
- MSc Cyber Security, Northumbria University, London UK
- MSc in Cyber Security, Swansea University, UK
- Master in Cybersecurity, University of Padova, Italy
- MSc Cyber Security and Data Governance, University of Law, Germany
- Master of Science in Artificial Intelligence & Cybersecurity, Università degli Studi di Udine, Italy
- Master in Cyber Security and Resilience, St. Pölten University of Applied Sciences, Austria

10.1. Exemplos de ciclos de estudos existentes em instituições de referência (EN)

There are multiple Master courses in the area of Cybersecurity. Among other, we identified the following:
- Master of Science in Computer Networks and Security, Technological University of the Shannon, Ireland
- MSc Cybersecurity, Munster Technological University, Cork, Ireland
- MSc Cyber Security, Northumbria University, London UK
- MSc in Cyber Security, Swansea University, UK
- Master in Cybersecurity, University of Padova, Italy
- MSc Cyber Security and Data Governance, University of Law, Germany
- Master of Science in Artificial Intelligence & Cybersecurity, Università degli Studi di Udine, Italy
- Master in Cyber Security and Resilience, St. Pölten University of Applied Sciences, Austria

10.2. Comparação com objetivos de aprendizagem de ciclos de estudos análogos (PT)

Todos os mestrados referidos anteriormente oferecem planos de estudos semelhantes ao que aqui é proposto para Cibersegurança. Isto demonstra a relevância técnica e científica desta proposta ao estar alinhada com outras ofertas educativas na mesma área científica. Uma das principais diferenças é a duração de 2 anos letivos, ou 1 ano completo a tempo inteiro, maioritariamente sem a possibilidade de estágio em empresas, por parte das propostas europeias.
Dos mestrados anteriores, esta proposta está muito alinhada quer em conteúdos quer em duração lectiva com o Master of Science in Computer Networks and Security, da TUS - Irlanda, que é oferecido por um parceiro do IPCA na rede RUN-EU. Este alinhamento permitirá a troca de docentes e alunos no futuro, através de protocolos de colaboração que estão a ser desenvolvidos.
Finalmente, esta proposta de Mestrado Profissionalizante tem uma forte vertente prática obtida através de um estágio ou projeto a ser desenvolvido em parceria com empresas.

10.2. Comparação com objetivos de aprendizagem de ciclos de estudos análogos (EN)

All the previously mentioned masters offer similar study plans to the one proposed here. This demonstrates the technical and scientific relevance of this proposal in being aligned with other educational offers in the same scientific area. One of the main differences is the duration of 2 academic years, or 1 full year full-time, mostly without the possibility of internship in companies, from the European proposals.
From the previous masters, this proposal is very aligned both in contents and in duration with the Master of Science in Computer Networks and Security, from TUS - Ireland, which is offered by an IPCA partner in the RUN-EU network. This alignment will allow the exchange of teachers and students in the future, through collaboration protocols which are being developed.
Finally, this Professional Master proposal has a strong practical aspect obtained through an internship or project to be developed in partnership with companies.

11. Estágios-Formação

11.1. e 11.2 Estágios e/ou Formação em Serviço

Mapa VI - Checkmarx

11.1.1. Entidade onde os estudantes completam a sua formação:

Checkmarx

11.1.2. Protocolo:

Protocolo IPCA Checkmarx_assinado.pdf

Mapa VI - Digiheart - Consultadoria e Serviços em Tecnologias de Informação Lda

11.1.1. Entidade onde os estudantes completam a sua formação:

Digiheart - Consultadoria e Serviços em Tecnologias de Informação Lda

11.1.2. Protocolo:

Digiheart - Protocolo Mestrado Ciberseguranc?a IPCA_signed.pdf

Mapa VI - Eurotux Informática SA

11.1.1. Entidade onde os estudantes completam a sua formação:

Eurotux Informática SA

11.1.2. Protocolo:

Eurotux Protocolo Mestrado Ciberseguranc?a IPCA.signed.pdf

Mapa VI - F3M

11.1.1. Entidade onde os estudantes completam a sua formação:

F3M

11.1.2. Protocolo:

F3M_assinado.pdf

Mapa VI - Squarenest

11.1.1. Entidade onde os estudantes completam a sua formação:

Squarenest

11.1.2. Protocolo:

SquareNest.pdf

Mapa VI - Squarenest - Engenharia de Sistemas de Informação e Multimédia Unip. Lda

11.1.1. Entidade onde os estudantes completam a sua formação:

Squarenest - Engenharia de Sistemas de Informação e Multimédia Unip. Lda

11.1.2. Protocolo:

SquareNest.pdf

Mapa VI - Trackdream Lda

11.1.1. Entidade onde os estudantes completam a sua formação:

Trackdream Lda

11.1.2. Protocolo:

Trackdream-size.pdf

Mapa VI - Trackdream, Lda

11.1.1. Entidade onde os estudantes completam a sua formação:

Trackdream, Lda

11.1.2. Protocolo:

Trackdream-size.pdf

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:

11.3.1_Reg_UC_Projecto_Mestrado_IPCA copy.pdf

11.3. Recursos institucionais

11.3. Recursos da instituição para o acompanhamento dos estudantes (PT):

Os estudantes do mestrado em Cibersegurança Aplicada poderão concluir o grau através da realização de um projeto de investigação aplicado para a resolução de um problema (que pode ser proposto por empresas externas) ou da realização de um estágio numa empresa. Caso o estudante opte pela via do estágio, a EST possui protocolos de cooperação com empresas nacionais e internacionais, de diversos setores (Checkmarx, Digiheart, Eurotux, F3M, Squarenest, Trackdream, Faurecia, Primavera BSS, Optimizer, entre outras). Toda a informação relativa à unidade curricular, bem como em concreto no que diz respeito ao acompanhamento efetivo dos estudantes pelos orientadores (da instituição e entidade de acolhimento), encontra-se disponível no 'Regulamento da UC Dissertação/Projeto/Estágio' publicado pelo Despacho n.o 8642/2020 de 8 de setembro de 2020 e anexado no ponto seguinte.

11.3. Recursos da instituição para o acompanhamento dos estudantes (EN):

The students of the master's degree in Applied Cybersecurity will be able to complete the degree through a research project applied to the resolution of a problem (which may be proposed by external companies) or an internship to be made within a company. If the student chooses the internship route, EST has cooperation protocols with national and international companies, from different sectors (Checkmarx, Digiheart, Eurotux, F3M, Squarenest, Trackdream, Primavera BSS, Faurecia, Optimizer, among others). All the information related to the course unit, as well as in particular with regard to the effective monitoring of students by supervisors (from host institution and organization), is available in the “Regulations of the UC Dissertation / Project / Internship” published by Order No. 8642/2020 of September 8, 2020 and annexed in the following section.

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:

11.4.1_Reg_UC_Projecto_Mestrado_IPCA.pdf

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

Nome	Instituição	Categoria	Habilitação Profissional	Nº de anos de serviço
Bruno rodrigues	Trackdream	Técnico de Cibersegurança	Licenciatura em Informática	4

Nome	Instituição	Categoria	Habilitação Profissional	Nº de anos de serviço
Fernando Gomes	Eurotux Informática SA	Director de Operações e Suporte	Licenciatura em Engenharia Informática	20
Manuel Pereira	F3M	Software Development Director	Licencicatura Engenharia Eletrónica e Informática	26
Nuno Oliveira	Checkmarx	Software Developer and Team Leader	Doutoramento em Informática	8
Nuno Ricardo Mateus Coelho	Squarenest	Gerente	Doutoramento em Informática	7
Nuno Ricardo Mateus Coleho	Squarenest	Gerente	Doutoramento Informática	8
Vítor Manuel Viana Manso	Digiheart - Consultadoria e Serviços em Tecnologias de Informação Lda	Sócio-gerente	Licenciatura em Informática	12

12. Análise SWOT

12.1. Pontos fortes. (PT)

- A EST/IPCA dispõe de um corpo docente qualificado, de carreira, com doutoramento, na área desta proposta de mestrado;
- Atividade científica dos docentes enquadrada no centro de investigação 2Ai com projetos na área da cibersegurança;
- Existência de empresas parceiras que já colaboram com a Licenciatura e Mestrado Engenharia Informática, que permitirá acolher propostas de estágio;
- Possui infra-estruturas de apoio ao estudo (Biblioteca), de apoio a melhoria contínua dos processos de ensino/aprendizagem (GAQ), de apoio à mobilidade internacional (GRI), de promoção da integração dos estudantes na vida Ativa (G3E);
- Existência da unidade curricular Projeto/Estágio, permitindo flexibilidade ao estudante escolher melhor abordagem para realizar um projeto em contexto empresarial;
- Disponibilização de regime pós-laboral dando oportunidade a alunos com forte motivação para continuar estudo ao longo da carreira profissional.

12.1. Pontos fortes. (EN)

- EST/IPCA has a qualified, dedicated faculty, with PhD, in the area of this master's proposal;
- Faculty scientific activity integrated in the research centre 2Ai with projects in the area of cybersecurity;
- Existence of partner companies that already collaborate with the Bachelor and Master in Computer Engineering, allowing the accommodation of internships;
- It has infrastructures to support the study (Library), to support the continuous improvement of the teaching/learning processes (GAQ), to support international mobility (GRI), and to promote the integration of students in Active Life (G3E);
- Existence of the curricular unit Project/Internship, allowing flexibility for the student to choose the best path to carry out a project in a business context;
- Availability of an after-working regime giving opportunity to students with strong motivation to continue studying along with their professional career.

12.2. Pontos fracos. (PT)

Como pontos fracos identificamos os seguintes:
- Reduzido nível de mobilidade internacional de pessoal docente e não docente;
- Reduzido nível de mobilidade internacional dos estudantes;
- Reduzido número de técnicos de apoio aos laboratórios.

12.2. Pontos fracos. (EN)

As weaknesses we identify the following:
- Low level of international mobility of teaching and non-teaching staff;
- Reduced level of international mobility of students;
- Reduced number of laboratory support technicians.

12.3. Oportunidades. (PT)

- Em conjunto com 7 IES de seis países europeus, o IPCA é membro fundador do consórcio Regional University Network – European University (RUN-EU), participação que permite dar um cariz europeu ao ciclo de estudos ora proposto quer através da co-orientação de projetos/dissertações por colegas da IES parceiras, quer pela via da mobilidade, de projetos de cooperação internacional de investigação e desenvolvimento, e por múltiplas titulações europeias.
- Inserção em região com desenvolvimento forte de empresas na área da informática;
- Ligação do IPCA a indústrias, empresas e associações empresariais;
- Na conjuntura atual existe uma grande procura de recursos humanos qualificados no setor da Cibersegurança;
- Necessidade de os profissionais que trabalhem na engenharia informática atualizarem os seus conhecimentos e melhorarem as suas qualificações para a segurança informática;

12.3. Oportunidades. (EN)

- Together with 7 HEI from six European countries, IPCA is a founding member of the consortium Regional University Network - European University (RUN-EU), participation that allows giving a European nature to the proposed study cycle either through the co-supervision of projects/dissertations by colleagues from partner HEI, or through mobility, international cooperation projects of research and development, and in the future, multiple European degrees.
- Strong demand for professionals in the area of Computer Engineering, specifically in the area of cybersecurity;
- Insertion in a region with strong development of companies in the area of Computer Science;
- Liaison between IPCA and industries, companies and business associations;
- Need for professionals working in computer engineering to update their knowledge and improve their skills in cybersecurity;

12.4. Constrangimentos. (PT)

Os principais constrangimentos são:
- Contração económica e conjuntura social desfavorável provocada pela atual situação de guerra na Europa;
- Oferta formativa congénere na região do norte do país, nomeadamente o curso de Mestrado em Cibersegurança do Instituto Politécnico de Viana do Castelo, com a duração de 2 anos. Esta proposta de mestrado profissionalizante do Instituto Politécnico do Cávado e do Ave difere na sua abordagem por ter uma duração inferior, permitindo uma rápida integração dos alunos no mercado de trabalho e mantendo essa mesma ligação durante o estudo do curso através do funcionamento em regime Pós-laboral e da UC de projeto ou estágio.

12.4. Constrangimentos. (EN)

The main threats are:
- Economic contraction and unfavourable social situation caused by the current war situation in Europe;
- Similar training offer in the northern region of the country, namely the Master's degree course in Cybersecurity at the Polytechnic Institute of Viana do Castelo, with the duration of 2 years. Our Professionalizing Master's proposal differs in its approach by having a shorter duration, allowing a quick integration of the students in the labour market and maintaining that same connection during the study of the course through the use of after working hours classes and providing a high ects credit curricular unit of Project or Internship.

12.5. Conclusões. (PT)

Considerando a presente análise SWOT do ciclo de estudos, os proponentes têm a convicção que estão reunidas as condições para o sucesso desta oferta formativa, ao nível de recursos humanos e materiais, no alinhamento com as necessidades das organizações (à escala regional, nacional e transnacional).
A instituição está comprometida, através da sua missão, com elevados padrões de qualidade, sustentabilidade, resposta rápida ao mercado e internacionalização. É no seio destes valores que a proposta de criação do Mestrado em Cibersegurança Aplicada é desenvolvida.
O corpo docente jovem, dinâmico e responsável, especializado nas áreas científicas do Mestrado está à altura deste desafio, bem como o pessoal não docente motivado e empenhado no sucesso deste projeto e da instituição.
Na elaboração desta proposta foram ouvidas as empresas com as quais a EST colabora, as que pertencem ao Conselho Consultivo da EST e as que acolhem estudantes da EST, em particular da Licenciatura em Engenharia de Sistemas Informáticos nas disciplinas de Projeto/Estágio, as quais se manifestaram interessadas e disponíveis para colaborar neste Mestrado.
O centro de investigação 2Ai (Applied Artificial Intelligence Laboratory), acreditado pela FCT em 2018 como Muito Bom, desenvolve investigação nas áreas científicas do mestrado e permite envolver estudantes em projetos de investigação aplicada já aprovados ou em fase de candidatura (os principais projetos do 2AI são elencados na secção 8 desta proposta).
A participação em redes internacionais, em particular as oportunidades da recentemente constituída rede RUN.EU, e os projetos de mobilidade ERASMUS+ dão à formação um cariz internacional que preparam o profissional para uma atuação no mercado global.
Simultaneamente a rede RUN.EU contribuirá para que as fragilidades identificadas ao nível da mobilidade sejam ultrapassadas.
Outra das debilidades da Instituição prende-se com a falta de pessoal de apoio aos laboratórios, que será ultrapassada em breve através de um procedimento concursal para recrutamento de um técnico.
Os constrangimentos relacionados com contração económica e restrições orçamentais são fruto da atual conjuntura nacional e internacional e comuns a grande parte das IES, e difíceis de ultrapassar.
Relativamente ao constrangimento referente à oferta formativa congénere na região, acreditamos poder ser

atenuado pelo caráter diferenciador da proposta deste Mestrado por ser uma oferta atual e alinhada com as expectativas das empresas, com uma duração inferior o que permite uma rápida integração dos estudantes no mercado de trabalho, e contando com a colaboração das empresas parceiras do IPCA no acolhimento de alunos para o desenvolvimento de projetos e estágios, conforme os protocolos de colaboração anteriormente apresentados.
Em suma, encontram-se reunidas as condições para a formação de profissionais capazes de dar resposta aos desafios de hoje.

12.5. Conclusões. (EN)

Considering the present SWOT analysis of the study cycle, the proponents are convinced that the conditions are met for the success of this Master, at the level of human and material resources, in alignment with the needs of organisations (on a regional, national and transnational scale).
The institution is committed, through its mission, to high standards of quality, sustainability, rapid market response and internationalisation. It is in the midst of these values that the proposal for the creation of the Master in Applied Cybersecurity is developed.
The young, dynamic and responsible faculty, specialised in the scientific areas of the Master's degree, is up to this challenge, as well as the non-teaching staff motivated and committed to the success of this project and the institution. In the development of this proposal, the companies, those which belong to EST's Advisory Board and those which host EST students, have been heard, and they have shown themselves to be interested and available to collaborate in this Master's program.
The research center 2Ai (Applied Artificial Intelligence Laboratory), accredited by FCT in 2018 as Very Good, develops research in the scientific areas of the Master's degree and allows to involve students in applied research projects already approved or in application phase (the main projects of 2AI are listed in section 8 of this proposal).
Participation in international networks, in particular the opportunities of the recently formed RUN.EU network, and ERASMUS+ mobility projects give the training an international character that prepares the professional to act in the global market. Simultaneously the RUN.EU network will contribute to overcome the weaknesses identified at the level of mobility.
Another weakness of the institution is the lack of support staff for the laboratories, which will soon be overcome through a procedure for the recruitment of a technician.
The constraints related to economic contraction and budget restrictions are the result of the current national and international situation and common to most institutions, and difficult to overcome.
Regarding the constraint related to the similar Masters in the region, we believe it can be mitigated by the differentiating with a shorter duration which allows a rapid integration of students into the labor market, and relying on the collaboration of IPCA partner companies in hosting students for the development of projects and internships.
In short, the conditions are met for the training of professionals able to meet the challenges of today and prepared to evolve and meet the challenges of tomorrow.