1. Caracterização

1.1. Instituição de Ensino Superior:

ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)

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 de Tecnologias Aplicadas, ISCTE - Sintra

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 e Resiliência

1.3. Designação do ciclo de estudos (EN):

Cybersecurity and Resiliency

1.4. Grau (PT):

Mestre

1.4. Grau (EN):

Master

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

480 - Informática

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

480 - Computer Science

1.6.1. Classificação CNAEF – primeira área fundamental

[0480] 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)

120.0

1.8. Duração do ciclo de estudos.

2 anos

1.8.1. Outra

[sem resposta]

1.9. Número máximo de admissões proposto

35.0

1.10. Condições específicas de ingresso. (PT)

Requisitos gerais definidos por lei:
- Titulares do grau de licenciado ou equivalente legal;
- Titulares de um grau académico superior estrangeiro conferido na sequência de um primeiro ciclo de estudo organizado segundo o processo de Bolonha;
- Titulares de um grau académico superior estrangeiro que seja reconhecido como satisfazendo os objetivos do grau de licenciado;
- Detentores de um curriculum escolar, científico ou profissional reconhecido como atestando capacidade para realização do mestrado.

Para serem elegíveis ao Mestrado, recomenda-se que os candidatos possuam formação na área das ciências informáticas. Na avaliação e seriação dos candidatos serão tidos em conta a formação académica e o desempenho curricular, bem como a experiência profissional.

1.10. Condições específicas de ingresso. (EN)

General requirements defined by law:
- Holders of an under-graduate degree or legal equivalent;
- Foreign under-graduate degree according to Bologna;
- Foreign college degree that meets the objectives of the under-graduate degree;
- Holders of academic, scientific or professional curriculum, attesting the ability to carry out the master's degree.

To be eligible for the Master's degree, it is recommended that candidates have a background in the field of computer science. In the evaluation and ranking of candidates, consideration will be given to their education, academic performance, as well as professional experience.

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)

Iscte-Sintra
Avenida Heliodoro Salgado nº 3, Sintra
2710-569 Sintra

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

Iscte – University Institute of Lisbon (Sintra)
Avenida Heliodoro Salgado nº 3, Sintra
2710-569 Sintra

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

RegulamentoCreditacoes_Iscte_emRevisao.pdf

1.14. Tipo de atribuição do grau ou diploma

[sem resposta]

1.15. Observações. (PT)

As organizações atuais dependem das tecnologias digitais para implementarem os seus processos de negócio e cumprirem com a sua missão. No entanto, existe atualmente uma enorme carência de profissionais com competências nesta área, no domínio da cibersegurança, que precisam de ser supridas através de formação adequada. De acordo com o estudo levado a cabo pela ISC^2 em 2022, sobre a "Global Cybersecurity Workforce Gap", existe uma carência global de mais de 3 milhões de profissionais, sendo que só na Europa, serão mais de 300 mil.
Esta proposta de mestrado em "Cibersegurança e Resiliência" visa contribuir para a resolução do problema identificado anteriormente. A mesma irá tirar proveito da experiência que o Iscte já possui em diversas áreas da cibersegurança (redes de comunicação, segurança da informação, gestão de risco, desenvolvimento de software, inteligência artificial, entre outras), mas igualmente procura uma integração mais estreita com organizações externas (empresas e outras) que atuam no mercado da cibersegurança e que podem contribuir com a sua experiência na formação dos estudantes.
O Iscte já oferece formação na área da cibersegurança a nível do 1.º ciclo, com a "Licenciatura em Tecnologias Digitais e Segurança de Informação", e este mestrado posiciona-se, em parte, como a continuidade natural dos estudantes que pretendam aprofundar os seus conhecimentos na área da cibersegurança e da resiliência. De igual forma, e devido à natureza eclética da cibersegurança, este mestrado pode ser uma excelente opção para estudantes que possuam alguma forma de formação técnica na área das ciências informáticas e dos sistemas de informação e que pretendam aprender ou aprofundar temas de cibersegurança e resiliência.
Nos últimos tempos, o Iscte tem vindo a apostar fortemente na área da cibersegurança, com a criação de uma Academia de Segurança e Redes, assim como na colaboração com projectos com a C-Academy do CNCS (Centro Nacional de Cibersegurança). De igual forma, através do seu centro de investigação ISTAR_Iscte, está envolvido em alguns projetos de investigação nesta área. Por isto, é estratégico para uma instituição de ensino superior como o Iscte possuir uma oferta formativa de segundo ciclo nesta área.
O curso funcionará num formato híbrido de ensino, o que constitui outro facto diferenciador. Cerca metade dos ECTS correspondem a unidades curriculares disponibilizadas na modalidade de ensino à distância, resultando numa significativa flexibilidade na gestão dos estudos, considerando que o público-alvo é constituído por um número expressivo de trabalhadores-estudantes e/ou estudantes que residem noutras regiões ou países.
Este mestrado aposta na diferenciação da oferta que existe a nível nacional e até mesmo internacional, procurando oferecer um produto que pode contribuir para a formação de profissionais especializados em cibersegurança, e que depois possam especializar-se um pouco mais durante o trabalho de dissertação de mestrado.

1.15. Observações. (EN)

Today's organizations depend on digital technologies to implement their business processes and fulfill their mission. However, there is currently a huge shortage of professionals with skills in this area, which needs to be filled through proper training, which poses a significant challenge for organizations today. According to the study conducted by ISC^2 in 2022 on the "Global Cybersecurity Workforce Gap", there is a worldwide deficit of over 3 million professionals, with Europe facing a shortage of more than 300,000 cybersecurity experts.
This master's degree proposal in "Cybersecurity and Resilience" aims to contribute to solving the problem identified above. It will take advantage of the experience that Iscte already has in several areas of cybersecurity (communication networks, information security, risk management, software development, artificial intelligence, among others), but also seeks closer integration with external organizations (companies and others) that operate in the cybersecurity market and can contribute with their experience in the training of students.
Similarly, Iscte already offers training in the area of cybersecurity at the first cycle level, with the "Degree in Digital Technologies and Information Security", and this master's degree will be, in part, the natural continuity for students who wish to deepen their knowledge in the area of cybersecurity and resilience. Similarly, and due to the eclectic nature of cybersecurity, this master's degree may be an excellent option for students coming from other educational areas, such as computer science or information systems, and wishing to learn or develop a deeper understanding of cybersecurity topics.
In recent times, Iscte has been investing heavily in the area of cybersecurity, with the creation of a Security and Network Academy, as well as collaborating on projects with the C-Academy of the CNCS (National Cybersecurity Centre). Likewise, through its ISTAR_Iscte research centre, it is involved in a number of research projects in this area. It is therefore strategic for a higher education institution like Iscte to have a second cycle training programme in this area.
The course will operate in a hybrid teaching format, which is another differentiating fact. About half of the ECTS correspond to course units provided in distance learning modality, resulting in a significant flexibility in the management of studies, considering that the target audience is composed of a significant number of working-students and/or students residing in other regions or countries.
This master's degree aims at differentiating the offer that exists at a national and even international level, seeking to offer a product that may contribute to the training of professionals specialized in cybersecurity, and that may

then specialize a little more during the master's dissertation work.

2. Formalização do Pedido

Mapa I - 1 - Reitora do Iscte / 1 - Rector of Iscte

Órgão ouvido:

1 - Reitora do Iscte / 1 - Rector of Iscte

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

DESPACHO Nº 54_2023 - Criação mestrado Cibersegurança e Resiliência.pdf | PDF | 71.9 Kb

Mapa I - 2 - Conselho Científico do Iscte / 2 - Scientific Council of Iscte

Órgão ouvido:

2 - Conselho Científico do Iscte / 2 - Scientific Council of Iscte

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

DeliberacaoCC_MestCiberseguranca Resiliencia.pdf | PDF | 292.2 Kb

Mapa I - 3 - Conselho Pedagógico do Iscte / 3 - Pedagogical Council of Iscte

Órgão ouvido:

3 - Conselho Pedagógico do Iscte / 3 - Pedagogical Council of Iscte

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

ParecerCP_MestCiberseguranca Resiliencia.pdf | PDF | 307.5 Kb

Mapa I - 4 - Comissão Científica do Iscte-Sintra / 4 - Scientific Committee of Iscte-Sintra

Órgão ouvido:

4 - Comissão Científica do Iscte-Sintra / 4 - Scientific Committee of Iscte-Sintra

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

ParecerEscola_Criacao_MestCiberseguranca Resiliencia.pdf | PDF | 276 Kb

3. Âmbito e Objetivos

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

O mestrado em "Cibersegurança e Resiliência" oferece aos estudantes formação interdisciplinar relacionada com os principais pilares da cibersegurança – pessoas, processos e tecnologias, e irá incluir valências de múltiplas áreas e estabelecer uma relação com profissionais para oferecer uma formação abrangente aos estudantes. Os principais objetivos deste mestrado são: permitir que os estudantes possam ajudar as organizações no planeamento e implementação de soluções com o objetivo de maximizar a sua resiliência face a ciber-ameaças, fomentar e promover a inovação através do desenvolvimento de produtos e serviços inovadores na área da cibersegurança e, finalmente, gerar e garantir os recursos necessários para endereçar as necessidades das organizações em termos de cibersegurança. O mestrado está estruturado para oferecer uma cobertura global às principais funções de cibersegurança e resiliência como: PREPARAÇÃO/IDENTIFICAÇÃO, PROTEÇÃO, DETEÇÃO, RESPOSTA e RECUPERAÇÃO.

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

The Master in "Cybersecurity and Resilience" offers students interdisciplinary training in aspects related to the main pillars of cybersecurity - people, processes and technologies. In this perspective, this master will include expertise from multiple areas and establish a strong relationship with professionals to offer comprehensive training to different students. The main objectives of this master are to enable students to help organizations in the planning and implementation of solutions to maximize their resilience to cyber threats, to foster and promote innovation

through the development of innovative products and services in the area of cybersecurity, and finally to generate and secure the necessary resources to address the cybersecurity needs of organizations. The master is structured to offer comprehensive coverage of the main cybersecurity and resilience functions as: PREPARATION/IDENTIFICATION, PROTECTION, DETECTION, RESPONSE, and RECOVERY.

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

No final do curso, os estudantes estarão capacitados para:
- Identificar os principais desafios de cibersegurança e resiliência enfrentados pelas organizações numa perspetiva holística (pessoas, processos e tecnologia);
- Conhecer as principais recomendações, normas, e legislação em termos de cibersegurança e resiliência para garantir a conformidade das organizações
- Desenvolver estratégias e programas de cibersegurança e resiliência para as organizações
- Desenvolver práticas de implementação de segurança e proteção de dados, informação e sistemas, resiliência organizacional e tecnológica, e ações de educação e sensibilização
- Conhecer e explorar o cruzamento de diferentes áreas com o tema da cibersegurança, nomeadamente a área da inteligência artificial, assim como da gestão e estratégia, ou da psicologia e comportamento organizacional
- Oferecer suporte nas funções de cibersegurança organizacional: PREPARAÇÃO/IDENTIFICAÇÃO, PROTEÇÃO, DETEÇÃO, RESPOSTA e RECUPERAÇÃO

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

At the end of the course, students will be able to:
- Identify the main cybersecurity and resilience challenges faced by organizations from a holistic perspective (people, process and technology);
- Know the main recommendations, standards, and legislation in terms of cybersecurity and resilience to ensure organizational compliance;
- Develop cybersecurity and resilience strategies and programs for organizations
- Implement practices for data, information, and system security and protection, organizational and technological resilience, and education and awareness initiatives.
- Explore the intersection of cybersecurity with different areas, such as artificial intelligence, management and strategy, as well as psychology and organizational behavior.
- To offer support in the organizational cybersecurity functions: PREPARATION/IDENTIFICATION, PROTECTION, DETECTION, RESPONSE and RECOVERY.

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)

O Mestrado em Cibersegurança e Resiliência num formato híbrido (50% ensino presencial e 50% ensino à distância) apresenta-se como um fator diferenciador do curso no panorama nacional e internacional, preparando os futuros profissionais deste mestrado com as competências necessárias para ajudar as organizações a lidar com os desafios de cibersegurança e resiliência que têm de enfrentar. As UC que não exigem práticas laboratoriais nem formações práticas com presença física obrigatória são adequadas para o formato de ensino à distância, conforme estabelecido no Decreto-Lei 133/2019, permitindo maior flexibilidade no processo de ensino-aprendizagem dos estudantes e conciliação com atividades profissionais e pessoais. As restantes UC beneficiarão do ensino em formato presencial, onde os estudantes terão oportunidade de desenvolver atividades presenciais em colaboração com outras entidades e profissionais que colaboram com o mestrado.

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)

The Master in Cybersecurity and Resilience in a hybrid format (50% face-to-face teaching and 50% distance learning) presents itself as a differentiating factor of the course in the national and international panorama, preparing future professionals of this Master with the necessary skills to help organizations deal with the cybersecurity and resilience challenges they have to face. The CUs that do not require laboratory practice or practical training with mandatory physical presence are suitable for distance learning format, as established in Decree-Law 133/2019, allowing greater flexibility in the teaching-learning process of students and conciliation with professional and personal activities. The remaining CU will benefit from teaching in face-to-face format, where students will have the opportunity to develop face-to-face activities in collaboration with other entities and professionals who collaborate with the master.

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 contributo que o Iscte pode dar à sociedade consiste em desenvolver, com elevados padrões de qualidade, a sua missão nestes três domínios: o ensino, em especial nos níveis pós-graduados, a investigação científica e a transferência de conhecimento para a sociedade.
A missão do Iscte está definida com clareza no artigo 2.º dos Estatutos da Fundação Iscte – Instituto Universitário de Lisboa (Anexo ao Decreto-Lei n.º 95/2009 de 27 de abril), Artigo 2.º:
- O Iscte promove a criação, transmissão e difusão de conhecimento científico e tecnológico nos seus domínios de especialização;
- O Iscte atribui especial relevo à investigação científica, à formação pós-graduada e à transferência de

conhecimentos para a sociedade;
- No cumprimento da sua missão, o Iscte promove a internacionalização das suas atividades.
O Plano Estratégico e de Ação do Iscte para o Quadriénio 2022-2025 inclui o desenvolvimento do ensino à distância como um dos seus objetivos centrais, como meio de ampliar a oferta de ensino e chegar a outros públicos e a outros quadrantes geográficos, nacionais e internacionais.
O Iscte possui competências científicas na área da cibersegurança, como demonstrado pela licenciatura em Tecnologias e Segurança (acreditada pela A3ES e em funcionamento desde 2022), pela criação de uma Academia de Segurança e Redes, assim como na colaboração com projetos com a C-Academy do CNCS (Centro Nacional de Cibersegurança).
Em suma, a inclusão do ciclo de estudos na estratégia institucional de oferta formativa do Iscte é plenamente justificada pela sua missão, pelo seu projeto educativo, científico e cultural, bem como pela sua capacidade de resposta aos desafios contemporâneos no campo do ensino, investigação e inovação.

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)

The contribution that Iscte can make to society consists of developing, with high standards of quality, its mission in these three areas: teaching, especially at postgraduate levels, scientific research and the transfer of knowledge to society.
Iscte's mission is clearly defined in Article 2 of the Statutes of the Iscte Foundation - University Institute of Lisbon (Annex to Decree Law No. 95/2009 of April 27), Article 2:
- Iscte promotes the creation, transmission and dissemination of scientific and technological knowledge in its fields of specialization;
- Iscte attaches particular importance to scientific research, postgraduate training and the transfer of knowledge to society;
- In fulfilling its mission, Iscte promotes the internationalization of its activities.
The Strategic and Action Plan of Iscte for the 4-year period 2022-2025 includes the development of distance education as one of its central objectives, as a means of expanding the teaching offer and reaching other audiences and other geographical, national and international quadrants.
Iscte has scientific competences in the area of cybersecurity, as demonstrated by the degree in Technologies and Security (accredited by A3ES and in operation since 2022), by the creation of a Security and Networking Academy, as well as in the collaboration with projects with the C-Academy of CNCS (National Center for Cybersecurity).
In conclusion, the inclusion of the study cycle in ISCTE's institutional training strategy is fully justified by its mission, its educational, scientific and cultural project, as well as its ability to respond to contemporary challenges in the field of teaching, research and innovation.

4. Desenvolvimento curricular

4.1. Estrutura Curricular

Mapa II - Plano de Estudos

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):
Plano de Estudos

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):
Study Plan

4.1.2. Áreas científicas e créditos necessários à obtenção do grau

Área Científica	Sigla	ECTS	ECTS Minímos
310 - Ciências sociais e do comportamento	310	6.0	0.0
480 - Informática	480	60.0	42.0
Não específicada	n.e.	0.0	12.0
Total: 3		Total: 66.0	Total: 54.0

4.1.3. Observações (PT)
[sem resposta]

4.1.3. Observações (EN)
[sem resposta]

4.2. Unidades Curriculares

Mapa III - Arquiteturas de Segurança e Modelos de Confiança Zero

4.2.1. Designação da unidade curricular (PT):
Arquiteturas de Segurança e Modelos de Confiança Zero

4.2.1. Designação da unidade curricular (EN):
Security Architectures and Zero-Trust Models

4.2.2. Sigla da área científica em que se insere (PT):
480

4.2.2. Sigla da área científica em que se insere (EN):
480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• João Carlos Amaro Ferreira - 24.0h

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):
OA1: Compreender o conceito de arquitecturas de segurança e o seu papel na cibersegurança e resiliência modernas.
OA2: Avaliar os modelos de segurança tradicionais e identificar os seus pontos fortes, fracos e limitações.
OA3: Explicar os princípios e componentes da arquitetura de Confiança Zero e a sua aplicação à cibersegurança e à resiliência.
OA4: Aprender os princípios de conceção e implementação de arquitecturas de Confiança Zero.
OA5: Aprender a aplicar os princípios de Confiança Zero à segurança na nuvem, segurança de equipamentos terminais, gestão de identidade e acesso e segurança de dados.
OA6: Compreender como desenvolver estratégias para implementar técnicas de resposta a incidentes de Confiança Zero.

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

LO1: Understand the concept of security architectures and their role in modern cybersecurity and resilience.
LO2: Evaluate traditional security models and identify their strengths, weaknesses, and limitations.
LO3: Explain the principles and components of Zero Trust architecture and its application in cybersecurity and resilience.
LO4: Learn the principles of designing and implementing Zero Trust architectures.
LO5: Learn to apply Zero Trust principles to cloud security, endpoint security, identity and access management and data security.
LO6: Understand how to develop strategies for implementing Zero Trust incident response techniques.

4.2.11. Conteúdos programáticos (PT):

CP1: Introdução às Arquitecturas de Segurança
CP2: Modelos Tradicionais de Segurança
CP3: Princípios de Confiança Zero
CP4: Implementação de Modelos de Confiança Zero
CP5: Confiança Zero e Segurança na Nuvem
CP6: Confiança Zero e Segurança de Endpoint
CP7: Confiança Zero e Gestão de Identidade e Acesso (IAM)
CP8: Confiança Zero e Segurança de Dados
CP9: Confiança Zero e Resposta a Incidentes
CP10: Desafios da implementação da Confiança Zero e tendências futuras

4.2.11. Conteúdos programáticos (EN):

PC1: Introduction to Security Architectures
PC2: Traditional Security Models
PC3: Zero Trust Principles
PC4: Implementing Zero Trust Models
PC5: Zero Trust and Cloud Security
PC6: Zero Trust and Endpoint Security
PC7: Zero Trust and Identity and Access Management (IAM)
PC8: Zero Trust and Data Security
PC9: Zero Trust and Incident Response
PC10: Zero Trust Implementation Challenges and Future Trends

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Arquiteturas de Segurança e Modelos de Confiança Zero adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The Security Architectures and Zero Trust Models CU will adopt as core teaching and learning methodology Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de dois testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, a contar com 30% para a nota final.
Realização de um conjunto de atividades individuais e colaborativas propostas ao longo do semestre, a contar com 30% para a nota final.
Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 40%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of two assessment tests throughout the semester, each with a minimum score of 8 points, counting 30% towards the final grade. Completion of a set of individual and collaborative activities proposed throughout the semester, counting 30% towards the final grade. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 40%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá conhecer os principaus modelos de segurança e confiança, assim como as suas limitações. Irão igualmente ter conhecimento sobre formas de garantir a ciber-resiliência das organizações através de modelos de Confiança Zero. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar tarefas, laboratórios e projetos específicos relacionados com os diferentes temas que serão abordados na unidade curricular.
No caso dos projetos os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes perceber e avaliar o desenho e aplicações de modelos de Confiança Zero, como forma de contribuir para a cibersegurança e ciber-resiliência das organizações. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected in order to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the CU that will allow them to know the main models of security and trust, as well as their limitations. They will also learn about ways to ensure the cyber resilience of organisations through Zero Trust models. The lecturer will give feedback (corrective and/or cognitive) on the tasks carried out by the students. Students will also carry out specific tasks, laboratories and projects related to the different topics that will be addressed in the curricular unit.
In the case of projects, students will have access to all the details of the work to be carried out, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to understand and evaluate the design and applications of Zero Trust models, as a way to contribute to the cybersecurity and cyber-resilience of organisations. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their involvement throughout the CU.

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

Das, R. (2023). The Zero Trust Framework (1st edition). CRC Press.
Finney, G., & Kindervag, J. (2022). Project Zero Trust: A Story about a Strategy for Aligning Security and the Business (1st edition). Wiley.
Green-Ortiz, C., Fowler, B., Houck, D., Hensel, H., Lloyd, P., McDonald, A., & Frazier, J. (2023). Zero Trust Architecture (1st edition). Cisco Press.
King, C., Osmanoglu, E., & Dalton, C. (2001). Security Architecture: Design, Deployment and Operations (First Edition). McGraw-Hill Osborne Media.
Moyle, E., & Kelley, D. (2020). Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects. Packt Publishing.
Sherwood, N. (2021). Enterprise Security Architecture: A Business-Driven Approach (1st edition). CRC Press.

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

Das, R. (2023). The Zero Trust Framework (1st edition). CRC Press.
Finney, G., & Kindervag, J. (2022). Project Zero Trust: A Story about a Strategy for Aligning Security and the Business (1st edition). Wiley.
Green-Ortiz, C., Fowler, B., Houck, D., Hensel, H., Lloyd, P., McDonald, A., & Frazier, J. (2023). Zero Trust Architecture (1st edition). Cisco Press.
King, C., Osmanoglu, E., & Dalton, C. (2001). Security Architecture: Design, Deployment and Operations (First Edition). McGraw-Hill Osborne Media.
Moyle, E., & Kelley, D. (2020). Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects. Packt Publishing.
Sherwood, N. (2021). Enterprise Security Architecture: A Business-Driven Approach (1st edition). CRC Press.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Criptografia para Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Criptografia para Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Cryptography for Cybersecurity and Resilience

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

480

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

480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:

92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Maria do Rosário Domingos Laureano - 24.0h

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):
OA1: Identificar os principais mecanismos, algoritmos e protocolos criptográficos atuais.
OA2: Compreender o papel da criptografia na cibersegurança e resiliência de dados, informação e sistemas.
OA3: Determinar as principais ameaças e ataques à criptografia e aprender a mitigar os mesmos. Desenvolver as soluções baseadas em mecanismos e protocolos criptográficos.
OA4: Identificar problemas de cibersegurança e resiliência e aplicar criptografia na solução dos mesmos.
OA5: Compreender os desafios futuros da criptografia e o impacto dos mesmos na cibersegurança e resiliência. Desenvolver as soluções.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Identify the main current cryptographic mechanisms, algorithms and protocols.
LO2: Understand the role of cryptography in cybersecurity and resilience of data, information and systems.
LO3: Determine the main threats and attacks to cryptography and learn how to mitigate them. Develop solutions based on cryptographic mechanisms and protocols.
LO4: Identify cybersecurity and resilience problems and apply cryptography to solve them.
LO5: Understand the future challenges of cryptography and their impact on cybersecurity and resilience. Develop the solutions.

4.2.11. Conteúdos programáticos (PT):
CP1: Introdução e Fundamentos da Criptografia Moderna
CP2: Mecanismos e Algoritmos de Criptografia Simétrica
CP3: Mecanismos e Algoritmos de Criptografia Assimétrica
CP4: Aplicações e Protocolos Criptográficos
CP5: Vulnerabilidades da Criptografia e Contramedidas
CP6: Tópicos avançados de Criptografia
CP7: Aplicações da Criptografia para a Ciber-resiliência
CP8: Casos de Estudo e Aplicações Práticas

4.2.11. Conteúdos programáticos (EN):
PC1: Introduction and Fundamentals of Modern Cryptography
PC2: Mechanisms and Algorithms of Symmetric Cryptography
PC3: Mechanisms and Algorithms of Asymmetric Cryptography
PC4: Cryptographic Applications and Protocols
PC5: Cryptographic Vulnerabilities and Countermeasures
PC6: Advanced Cryptography Topics
PC7: Applications of Cryptography for Cyber Resilience
PC8: Case Studies and Practical Applications

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC Criptografia Aplicada para a Cibersegurança e Resiliência adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The CU of Applied Cryptography for Cybersecurity and Resilience will adopt as core teaching and learning methodology Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de 2 mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, cada um deles a contar com 15% para a nota final. Realização de 4 laboratórios em grupo, cada um deles a contar com 10% para a nota final. Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 30%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of 2 mini-assessment tests throughout the semester, each with a minimum score of 8, each counting 15% towards the final grade. Completion of 4 laboratories, each of which will count for 10% of the final grade. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 30%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, numa primeira fase compreender os princípios e conceitos da criptografia e posteriormente, analisar as suas implicações na segurança e resiliência de dados, informação e sistemas. Irão ainda aplicar conhecimentos teóricos e desenvolver competências de análise e pensamento crítico, necessários à identificação dos principais desafios e oportunidades da criptografia. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar projetos específicos e realizar laboratórios relacionados com os diferentes temas que serão abordados na unidade curricular. No caso dos projetos os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes avaliar a aplicação da criptografia como uma ferramenta que pode ajudar a resolver problemas cibersegurança e ciber-resiliência. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the CU that will allow them, in a first phase, to understand the principles and concepts of cryptography and later, to analyse its implications for the security and resilience of data, information and systems. They will also apply theoretical knowledge and develop analytical and critical thinking skills, necessary to identify the main challenges and opportunities of cryptography. The teacher will provide feedback (corrective and/or cognitive) on the tasks carried out by the students. Students will also carry out specific projects and perform laboratories related to the different topics that will be addressed in the curricular unit. In the case of projects, students will have access to all the details of the work to be carried out, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to evaluate the application of cryptography as a tool that can help solve cybersecurity and cyber-resilience problems. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Stinson D. R., Paterson M. (2019). Cryptography: Theory and Practice. Chapman and Hall/CRC. ISBN: 978-1138197015.
Stallings W. (2022). Cryptography and Network Security - Principles and Practice. Pearson. ISBN: 978-0-13-670722-6.
Bertaccini M. (2022). Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption. Packt Publishing. ISBN: 978-1789617139
Aumasson J. (2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press. ISBN: 978-1593278267.
Tilborg H., Jajodia S. (2011). Encyclopedia of Cryptography and Security. Springer. ISBN: 978-1441959058.
Paar C., Pelzl J., Preneel B. (2014). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. ISBN: 978-3642446498.

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

Stinson D. R., Paterson M. (2019). Cryptography: Theory and Practice. Chapman and Hall/CRC. ISBN: 978-1138197015.
Stallings W. (2022). Cryptography and Network Security - Principles and Practice. Pearson. ISBN: 978-0-13-670722-6.
Bertaccini M. (2022). Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption. Packt Publishing. ISBN: 978-1789617139
Aumasson J. (2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press. ISBN: 978-1593278267.
Tilborg H., Jajodia S. (2011). Encyclopedia of Cryptography and Security. Springer. ISBN: 978-1441959058.
Paar C., Pelzl J., Preneel B. (2014). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. ISBN: 978-3642446498.

4.2.17. Observações (PT):

--

4.2.17. Observações (EN):

--

Mapa III - Dissertação em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Dissertação em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Master Dissertation in Cybersecurity and Resiliency

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

480

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

480

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

Anual

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

4.2.4. Horas de trabalho (número total de horas de trabalho):
1,050.0

4.2.5. Horas de contacto:
Presencial (P) - S-32.0; OT-8.0
Assíncrona a distância (AD) - S-8.0
Síncrona a distância (SD) - S-8.0

4.2.6. % Horas de contacto a distância:
28.57%

4.2.7. Créditos ECTS:
42.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Carlos José Corredoura Serrão - 56.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
• Carlos Eduardo Dias Coutinho - 8.0h
• João Carlos Amaro Ferreira - 8.0h
• João Pedro Calado Barradas Branco Pavia - 8.0h
• Margarida Tavares Peralta Couto dos Santos - 8.0h
• Maria do Rosário Domingos Laureano - 8.0h

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
OA1: Adquirir a capacidade de efetuar investigação de forma independente.
OA2: Saber elaborar uma revisão da literatura relevante numa determinada área científica
OA3: Selecionar uma ou mais abordagens metodológicas para a concretização do projeto
OA4: Saber validar os artefactos que constituem a solução para o problema escolhido e identificar as correspondentes ameaças à validade.
OA5: Ter aprendido sobre a complexidade e o modo de preparar uma dissertação de mestrado bem sucedida e de elevada qualidade, tanto na forma como no conteúdo.
OA6: Ser capaz de apresentar um problema técnico-científico e a sua motivação, para produzir soluções adequadas e validadas.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Acquire the capacity to undertake research independently.
LO2: Know how to develop a review based on relevant literature in a given-scientific field
LO3: Select one or more methodological approaches to achieve the project
LO4: Know how to validate the artifacts that constitute the solution to the chosen problem and identify the corresponding validity threats.
LO5: Have learned about the complexity and how to prepare a successful master dissertation with high quality, both in form and content.
LO6: To be able to present a technical-scientific problem and its motivation, to produce appropriate and validated solutions.

4.2.11. Conteúdos programáticos (PT):
O programa de trabalho parte de um tema suscitado pelo interesse intelectual do aluno, tema esse que será abordado de acordo com um programa de trabalho personalizado a acordar com os possíveis orientadores. Não obstante, o trabalho a realizar deve materializar-se num documento com:
1. A formulação de uma questão ou de um problema, teoricamente suscetível de ter uma resposta adequada através da mobilização de metodologia de investigação científica.
2. Uma revisão das questões teóricas subjacentes à questão acima enunciada, obtida através da pesquisa, análise e interpretação crítica da mais recente literatura científica internacionalmente aceite.
3. Em articulação com o balanço teórico anterior, a dissertação deve conter um exercício (teórico e/ou empírico) que complemente uma forma inovadora de abordar o tema em investigação.
4. Por fim, a dissertação deve conter uma síntese conclusiva que responda ao ponto de partida da investigação, bem como sugestões para investigação futura

4.2.11. Conteúdos programáticos (EN):

The work program starts from a topic raised by the student's intellectual interest, a topic that will be addressed according to a customized program of work to be agreed with the possible supervisors. Notwithstanding this, the work to be done must materialize in a document with:
1. The formulation of a question or a problem, theoretically capable of having an appropriate response through the mobilization of scientific research methodology.
2. A review of the theoretical issues underlying the question above, obtained through research, analysis and critical interpretation of the latest internationally accepted scientific literature.
3. In coordination with the earlier theoretical balance, the dissertation must contain an exercise (theoretical and / or empirical) that complements an innovative way to approach the topic under investigation.
4. Finally, the dissertation must contain a conclusive synthesis answering the research starting point, as well as suggestions for further rese

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

Nesta UC os conteúdos programáticos decorrem da natureza e exigência da própria dissertação, nos moldes em que uma definição legal e uma boa prática académica entendem uma dissertação.
O principal objetivo da UC é permitir aos alunos a aquisição de competências de investigação. Estas competências devem ser materializadas na elaboração de uma dissertação. Naturalmente que existe uma total convergência entre os conteúdos programáticos e os objectivos da UC.
Com efeito, todos os tópicos dos conteúdos programáticos estão subordinados à utilidade que têm como instrumentos para viabilizar os objectivos da UC.
O programa de trabalhos do aluno é especificamente concebido para lhe permitir uma agenda de investigação com sucesso, que se consubstancia numa dissertação ou projeto.

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

In this CU the syllabus stems from the nature and requirement of which is itself a dissertation, in a way that a legal definition and a good academic practice understand a dissertation.
The main CU objective is enabling the students to acquire research skills. These skills must be materialized in the preparation of a dissertation. Naturally there is a complete convergence between syllabus content and objectives of the CU.
Indeed, all syllabus topics are subordinated to the utility that they have as tools to enable the objectives of the CU.
The student's work program is specifically designed to allow him a successfully research agenda, that is embodied in a dissertation or project.

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

O processo de aprendizagem envolve quatro dimensões complementares:
1. Sessões de seminários simplificadas pelo professor.
2. Sessões de tutoria individual com o supervisor.
3. Sessões de trabalho individual, em que os alunos procedem à pesquisa bibliográfica e à sua leitura crítica. Ou em que escrevem o texto que evidencia a metodologia e os conhecimentos retidos.
4. Sessões de seminários em que os alunos submetem ao escrutínio o trabalho já realizado e o discutem coletivamente.

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

The learning process involves four complementary dimensions:
1. Streamlined seminar sessions by the teacher.
2. Sessions of individual tutorials with the supervisor.
3. Individual working sessions, in which the students proceed the literature search and it critical reading. Or in which they written the text that show the methodology and the knowledge retained.
4. Seminars sessions in which students submit to the scrutiny work already done and collectively discuss it.

4.2.14. Avaliação (PT):

A avaliação do processo da UC será efectuada através da discussão pública da dissertação apresentada pelo aluno, conduzida por um júri.
A classificação final (0 a 20 valores) será atribuída pelo júri, tendo em conta a qualidade académica do trabalho escrito apresentado (especialmente a relevância, originalidade e consistência teórica e metodológica demonstradas), bem como o desempenho do estudante durante a apresentação e discussão do texto.

4.2.14. Avaliação (EN):

The evaluation of the CU process will be through the public discussion of the dissertation presented by the student, conducted by a panel. The final rating (0 to 20) will be assigned by the panel, given the academic quality of written work presented (especially the relevance, originality and consistency of theoretical and methodological shown), as well as the student's performance during the presentation and discussion of the text.

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

Como referido, a UC tem como objetivo desenvolver no aluno a capacidade de realizar investigação de forma autónoma. As quatro dimensões do processo de ensino/aprendizagem reforçam-se mutuamente contribuindo para este objetivo:
1. As sessões com o professor visam clarificar a natureza do trabalho a realizar e as exigências metodológicas do trabalho de investigação.
2. As sessões tutoriais com o orientador são úteis para sugerir aos alunos o caminho a seguir e para validar os resultados obtidos.
3. As sessões de trabalho individual são o principal instrumento de aprendizagem, durante as quais o aluno se familiariza com a literatura relevante e reflecte sobre ela.
4. As sessões de seminário são um momento privilegiado de aprendizagem colectiva, onde cada aluno beneficia da aprendizagem realizada pelos outros alunos.

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

As mentioned, the CU aims to develop the student's ability to conduct research independently. The four dimensions of the teaching/learning process reinforce each other contributing to this goal:
1. The sessions with the teacher aims clarify the nature of the work to do and the methodological requirements of the research work.
2. The tutorial sessions with the supervisor, are useful to suggest to students the way to go, and to validate on going the results obtained.
3. The individual work sessions are the key tool of learning, during which the student becomes familiar with the relevant literature and reflect on it.
4. The seminarial sessions are a privileged moment of collective learning, where each student benefits from learning held by the other students.

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

The bibliography adopted results from the survey conducted by the students themselves, taking into account the "Question of Departure" that guides the work of each student.
Special attention should be given to bibliographical information provided by the Advisor.

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

The bibliography adopted results from the survey conducted by the students themselves, taking into account the "Question of Departure" that guides the work of each student.
Special attention should be given to bibliographical information provided by the Advisor.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Fator Humano na Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Fator Humano na Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Human Factor in Cybersecurity and Resilience

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

310

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

310

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Margarida Tavares Peralta Couto dos Santos - 24.0h

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):
OA1: Compreender a importância do fator humano na cibersegurança
OA2: Conhecer a psicologia dos ciberataques
OA3: Distinguir técnicas de engenharia social na cibersegurança
OA4: Identificar o erro humano em cibersegurança e avaliar campanhas de sensibilização no seio das organizações
OA5: Refletir sobre questões éticas ligadas ao fator humano na cibersegurança
OA6: Analisar criticamente abordagens emergentes no âmbito da sensibilização para a cibersegurança e resiliências das organizações

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Understand the importance of the human factor in cybersecurity
LO2: Familiarize with the psychology of cyberattacks
LO3: Distinguish social engineering techniques in cybersecurity
LO4: Identify human error in cybersecurity and evaluate awareness campaigns within organizations
LO5: Reflect on ethical issues related to the human factor in cybersecurity
LO6: Critically analyze emerging approaches in cybersecurity awareness and organizational resilience

4.2.11. Conteúdos programáticos (PT):
PC1 Psicologia do comportamento humano e cibersegurança
Tecnologia, pessoas e segurança
Crenças, atitudes e comportamentos
Importância do fator humano
Vulnerabilidades e ameaças
PC2 Ciberataques
Perfis psicológicos de hackers e cibercriminosos
Políticas de segurança nas organizações
Utilização segura de redes sociais e media digital
PC3 Engenharia Social e Técnicas de Manipulação Psicológica
Técnicas de engenharia social
Reconhecimento e resposta a tentativas de manipulação (phishing, spear-phishing, etc.)
Psicologia comportamental na engenharia social
PC4 Erro humano e campanhas de sensibilização
Tipo de erro humano e medidas de mitigação
Aspetos psicológicos na resposta a incidentes de cibersegurança
Papel das lideranças na cibersegurança
Campanhas de sensibilização
PC5 Tendências futuras e desafios
Desafios na cibersegurança e fator humano
Questões éticas ligadas à cibersegurança centrada no ser humano
Abordagens inovadoras para melhorar a consciencialização

4.2.11. Conteúdos programáticos (EN):

PC1. Psychology of human behavior and cybersecurity
Technology, people, and security
Beliefs, attitudes, and behaviors
Importance of the human factor
Vulnerabilities and threats
PC2. Cyberattacks
Psychological profiles of hackers and cybercriminals
Security policies in organizations
Safe use of social networks and digital media
PC3. Social Engineering and Psychological Manipulation Techniques
Social engineering techniques
Recognition and response to manipulation attempts (phishing, spear-phishing, etc.)
Behavioral psychology in social engineering
PC4. Human error and awareness campaigns
Types of human error and mitigation measures
Psychological aspects in responding to cybersecurity incidents
Role of leadership in cybersecurity
Awareness campaigns
PC5. Future trends and challenges
Challenges in cybersecurity and the human factor
Ethical issues related to human-centric cybersecurity
Innovative approaches to improving awareness and cyber resilience

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

Através de uma introdução a alguns dos principais conceitos da Psicologia, crenças, atitudes e comportamentos, os estudantes devem analisar criticamente os efeitos do fator humano na cibersegurança de uma organização. A compreensão da importância do fator humano na cibersegurança permitirá aos estudantes olhar para os ciberataques de uma perspectiva psicológica, tendo em conta as motivações dos cibercriminosos, desenhando perfis psicológicos. Os estudantes também irão aprofundar técnicas de engenharia social e de manipulação psicológica, que sustentam muitos dos ciberataques de que ouvimos falar. Esse conhecimento irá facilitar a sensibilização para a necessidade de se promover uma cultura de segurança nas organizações, bem como o papel que as equipas e as lideranças têm nestas questões. Os estudantes terão ainda que refletir sobre questões éticas ligadas a uma cibersegurança centrada no fator humano e as implicações que esta abordagem traz ao funcionamento das organizações.

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

Through an introduction to key concepts in Psychology, such as beliefs, attitudes, and behaviors, students will critically analyze the effects of the human factor within organization's cybersecurity. Understanding the importance of the human factor in cybersecurity will allow students to examine cyberattacks from a psychological perspective, considering the motivations of cybercriminals and developing psychological profiles. Students will also delve into social engineering techniques and psychological manipulation, which underpin many of the cyberattacks we hear about. This knowledge will facilitate awareness of the need to promote a security culture within organizations, as well as the role that teams and leadership play in these matters. Students will also need to reflect on ethical issues related to a human-centric approach to cybersecurity and the implications this approach has on organizational functioning.

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

Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico. O docente dará feedback (corretivo e/ou cognitivo) sobre as atividades e tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Em particular, a UC adotará como metodologias de ensino e aprendizagem as seguintes: aprendizagem baseada em estudos de caso, pretende-se que a utilização de casos reais ou fictícios como ponto de partida para a aprendizagem seja capaz de colocar os estudantes perante cenários de incidentes de cibersegurança, em determinados contextos organizacionais, e que esse exercício possibilite aplicar, testar e avaliar diferentes conceitos relacionados com o fator humano na cibersegurança e na ciber-resiliência das organizações; aprendizagem baseada em tarefas, segundo a qual os estudantes irão realizar tarefas definidas de acordo com a ordem definida pelo docente, com crescente grau de dificuldade e distintos níveis de apoio, será também uma forma de ir aferindo os conhecimentos adquiridos e a adequação da sua aplicação por parte dos estudantes; finalmente, esta UC utilizará também a aprendizagem colaborativa, que por ser centrada na interação entre os estudantes, irá promover a colaboração para construir conhecimento em conjunto. A participação através de debates, discussões e reflexão sobre problemas reais, permitirá uma apreensão coletiva e em conjunto dos vários conteúdos da UC. Como estratégia de motivação dos estudantes, esta UC irá incentivar ao máximo o estabelecimento de Tutorias entre Pares, ou seja, estudantes com mais conhecimento/facilidade de aprendizagem numa temática irão apoiar o(s) outro(s) colega(s), em modo síncrono ou assíncrono (mensagens, fóruns de discussão), em momentos/atividades criadas especificamente para o efeito. Tanto quanto possível, esta UC propicia também o recurso à metodologia do storytelling, na qual se pretende que o docente crie uma narrativa que relacione os conteúdos a serem aprendidos com situações reais, experiências pessoais ou histórias fictícias, através de vários recursos tais como vídeos, podcasts, textos ou apresentações interativas. Estas abordagens pedagógicas estão articuladas com o modelo pedagógico do Iscte, na medida em que o ensino é centrado na aquisição de conhecimento e no desenvolvimento de competências, assim como se promove a construção da aprendizagem na relação com o outro (pares e docentes).

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

Through a combination of synchronous and asynchronous online learning activities, students will engage in tasks with varying levels of support and guidance from the instructor, apply theoretical knowledge, and develop problem-solving and critical thinking skills. The instructor will provide feedback (corrective and/or cognitive) on the activities and tasks completed. This approach will enable students to make connections between theoretical and practical knowledge, enhancing their understanding and application of the concepts learned. Specifically, the following teaching and learning methodologies will be adopted in this course: case-based learning, where real or fictional cases are used as a starting point for learning, presenting students with cybersecurity incident scenarios in specific organizational contexts to apply, test, and evaluate different concepts related to the human factor in cybersecurity and organizational cyber resilience; task-based learning, in which students will perform defined tasks in a sequence determined by the instructor, with increasing levels of difficulty and varying degrees of support, serving as a means to assess the acquired knowledge and the students' ability to apply it; and collaborative learning, which emphasizes interaction among students to promote collaboration in constructing knowledge together. Participation through debates, discussions, and reflection on real-world problems will enable collective and collaborative understanding of the course content. As a student motivation strategy, this course will strongly encourage Peer Tutoring, where students with greater knowledge or learning proficiency in a specific topic will support their peers through synchronous or asynchronous means (messaging, discussion forums) during designated moments/activities. Whenever possible, the course also incorporates the storytelling methodology, in which the instructor creates a narrative that relates the content to be learned to real situations, personal experiences, or fictional stories, using various resources such as videos, podcasts, texts, or interactive presentations.
These pedagogical approaches are aligned with the pedagogical model of Iscte, as they center on the acquisition of knowledge and the development of skills, while fostering learning through interactions with peers and instructors.

4.2.14. Avaliação (PT):

Avaliação periódica:
Análise de 2 estudos de caso ao longo do semestre: um individual e um em grupo. Cada estudo de caso (cuja análise será desenvolvida com estrutura pré-definida pelo docente) e respetiva discussão tem o peso de 35% na nota final, com nota mínima de 8 valores. A média da análise dos estudos de caso terá de ser igual ou superior a 9,5 valores.
Realização de 2 mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, cada um deles a contar com 15% para a nota final.
Avaliação por exame (1ª Época, 2ª Época): Exame presencial (100% da nota final).

4.2.14. Avaliação (EN):

Periodic Assessment (only available in 1st Season):
Analysis of 2 case studies throughout the semester: one individual and one in group. Each case study analysis (to be developed with a predefined structure by the instructor) and its respective discussion carry a weight of 35% towards the final grade, with a minimum grade of 8 points. The average grade of the two case study analyses must be equal to or greater than 9.5 points.
Completion of 2 mini-assessment tests throughout the semester, each with a minimum grade of 8 points. Each test contributes 15% towards the final grade.
Assessment by exam (1st Season, 2nd Season): Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. A opção por uma metodologia assente na aprendizagem baseada em estudos de caso, ao utilizar casos reais ou fictícios como ponto de partida para a aprendizagem, permitirá que os estudantes tenham acesso a informações detalhadas sobre o caso, incluindo contexto, personagens e problemas específicos a serem resolvidos. Esta metodologia é a mais adequada para que os estudantes possam, por um lado, conhecer a psicologia dos ciberataques e, por outro, distinguir técnicas de engenharia social na cibersegurança. O recurso à aprendizagem baseada em tarefas, segundo a qual os estudantes irão realizar tarefas definidas de acordo com a ordem definida pelo docente, com crescente grau de dificuldade, distintos níveis de apoio e feedback por parte do docente no final de cada tarefa permite, por sua vez, que os estudantes compreendam os conceitos relacionados com a importância do fator humano na cibersegurança, e que sejam capazes de identificar o erro humano em cibersegurança e avaliar campanhas de sensibilização para a cibersegurança no seio das organizações. Finalmente, a opção pela aprendizagem colaborativa, em que a aprendizagem está centrada na interação entre os estudantes, e a participação ativa é incentivada, visando a criação de uma compreensão partilhada pelo grupo, proporciona uma reflexão sobre questões éticas ligadas ao fator humano na cibersegurança, bem como a análise critica das abordagens emergentes no âmbito da sensibilização para a cibersegurança e resiliências das organizações. Ao longo do semestre, e como estratégia motivacional, esta UC irá incentivar ao máximo o estabelecimento de Tutorias entre Pares, para que os estudantes se apoiem mutuamente na medida das suas capacidades e necessidades, bem como o recurso à metodologia do storytelling, na qual o docente irá promover a aprendizagem a partir de uma narrativa criada pelo próprio, relacionado conteúdos e situações reais.

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

The teaching methodologies have been selected to align with the learning objectives of the course. The choice of a methodology based on case-based learning, using real or fictional cases as a starting point for learning, will provide students with detailed information about the case, including context, characters, and specific problems to be solved. This methodology is most suitable for students to, on one hand, understand the psychology of cyberattacks and, on the other hand, distinguish social engineering techniques in cybersecurity. The use of task-based learning, where students will perform defined tasks in a sequence determined by the instructor, with increasing levels of difficulty, different levels of support, and feedback from the instructor at the end of each task, allows students to comprehend the concepts related to the importance of the human factor in cybersecurity. It also enables them to identify human error in cybersecurity and evaluate awareness campaigns for cybersecurity within organizations. Lastly, the choice of collaborative learning, where learning is centered around interaction among students and active participation is encouraged, aiming to create shared understanding within the group, provides an opportunity for reflection on ethical issues related to the human factor in cybersecurity, as well as critical analysis of emerging approaches in cybersecurity awareness and organizational resilience. Throughout the semester, as a motivational strategy, this course will strongly encourage Peer Tutoring, where students support each other to the best of their abilities and needs. Additionally, the storytelling methodology will be utilized, where the instructor will promote learning through narratives created by themselves, relating to real content and situations.

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

Gaspar de Matos, M. & Ferreira, M. (2013). Nascidos Digitais: Novas Linguagens, Lazer e Dependências. Lisboa: Coisas de Ler.
Blokdyk G. (2023). Cybersecurity Awareness A Complete Guide. The Art of Service - Cybersecurity Awareness Publishing. ISBN: 978-1038801517.
Leukfeldt, R. & Holt, T. J. (2019). The Human Factor of Cybercrime. NY: Routledge.
Hallas B. (2018). Re-Thinking The Human Factor: A Philosophical Approach to Information Security Awareness Behaviour and Culture. Hallas Institute. ISBN: 978-1999695514.
Hadnagy C. (2018). Social Engineering: The Science of Human Hacking. Wiley. ISBN: 978-1119433385.
Nicholson, D. (Editor). Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31. Florida: Springer.
Gheorghe A., Katina P. (2023). Gamification for Resilience: Resilient Informed Decision Making. Wiley. ISBN: 978-1394157747

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

Gaspar de Matos, M. & Ferreira, M. (2013). Nascidos Digitais: Novas Linguagens, Lazer e Dependências. Lisboa: Coisas de Ler.
Blokdyk G. (2023). Cybersecurity Awareness A Complete Guide. The Art of Service - Cybersecurity Awareness Publishing. ISBN: 978-1038801517.
Leukfeldt, R. & Holt, T. J. (2019). The Human Factor of Cybercrime. NY: Routledge.
Hallas B. (2018). Re-Thinking The Human Factor: A Philosophical Approach to Information Security Awareness Behaviour and Culture. Hallas Institute. ISBN: 978-1999695514.
Hadnagy C. (2018). Social Engineering: The Science of Human Hacking. Wiley. ISBN: 978-1119433385.
Nicholson, D. (Editor). Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31. Florida: Springer.
Gheorghe A., Katina P. (2023). Gamification for Resilience: Resilient Informed Decision Making. Wiley. ISBN: 978-1394157747

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Fundamentos de Gestão da Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):
Fundamentos de Gestão da Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):
Fundamentals of Cybersecurity and Resilience Management

4.2.2. Sigla da área científica em que se insere (PT):
480

4.2.2. Sigla da área científica em que se insere (EN):
480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Carlos Eduardo Dias Coutinho - 24.0h

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):
OA1: Compreender os conceitos e terminologias fundamentais da cibersegurança e da ciber-resiliência.
OA2: Reconhecer o alinhamento estratégico entre a cibersegurança e os objectivos e estratégias organizacionais.
OA3: Adquirir conhecimentos sobre os principais quadros de referência de cibersegurança, normas e requisitos regulamentares.
OA4: Desenvolver competências em governação, avaliação de risco e gestão da cibersegurança.
OA5: Aprender a medir e monitorizar os controlos de segurança utilizando métricas relevantes e indicadores-chave de desempenho (KPIs).
OA6: Manter-se atualizado sobre as tendências, tecnologias e desafios emergentes em matéria de cibersegurança e resiliência.

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

LO1: Understand the fundamental concepts and terminologies of cybersecurity and cyber resilience.
LO2: Recognize the strategic alignment between cybersecurity and organizational goals and strategies.
LO3: Gain knowledge of key cybersecurity reference frameworks, standards, and regulatory requirements.
LO4: Develop skills in cybersecurity governance, risk assessment, and management.
LO5: Learn to measure and monitor security controls using relevant metrics and key performance indicators (KPIs).
LO6: Stay updated with emerging trends, technologies, and challenges in cybersecurity and resilience.

4.2.11. Conteúdos programáticos (PT):

CP1: Introdução à Cibersegurança e à Ciber-resiliência
CP2: Quadros de Referência e Normas de Cibersegurança
CP3: Quadro Regulamentar e Legislativo de Cibersegurança
CP4: Conceitos de Gestão de Cibersegurança e Ciber-resiliência
CP5: Alinhamento Estratégico da Cibersegurança com a Estratégia Organizacional
CP6: Governação da Cibersegurança, Políticas e Gestão de Risco
CP7: Métricas de cibersegurança e gestão do desempenho
CP8: Tendências Emergentes e Direcções Futuras

4.2.11. Conteúdos programáticos (EN):

PC1: Introduction to Cybersecurity and Cyber Resilience
PC2: Cybersecurity Frameworks and Standards
PC3: Regulatory and Legislative Framework for Cybersecurity
PC4: Concepts of Cybersecurity and Cyber-resilience Management
PC5: Strategic Alignment of Cybersecurity with Organisational Strategy
PC6: Cybersecurity Governance, Policies and Risk Management
PC7: Cybersecurity Metrics and Performance Management
PC8: Emerging Trends and Future Directions

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas, aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Fundamentos de Gestão da Cibersegurança e Resiliência adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The Fundamentals of Cybersecurity and Resilience Management course will adopt Task-Based Learning combined with Problem-Based Learning as its core teaching and learning methodology. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in their learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de 2 mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, cada um deles a contar com 20% para a nota final. Realização a apresentação de 4 trabalhos em grupo, cada um deles a contar com 15% para a nota final.
Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of 2 mini-assessment tests throughout the semester, each with a minimum score of 8, each counting 20% towards the final grade. Completion and presentation of 4 group assignments, each of which will count for 15% of the final grade.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, numa primeira fase compreender os princípios e conceitos da cibersegurança e da ciber-resiliência. Irão ainda aplicar conhecimentos teóricos e desenvolver competências de análise e pensamento crítico. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar tarefas específicas e realizar trabalhos relacionados com os diferentes temas que serão abordados na unidade curricular. No caso dos trabalhos os estudantes terão acesso a todos os detalhes dos mesmos, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes aprender e aplicar os conhecimentos adquiridos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the CU that will allow them, in a first phase, to understand the principles and concepts of cybersecurity and cyber resilience. They will also apply theoretical knowledge and develop analytical and critical thinking skills. The lecturer will provide feedback (corrective and/or cognitive) on the tasks carried out by the students. Students will also carry out specific tasks and assignments related to the different topics that will be addressed in the course. In the case of the assignments, students will have access to all the details of the assignments, as well as the tools that should be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to learn and apply the knowledge acquired. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Brumfield, C. (2021). Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework (1st edition). Wiley.
Calder, A. (2018). NIST Cybersecurity Framework: A pocket guide. ITGP.
Hodson, C. J. (2019). Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls (1st edition). Kogan Page.
Petrenko, S. (2022). Cyber Resilience (1st edition). River Publishers.
Siegel, C. A., & Sweeney, M. (2020). Cyber Strategy: Risk-Driven Security and Resiliency (1st edition). Auerbach Publications.
Trim, D. P., & Lee, D. Y.-I. (2014). Cyber Security Management: A Governance, Risk and Compliance Framework (1st edition). Gower.
Wens, C. van der. (2019). ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. Independently published.
Wong, C. (2011). Security Metrics, a Beginner's Guide (1st edition). McGraw Hill.

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

Brumfield, C. (2021). Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework (1st edition). Wiley.
Calder, A. (2018). NIST Cybersecurity Framework: A pocket guide. ITGP.
Hodson, C. J. (2019). Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls (1st edition). Kogan Page.
Petrenko, S. (2022). Cyber Resilience (1st edition). River Publishers.
Siegel, C. A., & Sweeney, M. (2020). Cyber Strategy: Risk-Driven Security and Resiliency (1st edition). Auerbach Publications.
Trim, D. P., & Lee, D. Y.-I. (2014). Cyber Security Management: A Governance, Risk and Compliance Framework (1st edition). Gower.
Wens, C. van der. (2019). ISO 27001 Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses. Independently published.
Wong, C. (2011). Security Metrics, a Beginner's Guide (1st edition). McGraw Hill.

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Gestão do Ciber-risco para Resiliência

4.2.1. Designação da unidade curricular (PT):
Gestão do Ciber-risco para Resiliência

4.2.1. Designação da unidade curricular (EN):
Cyber-risk Management for Resilience

4.2.2. Sigla da área científica em que se insere (PT):
480

4.2.2. Sigla da área científica em que se insere (EN):
480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Carlos José Corredoura Serrão - 25.0h

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):
OA1: Compreender os conceitos fundamentais, os enquadramentos e as melhores práticas na gestão do risco de cibersegurança.
OA2: Identificar e avaliar riscos de cibersegurança em contextos organizacionais, considerando ameaças e vulnerabilidades específicas.
OA3: Desenvolver estratégias de mitigação de riscos adaptadas à postura e aos objectivos de uma organização, incluindo a implementação de controlos e contramedidas.
OA4: Implementar práticas de monitorização de segurança e utilizar inteligência de ameaças para detetar e responder proactivamente a ameaças emergentes.
OA5: Compreender o papel da governação, do risco e da conformidade (GRC) na gestão do risco de cibersegurança e aderir a quadros e regulamentos de conformidade relevantes.
OA6: Aplicar os conhecimentos e competências adquiridos para realizar uma avaliação abrangente dos riscos de cibersegurança para uma organização.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Understand the fundamental concepts, frameworks, and best practices in cybersecurity risk management.
LO2: Identify and assess cybersecurity risks within organizational contexts, considering specific threats and vulnerabilities.
LO3: Develop risk mitigation strategies tailored to an organization's posture and objectives, including the implementation of controls and countermeasures.
LO4: Implement security monitoring practices and utilize threat intelligence to proactively detect and respond to emerging threats.
LO5: Comprehend the role of governance, risk, and compliance (GRC) in cybersecurity risk management and adhere to relevant compliance frameworks and regulations.
LO6: Apply the knowledge and skills acquired to conduct a comprehensive cybersecurity risk assessment for an organization.

4.2.11. Conteúdos programáticos (PT):
PC1: Princípios da Gestão do Risco em Cibersegurança e Resiliência
PC2: Identificação e Avaliação de Riscos
PC3: Análise de Risco e Estratégias de Mitigação
PC4: Controlos de Segurança e Contramedidas
PC5: Governança de Segurança e Conformidade
PC6: Gestão de Risco da Cadeia de Suprimentos
PC7: Monitorização e Comunicação do Risco
PC8: Tendências Emergentes e Desafios Futuros na Gestão de Risco
PC9: Plano de Gestão de Risco e Estudos de Caso

4.2.11. Conteúdos programáticos (EN):
PC1: Principles of Cybersecurity Risk Management and Resilience
PC2: Risk Identification and Assessment
PC3: Risk Analysis and Mitigation Strategies
PC4: Security Controls and Countermeasures
PC5: Security Governance and Compliance
PC6: Supply Chain Risk Management
PC7: Risk Monitoring and Communication
PC8: Emerging Trends and Future Challenges in Risk Management
PC9: Risk Management Plan and Case Studies

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Gestão do Ciber-risco para a Resiliência adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The UC Cyber-risk Management for Resilience will adopt as core teaching and learning methodology Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de uma série de mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores - estes testes contam com 30% para a nota final. Realização de um conjunto de exercícios práticos em grupo, que contam com 30% para a nota final. Realização de projeto final colaborativo, através da realização de um caso de estudo, em grupo, e com apresentação final. O projeto terá uma ponderação total de 40%, sendo que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of a series of mini-assessment tests throughout the semester, each with a minimum score of 8 - these tests count for 30% of the final grade. Completion of a set of practical group exercises, which count for 30% of the final grade. Completion of a final collaborative project, through the realisation of a case study, in group, and with a final presentation. The project will have a total weighting of 40%, and the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem desta unidade curricular. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, numa primeira fase compreender os princípios gestão de risco em cibersegurança e posteriormente, aplicar esses mesmos princípios para poderem determinar a avaliar o risco em cibersegurança, para contribuirem para a resiliência de dados e sistemas. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos ao longo do semestre - relativamente aos testes e trabalhos realizados. Os estudantes irão ainda realizar trabalhos específicos relacionados com os diferentes temas que serão abordados na unidade curricular. No caso dos trabalhos os estudantes terão acesso a todos os detalhes dos mesmos, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes avaliar a aplicação desses conhecimentos para atingir objetivos de cibersegurança e ciber-resiliência. O projeto final desta UC irá ser realizado em grupo, onde os alunos irão trabalhar um caso de estudo e onde podem aplicar os diferentes conhecimentos aprendidos ao longo do semestre. Depois irão partilhar e discutir o projeto com os restantes colegas. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected in order to fulfil the learning objectives of this curricular unit. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the UC that will allow them, in a first phase, to understand the principles of cybersecurity risk management and later, to apply these same principles to be able to determine and assess cybersecurity risk, to contribute to the resilience of data and systems. The lecturer will give feedback (corrective and/or cognitive) on the tasks carried out by the students throughout the semester - regarding the tests and assignments. Students will also carry out specific assignments related to the different topics that will be addressed in the curricular unit. In the case of the assignments, students will have access to all the details of the assignments, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to evaluate the application of this knowledge to achieve cybersecurity and cyber resilience objectives. The final project of this CU will be carried out in groups, where students will work on a case study and where they can apply the different knowledge learnt throughout the semester. Then they will share and discuss the project with the rest of their classmates. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Brumfield, C. (2021). Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework (1st edition). Wiley.
Calder, A., & Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002 (7th edition). Kogan Page.
Freund, J., & Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach (1st edition). Butterworth-Heinemann.
Talabis, M., & Martin, J. (2012). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis (1st edition). Syngress.
Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up (1st edition). Syngress.

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

Brumfield, C. (2021). Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework (1st edition). Wiley.
Calder, A., & Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002 (7th edition). Kogan Page.
Freund, J., & Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach (1st edition). Butterworth-Heinemann.
Talabis, M., & Martin, J. (2012). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis (1st edition). Syngress.
Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up (1st edition). Syngress.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Incidentes de Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Incidentes de Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Cybersecurity and Resilience Incidents

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

480

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

480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• João Carlos Amaro Ferreira - 24.0h

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):
OA1: Identificar e analisar diversas ameaças à cibersegurança, incluindo os agentes das ameaças e as suas motivações.
OA2: Recolher e analisar informações sobre ameaças para avaliar os riscos de cibersegurança.
OA3: Implementar técnicas avançadas de procura e deteção de ameaças.
OA4: Desenvolver planos e estruturas eficazes de resposta a incidentes.
OA5: Compreender como conduzir investigações completas de incidentes de cibersegurança usando técnicas forenses.
OA6: Utilizar ferramentas e tecnologias de resposta a incidentes para deteção e contenção.
OA7: Executar processos de resposta a incidentes, incluindo triagem, comunicação e actividades pós-incidente.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Identify and analyze diverse cybersecurity threats, including threat actors and motivations.
LO2: Collect and analyze threat intelligence to assess cybersecurity risks.
LO3: Implement advanced threat hunting and detection techniques.
LO4: Develop effective incident response plans and frameworks.
LO5: Understand how to conduct thorough investigations of cybersecurity incidents using forensic techniques.
LO6: Utilize incident response tools and technologies for detection and containment.
LO7: Execute incident response processes, including triage, communication, and post-incident activities.

4.2.11. Conteúdos programáticos (PT):
CP1: Introdução às Ameaças e Incidentes de Cibersegurança
CP2: Recolha e análise de informações sobre ameaças
CP3: Procura e Deteção de Ameaças
CP4: Planeamento de Resposta a Incidentes
CP5: Deteção e Monitorização de Incidentes
CP6: Tratamento e contenção de incidentes
CP7: Resiliência e Recuperação
CP8: Aspectos Éticos e Legais de Incidentes de Cibersegurança
CP9: Colaboração da Equipa de Resposta a Incidentes
CP10: Estudos de Caso e Cenários do Mundo Real

4.2.11. Conteúdos programáticos (EN):

PC1: Introduction to Cybersecurity Threats and Incidents
PC2: Collection and Analysis of Threat Intelligence
PC3: Threat Hunting and Detection
PC4: Incident Response Planning
PC5: Incident Detection and Monitoring
PC6: Incident Handling and Containment
PC7: Resilience and Recovery
PC8: Ethical and Legal Aspects of Cybersecurity Incidents
PC9: Incident Response Team Collaboration
PC10: Case Studies and Real-World Scenarios

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Incidentes de Cibersegurança e Resiliência adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The Cybersecurity Incidents and Resilience CU will adopt Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning as its core teaching and learning methodology. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de 2 mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, cada um deles a contar com 15% para a nota final. Realização de 4 laboratórios em grupo, cada um deles a contar com 10% para a nota final. Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 30%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of 2 mini-assessment tests throughout the semester, each with a minimum score of 8, each counting 15% towards the final grade. Completion of 4 group laboratories, each of which will count for 10% of the final grade. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 30%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá identificar formas de recolha de informação sobre possíveis ameaças a dados, informação e sistemas, e compreender o risco dessas mesmas ameaças. Por outro lado, os alunos aprendem através de tarefas como as ameaças identificadas se podem converter em incidentes que podem comprometer a cibersegurança e resiliência das organizações. Finalmente, irão igualmente identificar formas de investigação dos incidentes e recomendar as respostas mais adequadas para os mesmos. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar projetos específicos e realizar laboratórios relacionados com os diferentes temas que serão abordados na unidade curricular. No caso dos projetos os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes perceber a importância da recolha de inteligência sobre ameaças prevalentes e formas de resposta a incidentes que possam ocorrer dessas mesmas ameaças. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected in order to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the CU that will allow them to identify ways of collecting information about possible threats to data, information and systems, and to understand the risk of these threats. On the other hand, students will learn through tasks how the identified threats can turn into incidents that can compromise the cybersecurity and resilience of organisations. Finally, they will also identify ways to investigate incidents and recommend the most appropriate responses to them. The lecturer will provide feedback (corrective and/or cognitive) on the tasks carried out by the students. Students will also carry out specific projects and perform laboratories related to the different topics that will be addressed in the course. In the case of projects, students will have access to all the details of the work to be carried out, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to realise the importance of gathering intelligence on prevalent threats and ways of responding to incidents that may occur from those same threats. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Costa-Gazcon, V. (2021). Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools. Packt Publishing.
Dahj, J. N. M. (2022). Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense. Packt Publishing.
Johansen, G. (2022). Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, 3rd Edition (3rd ed. edition). Packt Publishing.
Martinez, R. (2022). Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting. Packt Publishing.
Wilhoit, K., & Opacki, J. (2022). Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs. Packt Publishing.

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

Costa-Gazcon, V. (2021). Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools. Packt Publishing.
Dahj, J. N. M. (2022). Mastering Cyber Intelligence: Gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense. Packt Publishing.
Johansen, G. (2022). Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, 3rd Edition (3rd ed. edition). Packt Publishing.
Martinez, R. (2022). Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting. Packt Publishing.
Wilhoit, K., & Opacki, J. (2022). Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs. Packt Publishing.

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Optativa

4.2.1. Designação da unidade curricular (PT):
Optativa

4.2.1. Designação da unidade curricular (EN):
Optional Course

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

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

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Carlos José Corredoura Serrão - 0.0h

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):
--

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

4.2.11. Conteúdos programáticos (PT):
--

4.2.11. Conteúdos programáticos (EN):
--

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

--

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

--

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

--

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

--

4.2.14. Avaliação (PT):
--

4.2.14. Avaliação (EN):
--

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

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

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

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

4.2.17. Observações (PT):
Optativa - Tempo médio de contato | Lista a definir anualmente

4.2.17. Observações (EN):
Optional - Medium contact hours | List to be defined annually

Mapa III - Resiliência e Continuidade do Negócio

4.2.1. Designação da unidade curricular (PT):
Resiliência e Continuidade do Negócio

4.2.1. Designação da unidade curricular (EN):
Resilience and Business Continuity

4.2.2. Sigla da área científica em que se insere (PT):
480

4.2.2. Sigla da área científica em que se insere (EN):
480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• João Pedro Calado Barradas Branco Pavia - 24.0h

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):
OA1: Identificar e avaliar as funções empresariais críticas numa organização e a sua vulnerabilidade às ciberameaças.
OA2: Desenvolver e implementar um plano de continuidade de negócios abrangente, incluindo medidas preventivas e estratégias de resposta a incidentes.
OA3: Compreender o impacto dos ciberataques nas funções empresariais e avaliar a eficácia das estratégias de resposta a catástrofes de cibersegurança.
OA4: Analisar e empregar tecnologias e soluções adequadas para garantir a continuidade do negócio, tais como estratégias de backup e recuperação, alta disponibilidade e soluções baseadas na nuvem.
OA5: Realizar testes e exercícios para validar e melhorar os planos de continuidade do negócio, garantindo a sua eficácia em cenários reais.
OA6: Avaliar a maturidade da resiliência organizacional, medir a resiliência através de métricas e indicadores e implementar estratégias de melhoria contínua para se adaptar à evolução das ciberameaças.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Identify and assess critical business functions within an organization and their vulnerability to cyber threats.
LO2: Develop and implement a comprehensive business continuity plan, including preventive measures and incident response strategies.
LO3: Understand the impact of cyber-attacks on business functions and evaluate the effectiveness of cybersecurity disaster response strategies.
LO4: Analyze and employ appropriate technologies and solutions to ensure business continuity, such as backup and recovery strategies, high availability, and cloud-based solutions.
LO5: Conduct testing and exercises to validate and improve business continuity plans, ensuring their effectiveness in real-world scenarios.
LO6: Evaluate organizational resilience maturity, measure resilience through metrics and indicators, and implement continuous improvement strategies to adapt to evolving cyber threats.

4.2.11. Conteúdos programáticos (PT):

CP1: Introdução à Resiliência e à Continuidade do Negócio
CP2: Análise do Impacto no Negócio
CP3: Ameaças à Continuidade do Negócio
CP4: Medidas Preventivas para a Continuidade do Negócio
CP5: Tecnologias e Soluções de Continuidade do Negócio
CP6: Teste e Exercício de Planos de Continuidade do Negócio
CP7: Estratégias de Resposta a Desastres de Cibersegurança
CP8: Estratégias de Recuperação de Desastres de Cibersegurança
CP9: Gestão de Crises e Comunicação
CP10: Avaliação da Resiliência e Melhoria Contínua

4.2.11. Conteúdos programáticos (EN):

PC1: Introduction to Resilience and Business Continuity
PC2: Business Impact Analysis
PC3: Threats to Business Continuity
PC4: Preventive Measures for Business Continuity
PC5: Business Continuity Technologies and Solutions
PC6: Testing and Exercising Business Continuity Plans
PC7: Cybersecurity Disaster Response Strategies
PC8: Cybersecurity Disaster Recovery Strategies
PC9: Crisis Management and Communication
PC10: Resilience Assessment and Continuous Improvement

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Resiliência e Continuidade do Negócio adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The Business Resilience and Continuity CU will adopt Task-Based Learning, combined with Project-Based Learning, as its core teaching and learning methodology. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his/her learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de 1 teste de avaliação no final do semestre, com nota mínima de 8 valores, a contar com 40% para a nota final. Realização de 4 laboratórios em grupo, cada um deles a contar com 10% para a nota final. Realização de um projeto final colaborativo (em grupo) realizado por fases ao longo do semestre. O projeto terá uma ponderação total de 60%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of 1 final assessment test of the semester, with a minimum score of 8, counting 40% towards the final grade. Completion of 4 group laboratories, each of which will count for 10% of the final grade. Completion of a final collaborative (group) project carried out in stages throughout the semester. The project will have a total weighting of 60%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, identificar as funções críticas de negócio de uma organização, perceber quais são as principais ameaças que podem ameaçar a continuidade das mesmas, e como garantir a resposta a incidentes e a continuidade das operações da organização. Irão ainda aplicar conhecimentos teóricos e desenvolver competências de análise e pensamento crítico, necessários à percepção de como a resiliência pode contribuir para a continuidade do negócio. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar um projeto específico relacionado com os diferentes temas que serão abordados na unidade curricular. No caso do projeto os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes avaliar a como a resiliência pode contribuir para a continuidade do negócio. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies were selected in order to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will perform tasks with different levels of support and teacher guidance throughout the CU that will allow them to identify the critical business functions of an organisation, understand what are the main threats that can threaten their continuity, and how to ensure incident response and continuity of the organisation's operations. They will also apply theoretical knowledge and develop analytical and critical thinking skills necessary to understand how resilience can contribute to business continuity. The lecturer will provide feedback (corrective and/or cognitive) on the tasks carried out by the students. Students will also carry out a specific project related to the different topics that will be addressed in the curricular unit. In the case of the project, students will have access to all the details of the work to be carried out, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to assess how resilience can contribute to business continuity. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Charters, I. (n.d.). A practical approach to Business Impact Analysis: Understanding the Organisation through Business Continuity Management.
Crask, J. (2021). Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301 (1st edition). Kogan Page.
Engemann, K. J., & Henderson, D. M. (2014). Business Continuity and Risk Management: Essentials of Organizational Resilience (1st edition). Rothstein Publishing.
Fullick, A. A. (2015). Business Impact Analysis: Building the Foundation for a Strong Business Continuity Program. A. Alex Fullick.
Phillips, B. D., & Landahl, M. (2020). Business Continuity Planning: Increasing Workplace Resilience to Disasters (1st edition). Butterworth-Heinemann.
Snedaker, S. (2013). Business Continuity and Disaster Recovery Planning for IT Professionals (2nd edition). Syngress.
Whitman, M. E., & Mattord, H. J. (2021). Principles of Incident Response & Disaster Recovery (3rd edition). Cengage Learning.

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

Charters, I. (n.d.). A practical approach to Business Impact Analysis: Understanding the Organisation through Business Continuity Management.
Crask, J. (2021). Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301 (1st edition). Kogan Page.
Engemann, K. J., & Henderson, D. M. (2014). Business Continuity and Risk Management: Essentials of Organizational Resilience (1st edition). Rothstein Publishing.
Fullick, A. A. (2015). Business Impact Analysis: Building the Foundation for a Strong Business Continuity Program. A. Alex Fullick.
Phillips, B. D., & Landahl, M. (2020). Business Continuity Planning: Increasing Workplace Resilience to Disasters (1st edition). Butterworth-Heinemann.
Snedaker, S. (2013). Business Continuity and Disaster Recovery Planning for IT Professionals (2nd edition). Syngress.
Whitman, M. E., & Mattord, H. J. (2021). Principles of Incident Response & Disaster Recovery (3rd edition). Cengage Learning.

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Segurança e Resiliência de Infraestruturas e Redes de Comunicação

4.2.1. Designação da unidade curricular (PT):
Segurança e Resiliência de Infraestruturas e Redes de Comunicação

4.2.1. Designação da unidade curricular (EN):
Security and Resilience of Infrastructures and Communication Networks

4.2.2. Sigla da área científica em que se insere (PT):
480

4.2.2. Sigla da área científica em que se insere (EN):
480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:
92.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• João Pedro Calado Barradas Branco Pavia - 25.0h

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):
OA1: Analisar as diferenças entre as várias infraestruturas on-premises, cloud-based, comunitárias, híbridas e distribuídas.
OA2: Analisar diferentes tipos de redes de comunicação utilizados pela indústria.
OA3: Analisar tipos de ameaças de cibersegurança de uma forma holística, e especificando os desafios associados aos mesmos.
OA4: Analisar para cada tipo de infraestrutura e rede de comunicação os riscos e ameaças de cibersegurança associados.
OA5: Analisar para cada tipo de infraestrutura e rede de comunicação as técnicas mais comuns para mitigar os riscos associados a 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):
LO1: Analyze the differences between on-premises, cloud-based, community, and hybrid infrastructures.
LO2: Analyze different types of communication networks used by industry.
LO3: Analyze types of cybersecurity threats in a holistic way, and specify the challenges associated with them.
LO4: Analyze for each type of infrastructure and communication network the associated cybersecurity risks and threats.
LO5: Analyze for each type of infrastructure and communication network the most common techniques to mitigate the risks associated with cybersecurity.

4.2.11. Conteúdos programáticos (PT):
CP1: Infraestruturas de Sistemas de Informação e Redes de Comunicação.
CP2: Tecnologias de Segurança de Redes.
CP3: Segurança de Sistemas Distribuídos.
CP4: Sistemas de Controlo Industriais (ICS).
CP5: Segurança de Sistemas Operativos, Cloud e Virtualizados.
CP6: Segurança de Sistemas de Internet das Coisas (IoT)
CP7: Novas tendências para Segurança de Infraestruturas e Redes

4.2.11. Conteúdos programáticos (EN):
PC1: Information Systems and Communication Networks Infrastructures.
PC2: Network Security Technologies.
PC3: Distributed Systems Security.
PC4: Industrial Control Systems (ICS).
PC5: Security of Operating Systems, Cloud and Virtualized.
PC6: Security of Internet of Things (IoT) Systems
PC7: New Trends for Infrastructure and Network Security

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

Esta UC adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

This UC will adopt as core teaching and learning methodology Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his/her learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de 2 mini-testes de avaliação ao longo do semestre, cada um com nota mínima de 8 valores, cada um deles a contar com 15% para a nota final. Realização de 4 laboratórios em grupo, cada um deles a contar com 10% para a nota final. Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 30%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of several mini-assessment tests throughout the semester, counting a total of 30% for the final assessment - each mini-test has a minimum grade of 8. Realisation of a set of proposed practical group activities (laboratories), which count for 40% for the final assessment. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 30%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

Hwang, K., Fox, G., and Dongarra, J., "Distributed and Cloud Computing (From Parallel Processing to the Internet of Things)", Elsevier, 2011
Earl, T., Puttini, R., Mahmood, Z., "Cloud Computing: Concepts, Technology & Architecture", Prentice-Hall, 2014
Buyya, R., Broberg, J, Goscinski, A., "Cloud Computing Principles and Paradigms", Wiley & Sons, 2011
Herbst, N., Kounev, S., and Reussner, R., "Elasticity in Cloud Computing: What It Is, and What It Is Not", in Proceedings of the 10th International Conference on Autonomic Computing (ICAC 2013), San Jose, June 24–28
Smith, J., Nair, R., "The Architecture of Virtual Machines", 2005, IEEE
Josyula, V., Orr, M., Page, G., "Cloud Computing: Automating the Virtualized Data Center", Cisco Press, 2012

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

Hwang, K., Fox, G., and Dongarra, J., "Distributed and Cloud Computing (From Parallel Processing to the Internet of Things)", Elsevier, 2011
Earl, T., Puttini, R., Mahmood, Z., "Cloud Computing: Concepts, Technology & Architecture", Prentice-Hall, 2014
Buyya, R., Broberg, J, Goscinski, A., "Cloud Computing Principles and Paradigms", Wiley & Sons, 2011
Herbst, N., Kounev, S., and Reussner, R., "Elasticity in Cloud Computing: What It Is, and What It Is Not", in Proceedings of the 10th International Conference on Autonomic Computing (ICAC 2013), San Jose, June 24–28
Smith, J., Nair, R., "The Architecture of Virtual Machines", 2005, IEEE
Josyula, V., Orr, M., Page, G., "Cloud Computing: Automating the Virtualized Data Center", Cisco Press, 2012

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Segurança e Resiliência de Software e Aplicações

4.2.1. Designação da unidade curricular (PT):

Segurança e Resiliência de Software e Aplicações

4.2.1. Designação da unidade curricular (EN):

Software and Application Security and Resilience

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

480

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

480

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) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.2.6. % Horas de contacto a distância:

92.00%

4.2.7. Créditos ECTS:

6.0

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

• Carlos José Corredoura Serrão - 24.0h

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):

OA1: Identificar e analisar vulnerabilidades e ameaças em software e aplicações utilizadas nas organizações, e compreender os riscos que representam para a segurança e resiliência.
OA2: Aprender a aplicar práticas de codificação segura para desenvolver software, considerando diferentes metodologias de desenvolvimento e fases do ciclo de vida de desenvolvimento de software (SDLC).
OA3: Avaliar e implementar medidas de segurança para mitigar vulnerabilidades e abordar riscos específicos para aplicações web, móveis, na nuvem e empresariais.
OA4: Aprender a usar técnicas e ferramentas de teste de segurança para avaliar a segurança de software, incluindo análise dinâmica e estática, teste de penetração e revisão de código.
OA5: Conhecer e aprender a integrar considerações de segurança e resiliência no ciclo de vida de desenvolvimento de software (SDLC), garantindo que o software é concebido, desenvolvidos e mantidos com enfoque na segurança e resiliência contra potenciais ataques e risc

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

LO1: Identify and analyze vulnerabilities and threats in software and applications used in organizations, and understand the risks they pose to security and resilience.
LO2: Learn to apply secure coding practices to develop software and applications, considering different development methodologies and stages of the software development life cycle (SDLC).
LO3: Evaluate and implement security measures to mitigate vulnerabilities and address risks specific to web, mobile, cloud, and enterprise applications.
LO4: Learn to use security testing techniques and tools to assess the security posture of software and applications, including dynamic and static analysis, penetration testing, and code review.
LO5: Know and learn to integrate security and resilience considerations into the software development life cycle (SDLC), ensuring that software and applications are designed, developed, and maintained with a strong focus on security and resilience against potential attacks and risks.

4.2.11. Conteúdos programáticos (PT):

PC1: Introdução à Segurança de Software e Aplicações
PC2: Processos de Desenvolvimento de Software e Segurança
PC3: Segurança de Aplicações Web
PC4: Segurança de Aplicações Móveis
PC5: Segurança de Aplicações na Nuvem
PC6: Segurança de Aplicações Empresariais
PC7: Teste e Avaliação de Segurança de Software
PC8: Manutenção de Software Seguro e Resiliente e Gestão de Correções
PC9: Resposta e Recuperação de Incidentes em Software e Aplicações
PC10: Ciclo de Vida de Desenvolvimento de Software Seguro e Resiliente

4.2.11. Conteúdos programáticos (EN):

PC1: Introduction to Software and Application Security
PC2: Software Development Processes and Security
PC3: Security of Web Applications
PC4: Security of Mobile Applications
PC5: Security of Cloud Applications
PC6: Security of Enterprise Applications
PC7: Software Security Testing and Assessment
PC8: Secure and Resilient Software Maintenance and Patch Management
PC9: Incident Response and Recovery in Software and Applications
PC10: Secure and Resilient Software Development Lifecycle

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the learnt concepts. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Segurança e Resiliência de Software e Aplicações adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Problemas combinada com Aprendizagem Baseada em Projetos. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The Software and Applications Security and Resilience CU will adopt as core teaching and learning methodology Problem-Based Learning combined with Project-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de um conjunto de laboratórios e trabalhos em grupo ao longo do semestre, com uma ponderação de 50% na nota final. Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 50%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of a set of group laboratories and assignments throughout the semester, with a weighting of 50% in the final grade. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 50%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, numa primeira fase compreender os diferentes desafions de segurança e de resiliência do software e aplicações, assim como ganhar a consciência das principais ameaças e riscos, em diferentes tipologias de aplicações e software. Irão ainda aplicar conhecimentos teóricos e desenvolver competências que permitem desenvolver capacidades de resiliência e cibersegurança em software e aplicações e aprender a mitigar ameaças. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas que forem sendo realizadas pelos alunos. Os estudantes irão ainda realizar trabalhos e laboratórios específicos relacionados com os diferentes temas que serão abordados na unidade curricular. No projeto final os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes avaliar os problemas de segurança de aplicações e software e perceber como os mesmos afetam a cibersegurança e ciber-resiliência. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected in order to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will perform tasks with different levels of support and teacher guidance throughout the CU that will allow them, in a first phase, to understand the different security and resilience challenges of software and applications, as well as to gain awareness of the main threats and risks, in different types of applications and software. They will also apply theoretical knowledge and develop skills to build resilience and cybersecurity capabilities in software and applications and learn how to mitigate threats. The teacher will give feedback (corrective and/or cognitive) on the tasks that are being carried out by the students. Students will also carry out specific assignments and laboratories related to the different topics that will be addressed in the course. In the final project students will have access to all the details of the work to be done, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to evaluate application and software security problems and to realise how they affect cybersecurity and cyber-resilience. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their engagement throughout the CU.

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

Harwood, M., & Price, R. (2022). Internet and Web Application Security (3rd edition). Jones & Bartlett Learning.
Hoffman, A. (2020). Web Application Security: Exploitation and Countermeasures for Modern Web Applications (1st edition). O'Reilly Media.
Howard, M., LeBlanc, D., & Viega, J. (2009). 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (1st edition). McGraw Hill.
Kohnfelder, L. (2021). Designing Secure Software: A Guide for Developers. No Starch Press.
McGraw, G. (2006). Software Security: Building Security In (1st edition). Addison-Wesley Professional.
Mead, N. R., & Woody, C. (2016). Cyber Security Engineering: A Practical Approach for Systems and Software Assurance (1st edition). Addison-Wesley Professional.
Schagaev, I., Zouev, E., & Thomas, K. (2019). Software Design for Resilient Computer Systems (2nd edition). Springer.

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

Harwood, M., & Price, R. (2022). Internet and Web Application Security (3rd edition). Jones & Bartlett Learning.
Hoffman, A. (2020). Web Application Security: Exploitation and Countermeasures for Modern Web Applications (1st edition). O'Reilly Media.
Howard, M., LeBlanc, D., & Viega, J. (2009). 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them (1st edition). McGraw Hill.
Kohnfelder, L. (2021). Designing Secure Software: A Guide for Developers. No Starch Press.
McGraw, G. (2006). Software Security: Building Security In (1st edition). Addison-Wesley Professional.
Mead, N. R., & Woody, C. (2016). Cyber Security Engineering: A Practical Approach for Systems and Software Assurance (1st edition). Addison-Wesley Professional.
Schagaev, I., Zouev, E., & Thomas, K. (2019). Software Design for Resilient Computer Systems (2nd edition). Springer.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Seminário de Investigação em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Seminário de Investigação em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Research Seminar Cybersecurity and Resiliency

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

480

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

480

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:

Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-12.0; OT-2.0

4.2.6. % Horas de contacto a distância:
100.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Carlos José Corredoura Serrão - 24.0h

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):
Os objetivos de aprendizagem são:
OA1 Enquadrar a investigação científica e compreender os principais métodos de investigação em tecnologias digitais
OA2 Aplicar no decorrer da investigação, os princípios e os principais debates éticos na área das tecnologias digitais
OA3 Definir o problema central de investigação
OA4 Criar as perguntas de investigação e desenvolver de forma fundamentada as hipóteses de investigação
OA5 Conhecer e saber aplicar metodologias e ferramentas de revisão sistemática da literatura e análise bibliomátrica
OA6 Avaliar as metodologias de desenho da investigação e saber aplicar a mais apropriada tendo em atenção as perguntas e as hipóteses de investigação
OA7 Avaliar as práticas da escrita de artigo científico e apresentação científica e saber aplicar ao caso concreto da investigação

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 learning outcomes are:
LO1 Frame scientific research and understand the main research methods in digital technologies
LO2 Apply the principles and major ethical debates in the field of digital technologies during the course of the investigation
LO3 Define the central research problem
LO4 Create research questions and develop research hypotheses in a substantiated manner
LO5 Understand and know how to apply methodologies and tools for systematic literature review and bibliometric analysis
LO6 Evaluate research design methodologies and know how to apply the most appropriate one considering the research questions and hypotheses
LO7 Evaluate the practices of scientific article writing and scientific presentation and know how to apply them to the specific case of the investigation

4.2.11. Conteúdos programáticos (PT):
CP1:Investigação científica e seus principais métodos
CP2:Princípios e debates éticos transversais
CP3:Apresentações de temas e propostas de teses por Professores, Investigadores e Empresas
CP4:Problema, perguntas e hipóteses de investigação
CP5:Metodologias e ferramentas para revisão sistemática da literatura e análise bibliométrica
CP6:Metodologias de desenho da investigação
CP7:Escrita de artigo científico e apresentação científica
CP8:Apresentações individuais da componente metodológica dos projetos de tese

4.2.11. Conteúdos programáticos (EN):

PC1:Scientific research and its main methods
PC2:Cross-cutting ethical principles and debates
PC3:Presentations of themes and thesis proposals by Professors, Researchers and Companies
PC4:Research problem, questions and hypotheses
PC5:Methodologies and tools for systematic literature review and bibliometric analysis
PC6:Research design methodologies
PC7:Scientific paper writing and scientific presentation
PC8:Individual presentations of the methodological component of the thesis projects

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, analisar vários casos de estudo, aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico. O docente responsável e outros docentes e investigadores convidados, darão feedback (corretivo e/ou cognitivo) sobre os problemas, temas de investigação e estudos de caso. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação e desenvolvimento da capacidade criativa e de inovação, a unidade curricular adotará Design Thinking ao longo do ano.

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

The teaching methodologies were selected to correspond to the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with varying levels of teacher support and guidance, analyze various case studies, apply theoretical knowledge, and develop problem-solving and critical thinking skills. The responsible teacher and other invited teachers and researchers will provide feedback (corrective and/or cognitive) on problems, research topics, and case studies. This approach will allow students to establish connections between theoretical and practical knowledge, improving their understanding and application of the learned concepts. As a strategy for motivation and development of creative and innovative capacity, the course will adopt Design Thinking throughout the year.

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

A UC Metodologias de Investigação Aplicada adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Estudos de Caso, combinada com Aprendizagem Baseada em Problemas. Design Thinking será utilizada como estratégia de motivação, criatividade, pensamento inovador e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos e o conhecimento é visto como ferramenta de transformação das sociedades, devendo ser transferido e aplicado em diferentes contextos e com diferentes públicos (conhecimento aplicado).

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

The CU Applied Research Methodologies will adopt Case-Based Learning as the central teaching and learning methodology, combined with Problem-Based Learning. Design Thinking will be used as a strategy for motivation, creativity, innovative thinking, and student engagement. This pedagogical approach is articulated with ISCTE's pedagogical model because the student is considered an active agent in their learning process, knowledge is worked on as a tool for the construction and development of more knowledge and applied in various contexts, and knowledge is seen as a tool for societal transformation, which should be transferred and applied in different contexts and with different audiences (applied knowledge).

4.2.14. Avaliação (PT):

A avaliação inclui as os seguintes momentos, em modalidade de avaliação contínua:
- Participação (10%)
- Apresentação e discussão da proposta de tese e estratégia metodológica de pesquisa desenhada para o projeto de investigação na área do mestrado (20%, apresentação individual)
- Apresentação de um artigo da literatura selecionado pelo/a estudante, dentro to tópico da tese (20%, apresentação individual)
- Trabalho escrito com a proposta de tese, a descrição da estratégia metodológica a adotar no projeto de mestrado (50%, trabalho individual), com estrutura pré-definida pelo docente
A avaliação desta UC não contempla a realização de exame escrito final.

4.2.14. Avaliação (EN):

The evaluation includes the following moments, in continuous evaluation modality:
- Participation (10%)
- Presentation and discussion of the thesis proposal and methodological research strategy designed for the research project in the Master's area (20%, individual presentation).
- Presentation of an article from the literature selected by the student, within the topic of the thesis (20%, individual presentation)
- Written work with the thesis proposal, the description of the methodological strategy to be adopted in the master's project (50%, individual work), with a structure pre-defined by the teacher.
The assessment of this CU does not include the final written exam.

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, numa primeira fase enquadrar a investigação científica e compreender os principais métodos de investigação em tecnologias digitais e posteriormente, analisar, os princípios e os principais debates éticos na área das tecnologias digitais. Irão ainda aplicar conhecimentos teóricos e desenvolver competências de análise e pensamento crítico, necessários à identificação do problema central de investigação que irão endereçar durante o programa. Para esse efeito, o docente responsável e outros docentes, investigadores convidados e empresas, que irão apresentar ideias e temas de investigação sob a forma de estudos de caso, darão feedback (corretivo e/ou cognitivo) sobre os mesmos e as correspondentes propostas de tópicos de investigação. Os estudantes terão acesso a informações detalhadas sobre o caso e tema de investigação, incluindo contexto, personagens e problemas específicos a serem resolvidos. Seguirão uma sequência predefinida de análise, discussão e abordagem do caso. Escolhido o tema de investigação e o orientador, os alunos realizarão então uma aprendizagem baseada em problemas, aplicada ao seu tópico específico, exigindo pesquisa, análise crítica e um caminho para a solução, baseado na procura ativa do conhecimento necessário. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, e endereçar o seu tema de investigação. De seguida, os estudantes farão o enunciado das perguntas de investigação e o consequente levantamento, de forma fundamentada, das hipóteses de investigação que irão demonstrar durante o programa. Na fase seguinte, irão conhecer e saber aplicar na prática, metodologias e ferramentas de revisão sistemática da literatura e análise bibliométrica, de modo a identificar as oportunidades mais promissoras e relevantes de inovação científica. Segue-se a compreensão e avaliação das metodologias de desenho da investigação e a sua aplicação ao caso concreto da investigação de cada estudante, tendo em atenção as respetivas perguntas e hipóteses de investigação. Por fim, cada estudante deverá conhecer e saber avaliar as práticas da escrita de artigo científico e apresentação científica, mais apropriadas para o seu caso. Como estratégia de motivação e desenvolvimento da capacidade criativa e de inovação, a unidade curricular adotará Design Thinking ao longo do ano. Com esta metodologia de resolução de problemas, centrada no ser humano, os estudantes utilizarão ferramentas como a empatia, a experimentação, a ideação, a iteração e a prototipagem rápida, para criar soluções inovadoras, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies were selected in order to correspond to the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance throughout the CU that will allow them, in a first phase, to frame scientific research and understand the main research methods in digital technologies and later, to analyse the principles and the main ethical debates in the area of digital technologies. They will also apply theoretical knowledge and develop analytical and critical thinking skills, necessary to identify the central research problem that they will address during the programme. To this end, the lead lecturer and other lecturers, guest researchers and companies, who will present research ideas and topics in the form of case studies, will provide feedback (corrective and/or cognitive) on them and the corresponding research topic proposals. Students will have access to detailed information about the case and research topic, including context, characters and specific problems to be solved. They will follow a predefined sequence of analysing, discussing and addressing the case. Once the research topic and supervisor have been chosen, students will then undertake problem-based learning, applied to their specific topic, requiring research, critical analysis and a pathway to solution, based on the active search for the necessary knowledge. This approach will allow students to make connections between theoretical and practical knowledge, and address their research topic. Next, students will state their research questions and the consequent survey, in a reasoned manner, of the research hypotheses that they will demonstrate during the programme. In the next phase, they will know and know how to apply in practice, methodologies and tools of systematic literature review and bibliometric analysis, in order to identify the most promising and relevant opportunities for scientific innovation. This is followed by the understanding and evaluation of research design methodologies and their application to the specific case of each student's research, taking into account the respective research questions and hypotheses. Finally, each student should know and be able to evaluate the practices of scientific article writing and scientific presentation, most appropriate for their case. As a strategy to motivate and develop creative and innovative capacity, the curricular unit will adopt Design Thinking throughout the year. With this human-centred problem-solving methodology, students will use tools such as empathy, experimentation, ideation, iteration and rapid prototyping to create innovative solutions, ensuring their involvement throughout the CU. Translated with www.DeepL.com/Translator (free version)

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

Kumar, R. (2014), Research Methodology, 4th Ed., SAGE, 2011, ISBN 978-1-84920-301-2
Dawson, C. (2009), Introduction to Research Methods, 4th Ed., Howtobooks, 2009, ISBN 978-1-84528-367-4
Jackson, S.L. (2008), Research Methods, a modular approach, Wadsworth, 2008
Dodig, G. (2003), Theory of Science, Maelardaen University Sweden, 2003
Christopher Turk; John Kirkman. 1989. Effective Writing: Improving Scientific, Technical, and Business Communication. E & FN Spon, 1989
Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. (2009), The PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med. 2009, 6, e1000097

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

Kumar, R. (2014), Research Methodology, 4th Ed., SAGE, 2011, ISBN 978-1-84920-301-2
Dawson, C. (2009), Introduction to Research Methods, 4th Ed., Howtobooks, 2009, ISBN 978-1-84528-367-4
Jackson, S.L. (2008), Research Methods, a modular approach, Wadsworth, 2008
Dodig, G. (2003), Theory of Science, Maelardaen University Sweden, 2003
Christopher Turk; John Kirkman. 1989. Effective Writing: Improving Scientific, Technical, and Business Communication. E & FN Spon, 1989
Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. (2009), The PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med. 2009, 6, e1000097

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Trabalho de Projecto em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (PT):

Trabalho de Projecto em Cibersegurança e Resiliência

4.2.1. Designação da unidade curricular (EN):

Research Project in Cybersecurity and Resiliency

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

480

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

480

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

Anual

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

Annual

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

1,050.0

4.2.5. Horas de contacto:

Presencial (P) - S-32.0; OT-8.0
Assíncrona a distância (AD) - S-8.0
Síncrona a distância (SD) - S-8.0

4.2.6. % Horas de contacto a distância:

28.57%

4.2.7. Créditos ECTS:

42.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• *Carlos José Corredoura Serrão - 56.0h*

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
• *Carlos Eduardo Dias Coutinho - 8.0h*
• *João Carlos Amaro Ferreira - 8.0h*
• *João Pedro Calado Barradas Branco Pavia - 8.0h*
• *Margarida Tavares Peralta Couto dos Santos - 8.0h*
• *Maria do Rosário Domingos Laureano - 8.0h*

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
OA1: Adquirir a capacidade de efetuar um trabalho de projecto de forma independente.
OA2: Selecionar uma ou mais abordagens metodológicas para a concretização do projeto
OA3: Saber validar os artefactos que constituem a solução para o problema escolhido e identificar as correspondentes ameaças à validade.
OA4: Ter aprendido sobre a complexidade e o modo de preparar um trabalho de projecto bem sucedido e de elevada qualidade, tanto na forma como no conteúdo.
OA5: Ser capaz de apresentar um problema técnico-científico e a sua motivação, para produzir soluções adequadas e validadas.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Acquire the capacity to undertake an independent research project.
LO2: Select one or more methodological approaches to achieve the project
LO3: Know how to validate the artifacts that constitute the solution to the chosen problem and identify the corresponding validity threats.
LO4: Have learned about the complexity and how to prepare a successful research project with high quality, both in form and content.
LO5: To be able to present a technical-scientific problem and its motivation, to produce appropriate and validated solutions.

4.2.11. Conteúdos programáticos (PT):
1: Etapas e processos na elaboração de um projecto de investigação (P.I.) :
Estrutura e objectivos de um P.I
Fases de desenvolvimento de um P.I
Orientações normativas para a elaboração de um P.I.
2: Delineamento da estratégia metodológica:
Em que consiste uma estratégia metodológica: articulação entre conceptualização e operacionalização
Principais opções metodológicas: métodos quantitativos e qualitativos
Delineamento do plano de estudo
Planeamento do processo de análise de dados
Questões éticas na investigação em Cibersegurança e Resiliência
3: Análise e interpretação dos resultados
Análise de dados
Discussão e conclusões
Normas de redacção de escrita científica
Referências, anexos
4. Preparação para defesa oral

4.2.11. Conteúdos programáticos (EN):
1. Steps and processes for designing a research project.
Structure and goals of the research project.
Development stages of a research project.
Norms for the elaboration of a research project.
2. Outlining the methodological strategy:
What is the methodological strategy: the link between conceptual and operationalization stages
Main methodological options: quantitative and qualitative
Research design
Planning data analysis
Ethical Issues in Cybersecurity and Resiliency research
3: Analysing and presenting results
Data analysis
Discussion and conclusions
Norms for scientific writing
References and appendices
4: Preparing the public defense of the Applied Project

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

Nesta UC os conteúdos programáticos decorrem da natureza e exigência da própria dissertação, nos moldes em que uma definição legal e uma boa prática académica entendem uma dissertação.
O principal objetivo da UC é permitir aos alunos a aquisição de competências de investigação. Estas competências devem ser materializadas na elaboração de uma dissertação. Naturalmente que existe uma total convergência entre os conteúdos programáticos e os objectivos da UC.
Com efeito, todos os tópicos dos conteúdos programáticos estão subordinados à utilidade que têm como instrumentos para viabilizar os objectivos da UC.
O programa de trabalhos do aluno é especificamente concebido para lhe permitir uma agenda de investigação com sucesso, que se consubstancia numa dissertação ou projeto.

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

In this CU the syllabus stems from the nature and requirement of which is itself a dissertation, in a way that a legal definition and a good academic practice understand a dissertation.
The main CU objective is enabling the students to acquire research skills. These skills must be materialized in the preparation of a dissertation. Naturally there is a complete convergence between syllabus content and objectives of the CU.
Indeed, all syllabus topics are subordinated to the utility that they have as tools to enable the objectives of the CU.
The student's work program is specifically designed to allow him a successfully research agenda, that is embodied in a dissertation or project.

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

São utilizadas as seguintes metodologias:
- componente expositiva, para apresentação dos conceitos básicos de cada um dos temas abordados.
- componente participativa, com análise e resolução de exercícios práticos.
- componente de orientação e discussão individual dos projectos de "Trabalho de Projeto".
- componente de apresentação do trabalho desenvolvido a nível individual e apresentado ao longo das sessões de supervisão e de seminário organizadas em três blocos de sessões.

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

Several learning methodologies will be used:- expositive: presentation of basic concepts and theories of each topic addressed.
- participatory: analyses and resolution of practical problems.
- individual supervision and discussion: of project research.
- presentation of topics of research by the teachers of UC.
The CU is also based on the work developed individually by students and presented during the sessions of supervision and workshop organized in three blocks of sessions.

4.2.14. Avaliação (PT):
O Trabalho de Projeto de mestrado deverá ser defendido em provas públicas onde serão avaliadas as componentes técnica, a forma do trabalho escrito e a apresentação e defesa pública.
Critérios de avaliação:
a. componente técnica (30%)
b. componente formal e apresentação escrita (20%)
c. apresentação e defesa pública (20%)
d. processo (orientador) (30%)

4.2.14. Avaliação (EN):
The Applied Project should be defended in public, where the following components will be evaluated: a) technical component; b) written format and c) oral presentation and arguments.
Evaluation Criteria:
a. technical component (30%)
b. formal written component and presentation (20%)
c. public presentation and defense (20%)
d. process (evaluated by supervisor) (30%)

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-aprendizagem visam o desenvolvimento das principais competências de aprendizagem dos alunos que permitam cumprir com cada um dos objectivos de aprendizagem, pelo que, a seguir apresentam-se as principais interligações entre as metodologias de ensino-aprendizagem e os respectivos objectivos de aprendizagem (OA):
1. Orientação tutorial: Transversal a todos os AO.
2. Trabalho Autónomo: Transversal a todos os AO.

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

The learning-teaching methodologies are aimed at the development of the students' main learning competences that allow to fulfill each of the learning goals, therefore, below it is presented the main interlinks between the learning-teaching methodologies and the respective learning goals (LG):
1. Tutorial classes: Transversal to all the LG.
2. Autonomous Work: Transversal to all the LG.

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

--

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

--

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Verificação da Segurança e Resiliência de Sistemas

4.2.1. Designação da unidade curricular (PT):

Verificação da Segurança e Resiliência de Sistemas

4.2.1. Designação da unidade curricular (EN):

System Security and Resilience Verification

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

480

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

480

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) - TP-4.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-8.0; OT-1.0

4.2.6. % Horas de contacto a distância:

84.00%

4.2.7. Créditos ECTS:

6.0

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

• Carlos Eduardo Dias Coutinho - 24.0h

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):
OA1: Compreender a importância da verificação e validação da segurança dos sistemas.
OA2: Familiarizar-se com metodologias e frameworks de avaliação de segurança.
OA3: Desenvolver competências na auditoria de sistemas e na identificação de vulnerabilidades.
OA4: Aprender a realizar testes de penetração e testes de âmbito.
OA5: Adquirir conhecimentos de metodologias e ferramentas de testes de penetração, para diferentes tipos de sistemas e aplicações.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
LO1: Understand the importance of systems security verification and validation.
LO2: Familiarize with security assessment methodologies and frameworks.
LO3: Develop skills in system auditing and identifying vulnerabilities.
LO4: Learn how to conduct penetration testing and scoping tests.
LO5: Acquire knowledge of penetration testing methodologies and tools, for different types of systems and applications.

4.2.11. Conteúdos programáticos (PT):
CP1: Introdução à Verificação e Validação da Segurança de Sistemas
CP2: Metodologias de Avaliação de Segurança
CP3: Auditoria de Sistemas
CP4: Fundamentos de Testes de Intrusão
CP5: Metodologias de Testes de Intrusão
CP6: Testes de Segurança de Redes com e sem Fios
CP7: Testes de Segurança de Aplicações Web e Móveis
CP8: Produção de Relatórios de Resultados e Recomendações

4.2.11. Conteúdos programáticos (EN):
PC1: Introduction to Systems Security Verification and Validation
PC2: Security Assessment Methodologies
PC3: System Auditing
PC4: Penetration Testing Fundamentals
PC5: Penetration Testing Methodologies
PC6: Wired and Wireless Networks Security Testing
PC7: Web and Mobile Applications Security Testing
PC8: Reporting and Remediation

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

As metodologias de ensino foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente, realizar vários problemas (laboratórios), aplicar conhecimentos teóricos e desenvolver competências de resolução de problemas e pensamento crítico, e realizar um projeto final. O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas desenvolvidas. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, melhorando a compreensão e a aplicação dos conceitos aprendidos. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos à medida que as diferentes tarefas propostas aos alunos forem sendo concluídas com sucesso.

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

The teaching methodologies have been selected to match the learning objectives of the course. Through a combination of synchronous and asynchronous online learning moments, students will carry out tasks with different levels of support and teacher guidance, perform various problems (labs), apply theoretical knowledge and develop problem-solving and critical thinking skills, and carry out a final project. The lecturer will provide feedback (corrective and/or cognitive) on the tasks developed. This approach will allow students to establish connections between theoretical and practical knowledge, improving the understanding and application of the concepts learnt. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded as the different tasks proposed to students are successfully completed.

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

A UC de Verificação da Segurança e Resiliência de Sistemas adotará como metodologia de ensino e aprendizagem central a Aprendizagem Baseada em Tarefas, combinada com Aprendizagem Baseada em Projetos e a Aprendizagem Baseada em Problemas. A gamificação será utilizada como estratégia de motivação e envolvimento dos estudantes. Esta abordagem pedagógica está articulada com o modelo pedagógico do Iscte porque o estudante é considerado um agente ativo no seu processo de aprendizagem, o conhecimento é trabalhado como uma ferramenta para a construção e desenvolvimento de mais conhecimento e aplicado em diversos contextos.

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

The UC on System Security System Security and Resilience Verification will adopt as core teaching and learning methodology Task-Based Learning, combined with Project-Based Learning and Problem-Based Learning. Gamification will be used as a strategy for student motivation and engagement. This pedagogical approach is articulated with the ISCTE pedagogical model because the student is considered an active agent in his/her learning process, knowledge is worked as a tool for the construction and development of more knowledge and applied in various contexts.

4.2.14. Avaliação (PT):

Avaliação periódica:
Realização de diversos mini-testes de avaliação ao longo do semestre, contando com um total de 30% para a avaliação final - cada mini-teste tem uma nota mínima de 8 valores. Realização de um conjunto de atividades práticas propostas (laboratórios) em grupo, que contam com 40% para a avaliação final. Realização de projeto final colaborativo (em grupo) com apresentação final. O projeto terá uma ponderação total de 30%, em que a apresentação terá uma ponderação de 10%.

Avaliação por exame (1ª Época, 2ª Época):
Exame presencial (100% da nota final)

4.2.14. Avaliação (EN):

Periodic assessment:
Completion of several mini-assessment tests throughout the semester, counting a total of 30% for the final assessment - each mini-test has a minimum grade of 8. Realisation of a set of proposed practical group activities (laboratories), which count for 40% for the final assessment. Realisation of a final collaborative project (in group) with final presentation. The project will have a total weighting of 30%, where the presentation will have a weighting of 10%.

Assessment by exam (1st Season, 2nd Season):
Face-to-face exam (100% of the final grade)

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 foram selecionadas de forma a corresponder aos objetivos de aprendizagem da UC. Através de uma combinação de momentos de aprendizagem online síncrona e assíncrona, os estudantes irão realizar tarefas com diferentes níveis de apoio e orientação docente ao longo da UC que lhes permitirá, perceber e compreender a importância das organizações realizarem auditorias de segurança, que lhes permitam efetuar a verificação e validação da seguarança dos seus diversos sistemas. Por outro lado, os alunos irão igualmente familiarizar-se com metodologias e técnicas que lhes permitem realizar testes de intrusão, numa ótica de "red team", assim como perceberem quais as medidas de mitigação para resolução das vulnerabilidades encontradas, assumindo um papel de uma equipa "blue team". O docente dará feedback (corretivo e/ou cognitivo) sobre as tarefas realizadas pelos alunos. Os estudantes irão ainda realizar projetos específicos e realizar laboratórios relacionados com os diferentes temas que serão abordados na unidade curricular. No caso dos projetos os estudantes terão acesso a todos os detalhes do trabalho a realizar, assim como as ferramentas que devem ser usadas e os detalhes dos principais resultados a obter. Esta abordagem permitirá que os estudantes estabeleçam conexões entre os conhecimentos teóricos e práticos, permitindo-lhes perceber e aprender como as auditorias de segurança, nomeadamente os testes de intrusão, podem contribuir de forma decisiva para a prevenção de problemas de cibersegurança e aumentar a ciber-resiliência das organizações. Como estratégia de motivação, a unidade curricular incluirá a gamificação ao longo do semestre, onde serão atribuídos pontos aos estudantes à medida que as diferentes atividades forem concluídas com sucesso, garantindo o seu envolvimento ao longo da UC.

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

The teaching methodologies have been selected in order to match the learning objectives of the CU. Through a combination of synchronous and asynchronous online learning moments, students will perform tasks with different levels of support and teacher guidance throughout the CU that will allow them to understand the importance of organisations performing security audits, which allow them to verify and validate the security of their various systems. On the other hand, students will also familiarise themselves with methodologies and techniques that allow them to perform intrusion tests, from a "red team" perspective, as well as to understand the mitigation measures to resolve the vulnerabilities found, assuming a role of a "blue team". The teacher will give feedback (corrective and/or cognitive) on the tasks performed by the students. Students will also carry out specific projects and perform laboratories related to the different topics that will be addressed in the curricular unit. In the case of projects, students will have access to all the details of the work to be carried out, as well as the tools to be used and the details of the main results to be obtained. This approach will allow students to establish connections between theoretical and practical knowledge, allowing them to understand and learn how security audits, namely intrusion testing, can contribute decisively to the prevention of cybersecurity problems and increase the cyber resilience of organisations. As a motivation strategy, the curricular unit will include gamification throughout the semester, where points will be awarded to students as the different activities are successfully completed, ensuring their involvement throughout the CU.

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

Diogenes, Y., & Ozkaya, D. E. (2018). Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing.
Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd edition). Syngress.
Oriyano, S.-P. (2016). Penetration Testing Essentials (1st edition). Sybex.
Rehberger, J. (2020). Cybersecurity Attacks – Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage. Packt Publishing.
Sehgal, K., & Thymianis, N. (2023). Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization. Packt Publishing.
Sharma, H., & Singh, H. (2018). Hands-On Red Team Tactics: A practical guide to mastering Red Team operations. Packt Publishing.
Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking (1st edition). No Starch Press.

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

Diogenes, Y., & Ozkaya, D. E. (2018). Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing.
Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (2nd edition). Syngress.
Oriyano, S.-P. (2016). Penetration Testing Essentials (1st edition). Sybex.
Rehberger, J. (2020). Cybersecurity Attacks – Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage. Packt Publishing.
Sehgal, K., & Thymianis, N. (2023). Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization. Packt Publishing.
Sharma, H., & Singh, H. (2018). Hands-On Red Team Tactics: A practical guide to mastering Red Team operations. Packt Publishing.
Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking (1st edition). No Starch Press.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

4.3. Unidades Curriculares (opções)

Mapa IV - Dissertação ou Trabalho de Projecto em Cibersegurança e Resiliência

4.3.1. Designação da unidade curricular (PT):

Dissertação ou Trabalho de Projecto em Cibersegurança e Resiliência

4.3.1. Designação da unidade curricular (EN):

Master Dissertation or Research Project in Cybersecurity and Resiliency

4.3.2. Sigla da área científica em que se insere (PT):
480

4.3.2. Sigla da área científica em que se insere (EN):
480

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

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

4.3.4. Horas de trabalho (número total de horas de trabalho):
1,050.0

4.3.5. Horas de contacto:
Presencial (P) - OT-8.0
Assíncrona a distância (AD) - S-40.0
Síncrona a distância (SD) - S-8.0

4.3.6. % Horas de contacto a distância:
85.71%

4.3.7. Créditos ECTS:
42.0

4.3.8. Unidades Curriculares filhas:
- *Dissertação em Cibersegurança e Resiliência - 42.0 ECTS*
- *Trabalho de Projecto em Cibersegurança e Resiliência - 42.0 ECTS*

4.3.9. Observações (PT):
O estudante deve optar entre a modalidade de Dissertação e Trabalho de Projecto

4.3.9. Observações (EN):
The student must choose between the Dissertation and the Research Project

Mapa IV - Optativa Livre

4.3.1. Designação da unidade curricular (PT):
Optativa Livre

4.3.1. Designação da unidade curricular (EN):
Free Optional Course

4.3.2. Sigla da área científica em que se insere (PT):
n.e.

4.3.2. Sigla da área científica em que se insere (EN):
n.s.

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):
150.0

4.3.5. Horas de contacto:
Presencial (P) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.3.6. % Horas de contacto a distância:
92.00%

4.3.7. Créditos ECTS:
6.0

4.3.8. Unidades Curriculares filhas:
• Optativa - 6.0 ECTS

4.3.9. Observações (PT):
Optativa - Tempo médio de contato | Lista a definir anualmente

4.3.9. Observações (EN):
Optional - Medium contact hours | List to be defined annually

Mapa IV - Optativa Livre

4.3.1. Designação da unidade curricular (PT):
Optativa Livre

4.3.1. Designação da unidade curricular (EN):
Free Optional Course

4.3.2. Sigla da área científica em que se insere (PT):
n.e.

4.3.2. Sigla da área científica em que se insere (EN):
n.s.

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):
150.0

4.3.5. Horas de contacto:
Presencial (P) - TP-2.0
Assíncrona a distância (AD) - TP-12.0
Síncrona a distância (SD) - TP-10.0; OT-1.0

4.3.6. % Horas de contacto a distância:
92.00%

4.3.7. Créditos ECTS:
6.0

4.3.8. Unidades Curriculares filhas:
• *Optativa - 6.0 ECTS*

4.3.9. Observações (PT):
Optativa - Tempo médio de contato | Lista a definir anualmente

4.3.9. Observações (EN):
Optional - Medium contact hours | List to be defined annually

4.4. Plano de Estudos

Mapa V - Plano de Estudos - 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):
Plano de Estudos

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):
Study Plan

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
Arquiteturas de Segurança e Modelos de Confiança Zero	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Criptografia para Cibersegurança e Resiliência	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Fundamentos de Gestão da Cibersegurança e Resiliência	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Gestão do Ciber-risco para Resiliência	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Segurança e Resiliência de Infraestruturas e Redes de Comunicação	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Fator Humano na Cibersegurança e Resiliência	310	Semestral 2ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Incidentes de Cibersegurança e Resiliência	480	Semestral 2ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Optativa Livre	n.e.	Semestral 2ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%	UC de Opção	Não	6.0
Segurança e Resiliência de Software e Aplicações	480	Semestral 2ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0

Verificação da Segurança e Resiliência de Sistemas	480	Semestral 2ºS	150.0	P: TP-4.0 AD: TP-12.0 SD: OT-1.0; TP-8.0	84.00%		Não	6.0
Total: 10								

4.4.2. Ano curricular:

2

4.4.3. Plano de Estudos

Unidade Curricular	Área Científica	Duração	Horas Trabalho	Horas Contacto	% HC a distância	Tipo	Opcional	ECTS
Dissertação ou Trabalho de Projecto em Cibersegurança e Resiliência	480	Anual	1,050.0	P: OT-8.0 AD: S-40.0 SD: S-8.0	85.71%	UC de Opção	Não	42.0
Optativa Livre	n.e.	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%	UC de Opção	Não	6.0
Resiliência e Continuidade do Negócio	480	Semestral 1ºS	150.0	P: TP-2.0 AD: TP-12.0 SD: OT-1.0; TP-10.0	92.00%		Não	6.0
Seminário de Investigação em Cibersegurança e Resiliência	480	Semestral 1ºS	150.0	AD: TP-12.0 SD: OT-2.0; TP-12.0	100.00%		Não	6.0
Total: 4								

4.5. Metodologias e Fundamentação

4.5.1.1. Justificar o desenho curricular. (PT)

O mestrado está organizado em 4 semestres, dois dedicados à formação dos estudantes através de múltiplas unidades curriculares com os conteúdos específicos do mestrado e dois semestres finais dedicados à realização do projeto/dissertação de mestrado. As seguintes unidades curriculares são propostas:
- Fundamentos de Gestão da Cibersegurança e Resiliência: visa introduzir os principais conceitos de cibersegurança e resiliência, abordar os principais quadros de referência e normas, e apresentar o principal quadro regulamentar e legislativo na área.
- Segurança e Resiliência de Infraestruturas e Redes de Comunicação: aborda as questões relacionadas com as infraestruturas ("on-prem" e na cloud) digitais e ciber-físicas que suportam as organizações dos nossos dias e das respetivas redes de comunicação, apresentando as principais ameaças e as soluções e estratégias para garantir a sua segurança e resiliência.
- Arquiteturas de Segurança e Modelos Zero Trust: apresenta as arquiteturas de segurança (incluindo zero-trust) alinhadas com as organizações como forma de alinhar as medidas de segurança e de confiança mais adequadas para as mesmas.
- Criptografia para Cibersegurança e Resiliência: introduz os principais conceitos de criptografia, numa vertente aplicada à cibersegurança, principalmente no que respeita à proteção robusta e resiliente de dados e informação.
- Gestão do Ciber-risco para Resiliência: aborda os principais referenciais para a identificação, análise e gestão do risco para cibersegurança e resiliência.
- Incidentes de Cibersegurança e Resiliência: apresenta as metodologias e ferramentas de recolha, identificação e análise de ameaças à cibersegurança e resiliência das organizações e identificação das estratégias de resposta para tratar os principais incidentes que podem afetar a cibersegurança e resiliência das organizações.
- Fator Humano na Cibersegurança e Resiliência: aborda as questões relacionadas com as pessoas, o comportamento das mesmas e o impacto que isso pode ter na cibersegurança e resiliência das organizações.
- Segurança e Resiliência de Software e Aplicações: aborda o tema da segurança do software e das múltiplas aplicações nas organizações, relativamente aos diferentes processos de desenvolvimento e manutenção das mesmas, identificação dos principais problemas e riscos, e correção dos mesmos.
- Verificação da Segurança e Resiliência de Sistemas: aborda a temática da verificação e análise de segurança de sistemas, através de metodologias e técnicas de análise para procurar identificar vulnerabilidades.
- Resiliência e Continuidade do Negócio: aborda as questões que permitem garantir e manter a continuidade do negócio das organizações, identificando as funções de negócio mais críticas e medindo o impacto que os ciber-

ataques podem ter nas mesmas, e adotando as medidas adequadas para impedir a indisponibilidade dessas funções.

4.5.1.1. Justificar o desenho curricular. (EN)

The master's degree is organized in 4 semesters, two dedicated to the training of students through multiple course units with the specific contents of the master's degree and two final semesters dedicated to the realization of the master's project/dissertation. The following course units are proposed:
- Fundamentals of Cybersecurity and Resilience Management: aims to introduce the main concepts of cybersecurity and resilience, address the main frameworks and standards, and present the main regulatory and legislative framework in the area.
- Security and Resilience of Infrastructures and Communication Networks: addresses issues related to the digital and cyber-physical infrastructures (on-prem and cloud) that support today's organizations and their communication networks, presenting the main threats and the solutions and strategies to ensure their security and resilience.
- Security Architectures and Zero Trust Models: presents security architectures (including zero-trust) aligned with organizations as a way to align the most appropriate security and trust measures for them.
- Cryptography for Cybersecurity and Resilience: introduces the main concepts of cryptography, in an applied aspect to cybersecurity, mainly regarding the robust and resilient protection of data and information.
- Cyber-risk Management for Resilience: addresses the main references for the identification, analysis and management of risk in cybersecurity and resilience.
- Cybersecurity and Resilience Incidents: presents the methodologies and tools for collecting, identifying and analyzing threats to cybersecurity and resilience of organizations and identifying response strategies to address major incidents that can affect the cybersecurity and resilience of organizations.
- Human Factor in Cybersecurity and Resilience: addresses the issues related to people, their behavior and the impact this can have on the cybersecurity and resilience of organizations.
- Software and Application Security and Resilience: addresses the topic of software and application security in organizations, regarding the different development and maintenance processes, identification of the main problems and risks, and their correction.
- Systems Resilience Verification and Validation: addresses the topic of systems security verification and analysis, using methodologies and analysis techniques to seek to identify vulnerabilities.
- Resilience and Business Continuity: addresses the issues that allow ensuring and maintaining the business continuity of organizations, identifying the most critical business functions and measuring the impact that cyber-attacks can have on them, and adopting the appropriate measures to prevent the unavailability of these functions.

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

65.0

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

Tendo em vista o desenvolvimento de conhecimentos e competências pelos estudantes, bem como a sua relação com os conteúdos disciplinares, será privilegiada a utilização de metodologias ativas de aprendizagem, tanto nas UC em regime presencial como a distância (EaD). Dependendo dos objetivos de aprendizagem, o docente poderá integrar várias metodologias ativas, nomeadamente:
· Aprendizagem baseada em projetos: Desenvolvimento de projetos online onde os estudantes aplicam o conhecimento em contextos reais. Os estudantes colaboram virtualmente, pesquisam, resolvem problemas e criam produtos e/ou serviços.
· Aprendizagem baseada em problemas: Os estudantes resolvem problemas a partir de investigação e colaboração online. Os problemas exigem pesquisa, análise crítica e descrição de soluções. São os próprios estudantes que identificam o que precisam de aprender para resolver o problema e procuram ativamente o conhecimento necessário.
· Aprendizagem baseada em estudos de caso: Utilização de casos reais ou fictícios como ponto de partida para a aprendizagem. Os estudantes têm acesso a informações detalhadas sobre o caso, incluindo o contexto, as personagens e os problemas específicos a resolver. Seguem um processo predefinido de análise, discussão e resolução do caso.
· Aprendizagem baseada em tarefas: Os estudantes realizam tarefas definidas de acordo com a ordem definida pelo docente, com grau de dificuldade crescente e nível de apoio decrescente em cada tema. Os objetivos de cada tarefa são claros para os estudantes e no final de cada tarefa o docente fornece feedback.
· Ensino por tutoria online: Há uma grande ênfase na interação entre o estudante e o docente. Cada estudante recebe orientação e apoio individualizado por um docente à distância (síncrono e/ou assíncrono). O docente esclarece as dúvidas, acompanha o progresso do estudante e fornece orientação específica de acordo com as suas necessidades de aprendizagem.
· Aprendizagem adaptativa: O ensino é personalizado de acordo com as necessidades e o progresso individual de cada estudante. Com base em Inteligência Artificial, outros meios tecnológicos ou humanos, há um diagnóstico de necessidade de formação e posterior disponibilização de conteúdo e atividades personalizadas, ajudando o estudante a aprender ao seu próprio ritmo.
· Aprendizagem colaborativa: Abordagem centrada na interação entre os estudantes, promovendo a colaboração para construir conhecimento em conjunto. A participação ativa é incentivada através de debates, discussões e reflexão sobre problemas reais, visando à criação de uma compreensão partilhada pelo grupo.
· Ensino combinado: São combinados elementos de metodologias ativas apropriadas para ensino presencial e para

EaD, aproveitando as vantagens de cada abordagem.
· Microaprendizagem: Os conteúdos e as atividades são divididos em segmentos muito pequenos (vídeos breves, sínteses de conteúdos, quizzes interativos), permitindo que o estudante aprenda em momentos de disponibilidade restrita e em dispositivos móveis, onde a participação nas atividades requer pouca criação e edição de conteúdos.
Durante a implementação de metodologias ativas de aprendizagem, o docente deve selecionar recursos e estratégias específicas que contribuam para o aumento do envolvimento dos estudantes, estimulando a sua curiosidade, interesse e motivação. Destacam-se as seguintes estratégias de envolvimento na aprendizagem:
· Gamificação: Utilização de elementos de jogos para aumentar a motivação e o envolvimento no processo de ensino-aprendizagem. Os estudantes poderão ganhar pontos e emblemas, desbloquear conquistas e competir com os colegas em desafios, individuais e em equipas.
· Tutoria entre pares: Estudantes colaboram entre si, onde um dos estudantes com mais conhecimento num determinado conteúdo irá apoiar o(s) colega(s) (poderá incluir preparação prévia), em modo síncrono ou assíncrono. Permite que os estudantes se apoiem mutuamente, partilhem conhecimentos e desenvolvam o sentido de pertença de comunidade.
· Metodologias imersivas: Utilização de simulações e realidade virtual para criar experiências imersivas de aprendizagem, explorar ambientes virtuais e desenvolver experiências simuladas, permitindo uma aprendizagem mais interativa e contextualizada.
· Design Thinking: Metodologia de resolução de problemas complexos a partir da criatividade, da empatia e da iteração. Os estudantes são encorajados a identificar desafios, recolher informações, gerar ideias, e criar e testar protótipos que solucionem problemas reais, utilizando ferramentas colaborativas online.
· Storytelling: O docente cria uma narrativa que relaciona os conteúdos a serem aprendidos com situações reais, experiências pessoais ou histórias fictícias. Essas histórias podem ser transmitidas a partir de diversos recursos tais como vídeos, podcasts, textos ou apresentações interativas.
· Sala de aula invertida: O docente disponibiliza conteúdos através de diferentes suportes (aulas gravadas, artigos e outros materiais como PowerPoint semelhantes aos que apoiavam as aulas "tradicionais" de pendor mais expositivo.) em trabalho autónomo os estudantes familiarizam-se com esses conteúdos e depois em sala de aula virtual, envolvendo momentos de interatividade com docente e colegas, executam as aprendizagens em atividades concretas (grupos de discussão; exercícios em grupo; projetos, etc.).
As comunidades virtuais de aprendizagem ocupam um papel relevante no modelo pedagógico do Iscte para o EaD. Nesse sentido, promove-se a implementação de comunidades virtuais interativas, proporcionando aos estudantes um espaço de participação, colaboração, partilha de experiências e aprendizagem mútua em diversos domínios. Pretende-se, assim, incentivar a cooperação e empatia entre os estudantes, fortalecendo o sentimento de pertença à comunidade académica do Iscte. Além disso, estimula-se a construção conjunta do conhecimento em ambientes virtuais de aprendizagem colaborativos, fomentando a troca de ideias, a iniciativa na procura e prestação de apoio e a criação de sinergias entre os estudantes. Para alcançar este objetivo, deverão ser promovidas atividades em grupo que fortaleçam o sentimento de pertença e impulsionem a aprendizagem colaborativa, permitindo que os estudantes desenvolvam competências essenciais para o trabalho em equipa e o crescimento académico. Com estas iniciativas, espera-se proporcionar uma experiência de aprendizagem enriquecedora, que valorize a participação ativa dos estudantes e o reforço das suas competências sociais e académicas.
Os docentes desempenham um papel crucial de supervisão, orientação e monitorização do processo de ensino-aprendizagem. Para o efeito deverão orientar-se pelos seguintes princípios de atuação:
• Comunicação clara e acessível. Os docentes devem fornecer instruções claras sobre as atividades, prazos e expectativas de desempenho dos estudantes. Devem também estar disponíveis para esclarecer dúvidas e apoiar os estudantes ao longo do curso, através dos meios e em momentos claramente identificados no planeamento do curso.
• Interação, monitorização e feedback frequentes. A interação com os estudantes é fundamental para o sucesso de um ambiente de aprendizagem colaborativo. Os docentes devem incentivar a participação nos fóruns de discussão, realizar sessões de chat ou videoconferência, fornecer feedback frequente sobre o desempenho académico dos estudantes e monitorizar o envolvimento dos estudantes nas atividades.
• Sensibilidade à diversidade e inclusão. Os docentes devem estar atentos à diversidade dos estudantes e criar um ambiente inclusivo e respeitador. Devem disponibilizar soluções que permitam acomodar diferentes necessidades e níveis de progresso na aprendizagem.
• Melhoria contínua e feedback dos estudantes. Os docentes devem estar recetivos ao feedback dos estudantes e utilizar essa informação para reflexão e melhoria da qualidade do ensino e da formação. A procura constante por melhorias e a adaptação às necessidades dos estudantes são fundamentais para o aperfeiçoamento contínuo dos cursos de EaD.

Todas as UC aplicarão diferentes elementos de avaliação, tendo em vista uma compreensão mais abrangente do desempenho dos estudantes, respeitando o Regulamento Geral de Avaliação de Conhecimentos e Competências do Iscte.
Deverão ser previstos diferentes tipos de avaliação – diagnóstica, formativa e sumativa – nas várias fases do processo de ensino. A título de exemplo, listam-se aqui alguns instrumentos de avaliação a utilizar: Estudos de caso; Ensaios; Portfólio digital; Projetos individuais ou em grupo; Discussões; Artigos; Relatórios, Propostas e Planos; Apresentações; Demonstrações; Narrativas; Quizzes; Exames; Testes escritos ou orais.

O cumprimento dos requisitos especificados no artigo 10º do Decreto-Lei n.º 133/2019, de 3 de setembro, relativos ao ensino a distância, são desenvolvidos no Modelo Pedagógico para o Ensino a Distância do Iscte (em anexo).

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

In view of the development of knowledge and skills by students, as well as their relationship with the subject matter, the use of active learning methodologies will be favoured, both in the in-person and remote learning environments. Depending on the learning objectives, Teachers may integrate various active methodologies, including:

· Project-Based Learning: Online project development where students apply knowledge in real-world contexts. Students collaborate virtually, conduct research, solve problems, and create products and/or services.

· Problem-Based Learning: Students solve problems through online research and collaboration. These problems require research, critical analysis, and the description of solutions. Students identify what they need to learn to solve the problem and actively seek the necessary knowledge.

· Case-Based Learning: Using real or fictional cases as a starting point for learning. Students have access to detailed information about the case, including the context, characters, and specific problems to solve. They follow a predefined process of case analysis, discussion, and resolution.

· Task-Based Learning: Students perform defined tasks according to the order set by the instructor, with increasing difficulty and decreasing support in each topic. The objectives of each task are clear to students, and the instructor provides feedback at the end of each task.

· Online Tutoring: Emphasis on interaction between the student and the instructor. Each student receives individualized guidance and support from a distance instructor (synchronous and/or asynchronous). The instructor answers questions, monitors the student's progress, and provides specific guidance based on their learning needs.

· Adaptive Learning: Teaching is personalized based on the individual needs and progress of each student. Using Artificial Intelligence and other technological or human means, a training needs diagnosis is made, and personalized content and activities are provided to help the student learn at their own pace.

· Collaborative Learning: An approach centered on interaction among students, promoting collaboration to build knowledge together. Active participation is encouraged through debates, discussions, and reflection on real problems, aiming to create a shared understanding within the group.

· Blended Learning: Elements of appropriate active methodologies are combined for in-person and distance learning, leveraging the advantages of each approach.

· Microlearning: Content and activities are divided into very small segments (brief videos, content summaries, interactive quizzes), allowing students to learn during limited availability moments and on mobile devices, with minimal content creation and editing requirements.

During the implementation of active learning methodologies, the teacher should select specific resources and strategies that contribute to increasing student engagement, stimulating their curiosity, interest, and motivation. The following engagement strategies are highlighted:

· Gamification: Using game elements to increase motivation and engagement in the teaching-learning process. Students can earn points and badges, unlock achievements, and compete with peers in individual and team challenges.

· Peer Tutoring: Students collaborate with each other, where a student with more knowledge in a specific content area supports their peers (this may include prior preparation) in a synchronous or asynchronous mode. It allows students to support each other, share knowledge, and develop a sense of community belonging.

· Immersive Methodologies: Using simulations and virtual reality to create immersive learning experiences, explore virtual environments, and develop simulated experiences, allowing for more interactive and contextualized learning.

· Design Thinking: A methodology for solving complex problems based on creativity, empathy, and iteration. Students are encouraged to identify challenges, gather information, generate ideas, and create and test prototypes to solve real problems using online collaborative tools.

· Storytelling: The instructor creates a narrative that relates the content to be learned to real situations, personal experiences, or fictional stories. These stories can be conveyed through various resources such as videos, podcasts, texts, or interactive presentations.

· Flipped Classroom: The instructor provides content through various mediums (recorded lectures, articles, and other materials similar to those used in traditional, more expository teaching). In independent work, students familiarize themselves with these materials, and in the virtual classroom, involving interaction with the instructor and peers, they engage in concrete learning activities (discussion groups, group exercises, projects, etc.).

Virtual learning communities play a significant role in the pedagogical model of Iscte for distance education. In this regard, the implementation of interactive virtual communities is promoted, providing students with a space for participation, collaboration, sharing experiences, and mutual learning in various domains. The aim is to encourage cooperation and empathy among students, strengthening their sense of belonging to the Iscte academic community. Additionally, collaborative knowledge construction in virtual learning environments is stimulated, fostering the exchange of ideas, initiative in seeking and providing support, and the creation of synergies among students. To achieve this objective, group activities should be promoted to strengthen the sense of belonging and drive collaborative learning, allowing students to develop essential teamwork skills and academic growth. With these initiatives, it is hoped to provide an enriching learning experience that values active student participation and enhances their social and academic skills.

Teachers play a crucial role in supervising, guiding, and monitoring the teaching-learning process. To do so, they should follow the following principles of action:

· Clear and accessible communication: Teachers should provide clear instructions regarding activities, deadlines, and student performance expectations. They should also be available to clarify doubts and support students throughout the course, using means and moments clearly identified in the course planning.

· Frequent interaction, monitoring, and feedback: Interaction with students is essential for the success of a collaborative learning environment. Teachers should encourage participation in discussion forums, conduct chat or video conferencing sessions, provide frequent feedback on students' academic performance, and monitor student engagement in activities.
· Sensitivity to diversity and inclusion: Teachers should be attentive to the diversity of students and create an inclusive and respectful environment. They should provide solutions that accommodate different needs and levels of progress in learning.
· Continuous improvement and student feedback: Teachers should be open to student feedback and use that information for reflection and improving the quality of teaching and training. The constant pursuit of improvements and adaptation to student needs are essential for the continuous improvement of EaD courses.

All curricular units will apply different assessment elements to achieve a more comprehensive understanding of student performance, respecting Iscte's General Regulation for the Assessment of Knowledge and Competences. Different types of assessment - diagnostic, formative, and summative - should be foreseen at various stages of the teaching process. Some examples of assessment instruments to be used include case studies, essays, digital portfolios, individual or group projects, discussions, articles, reports, proposals, and plans, presentations, demonstrations, narratives, quizzes, exams, and written or oral tests.

The fulfillment of the specified requirements in Article 10 of Decree-Law No. 133/2019 of September 3, regarding distance education, is developed in Iscte's Pedagogical Model for Distance Education (attached).

4.5.2.1.2. Anexos do modelo pedagógico

<style forecolor='#15428B'>Modelo_pedagogico_Presencial_&_EaD.pdf</style>

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)

O alinhamento é garantido através de:
-Estratégias adequadas para ensino à distância, incluindo aplicação de atividades colaborativas online em torno de estudos de caso, resolução de problemas e desenvolvimento de projetos;
-Acompanhamento e feedback frequente a partir de tutorias, avaliações formativas e sumativas, individuais e em grupo;
-Promoção da autonomia e autorregulação com orientações tutoriais, definição de metas, acesso a recursos e acompanhamento do trabalho do estudante em todas as UC;
-Diagnóstico de necessidades, acesso a conteúdo e atividades personalizadas, permitindo o avanço ao ritmo do estudante e valorizando o seu percurso de aprendizagem;
-Tempo de contato assíncrono predominante para flexibilidade da aprendizagem;
- Estratégias de envolvimento e inclusão, como a "gamificação", tutoria entre pares, simulações, "design thinking" e "storytelling", de acordo com as características de cada UC.

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)

Alignment is ensured through:
-Strategies suitable for distance learning, including application of online collaborative activities around case studies, problem solving and project development;
-Frequent monitoring and feedback from tutorials, formative and summative assessments, individual and group;
-Promotion of autonomy and self-regulation with tutorial guidance, goal setting, access to resources and monitoring of student work in all CUs;
-Diagnosis of needs, access to content and personalized activities, allowing advancement at the student's pace and valuing the student's learning path;
-Predominant asynchronous contact time for learning flexibility;
- Engagement and inclusion strategies, such as gamification, peer tutoring, simulations, design thinking and storytelling, according to the characteristics of each CU.

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

Estão previstos mecanismos que garantem que as metodologias e os processos de avaliação sejam justos, fiáveis e acessíveis. A elaboração e revisão da FUC tem por base regulamentos e orientações científicas e pedagógicas relevantes, como o Regulamento Geral de Avaliação de Conhecimentos e Competências (RGACC) que define regras e modalidades de avaliação a aplicar em cada UC de acordo com a sua tipologia, as normas orientadoras fixadas anualmente pelo Conselho Pedagógico, e outros referenciais existentes na legislação. O processo é sujeito a validação pelos órgãos competentes e/ou pelo coordenador de ECTS de cada departamento, a quem compete verificar a adequabilidade dos normativos. Nos Conselhos de ano, órgão que integra estudantes e docentes do CE, são discutidos os métodos e calendários de avaliação, e são atendidas as especificidades dos estudantes em termos de estatutos e necessidades, por forma a garantir que seja inclusiva. Todas as FUC estão publicadas na página do Iscte.

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

Mechanisms are in place to ensure that assessment methodologies and processes are fair, reliable and accessible. The elaboration and revision of the FUC is based on relevant scientific and pedagogical regulations and guidelines, such as the General Regulations for the Assessment of Knowledge and Competences (RGACC) that define rules and assessment modalities to be applied in each UC according to its typology, the guidelines set annually by the Pedagogical Council, and other references existing in the legislation. The process is subject to validation by the competent bodies and/or by the ECTS coordinator of each department, responsible for checking the adequacy of the rules. In the Year Councils, a body that includes students and professors of the study cycle, the assessment methods and schedules are discussed, and the specificities of the students in terms of status and needs are taken into account, in order to ensure that it is inclusive. All FUCs are published on the Iscte website.

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)

A correspondência entre a avaliação e os objetivos de aprendizagem das UC está definida nas respetivas FUC. É orientada pelo Regulamento Geral de Avaliação de Conhecimentos e Competências do Iscte e materializa-se nos elementos de avaliação definidos em função dos objetivos de aprendizagem da UC, tais como o desempenho e a participação dos estudantes nas aulas, a realização de testes, trabalhos individuais e de grupo, apresentações orais e exames.
No quadro da concretização do SIGQ-Iscte, ao nível do ensino é aplicado em todos os semestres um inquérito aos estudantes com o objetivo de monitorizar o processo pedagógico com vista a melhorar o seu funcionamento no futuro. Os inquéritos pedagógicos incluem a satisfação geral com o Iscte, o curso, as UC e dos docentes. Também é aferida a opinião dos estudantes sobre os métodos de avaliação, por exemplo, através da questão 'Os procedimentos de avaliação das UC estão adequados aos respetivos objetivos de aprendizagem?'.

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 correspondence between the assessment and the learning objectives of the UC is defined in the respective FUC. It is guided by the General Regulations for the Assessment of Knowledge and Competences of the Iscte and is materialized in the evaluation elements defined according to the learning objectives of the UC, such as the performance and participation of students in class, the realization of tests, individual and group work, oral presentations and exams.
In the scope of the implementation of SIGQ-Iscte, at the teaching level, a student survey is applied every semester with the purpose of monitoring the pedagogical process in order to improve its functionality in the future. The pedagogical surveys include the general satisfaction with the Iscte, the course, the UCs and the professors. The students' opinion on the evaluation methods is also assessed, for example, through the question 'The units evaluation procedures are adequate to their learning goals'?

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

Enquadrado no SIGQ-Iscte, foram desenvolvidos vários mecanismos de monitorização do sucesso e abandono. Todas as UC e todos os cursos dispõem de um relatório próprio – o Relatório da Unidade Curricular (RUC) e o Relatório de Autoavaliação do Curso (RAC) que integram indicadores de sucesso. Nos relatórios anuais de atividades, do Iscte e das suas Escolas, são reportados os valores das taxas de conclusão (% diplomados, por curso) e as taxas de aprovação (por curso). Paralelamente, na última década, foram promovidos grupos de trabalho sobre sucesso académico, com docentes, investigadores e pessoal técnico.
Ainda neste âmbito, são realizados estudos específicos: de caracterização de novos estudantes, sobre a opinião dos empregadores, sobre a inserção na vida ativa/ empregabilidade. Mais ainda, todos os semestres os estudantes respondem ao inquérito de monitorização pedagógica, cujos resultados contribuem para a avaliação do docente.

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

Within the SIGQ-Iscte, several mechanisms for monitoring success and dropout were developed. All the UC and all the courses have their own report - the Course Unit Reports (RUC) and the Programme Self-Assessment Reports (RAC) that integrate success indicators. In the annual activity reports of Iscte and its Schools, the values of the completion rates (% graduates, per course) and the approval rates (per course) are reported. In parallel, in the last decade, working groups on academic success have been promoted with professors, researchers and technical staff.
Also within this scope, specific studies are carried out: characterization studies of new students, on the opinion of employers, on insertion in active life/ employability. Moreover, every semester students answer the pedagogical survey, whose results contribute to the evaluation of the professor.

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

A articulação entre o ensino e a investigação é alcançada a partir das seguintes estratégias:
- Inclusão de projetos como parte integrante do currículo, nos quais os estudantes têm a oportunidade de participar em atividades com uma componente de investigação relacionadas com a área de estudo;
- Promoção de parcerias com empresas, que proporcionam oportunidades para explorar, analisar e propor soluções para problemas reais;
- Integração de ferramentas e recursos digitais nas UC que facilitam a pesquisa científica, incluindo o acesso a bases de dados científicas, fóruns de discussão online e plataformas de colaboração virtual, que promovem a troca de

ideias e a realização de trabalhos conjuntos;
- O desenvolvimento de trabalhos nas diferentes UCs pode ainda beneficiar do acesso aos centros de investigação do Iscte relacionados com o curso, em particular o ISTAR e o CIES.

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

The integration between teaching and research is achieved through the following strategies:
- Inclusion of projects as an integral part of the curriculum, where students have the opportunity to participate in activities with a research component related to their field of study.
- Promotion of partnerships with firms, providing opportunities to explore, analyze, and propose solutions to real-world problems.
- Integration of digital tools and resources within the courses, facilitating scientific research, including access to scientific databases, online discussion forums, and virtual collaboration platforms, fostering idea exchange and joint work.
- The development of projects in different courses can also benefit from access to Iscte's research centers, particularly ISTAR and CIES, relevant to the specific course.

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

Tendo por base o artigo 18.o do Decreto-Lei no 74/2006, o ciclo de estudos proposto, e à semelhança de outros no espaço europeu na mesma área, tem uma duração de quatro semestres curriculares de trabalho dos estudantes, num total de 120 créditos. A distribuição homogénea dos créditos ao longo dos semestres faz com que cada um tenha uma carga de trabalho correspondente a 30 créditos.

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

According to article 18 of Decree-Law no. 74/2006, and like others in European Union in the same area, the proposed study cycle will last four semesters, coming to a total of 120 credits. The homogeneous distribution of credits throughout the semesters means that each semester has a workload corresponding to 30 credits.

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)

No âmbito do sistema de avaliação da qualidade do ensino do Iscte, é aplicado, de forma sistemática, no final de cada semestre, um inquérito aos estudantes que tem por objetivo recolher a sua opinião sobre diversos aspetos, entre os quais o volume de trabalho envolvido por unidade curricular e as suas estratégias de aprendizagem. A perceção dos estudantes sobre a carga de trabalho foi operacionalizada através de 3 indicadores de adequação: "O número de horas de trabalho requerido ao estudante está adequado ao número de ECTS"; "Nas UC o número de horas de contacto/aulas é adequado"; e "Nas UC o número de horas de trabalho autónomo é adequado". Foi ainda tido em conta na definição destas cargas de trabalho, a experiência com outros ciclos de estudo do Iscte, no mesmo nível de ensino, e já em funcionamento.

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)

In the context of Iscte's teaching quality assessment system, a survey is conducted at the end of each semester to systematically gather students' opinions on various aspects, including their perceptions of the workload associated with each course unit and their learning strategies. The students' perception of the workload was operationalised through 3 indicators of adequacy: "The number of hours of work required from the student is adequate to the number of ECTS"; "In the UC the number of contact hours/classes is adequate"; and "In the UC the number of hours of autonomous work is adequate". In defining these workloads it was also taken into account the experience with other study cycles of the Iscte, at the same level of education, and already in operation.

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 proposta resulta de um trabalho de equipa consolidado ao longo de vários anos em outros graus e cursos do Iscte. Os docentes responsáveis por cada UC foram consultados para adequar os objetivos e conteúdos programáticos à atribuição de 6 créditos, em linha com as orientações gerais do Iscte sobre a elaboração e revisão de planos de estudos. Estas orientações fixam que, ao nível do Iscte, 1 crédito corresponde a 25 horas de trabalho total. Este alinhamento permite ainda criar uma oferta institucional que possibilita o cruzamento científico das diversas áreas.
Para além da avaliação e monitorização de indicadores sobre o cálculo dos ECTS feitos no âmbito do SIGQ-Iscte, os planos de estudos e UC são submetidos a processos de apreciação científica e pedagógica nos vários níveis das Escolas e do Iscte.

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)

The proposal is the result of brainstorming among professors and consolidated teamwork over several years across various degrees and courses at Iscte. The professors responsible for each UC were consulted to adapt the objectives and syllabus contents to the attribution of 6 ECTS, in line with the general guidelines of Iscte on the elaboration and revision of study plans. These guidelines establish that, in the context of Iscte, 1 ECTS corresponds to 25 hours of total work. This alignment also facilitates the creation of an institutional offer that enables interdisciplinary collaboration across different areas.

In addition to evaluation and monitoring of indicators on the calculation of ECTS made within the scope of the SIGQ-Iscte, study plans and UCs undergo scientific and pedagogical assessment at various levels within the Schools and Iscte.

4.5.2.3. Observações (PT)

O Mestrado em Cibersegurança e Resiliência (MCSR) é um produto de formação de 2º ciclo que é inovador ao nível do ensino superior público nacional. A nível nacional, existe já alguma oferta de mestrados em cibersegurança (CS), mas uma forte tendência tecnológica nos mesmos. Neste mestrado, procuramos uma abordagem integrada entre os principais pilares da CS: as pessoas, os processos e a tecnologia. De igual forma, este mestrado coloca uma ênfase na vertente da resiliência, algo que o diferencia da oferta existente quer a nível nacional quer internacional.
A área da CS, tem sido e continuará a ser, uma das mais carentes em termos de profissionais disponíveis no mercado a nível global (estimada em 1.8 milhões de profissionais até ao final de 2022). Existe assim, uma imensa oportunidade para a absorção dos profissionais formados neste mestrado.
No desenho deste mestrado para além de olharmos para referenciais como o ACM Computer Curricula 2020, o ACM Cybersecurity Curricula 2017, o ACM Cybersecurity Curricular Guidance 2020 e o Cybersecurity Body of Knowledge (CyBOK) de 2021. Por outro lado, tivemos a preocupação de procurar alinhar os conteúdos deste mestrado com o "NIST Cybersecurity Framework" (NCSF) assim como com o "NIST SP 800-160 – Developing Cyber-Resilient Systems". O NCSF é particularmente relevante e serve de base ao "Quadro Nacional de Referência para a Cibersegurança" do CNCS, que identifica as funções principais de cibersegurança para uma organização: IDENTIFICAR, PROTEGER, DETETAR, RESPONDER e RECUPERAR. O desenho, a estrutura curricular do mestrado e o conteúdo das diferentes UC procuram estar alinhados com estas funções. Olhando para estas UC, temos:
- Fundamentos de Gestão da Cibersegurança e Resiliência [IDENTIFICAR]
- Segurança e Resiliência de Infraestruturas e Redes de Comunicação [PROTEGER]
- Arquiteturas de Segurança e Modelos Zero Trust [IDENTIFICAR, PROTEGER]
- Criptografia para Cibersegurança e Resiliência [PROTEGER]
- Gestão do Ciber-risco e da Resiliência [IDENTIFICAR]
- Incidentes de Cibersegurança e Resiliência [DETETAR, RESPONDER, RECUPERAR]
- Fator Humano na Cibersegurança e Resiliência [IDENTIFICAR, PROTEGER, RESPONDER, RECUPERAR]
- Segurança e Resiliência de Software e Aplicações [PROTEGER, DETETAR, RESPONDER]
- Verificação da Segurança e Resiliência de Sistemas [DETETAR, RESPONDER, RECUPERAR]
- Resiliência e Continuidade do Negócio [RESPONDER, RECUPERAR]
Nestas UC serão abordados temas emergentes da CS em conjunto com outras áreas como a Inteligência Artificial, IoT e 5G, e a computação quântica. Algumas destas áreas serão abordadas e exploradas em conjunto com centros de investigação do Iscte, nomeadamente o ISTAR_Iscte.
Os estudantes têm ainda a possibilidade de escolher UCs opcionais para complementar os seus conhecimentos. Todas as UC irão conter seminários, alguns deles lecionados por convidados externos, contribuindo para a formação dos estudantes.

4.5.2.3. Observações (EN)

The Master in Cybersecurity and Resilience (MCSR) is a 2nd cycle training product that is innovative at the national public higher education level. At national level, there is already some supply of master's degrees in cybersecurity (CS), but a strong technological trend in them. In this master's degree, we seek an integrated approach between the main pillars of CS: people, processes and technology. Likewise, this master's degree places an emphasis on resilience, something that differentiates it from the existing offer both nationally and internationally.
The CS area has been, and will continue to be, one of the most lacking in terms of professionals available in the global market (estimated at 1.8 million professionals by the end of 2022). There is thus an immense opportunity for the absorption of the professionals trained in this master's degree.
In the design of this master, we looked at references such as the ACM Computer Curricula 2020, the ACM Cybersecurity Curricula 2017, the ACM Cybersecurity Curricular Guidance 2020 and the Cybersecurity Body of Knowledge (CyBOK) of 2021. On the other hand, we were concerned to seek to align the contents of this master's degree with the "NIST Cybersecurity Framework" (NCSF) as well as with the "NIST SP 800-160 - Developing Cyber-Resilient Systems". The NCSF is particularly relevant and underpins the CNCS "National Cybersecurity Framework", which identifies the main cybersecurity functions for an organisation: IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER. The design and curricular structure of the master's degree and the content of the different CUs seek to be aligned with these functions. Looking at these CUs, we have:
- Fundamentals of Cybersecurity Management and Resilience [IDENTIFY].
- Security and Resilience of Infrastructures and Communication Networks [PROTECT].
- Security Architectures and Zero Trust Models [IDENTIFY, PROTECT]
- Cryptography for Cybersecurity and Resilience [PROTEGER]
- Cybersecurity Risk and Resilience Management [IDENTIFY]
- Cybersecurity Incidents and Resilience [DETECT, RESPOND, RECOVER]
- Human Factor in Cybersecurity and Resilience [IDENTIFY, PROTECT, RESPOND, RECOVER]
- Software and Application Security and Resilience [PROTECT, DETECT, RESPOND]
- Systems Security and Resilience Check [DETECT, RESPOND, RECOVER]
- Resilience and Business Continuity [RESPOND, RECOVER].
In these CUs emerging CS topics will be addressed in conjunction with other areas such as Artificial Intelligence, IoT and 5G, and quantum computing. Some of these areas will be addressed and explored together with Iscte research centres, namely ISTAR_Iscte. Students also have the possibility to choose optional CU to complement their knowledge. All the CU will contain

seminars, some of them taught by external guests, contributing to the students' education.

5. Pessoal Docente

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

• *Carlos José Corredoura Serrão*

5.2. Pessoal docente do ciclo de estudos

Nome	Categoria	Grau	Vínculo	Especialista	Regime de	Informação
Carlos Eduardo Dias Coutinho	Professor Auxiliar ou equivalente	Doutor Engenharia Eletrotécnica e de Computadores	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Carlos José Corredoura Serrão	Professor Associado ou equivalente	Doutor Arquitectura de Computadores e Sistemas Distribuidos	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 Amaro Ferreira	Professor Auxiliar ou equivalente	Doutor Engª Industrial	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
João Pedro Calado Barradas Branco Pavia	Professor Auxiliar ou equivalente	Doutor Ciências 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
Maria do Rosário Domingos Laureano	Professor Auxiliar ou equivalente	Doutor Métodos Quantitativos	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Margarida Tavares Peralta Couto dos Santos	Professor Auxiliar convidado ou equivalente	Doutor Psicologia	Outro vínculo		100	Ficha Submetida CienciaVitae OrcID
					Total: 600	

5.2.1. Ficha curricular do docente

5.2.1.1. Dados Pessoais - Carlos Eduardo Dias Coutinho

Vínculo com a IES

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

Categoria

Professor Auxiliar ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

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

2013

Instituição que conferiu este grau académico

Universidade Nova de Lisboa Faculdade de Ciências e Tecnologia

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

541A-4D38-4A67

Orcid

0000-0001-8065-1898

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - Carlos Eduardo Dias Coutinho

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura (ISTAR – IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	

5.2.1.3. Outros graus académicos ou títulos - Carlos Eduardo Dias Coutinho

Ano	Grau ou Título	Área	Instituição	Classificação
1994	Bacharelato	Engenharia de Sistemas das Telecomunicações e Electrónica	Instituto Politécnico de Lisboa Instituto Superior de Engenharia de Lisboa	
1997	Licenciatura	Engenharia Electrotécnica - Sistemas e Comunicações	Instituto Politécnico de Lisboa Instituto Superior de Engenharia de Lisboa	
2010	Pós-graduação	Gestão de Projetos	Instituto Superior Bissaya-Barreto	

5.2.1.4. Formação pedagógica - Carlos Eduardo Dias Coutinho

Formação pedagógica relevante para a docência
Práticas de Ensino à Distância (Iscte - 2023)

5.2.1.5. Distribuição do serviço docente - Carlos Eduardo Dias Coutinho

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Fundamentos de Arquitectura de Computadores	Licenciatura em Engenharia Informática / Licenciatura em Informática e Gestão de Empresas	36.0	18.0	18.0						
Sistemas Operativos	Licenciatura em Engenharia de Telecomunicações e Informática / Licenciatura em Engenharia Informática / Licenciatura em Informática e Gestão de Empresas	108.0		72.0	36.0					
Tecnologias e Sistemas Cloud	Curso Institucional em Escola de Tecnologias e Arquitetura	72.0	24.0	48.0						
Dissertação/Trabalho de Projecto em Tecnologias Digitais Emergentes	Mestrado em Tecnologias Digitais Emergentes	20.0							20.0	
Sistemas de IoT e Edge Computing	Mestrado em Tecnologias Digitais Emergentes	6.0	2.0	4.0						
Fundamentos de Gestão da Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	24.0		24.0						
Verificação da Segurança e Resiliência de Sistemas	Mestrado em Cibersegurança e Resiliência	24.0		24.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	8.0							8.0	

5.2.1.1. Dados Pessoais - Carlos José Corredoura Serrão

Vínculo com a IES

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

Categoria

Professor Associado ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Arquitectura de Computadores e Sistemas Distribuidos

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2008

Instituição que conferiu este grau académico

Universitat Politécnica de Catalunya

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

3219-BF7A-48A9

Orcid

0000-0002-4847-2432

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - Carlos José Corredoura Serrão

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura (ISTAR – IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	

5.2.1.3. Outros graus académicos ou títulos - Carlos José Corredoura Serrão

Ano	Grau ou Título	Área	Instituição	Classificação
1997	Licenciatura	Informática e Gestão de Empresas	ISCTE-IUL - Instituto Superior Ciências Trabalho e da Empresa	
2003	Mestrado	Gestão de Sistemas de Informação	ISCTE-IUL - Instituto Superior Ciências Trabalho e da Empresa	

5.2.1.4. Formação pedagógica - Carlos José Corredoura Serrão

Formação pedagógica relevante para a docência
Curso em Ensino a Distância (IPPS-Iscte) - 2023

5.2.1.5. Distribuição do serviço docente - Carlos José Corredoura Serrão

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Criptografia Aplicada	Licenciatura em Tecnologias Digitais e Segurança de Informação	36.0	12.0	12.0	12.0					
Introdução à Cibersegurança	Licenciatura em Tecnologias Digitais e Segurança de Informação / Licenciatura em Tecnologias Digitais Educativas	18.0	6.0	6.0	6.0					
Segurança em Redes e Sistemas de Informação	Mestrado em Engenharia de Telecomunicações e Informática / Mestrado em Engenharia Informática	108.0	36.0	36.0	36.0					
Segurança em Sistemas de Informação	Licenciatura em Informática e Gestão de Empresas	48.0	24.0	24.0	0.0					
Dissertação/Trabalho de Projecto em Tecnologias Digitais Emergentes	Mestrado em Tecnologias Digitais Emergentes	20.0							20.0	
Tecnologia de Registo Distribuído	Mestrado em Tecnologias Digitais Emergentes	6.0	2.0	4.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	56.0					56.0			
Gestão do Ciber-risco para Resiliência	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						
Segurança e Resiliência de Software e Aplicações	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						
Seminário de Investigação em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	24.0		24.0						
Seminário de Projeto em Tecnologias Digitais Aplicadas	Dout. Tecnologias Digitais Aplicadas	8.0		6.0			2.0			
Tese em Tecnologias Digitais Aplicadas	Doutouramento Tecnologias Digitais Aplicadas	4.0					4.0			

5.2.1.1. Dados Pessoais - João Carlos Amaro 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 Auxiliar ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Engª Industrial

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2013

Instituição que conferiu este grau académico

Universidade 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

7E1E-BA67-7DC9

Orcid

0000-0002-6662-0806

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - João Carlos Amaro Ferreira

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura (ISTAR – IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	

5.2.1.3. Outros graus académicos ou títulos - João Carlos Amaro Ferreira

Ano	Grau ou Título	Área	Instituição	Classificação
2019	Agregação	Ciências e Tecnologias de Informação	ISCTE-Instituto Universitario de Lisboa	
2006	Doutoramento	Engª Informática	Instituto Superior Tecnico	
1995	Mestrado	Engenharia Electrotécnica e de Computadores, na área Científica de Telecomunicações	Instituto Superior Tecnico	
1991	Licenciatura	Engª Fisica Tecnologica	Instituto Superior Tecnico	

5.2.1.4. Formação pedagógica - João Carlos Amaro Ferreira

5.2.1.5. Distribuição do serviço docente - João Carlos Amaro Ferreira

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Aplicações de Sistemas Integrados de Apoio à Decisão	Curso Institucional em Escola de Tecnologias e Arquitetura	18.0	6.0	12.0						
Blockchain	Curso Institucional em Escola de Tecnologias e Arquitetura	6.0	6.0							
Dissertação em Sistemas Integrados de Apoio à Decisão	Mestrado em Sistemas Integrados de Apoio à Decisão	18.0					18.0			
Extração de Padrões e Conhecimento Guiada por Dados	Mestrado em Sistemas Integrados de Apoio à Decisão	6.0		6.0						
Internet das Coisas para Cidades Inteligentes	Curso Institucional em Escola de Tecnologias e Arquitetura	12.0	4.0		8.0					
Laboratório de Internet das Coisas	Curso Institucional em Escola de Tecnologias e Arquitetura	6.0	6.0							
Projeto Final Aplicado em Ciência dos Dados	Licenciatura em Ciência de Dados	12.0		12.0						
Tecnologias Disruptivas	Curso Institucional em Escola de Tecnologias e Arquitetura	21.0		21.0						
Tomada de Decisão Baseada em Dados	Mestrado em Sistemas Integrados de Apoio à Decisão	12.0	9.0	3.0						
Aplicações IA e IoT (SmartAnything)	Mestrado em Tecnologias Digitais Emergentes	6.0	2.0	4.0						
Dissertação/Trabalho de Projecto em Tecnologias Digitais Emergentes	Mestrado em Tecnologias Digitais Emergentes	24.0	4.0						20.0	
Python para Análise de Dados	Mestrado em Tecnologias Digitais Emergentes	6.0	2.0	4.0						
Arquiteturas de Segurança e Modelos de Confiança Zero	Mestrado em Cibersegurança e Resiliência	24.0		24.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	8.0							8.0	
Incidentes de Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						
Tese em Tecnologias Digitais Aplicadas	Dout. Tecnologias Digitais Aplicadas	4.0					4.0			
Programação para Análise de Dados	Mestrado em Inovação de Produtos Digitais	12.0		12.0						
Trabalho de Projeto em Inovação de Produtos Digitais	Mestrado em Inovação de Produtos Digitais	13.0					13.0			

5.2.1.1. Dados Pessoais - João Pedro Calado Barradas Branco Pavia

Vínculo com a IES

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

Categoria

Professor Auxiliar ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Ciências e Tecnologias da Informação

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2022

Instituição que conferiu este grau académico

ISCTE-Instituto Universitário de Lisboa

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

4618-B076-34DF

Orcid

0000-0002-4759-4817

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - João Pedro Calado Barradas Branco Pavia

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Instituto de Telecomunicações (IT)	Muito Bom	Instituto de Telecomunicações (IT)	Polo	

5.2.1.3. Outros graus académicos ou títulos - João Pedro Calado Barradas Branco Pavia

Ano	Grau ou Título	Área	Instituição	Classificação
2018	Mestrado em Engenharia de Telecomunicações e Informática		ISCTE-IUL	
2016	Licenciatura em Engenharia de Telecomunicações e Informática		ISCTE-IUL	

5.2.1.4. Formação pedagógica - João Pedro Calado Barradas Branco Pavia

Formação pedagógica relevante para a docência
Formação de Ensino à Distância
Utilização do Moodle para o Ensino Superior

5.2.1.5. Distribuição do serviço docente - João Pedro Calado Barradas Branco Pavia

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Bases de Dados e Gestão de Informação	Licenciatura em Desenvolvimento de Software e Aplicações	36.0		12.0	24.0					
Introdução à Cibersegurança	Licenciatura em Tecnologias Digitais e Saúde	54.0	18.0	18.0	18.0					
Planeamento e Gestão de Projetos	Licenciatura em Tecnologias Digitais e Automação	36.0		36.0						
Segurança em Redes de Computadores	Licenciatura em Tecnologias Digitais e Segurança de Informação	36.0	12.0	12.0	12.0					
Sistemas Distribuídos e Segurança	Licenciatura em Tecnologias Digitais e Segurança de Informação	36.0	18.0	18.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	8.0							8.0	
Resiliência e Continuidade do Negócio	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						
Segurança e Resiliência de Infraestruturas e Redes de Comunicação	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						

5.2.1.1. Dados Pessoais - Maria do Rosário Domingos Laureano

Vínculo com a IES

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

Categoria

Professor Auxiliar ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Métodos Quantitativos

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2009

Instituição que conferiu este grau académico

ISCTE-IUL - Instituto Superior Ciências Trabalho e da Empresa

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

AD1C-9513-BEF9

Orcid

0000-0002-2669-2581

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - Maria do Rosário Domingos Laureano

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura (ISTAR – IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	

5.2.1.3. Outros graus académicos ou títulos - Maria do Rosário Domingos Laureano

Ano	Grau ou Título	Área	Instituição	Classificação
2002	Mestrado	Matemática Aplicada	Instituto Superior Técnico - UTL	
1990	Licenciatura	Matemática	Faculdade de Ciências - UL	

5.2.1.4. Formação pedagógica - Maria do Rosário Domingos Laureano

Formação pedagógica relevante para a docência
Curso em Ensino a Distância (IPPS-Iscte) - 2023

5.2.1.5. Distribuição do serviço docente - Maria do Rosário Domingos Laureano

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Álgebra Linear e Aplicações	Licenciatura em Matemática Aplicada e Tecnologias Digitais	36.0		33.0	3.0					
Álgebra Linear e Geometria	Licenciatura em Tecnologias Digitais e Automação	36.0		30.0	6.0					
Análise Numérica	Licenciatura em Matemática Aplicada e Tecnologias Digitais	36.0		18.0	18.0					
Cálculo A Múltiplas Variáveis	Licenciatura em Matemática Aplicada e Tecnologias Digitais	36.0		33.0	3.0					
Inteligência Computacional e Otimização	Optativa da Escola de Tecnologias e Arquitetura	18.0		18.0						
Otimização Matemática	Licenciatura em Matemática Aplicada e Tecnologias Digitais	36.0		21.0	15.0					
Criptografia para Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	24.0		24.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	8.0							8.0	

5.2.1.1. Dados Pessoais - Margarida Tavares Peralta Couto dos Santos

Vínculo com a IES

Outro vínculo

Categoria

Professor Auxiliar convidado ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Psicologia

Área científica deste grau académico (EN)

[no answer]

Ano em que foi obtido este grau académico

2019

Instituição que conferiu este grau académico

ISCTE-Instituto Universitário de Lisboa

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

0000-0000-0000

Orcid

0000-0000-0000-0000

Autorização para que as informações pessoais sejam guardadas e utilizadas para fins funcionais e analíticos

Sim

5.2.1.2. Filiação Unidades de Investigação - Margarida Tavares Peralta Couto dos Santos

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
DINÂMIA´CET-IUL, Centro de Estudos Sobre a Mudança Socioeconómica e o Território (DINÂMIA´CET-IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	

5.2.1.3. Outros graus académicos ou títulos - Margarida Tavares Peralta Couto dos Santos

Ano	Grau ou Título	Área	Instituição	Classificação
2010	Mestrado	Psicologia Social e das Organizações	ISCTE-Instituto Universitário de Lisboa	
2008	Licenciatura	Psicologia	ISCTE-Instituto Universitário de Lisboa	

5.2.1.4. Formação pedagógica - Margarida Tavares Peralta Couto dos Santos

Formação pedagógica relevante para a docência
Práticas de Ensino à Distância (Iscte - 2023)

5.2.1.5. Distribuição do serviço docente - Margarida Tavares Peralta Couto dos Santos

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Psicologia da Aprendizagem	Licenciatura em Tecnologias Digitais Educativas	36.0	18.0	18.0						
Psicologia Social da Saúde	Licenciatura em Tecnologias Digitais e Saúde	36.0		36.0						
Sistema de Saúde	Licenciatura em Tecnologias Digitais e Saúde	36.0		36.0						
Trabalho, Organizações e Tecnologia	Licenciatura em Política, Economia e Sociedade, Licenciatura em Tecnologias Digitais e Segurança de Informação	54.0	18.0	36.0						
Dissertação/Trabalho de Projecto em Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	8.0							8.0	
Fator Humano na Cibersegurança e Resiliência	Mestrado em Cibersegurança e Resiliência	24.0	2.0	22.0						

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.

6

5.3.1.2. Número total de ETI.

6.00

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	83.33%
Investigador de Carreira (Art. 3º, alínea l) do DL-74/2006, na redação	0.00%

fixada pelo DL-65/2018

Outro vínculo	16.67%

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)	600	100.00%

5.3.4. Corpo docente especializado

Corpo docente especializado	ETI	Percentagem*
Doutorados especializados na(s) área(s) fundamental(is) do CE (% total ETI)	4.0	66.67%
Não doutorados, especializados nas áreas fundamentais do CE (% total ETI)	0.0	0.00%
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%
% do corpo docente especializado na(s) área(s) fundamental(is) (% total ETI)		66.67%
% do corpo docente doutorado especializado na(s) área(s) fundamental(is) (% docentes especializados)		100.00%

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	0.0	0.00%

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	4.0	66.67%
Docentes do ciclo de estudos inscritos em programas de doutoramento há mais de um ano (ETI)	0.0	0.00%

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).

Os procedimentos de avaliação do desempenho do pessoal docente do Iscte encontram-se definidos no Regulamento de Avaliação de Desempenho dos Docentes do Iscte. Realiza-se em períodos trienais, tendo por base objetivos anuais, nas seguintes vertentes: investigação; ensino; gestão universitária; transferência de conhecimentos. O processo da avaliação do triénio inclui as seguintes fases: definição do objetivo geral para o triénio; autoavaliação; validação; avaliação; audiência e homologação e notificação da avaliação, e o resultado é obtido de acordo com o método e critérios definidos no Regulamento acima referido. A classificação global é expressa em cinco níveis: Inadequado; Suficiente; Bom; Muito Bom e Excelente. No processo de avaliação do desempenho dos docentes participam os seguintes intervenientes: Avaliado; Diretor do Departamento; Conselho Científico; Painel de Avaliadores; Conselho Coordenador da Avaliação do Desempenho dos Docentes.

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

The procedures for evaluating the performance of Iscte's faculty are defined in the Iscte Assessment of Faculty Performance. It is carried out in triennial periods, based on annual objectives, in the following areas: research; teaching; university management; knowledge transfer. The triennial evaluation process includes the following phases: definition of the general objective for the triennium; self-assessment; validation; evaluation; hearing and approval and notification of the evaluation, and the result is obtained according to the method and criteria defined

in the above mentioned Regulation. The overall classification is expressed in five levels: Inadequate; Sufficient; Good; Very Good and Excellent. The following participants take part in the Assessment of Faculty Performance process: the evaluated; the Department Director; Scientific Council; Panel of Evaluators; Coordinating Council for Assessment of Faculty Performance.

5.3.2.1. Observações (EN)

In this master's program, the involvement of a number of companies and professionals with experience in the area of cybersecurity is planned, and they will participate in the promotion of some classes, seminars and projects throughout the students' learning process. It is also important to point out that these companies and professionals will bring to the classroom a whole set of real use cases, which will be important in the students' learning. The management of the participation of these companies and professionals in the teaching-learning process of the students will be duly streamlined and coordinated by the teachers responsible for the different curricular units, as well as the type of sessions to be developed.
In accordance with Article 8 of Decree-Law No. 133/2019, professors overseeing 'Distance Learning' (EaD) courses will receive support from a dedicated team comprising three qualified professionals in this domain. This team, under the coordination of Professor Dr. Joana Costa, Vice-President of the Pedagogical Committee at Iscte-Sintra and a Ph.D. holder in Education with specialization in Information and Communication Technologies in Education, will actively contribute to the development of curriculum designs, study plans, and the creation of pedagogical materials.

5.3.2.1. Observações (PT)

Neste mestrado está previsto o envolvimento de um conjunto de empresas e de profissionais com experiência na área da cibersegurança que irão participar na dinamização de algumas aulas, seminários e projetos ao longo do processo de aprendizagem dos estudantes. É igualmente importante ressalvar que estas empresas e estes profissionais trarão para a sala aula todo um conjunto de casos de uso reais, que serão importantes na aprendizagem dos estudantes. A gestão da participação destas empresas e profissionais no processo de ensino-aprendizagem dos estudantes será devidamente dinamizada e coordenada pelos docentes responsáveis pelas diferentes unidades curriculares, assim como a tipologia de sessões a desenvolver.
Em cumprimento com o disposto no artigo 8.º do Decreto-Lei n.º 133/2019, os docentes responsáveis pelas UC na modalidade de Ensino a Distância contarão com o apoio de uma equipa de três técnicos qualificados para este âmbito, coordenada pela Professora doutora Joana Costa, vice-presidente da Comissão Pedagógica da Iscte-Sintra, e doutorada em Educação na especialidade de Tecnologias de Informação e Comunicação na Educação, que irá colaborar no desenho curricular dos planos de estudos e na preparação dos materiais pedagógicos.

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)

O Iscte integra na sua orgânica um conjunto de serviços e estruturas de apoio ao funcionamento da instituição e dos seus ciclos de estudos. Numa perspetiva global, todos os trabalhadores colaboram no funcionamento e gestão da instituição e da sua oferta formativa.
No entanto, existem serviços com apoio mais direto, como é o caso dos Serviços de Gestão do Ensino, com uma Unidade destinada ao apoio e integração dos estudantes, e uma Unidade que pretende o apoio académico e administrativo da oferta formativa de 1.º ciclo. Destacam-se também os Serviços de Relações Internacionais, que garantem o acompanhamento dos processos de mobilidade e internacionalização dos ciclos de estudos, em estreita articulação com as Unidades de Apoio Técnico e Administrativo (UATA) de cada escola do Iscte.
Assim, dado o número de estudantes previsto, estima-se que o pessoal técnico, em ETI, afeto ao ciclo de estudos, repartido pelos diferentes serviços e gabinetes, seja de 1,62.
Refletindo sobre esta afetação mais direta ao ciclo de estudos, esse papel cabe às UATA, a quem compete, essencialmente:
- assegurar o secretariado da Escola e apoio à Direção;
- prestar o apoio aos docentes;
- garantir o atendimento e encaminhamento de estudantes.
Mais detalhadamente, compete à UATA:
- preparar e disponibilizar no sítio da Internet informação sobre os cursos e outras atividades geridas pela escola;
- promover a imagem da Escola junto dos seus públicos-alvo, nomeadamente os estudantes do ensino secundário;
- organizar a representação da Escola em feiras e eventos;
- promover, formalizar e acompanhar a colocação de estudantes da Escola em estágios curriculares e extracurriculares;
- estabelecer contactos e gerir protocolos com entidades externas, com o objetivo de promover a empregabilidade dos diplomados;
- monitorizar os indicadores de desempenho e elaborar relatórios de avaliação das atividades de ensino da Escola;
- assegurar a receção e integração de estudantes estrangeiros, regulares e em mobilidade, bem como docentes, investigadores e pessoal não docente (Incoming);
- garantir o cumprimento de outras tarefas que lhes seja cometida.
Além das competências anteriormente referidas, esta unidade garante a ligação com os gabinetes e serviços centrais do Iscte.

Atualmente a UATA da Escola de Tecnologias Digitais Aplicadas, onde o ciclo de estudos se insere, conta com 6 colaboradores. O Iscte-Sintra cumpre os requisitos previstos no artigo 8.º do Decreto-Lei n.º 133/2019 tendo em vista assegurar as condições necessárias ao bom funcionamento do Ensino a Distância nas UC que o preveem. Em particular, a generalidade dos docentes tem formação pedagógica certificada para o ensino à distância, a UATA do Iscte-Sintra inclui também técnicos certificados para esta modalidade de ensino e a Escola conta também com uma equipa técnica de suporte que inclui um técnico de informática e um técnico de multimédia com competências na área.

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)

ISCTE includes in its structure a set of services and support structures for the functioning of the institution and its study cycles. From a global perspective, all non-teaching staff collaborate in the operation and management of the institution and its educational offerings.
However, there are services with more direct support, such as the Academic Services, with a Unit dedicated to supporting and integrating students, and a Unit that aims to provide academic and administrative support for the 1st cycle educational offerings. The International Relations Services also stand out, ensuring the follow-up of mobility and internationalization processes of study cycles, in close coordination with the Technical and Administrative Support Unit (UATA) of each school at ISCTE.
Therefore, given the projected number of students, it is estimated that the technical staff, in full-time equivalents, assigned to the study cycle and distributed across different services and offices, will be 1,62.
Reflecting on this more direct assignment to the study cycle, this role falls to the UATA, whose main responsibilities include:
- ensuring the secretariat of the School and support to the Management;
- providing support to teachers;
- ensuring the reception and guidance of students.
In more detail, the UATA is responsible for:
- preparing and making available on the website information about the courses and other activities managed by the school;
- promoting the image of the School to its target audiences, particularly secondary school students;
- organizing the School's representation at fairs and events;
- promoting, formalizing, and monitoring the placement of School students in curricular and extracurricular internships;
- establishing contacts and managing protocols with external entities, with the aim of promoting the employability of graduates;
- monitoring performance indicators and preparing evaluation reports on the School's teaching activities;
- ensuring the reception and integration of regular and mobile foreign students, as well as teachers, researchers, and non-teaching staff (Incoming);
- ensuring compliance with other assigned tasks.
In addition to the previously mentioned competencies, this unit ensures the connection with the central offices and services of ISCTE.
Currently, the UATA of the School of Applied Digital Technologies, where the study cycle is located, has 6 non-teaching staff.
Iscte-Sintra complies with the requirements set out in Article 8 of Decree-Law 133/2019 in order to ensure the necessary conditions for the proper functioning of distance learning in the courses that provide for it. In particular, most of the teachers have certified pedagogical training for distance learning, Iscte-Sintra's UATA also includes certified technicians for this type of teaching and the school also has a technical support team that includes a computer technician and a multimedia technician with skills in the area.

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

O Iscte dispõe de mecanismos que visam criar condições para que o nível de qualificação e competência do pessoal não docente assegure o cumprimento das suas funções, o que tem permitido aumentar em dimensão e qualificação.
Atualmente composto por 327 colaboradores, distribuídos pelas diferentes categorias profissionais, em que, cerca de 79,2% têm habilitação de nível superior, 28,13% dos quais detentores de mestrado e doutoramento. De referir ainda que apenas 3,06% têm habilitação inferior ao ensino secundário.
Em linha com as ações definidas no Plano Estratégico e de Ação para o Quadriénio 2022-2025, de melhorar a organização e funcionamento dos serviços centrais e das unidades orgânicas, o Iscte definiu como ação 'manter elevados níveis de qualificação do pessoal técnico e administrativo', através da promoção de inúmeras iniciativas de formação e do incentivo a frequência dos cursos ministrados na instituição.

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

Iscte has mechanisms that aim to create conditions to promote the level of qualification and competence of non-teaching staff in order to ensure the fulfilment of their functions. In this context, it has been possible to increase the dimension and qualification of the number of staff members.
Currently comprising 327 employees, distributed among the different professional categories, around 79,2% have higher education qualifications, 28,13% of whom have master's degrees and doctorates. It should also be noted that only 3,06% have less than secondary education.
In line with the actions defined in the Strategic and Action Plan for the Quadrennium 2022-2025, to improve the organization and functioning of the central services and organic units, Iscte defined as an action "to maintain high

levels of qualification of technical and administrative staff", through the promotion of numerous training initiatives and the incentive to attend the courses provided by the institution.

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

Tendo em conta o regime fundacional vigente no Iscte, um regime dual em que parte dos colaboradores estão sujeitos à legislação da administração pública e outros à legislação laboral do setor privado. O Iscte criou regulamentos e procedimentos específicos consoante o tipo de legislação.
Na avaliação do desempenho, ao pessoal não docente com contrato de trabalho em funções públicas aplica-se o SIADAP, ao pessoal não docente com contrato ao abrigo do Código do Trabalho aplica-se o regulamento de avaliação do desempenho próprio, com base no SIADAP. A avaliação realiza-se em períodos bianuais, e inclui as fases: definição de objetivos; autoavaliação; avaliação; audiência e homologação e notificação da avaliação, e o resultado é obtido de acordo com o método e critérios definidos. Anualmente, é realizado o diagnóstico das necessidades de formação pelos dirigentes, com os colaboradores, o que tem permitido maior investimento em formação qualificada no âmbito do contexto institucional.

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

Taking into account the foundational system at Iscte, there is a twofold evaluation type: part of the employees are subject to the public administration legislation and others to the private sector labour legislation. Iscte created regulations and procedures according to the legislation.
Regarding performance evaluation, the non-faculty staff members bound by public service employment contracts are subject to the SIADAP, and the non-faculty staff members bound by contracts under the Labour Code are subject to a performance evaluation regulation based on the SIADAP. Evaluation takes place every 2 years, and includes: goal definition; self-evaluation; evaluation; hearing and approval and evaluation results notification, and the result is obtained according to the defined method and criteria. Each year, the chief officers carry out a diagnostic of the training needs, with the employees, which has facilitated an investment in qualified training within the institutional context.

7. Instalações e equipamentos

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

No campus de Lisboa o Iscte contém 64 salas de aula, 22 laboratórios de informática, salas de estudo abertas 24h/7 dias com 697 lugares sentados e uma biblioteca com cerca de 2000m2, para além dos 4 espaços de trabalho no Laboratório de Ciências da Comunicação e 20 espaços na sala afeta à pós-graduação de Jornalismo. Os espaços de utilização comum funcionam em horário alargado. Nas instalações funcionam ainda 2 bares e 1 cantinas. Dispõe também de uma residência para alojamento temporário de estudantes nacionais e internacionais, assim como dos professores convidados. Na sala polivalente estão disponíveis serviços de impressão e reprografia. O Iscte dispõe ainda de 2 parques de estacionamento. De referir que, está em curso um projeto para expansão do campus em espaço contíguo.
O campus de Sintra inclui dois edifícios com um total de 12 salas de aula, um laboratório de informática, automação e robótica, um estúdio multimédia, uma sala multiusos de 200m2, duas copas e uma sala de refeições. Através de um protocolo realizado com a Câmara Municipal de Sintra, os estudantes do Iscte têm acesso à Biblioteca Municipal de Sintra (que contém um acervo bibliográfico dos cursos do Iscte-Sintra e permite a requisição de obras alojadas na biblioteca do Iscte), à Pousada de Jovens de Sintra a preços sociais, bem como às cantinas escolares da vila de Sintra. Todo o campus de Sintra tem acesso à internet com velocidade 10Gbps disponível para estudantes, pessoal docente e não docente, o que permite suportar uma elevada carga de tráfego adicional requerida em atividades de ensino com transmissão de conteúdo online em tempo real.

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

Given the number of students referred for admission to the programme, the physical facilities available at Iscte are sufficient to meet the space required. Iscte has 64 classrooms, 22 computer labs, study rooms open 24h/7 days with 697 seated places and a library with about 2000m2, in addition to the 4 workspaces in the Laboratory of Communication Sciences and 20 spaces in the Journalism post-graduate classroom. Spaces of common use work in extended hours. On the premises of Iscte there are also 3 bars and 2 canteens. The institute also has a university residence for temporary accommodation of national and international students, as well as guest teachers. In the multipurpose hall students have photocopying and printing facilities. The institute also has 2 parking spaces. It should be noted that there is an ongoing project to expand the campus into a contiguous space.
The Sintra campus includes two buildings with a total of 12 classrooms, a computer, automation and robotics laboratory, a multimedia studio, a 200m2 multipurpose room, two pantries and a dining room. Through a protocol signed with Sintra Municipality, Iscte students have access to the Sintra Municipal Library (which contains a bibliographic collection of Iscte-Sintra courses and allows them to request works housed in the Iscte library), the Sintra Youth Hostel at social prices, as well as the school canteens in the town of Sintra. The entire campus of Sintra has 10Gbps internet access available for students, teaching and non-teaching staff, which enables supporting a high additional traffic load required in teaching activities in streaming.

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

Os estudantes e os docentes têm à sua disposição um vasto conjunto de serviços de apoio ao ensino e à aprendizagem, quer na vertente presencial (apoio aos espaços), quer à distância, como sistemas de videoconferência (Zoom, Videocast, Microsoft Teams); plataformas colaborativas com armazenamento de dados em cloud (Office365, Google Apps), sistema de gestão de aprendizagem (Moodle) e de partilha de conteúdos (Educast,Filesender). O Iscte dispõe ainda de um conjunto de licenças Adobe Creative Cloud para a produção de recursos educativos digitais de qualidade.

O Iscte tem apostado fortemente no desenvolvimento e modernização dos seus sistemas de informação para garantir a sua capacitação para dar resposta aos desafios emergentes na recolha, análise e utilização da informação gerada nas atividades operacionais e estratégicas da instituição. A arquitetura dos sistemas de informação compreende um conjunto de plataformas articuladas entre si: o Fénix+ (informação académica); a plataforma de gestão de aprendizagem (Moodle); o iAjuda (helpdesk); o i-meritus (avaliação de desempenho dos docentes e investigadores); o Ciência-IUL (produção científica dos docentes e investigadores); o Dspace (repositório institucional dos documentos produzidos no ensino e investigação); o Koha (sistema integrado de gestão da biblioteca); o eDocLink (gestão documental); o MyIscte (intranet); o portal de internet; e o SINGAP (informação contabilística, financeira, patrimonial e operacional). Toda a informação proveniente dos sistemas de informação e gestão é usada pelos órgãos de governo e coordenação para a tomada de decisão e emissão de pareceres, bem como na atuação para a melhoria no âmbito da garantia da qualidade do ensino e aprendizagem, da investigação, da gestão de recursos humanos e materiais e da qualidade dos serviços do Iscte.

No âmbito das atividades de ensino destacamos os seguintes:

Fénix+ - sistema de gestão académica responsável pela gestão do percurso académico dos estudantes, nas diversas dimensões que lhe estão subjacentes, desde a candidatura, matrícula e inscrição, gestão de horários e da atividade docente.

Moodle - ferramenta de aprendizagem online que permite a estudantes e professores realizarem sessões síncronas de aulas online, compatível com os principais browsers (Google Chrome, Mozilla Firefox, Microsoft Edge) ou utilizando a aplicação dedicada (iOS, Android).

B-on disponibiliza o acesso ilimitado e permanente a milhares de periódicos e ebooks de alguns dos principais fornecedores de conteúdos científicos internacionais.

O Iscte disponibiliza licenças para softwares específicos. Nessa lista, encontramos: acesso gratuito ao software educativo Inventor, Revit, Autocad, 3ds Max, Maya, Tinkercad da Autodesk para instituições qualificadas, como é o caso do Iscte; acesso ao Microsoft Office 365; acesso ao Microsoft Windows, Microsoft Visio e Microsoft Project, e outros da Microsoft; acesso ao SPSS Statistics e IBM SPSS Amos.

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

Students and teachers have at their disposal a wide range of services to support teaching and learning, both face-to-face (support for spaces) and distance, such as video conferencing systems (Zoom, Videocast, Microsoft Teams); using learning management systems (Moodle); using collaborative platforms (Office365, Google Apps) and content sharing (Educast, Filesender), based on the academic management system. Iscte also has a set of Adobe Creative Cloud licenses for the production of quality digital educational resources.

Iscte has strongly invested in the development and modernisation of its information systems to ensure its capacity to respond to the emerging challenges in the gathering, analysis and use of the information produced in the operational and strategic activities of the institution. The architecture of the Iscte information system comprises a set of articulated information platforms/systems: Fénix+ (academic information); learning management system (Moodle); iAjuda (helpdesk); i-meritus (performance evaluation of faculty and researchers); o Ciência-IUL (scientific production of faculty and researchers); Dspace (institutional repository of documents produced in teaching and research); Koha (integrated library management system); eDocLink (document management); MyIscte (intranet); internet portal; and SINGAP (accounting, financial, asset and operational information). All the information from the information and management systems is used by the governance and coordination bodies to take decisions and issue assessments, as well as to improve the quality of teaching and learning, research, management of human and material resources and the quality of Iscte services.

In the scope of the teaching activities we highlight the following:

Fénix+ is the academic management system responsible for managing the academic path of students, in the various dimensions that underlie it, from application, enrolment and registration, management of timetables and teaching activity.

Moodle is an online learning tool that allows students and teachers to hold synchronous online class sessions, compatible with the main browsers (Google Chrome, Mozilla Firefox, Microsoft Edge) or using the dedicated application (iOS, Android).

B-on provides unlimited and permanent access to thousands of journals and ebooks from some of the main international scientific content providers.

Iscte provides licenses for specific software. Among them, we find: free access to educational software Inventor, Revit, Autocad, 3ds Max, Maya, Tinkercad from Autodesk for qualified institutions, such as Iscte; access to Microsoft Office 365; access to Microsoft Windows, Microsoft Visio, and Microsoft Project, and others from Microsoft; access to SPSS Statistics and IBM SPSS Amos.

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

A matrícula do estudante gera credenciais de acesso à rede informática, nomeadamente, ao sistema de gestão académica Fénix+, à plataforma de e-learning Moodle, à VPN, ao acesso wireless em todo o campus do Iscte e ao

sítio web da biblioteca, direcionado para estudantes, que garante o acesso perante a inúmeras bases de dados eletrónicas e revistas de especialidade das diversas áreas científicas. A plataforma de e-learning, acessível 24h/dia, contém funcionalidades de interação pedagógica, permanentemente acessível a todos os participantes do processo educativo.
O Iscte dispõe de salas de aula equipadas com computador, projetor e sistema de som, para utilização de docentes e estudantes, entre as quais se inclui o formato de laboratório (22 no campus de Lisboa e 1 no campus de Sintra) e "Bring Your Own Device" (3 no campus de Lisboa e 12 no campus de Sintra). Neste contexto atual houve um reforço significativo nos auditórios e salas de aulas para permitirem a gravação/ difusão de aulas e outros eventos. Existem ainda salas preparadas para videoconferências. O Iscte-Sintra dispõe ainda de um laboratório multimédia com acesso a um estúdio de gravação e software de pós-produção de recursos, para docentes e estudantes.
O acervo físico existente na biblioteca assegura igualmente, sobretudo do ponto de vista didático, os recursos bibliográficos necessários, embora se preveja expansão nas áreas recentes da oferta do Iscte.

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

Student enrollment generates access credentials to the computer network, including the Fénix+ academic management system, the e-learning platform Moodle, VPN, wireless access throughout the Iscte campus, and the library website, specifically designed for students, which provides access to numerous electronic databases and specialty journals in various scientific areas. The 24/7 accessible e-learning platform contains pedagogical interaction features available to all participants in the educational process.
Iscte provides classrooms equipped with computers, projectors, and sound systems for use by teachers and students, including laboratory formats (22 on the Lisbon campus and 1 on the Sintra campus) and "Bring Your Own Device" options (3 on the Lisbon campus and12 on the Sintra campus). In the current context, there has been a significant reinforcement in auditoriums and classrooms to enable the recording/dissemination of classes and other events. There are also rooms equipped for video conferencing. Iscte-Sintra also has a multimedia laboratory with access to a recording studio and post-production software for resources, available to teachers and students.
The existing physical collection in the library also ensures the necessary bibliographic resources, especially from a didactic standpoint, although expansion is expected in the recent areas of Iscte's offerings.

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 total de docentes	N.º de docentes do ciclo de estudos integrados
Centro de Investigação em Ciências da Informação, Tecnologias e Arquitetura (ISTAR – IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	4	0
DINÂMIA´CET-IUL, Centro de Estudos Sobre a Mudança Socioeconómica e o Território (DINÂMIA´CET-IUL)	Muito Bom	ISCTE - Instituto Universitário de Lisboa (ISCTE-IUL)	Institucional	1	0
Instituto de Telecomunicações (IT)	Muito Bom	Instituto de Telecomunicações (IT)	Polo	1	0

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

Envolvimento num conjunto de associações e atividades relacionadas com a cibersegurança, que podem promover o acesso a empresas e profissionais na área: - AP2SI – Associação Portuguesa para a Promoção da Segurança de Informação - OWASP – Open Worldwide Application Security Project Atividades de normalização internacional: - MPAI – Moving Picture, Audio and Data Coding By Artificial Intelligence (arquitetura de segurança para o MPAI-AIH) - CT 163 – Segurança em Sistemas de Informação (responsável por seguir a ISO/IEC JTC 001/SC 027 IT Security techniques; ISSO/IEC JTC 001/SC 027/WG 001 Information security management systems; ISSO/IEC JTC 001/SC 027/WG 005 Identity management and privacy technologies) - CT 208 – Blockchain e Distributed Ledger Technologies (DLT) (responsável por seguir a ISO/TC 307 - Blockchain and distributed ledger technologies; CEN/CLC/JTC 019 - Blockchain and Distributed Ledger Technologies) Alguns projetos relevantes na área: - C-Academy – Academia de Formação em Cibersegurança do Centro Nacional de Cibersegurança (projeto de formação e treino em cibersegurança) - AppSentinel – Cloud-based Anti Malware Technology for Android App Stores (P2020) - AIM-Health - Aplicações Móveis Baseadas em Inteligência Artificial para Resposta de Saúde Pública (FCT) - Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open

testbed stress-testing system (H2020 – Grant agreement ID: 833088) - Maritime Integrated Surveillance Awareness (H2020 - Grant agreement ID: 740698) - Strategic programs for advanced research and technology in Europe (H2020 – Grant agreement ID: 830892) - End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem (H2020 - Grant agreement ID: 883242)

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

Involvement in a set of associations and activities related to cybersecurity, which may promote access to companies and professionals in the area: - AP2SI - Portuguese Association for the Promotion of Information Security - OWASP - Open Worldwide Application Security Project International standardization activities: - MPAI - Moving Picture, Audio and Data Coding By Artificial Intelligence (security architecture for MPAI-AIH) - CT 163 - Information Systems Security (responsible for following ISO/IEC JTC 001/SC 027 IT Security techniques; ISSO/IEC JTC 001/SC 027/WG 001 Information security management systems; ISSO/IEC JTC 001/SC 027/WG 005 Identity management and privacy technologies) - CT 208 - Blockchain and Distributed Ledger Technologies (DLT) (responsible for following ISO/TC 307 - Blockchain and distributed ledger technologies; CEN/CLC/JTC 019 - Blockchain and Distributed Ledger Technologies) Some relevant projects in the area: - C-Academy - Cybersecurity Training Academy of the National Cybersecurity Center (cybersecurity training and education project) - AppSentinel - Cloud-based Anti Malware Technology for Android App Stores (research project) - AIM-Health - Artificial Intelligence-based Mobile Applications for Public Health Response (research project) - Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system (H2020 – Grant agreement ID: 833088) - Maritime Integrated Surveillance Awareness (H2020 - Grant agreement ID: 740698) - Strategic programs for advanced research and technology in Europe (H2020 – Grant agreement ID: 830892) - End-to-end Security of the Digital Single Market's E-commerce and Delivery Service Ecosystem (H2020 - Grant agreement ID: 883242)

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)

Politica_de_protecao_de_dados_Iscte.pdf | *PDF | 777 Kb*

10. Comparação com CE de referência

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

O Observatório da Cibersegurança do CNCS, em Portugal (2022), reporta 9 mestrados no tema da segurança, sendo 4 destes específicos em cibersegurança. 4 são oferecidos por institutos politécnicos, e 5 por universidades (U. Aveiro, U. Lisboa – F. Direito; IST; E. Naval, U. Coimbra – FCT, U. Lisboa – FC, U.Porto – FC). A nível europeu, recorrendo à "CYBERHEAD" da ENISA, encontramos 105 mestrados que abordam a temática da segurança, sendo 71 específicos em cibersegurança. Apenas um deles é específico em "Cibersegurança e Resiliência", oferecido pela Sankt Polten University of Applied Sciences, na Áustria. Este é o concorrente direto do mestrado apresentado.
A nível nacional, os seguintes apresentam algumas semelhanças:
- Mestrado em Cibersegurança, Univ. Aveiro
- Mestrado em Segurança Informática, Univ. Coimbra – Fac. de Ciências
- Mestrado em Segurança Informática, Univ. Lisboa – Fac. de Ciências
- Mestrado em Segurança Informática, Univ. Porto – Fac. de Ciências.

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

The CNCS Cybersecurity Observatory, in Portugal (2022), reports 9 master's degrees in the subject of security, 4 of these being specific in cybersecurity. 4 are offered by polytechnic institutes, and 5 by universities (U. Aveiro, U. Lisboa - F. Direito; IST; E. Naval, U. Coimbra - FCT, U. Lisboa - FC, U.Porto - FC). At a European level, using ENISA's "CYBERHEAD", we found 105 master's degrees that address the topic of security, 71 of which are specific in cybersecurity. Only one of them is specific in "Cybersecurity and Resilience", offered by the Sankt Polten University of Applied Sciences, in Austria. This is the direct competitor of the presented master's degree.
At the national level, the following have some similarities:
- Master in Cybersecurity, Univ. Aveiro
- Master in Computer Security, Univ. Coimbra - Fac. de Ciências
- Master in Information Security, Univ. Lisbon - Fac. de Ciências
- Master in Computer Security, Univ. Porto - Fac.

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

A oferta nacional e internacional é demasiado centrada na vertente tecnológica da cibersegurança (CS). Esta proposta aborda a CS de forma integrada na tecnologia, nos processos e nas pessoas. Inclui unidades curriculares alinhadas com estes três pilares. Outro fator diferenciador consiste na cobertura das diferentes funções de CS conforme é especificado pelo CSF da NIST. Outros mestrados centram-se fundamentalmente na função de PROTEÇÃO. Este mestrado aborda todas as outras funções.

Outra diferença advém da vertente de resiliência. A CS é reação, a resiliência tem a ver com a antecipação. No nosso mestrado abordamos a resiliência como princípio fundamental para futuros profissionais possam ajudar as organizações a anteciparem as ameaças emergentes.
A abordagem mista de ensino à distância (EaD) e presencial, vai facilitar a interação entre as organizações e profissionais da área, permitindo que os estudantes possam ter um contacto muito mais próximo com a realidade e atualidade.

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

The national and international offer is too focused on the technological side of cybersecurity (CS). This proposal addresses CS in an integrated way in technology, processes and people. It includes curricular units aligned with these three pillars. Another differentiating factor is the coverage of the different CS functions as specified by the NIST CSF. Other masters focus fundamentally on the PROTECTION function. This master's degree covers all the other functions.
Another difference comes from the resilience aspect. CS is reaction, resilience is about anticipation. In our master we address resilience as a fundamental principle for future professionals to help organisations anticipate emerging threats.
The mixed approach of distance learning and face-to-face, will facilitate the interaction between organisations and professionals in the area, allowing students to have a much closer contact with reality and actuality.

11. Estágios-Formação

11.1. e 11.2 Estágios e/ou Formação em Serviço

Mapa VI - null

11.1.1. Entidade onde os estudantes completam a sua formação:

[sem resposta]

11.1.2. Protocolo:

[sem resposta]

11.2. Plano de distribuição dos estudantes

11.2. Plano de distribuição dos estudantes pelos locais de estágio e/ou formação em serviço demonstrando a adequação dos recursos disponíveis:

[sem resposta]

11.3. Recursos institucionais

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

[sem resposta]

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

[sem resposta]

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:

[sem resposta]

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

12. Análise SWOT

12.1. Pontos fortes. (PT)

- Alinhamento com as necessidades do mercado em cibersegurança.
- Abordagem multidisciplinar à cibersegurança e resiliência.
- Parte da formação com abordagem em ensino à distância.
- Diversidade dos domínios de qualificação contemplados, incrementando o potencial de inserção profissional.
- Ensino o que aposta na colaboração com empresas e profissionais do setor permitindo aos estudantes a aquisição de mais conhecimentos, orientada a problemas reais.
- Mestrado alinhado com as áreas científicas de investigação de algumas unidades de investigação do Iscte.
- Objetivos do ciclo de estudos coerente com a missão estratégia do Iscte-Sintra.
- Flexibilidade da estrutura curricular, com um conjunto de UC opcionais para escolha dos estudantes.
- Possibilidade da realização de projetos de mestrado integrados em empresas de cibersegurança.

12.1. Pontos fortes. (EN)

- Alignment with market needs in cybersecurity.
- Multidisciplinary approach to cybersecurity and resilience.
- Part of the training with a distance learning approach.
- Diversity of the qualification domains covered, increasing the potential for professional insertion.
- Teaching which focuses on collaboration with companies and professionals in the sector allowing students to acquire more knowledge, oriented to real problems.
- Master aligned with the scientific areas of research of some research units of the Iscte.
- Objectives of the study cycle coherent with the strategic mission of Iscte-Sintra.
- Flexibility of the curricular structure, with a set of optional CU to choose from.
- Possibility of carrying out integrated master's projects in cybersecurity companies.

12.2. Pontos fracos. (PT)

- Produto de 2º ciclo novo no mercado, que apesar de ter as suas próprias especificidades, tem alguma concorrência no mercado nacional e internacional.

12.2. Pontos fracos. (EN)

- A 2nd cycle product new to the market, which despite having its own specificities, has some competition in the national and international market.

12.3. Oportunidades. (PT)

-O mercado apresenta uma enorme carência de recursos na área de cibersegurança
-Estudantes da licenciatura em Tecnologias Digitais de Segurança de Informação que podem transitar para o mestrado para aprofundarem os seus conhecimentos
-Dinâmica de transição digital das atividades económicas e sociais aumentam as necessidades de cibersegurança e resiliência
-Atual conversão de profissionais para outras áreas, nomeadamente em cibersegurança
-Crescente procura de estudantes pela área de cibersegurança
-Apesar de existir oferta de 2º ciclo a nível nacional e internacional,é insuficiente face às necessidades
-Maior preocupação dos negócios com as questões da cibersegurança e resiliência
-Obrigações legais e regulamentares das organizações (RGPD,NIS,NIS2) que aumentam a necessidade de profissionais de cibersegurança
-Possibilidade da criação de conhecimentos, produtos e serviços em cibersegurança, resultantes dos trabalhos de mestrados dos estudantes com organizações e profissionais na área.

12.3. Oportunidades. (EN)

-Currently, the market presents a severe deficiency of this type of resources in the area of cybersecurity
-Students from the degree in Digital Security Technologies can transition to the master's degree in order to deepen their knowledge
-Dynamics of digital transition of economic and social activities increase the needs of cybersecurity and resilience
-Current conversion of professionals to other areas, particularly in cybersecurity
-Growing demand for the area of cybersecurity
-Although there is supply of 2nd cycle courses at national and international level, it is insufficient considering the needs
-Greater concern of businesses with cybersecurity and resilience issues.
-Legal and regulatory obligations of organisations (GDPR, NIS, NIS2) that increase the need for cybersecurity professionals
-Possibility of creating new knowledge, products and services in cybersecurity, resulting from the students' masters' work with organisations and professionals in the area.

12.4. Constrangimentos. (PT)

- A rápida evolução da área da cibersegurança, quer tecnológica quer metodológica, dificulta o ajustamento da oferta formativa à procura existente.
- Potencial surgimento de oferta concorrente na área da Cibersegurança, nomeadamente em Instituições privadas e que possam concorrer geograficamente com a proposta apresentada.
- A concorrência de ciclos de estudo semelhantes noutros países europeus pode reduzir o número de potenciais candidatos internacionais.

12.4. Constrangimentos. (EN)

- The rapid evolution of the cyber-security area, both technological and methodological, makes it difficult to adjust the training offer to the existing demand.
- Potential emergence of competing offers in the area of Cyber-security, namely from private institutions that may geographically compete with the presented proposal.
- Competition from similar study cycles in other European countries may reduce the number of potential international candidates.

12.5. Conclusões. (PT)

A área da cibersegurança continua a registar um franco crescimento em termos de procura no mercado profissional. Existe uma pronunciada carência deste tipo de profissionais no mercado, sendo que a mesma continua a registar uma tendência para crescer. Por isso mesmo, a oferta de um mestrado em "Cibersegurança e Resiliência" é uma excelente oportunidade como uma resposta a esta carência. Por outro lado, esta proposta de mestrado aborda o tema da "ciber-resiliência" que é um dos temas abrangentes da cibersegurança, e que ajuda as organizações a estarem preparadas, construírem capacidades de resposta e de recuperação de ciber-ameaças. Finalmente, este mestrado está alinhado com a estratégia do Iscte-Sintra e com a oferta formativa existente na área.

12.5. Conclusões. (EN)

The area of cybersecurity continues to grow rapidly in terms of demand in the professional market. There is a pronounced shortage of this type of professional on the market, and it continues to grow. This is why offering a master's programme in "Cybersecurity and Resilience" is an excellent opportunity to respond to this shortage. On the other hand, this master's proposal addresses the topic of "cyber resilience", which is one of the overarching themes of cybersecurity, and which helps organisations to be prepared, build response capacities and recover from cyber threats. Finally, this master's programme is aligned with Iscte-Sintra's strategy and the existing training offer in the area.