1. Caracterização geral do ciclo de estudos

1.1. Instituição de Ensino Superior:

Instituto Politécnico De Viana Do Castelo

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

[sem resposta]

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

[sem resposta]

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

[sem resposta]

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

Escola Superior De Tecnologia E Gestão De Viana Do Castelo

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

1.3. Designação do ciclo de estudos (EN):

Cybersecurity

1.4. Grau (PT):

Mestre

1.4. Grau (EN):

Master

1.5. Publicação do plano de estudos em Diário da República.

Despacho 8235-2019.pdf | *PDF* | *442.9 Kb*

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

Ciência de Computadores

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

Computer Science

1.7.1. Classificação CNAEF - primeira área fundamental

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

1.7.2. Classificação CNAEF - segunda área fundamental, se aplicável

*[0523] Eletrónica e Automação
Engenharia e Técnicas Afins
Engenharia, Indústrias Transformadoras e Construção*

1.7.3. Classificação CNAEF - terceira área fundamental, se aplicável

[sem resposta]

1.8. Número de créditos ECTS necessário à obtenção do grau.

120.0

1.9. Duração do ciclo de estudos

2 anos

1.10.1. Número máximo de admissões em vigor.

30

1.10.2. Número máximo de admissões pretendido (se diferente do número em vigor) e respetiva justificação.

[sem resposta]

1.11. Condições específicas de ingresso (PT)

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

1.11. Condições específicas de ingresso (EN)

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

1.12. Modalidade do ensino

[ ] Presencial (Decreto-Lei n.º 65/2018, de 16 de agosto) [X] A Distância (EaD) (Decreto-Lei n.º 133/2019, de 3 de setembro)

1.12.1. Regime de funcionamento, se presencial

[sem resposta]

1.12.1.1. Se outro, especifique. (PT)

[sem resposta]

1.12.1.1. Se outro, especifique. (EN)

[sem resposta]

1.13. Local onde o ciclo de estudos será ministrado, se presencial (PT)

Escola Superior de Tecnologia e Gestão do Instituto Politecnico de Viana do Castelo

1.13. Local onde o ciclo de estudos será ministrado, se presencial. (EN)

Escola Superior de Tecnologia e Gestão from Instituto Politecnico de Viana do Castelo

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

1.14._1.14._Despacho_4872-2016_e_Despacho 9946-2019-Revisao-Reg-Creditacao-Competencias e Alteracao.pdf | PDF | 242.3 Kb

1.15. Tipo de atribuição do grau ou diploma

[sem resposta]

1.16. Observações. (PT)

[sem resposta]

1.16. Observações. (EN)

[sem resposta]

2. Decisão de acreditação na avaliação anterior.

2.1. Referência do processo de avaliação anterior.

NCE/18/1800154

2.2. Data da decisão.

21/05/2019

2.3. Decisão do Conselho de Administração.

Acreditar com condições | Accredit with conditions

2.4. Período de acreditação.

6 anos | 6 years

2.5. A partir de:

31/07/2019

3. Sintese medidas de melhoria

3. Síntese de medidas de melhoria e alterações ao ciclo de estudos desde a avaliação anterior (PT)

O relatório final da CAE NCE/18/0000154 - Novo ciclo de estudos, no seu ponto 3.4.3. Recomendações de melhoria, indica "Nada a referir."

3. Síntese de medidas de melhoria e alterações ao ciclo de estudos desde a avaliação anterior (EN)

The CAE final report NCE/18/0000154 - New study cycle, in point 3.4.3. Recommendations for improvement, indicates "Nothing to mention."

4.Estrutura curricular e plano de estudos.

4.1. Estrutura curricular

4.1. Estrutura curricular e plano de estudos em vigor, correspondem ao publicado em Diário da República (ponto 1.5)?

[ ] Sim [X] Não

4.2. Serão feitas alterações nos dados curriculares?

[X] Sim [ ] Não

4.2.1. Síntese das alterações pretendidas e respetiva fundamentação. (PT)

A reestruturação do curso compreendeu uma reorganização dos ECTS e uma adaptação para o ensino a distância e híbrido, com o objetivo de promover a flexibilidade e alinhamento com as normativas vigentes.

- Uniformização dos ECTS
Com o intuito de simplificar a mobilidade e a transferibilidade de créditos entre instituições, os planos curriculares de licenciatura e mestrado foram uniformizados para que todas as Unidades Curriculares (UC) possuam créditos em múltiplos de três. Assim, UCs anteriormente com 5 ECTS passaram a ter 6, e UCs com 4 ECTS passaram a ter 3. Esta uniformização facilita o cálculo e o reconhecimento de créditos, promovendo uma coerência no sistema europeu de créditos.

- Ensino a Distância e Híbrido
De acordo com o Modelo Pedagógico de Ensino a Distância (EaD) do IPVC, em conformidade com a legislação (DL 133/2019) e critérios da A3ES (Despacho nº 16/2022), o curso poderá oferecer até 15% das horas de contacto em formato de ensino a distância (EaD), distribuídas entre sessões síncronas e assíncronas. Para esta modalidade, é obrigatória a submissão de uma proposta ao conselho técnico-científico (CTC), que, após aprovação, será publicada pela DGES. Esta proposta deve incluir:
1. Qualificação do Corpo Docente: Demonstração de formação certificada dos docentes em EaD, conforme exigências do Despacho nº 16/2022.
2. Metodologia Adaptada: Justificação da metodologia aplicada para o ensino a distância e/ou híbrido, detalhando as abordagens pedagógicas e as ferramentas que viabilizam o ensino não presencial.
3. Calendarização e Conteúdos: Apresentação de um cronograma específico com datas de sessões presenciais e online, e descrição dos conteúdos programáticos a serem lecionados em EaD, incluindo objetivos de aprendizagem, e-atividades e recursos digitais associados.

Nas UC's com docentes que tem formação em EaD, foram incluídas percentagens de horas em EaD, cuja abordagem às mesmas é descrita na metodologia de ensino das unidades curriculares em causa.

- Ajuste nas Semanas de Aulas
Para otimizar a organização do semestre, o número de semanas letivas foi ajustado de 16 para 15, através da redução de duas horas de contacto em cada UC. Esta redução foi compensada com a transferência de horas necessárias à abordagem dos conteúdos programáticos para horas de trabalho autónomo, garantindo a continuidade e a qualidade dos objetivos de aprendizagem. As adaptações foram realizadas de forma a manter a coerência do curso e o cumprimento dos resultados esperados de aprendizagem.

4.2.1. Síntese das alterações pretendidas e respetiva fundamentação. (EN)

The restructuring of the course included a reorganization of the ECTS and an adaptation to distance and hybrid learning, with the aim of promoting flexibility and alignment with current regulations.

- Standardization of ECTS
With the intention of simplifying mobility and transferability of credits between institutions, the undergraduate and master's curricular plans were standardized so that all Curricular Units (CU) have credits in multiples of three. Thus, CUs previously with 5 ECTS now have 6, and CUs with 4 ECTS now have 3. This standardization facilitates the calculation and recognition of credits, promoting coherence in the European credit system.

- Distance and Hybrid Learning
According to the IPVC Distance Learning Pedagogical Model (EaD), in accordance with legislation (DL 133/2019) and A3ES criteria (Order nº 16/2022), the course may offer up to 15% of contact hours in a distance learning (EaD) format, distributed between synchronous and asynchronous sessions. For this modality, it is mandatory to submit a proposal to the technical-scientific council (TSC), which, after approval, will be published by DGES. This proposal must include:
1. Qualification of the Teaching Staff: Demonstration of certified training of teachers in distance learning, in accordance with the requirements of Order No. 16/2022.
2. Adapted Methodology: Justification of the methodology applied for distance and/or hybrid teaching, detailing the pedagogical approaches and tools that enable non-face-to-face teaching.
3. Schedule and Content: Presentation of a specific schedule with dates for in-person and online sessions, and description of the programmatic contents to be taught in distance learning, including learning objectives, e-activities and associated digital resources.

In curricular units with teachers who have distance learning training, percentages of hours in distance learning were included, and the approach to them is described in the teaching methodology of the curricular units.

- Adjustment in Class Weeks
To optimize the organization of the semester, the number of academic weeks was adjusted from 16 to 15, by reducing two contact hours in each UC. This reduction was compensated by transferring the hours needed to cover the syllabus to hours of independent work, ensuring the continuity and quality of the learning objectives. The adaptations were made in order to maintain the coherence of the course and the fulfillment of the expected learning results.

Mapa II - Percurso Geral

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

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

4.1.2. Áreas científicas e créditos necessários à obtenção do grau

Área Científica	Sigla	ECTS	ECTS Minímos
Ciência de Computadores e Telecomunicações	CCT	63.0	57.0
Total: 1		Total: 63.0	Total: 57.0

4.1.3. Observações (PT)
O CE tem um plano de estudos que consiste num plano curricular com um único percurso geral.

4.1.3. Observações (EN)
The SC comprehends a unique curricular plan without branches or specializations.

4.2. Unidades Curriculares

Mapa III - Análise de Dados e Ciberinteligência

4.2.1. Designação da unidade curricular (PT):
Análise de Dados e Ciberinteligência

4.2.1. Designação da unidade curricular (EN):
Data Analytics and Cyber Intelligence

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 2ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 2nd S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-11.0; PL-15.0
Síncrona a distância (SD) - TP-4.0

4.2.6. % Horas de contacto a distância:
13.33%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Jorge Manuel Ferreira Barbosa Ribeiro - 15.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
• Ricardo Jorge da Silva Santos - 15.0h

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A. Compreender as ameaças e as motivações por detrás destas;
B. Reconhecer diferentes tipos de ciber ameaças;
C. Compreender a diferença entre dados, informação e inteligência ao nível das ciber ameaças;
D. Compreender o processo de aquisição, análise de dados e apresentação de indicadores de compromisso relacionados com ciber ameaças;
E. Identificar e sugerir ferramentas e fontes de inteligência adequados à organização;
F. Auxiliar as organizações na avaliação do seu conhecimento situacional sobre ciber ameaças;
G. Desenhar, gerir ou apoiar a implementação e manutenção de um programa de cyber intelligence e cyber awareness.

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

A. Understand the cyber threats and the motivations behind these;
B. Recognize different types of cyber threats;
C. Understand the difference between data, information and intelligence;
D. Understand the process of data acquisition, data analysis and data presentation;
E. Identify and suggest tools and sources of intelligence according to the organization needs;
F. Support organizations in assessing their situational awareness on cyber threats;
G. Design, manage or support the implementation of cyber intelligence and awareness programs.

4.2.11. Conteúdos programáticos (PT):

1. Ameaças cibernéticas - Tipos de ameaças - Motivações - O negócio das ameaças - Utilizar/mostrar casos
2. Inteligência Cibernética - O ciclo da inteligência - Tipos de inteligência - Negação e engano - Inteligência cibernética - O profissional de inteligência cibernética
3. Construir um modelo de inteligência cibernética - A anatomia de um ataque - Limitações das soluções de segurança tradicionais - Abordagem dos ataques cibernéticos - Incorporar o ciclo de vida da inteligência no fluxo de trabalho de segurança
4. Construir e manter um programa de ciberinteligência - Recolha de dados - Análise e apresentação de dados - Fazê-lo internamente, externamente ou ambos?
5. Partilha de inteligência - Plataformas de Inteligência de Ameaças - Comunidades - Esforços de interoperabilidade
6. Consciência situacional cibernética - Quadro Operacional Comum Cibernético - Infraestrutura Crítica e Recursos Chave - Avaliação Contínua
7. Inteligência Cibernética e Análise de Dados na prática

4.2.11. Conteúdos programáticos (EN):

1. Cyber threats- Types of threats- Motivations- The threats business- Use/show cases
2. Cyber Intelligence- The intelligence cycle - Types of intelligence (strategic, operational, tactical)- Denial and deception- Cyber (threat) intelligence- The cyber intelligence professional
3. Building a cyber intelligence model- The anatomy of an attack- Limitations traditional security solutions- Approaching cyber attacks- Incorporating the intelligence lifecycle into security workflow
4. Building and maintaining a cyber intelligence program - Data gathering- Data analysis and presentation- Do it internally, externally or both?
5. Intelligence sharing- Threat Intelligence Platforms- Communities - Interoperability efforts
6. Cyber situational awareness- Cyber Common Operating Picture- Critical Infrastructure and Key Resources- Continuous Assessment
7. Cyber Intelligence and Data Analytics in practice

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A
2 – B
3 – C
4 – D, E
5 – D, E
6 – E, F
7 -F, G

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A
2 – B
3 – C
4 – D, E
5 – D, E
6 – E, F
7 -F, G

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

As aulas incluem sessões teóricas, discussões dirigidas e sessões de carácter prático. Nas sessões teóricas será utilizado o método expositivo. As discussões dirigidas serão orientadas para o estudo de casos. As sessões de carácter prático incluem a resolução de exercícios destinados a validar as competências adquiridas.
O ensino contará ainda com o estímulo à criatividade e autonomia do aluno. Este estímulo será implementado através da leitura de artigos e da apresentação dos resultados dos trabalhos de pesquisa e de aplicação prática das competências adquiridas.
Complementarmente, nesta unidade curricular, no sentido de potenciar o pensamento crítico dos alunos serão usadas abordagens pedagógicas ativas, ensino híbrido e a distância conforme o modelo pedagógico do IPVC.

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

Classes include theoretical sessions, guided discussions and practical sessions. In the theoretical sessions will be used the expository method. The guided discussions will be supported by case studies. The practical sessions include exercises designed to assess the competencies acquired.
The teaching will also stimulate the creativity and learning autonomy. This will be achieved by promoting the reading of articles and their public presentation, as well as, the practical application of competencies acquired during the course.
In addition, this curricular unit will use active pedagogical approaches, hybrid and distance learning, in line with IPVC's pedagogical model, in order to enhance students' critical thinking.

4.2.14. Avaliação (PT):
A avaliação dos alunos é contínua ou por exame final.
Na avaliação contínua a classificação final é obtida com base em:

a) Teste escrito (30%);
b) Trabalho prático (70%): Submissão de documentação (documento tipo artigo científico, apresentação em formato PPT/PDF) e código de execução (na linguagem de programação python, java, c ou outra).

Na avaliação por exame final a classificação final é obtida com base em: Exame teórico-prático composto por duas partes (parte teórica 50% e parte prática 50%)
Os estudantes que obtenham aprovação a uma das partes só tem que realizar em exame a parte que falta.

4.2.14. Avaliação (EN):
The assessment can be done by continuous assessment or final exam.

In the continuous assessment the final classification is obtained as follows:
(a) Written test (30%);
(b) Practical work (70%): Submission of documentation (scientific paper type document, presentation in PPT/PDF format) and execution code (in python, java, c or other programming language).

In the final exam assessment, the classification is obtained as follows:
a) Theoretical and practical exam with two parts (theoretical part 50% and practical part 50%).

Students who get approval just to one of the parts only have to do the missing part in the 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 estão em coerência com os objetivos da unidade curricular dado que:
1) Os métodos de ensino utilizados, ajustam-se à natureza dos conteúdos programáticos e dos objetivos a atingir em cada sessão. A realização de exposições sobre as diferentes matérias (palestra, discussão dirigida, execução), quer por parte do docente, quer dos estudantes, conjuga-se com a metodologia de avaliação estabelecida, permitindo assim atingir os objetivos definidos.

2) As metodologias de ensino utilizadas procuram, sempre que possível, potenciar a participação ativa dos discentes. Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC.

O regime de avaliação foi concebido para avaliar a extensão e o nível de aquisição das competências a desenvolver.

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

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

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

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

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

Building an Intelligence-Led Security Program, Allan Liska, ISBN: 9780128021453, Syngress Media, U.S., 2014
Janeja, V. (2022). Data Analytics for Cybersecurity. Cambridge University Press.
How to Define and Build an Effective Cyber Threat Intelligence Capability, Henry Dalziel, ISBN: 978-0128027301, Syngress, 2014
Effective Threat Intelligence: Building and running an intel team for your organization, James Dietle, ISBN-13: 978-1533314550, CreateSpace Independent, 2016

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

Building an Intelligence-Led Security Program, Allan Liska, ISBN: 9780128021453, Syngress Media, U.S., 2014
Janeja, V. (2022). Data Analytics for Cybersecurity. Cambridge University Press.
How to Define and Build an Effective Cyber Threat Intelligence Capability, Henry Dalziel, ISBN: 978-0128027301, Syngress, 2014
Effective Threat Intelligence: Building and running an intel team for your organization, James Dietle, ISBN-13: 978-1533314550, CreateSpace Independent, 2016

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Auditoria e Conformidade em Cibersegurança

4.2.1. Designação da unidade curricular (PT):

Auditoria e Conformidade em Cibersegurança

4.2.1. Designação da unidade curricular (EN):

Cybersecurity Audit and Compliance

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

CCT

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

CST

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

Semestral 2ºS

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

Semiannual 2nd S

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

81.0

4.2.5. Horas de contacto:

Presencial (P) - T-0.0; TP-21.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:

0.00%

4.2.7. Créditos ECTS:

3.0

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

• Pedro Miguel Simões Pinto Carneiro - 21.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:

[sem resposta]

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

A. Explicar o uso de standards em auditoria (ISO 19011) e verificar a conformidade do SGSI.
B. Desenvolver, implementar e executar uma estratégia de auditoria ao SGSI
C. Descrever os componentes e os requisitos básicos necessários num plano de auditoria.
D. Descrever os parâmetros necessários para conduzir e relatar uma auditoria.
E. Avaliar o desenho, implementação e monitorização dos controles de segurança implementados e verificar se garantem a proteção dos ativos de informação da organização.
F. Realizar uma análise critica de situações legais e éticas, examinar a sua possível resolução e recomendar um conjunto de ações.

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

A. Describe the role of Audit Standard (ISO 19011) and verify compliance with the security standard ISO/IEC 27001.
B. Explain the use of standards and frameworks in a compliance audit of an ISMS.
C. Develop, implement and execute an ISMS audit strategy in compliance with the standard ISO/IEC 27001.
D. Describe the components and basic requirements for creating an audit plan.
E. Evaluate the design, implementation, and monitoring of various security controls to ensure information assets are adequately protected.
F. Critically analyze legal and ethical situations, examine their possible resolution and recommend a justifiable course of action.

4.2.11. Conteúdos programáticos (PT):

1 - (Conceitos e definições)
1.1 Modelo PDCA e sua aplicação num SGSI
1.2. Normas e diretrizes para auditoria de um SGSI (por exemplo, ISACA, COBIT, ITIL)
2 - (Processo de auditoria)
2.1. Compreender o negócio da organização
2.2. O ciclo de vida da auditoria do SGSI
2.3. Responsabilidade, autoridade e responsabilidade do auditor do SGSI4. Código de ética profissional, leis e regulamentação
3 - (Processo de Risco de Auditoria)
3.1. Elementos de uma análise de risco
3.2. Auditoria baseada na análise do risco e métodos de avaliação de risco
4 - (Planeamento e Gestão de Auditorias)
4.1. Desenvolvimento do plano de auditoria
4.2. Classificação de auditorias e âmbito
4.3. Missão da auditoria
5 - (Evidência de Auditoria)
5.1. Procedimento de recolha de evidências de auditoria
5.2. Conformidade
6 - (Relatório de Auditoria)
6.1. Elaboração do relatório executivo e os resultados
6.2. Comunicação dos resultados da auditoria

4.2.11. Conteúdos programáticos (EN):

1 (Concepts and definitions)
1.1. PDCA model and its application in an ISMS
1.2. Standards and guidelines for ISMS auditing (e.g. ISACA, COBIT, ITIL)
2 (Audit Process)
2.1. Understanding the organization?s business
2.2. The ISMS audit life-cycle
2.3. The ISMS auditor responsibility, authority and accountability
2.4. Code of professional ethics, laws, and regulations
3 (Audit Risk Process)
3.1. Elements of a risk analysis
3.2. Risk-based auditing and risk assessment methods
4 (Audit Planning and Management)
4.1. Developing the audit plan
4.2. Classification and scope audits
4.3. Audit mission
5 (Audit Evidence)
5.1. Audit evidence procedures
5.2. Compliance
6 (Audit Reporting)
6.1. Writing the executive summary and findings
6.2. Communicate the auditing results

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A,B,C,F
2 – C,D,E,F
3 – C,E,F
4 – E,F
5 – E,F
6 – F

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A,B,C,F
2 – C,D,E,F
3 – C,E,F
4 – E,F
5 – E,F
6 – F

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

As aulas incluem sessões teóricas. Nas sessões teóricas será utilizado essencialmente o método expositivo e demonstrações. As discussões dirigidas serão orientadas para o estudo de casos. As sessões de carácter prático incluem a utilização de ferramentas (treino) e a resolução de exercícios destinados a validar as competências adquiridas.
A maioria das atividades a desenvolver pelos alunos são supervisionadas. Não obstante, em alguns tópicos onde existem questões em aberto, as atividades de ensino procurarão estimular a criatividade e autonomia do aluno. Estas tarefes assentarão predominantemente na leitura de artigos científicos e relatórios técnicos, complementada com produção de trabalhos de síntese.

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

Classes include theoretical sessions. In theoretical sessions, the expository method and projections will essentially be used. Directed discussions will focus on case studies. Specific sessions include the use of tools (training) and the resolution of exercises designed to validate the skills acquired.

Most of the activities to be developed by students are supervised. However, in some topics where there are open questions, academic activities will seek to stimulate student creativity and autonomy. These rates will be based predominantly on reading scientific articles and technical reports, complemented by the production of synthesis works.

4.2.14. Avaliação (PT):

1. Avaliação Contínua consiste numa simulação de auditoria prática resultante de reporting de auditoria tida, como auditor e auditado. Para aprovação tem de ter no mínimo 10 valores.

2. Avaliação: Normal e Recurso ou Especial:
O Exame Normal é 100% escrito e acessível apenas para os alunos que não realizaram a avaliação contínua e que não faltaram.

4.2.14. Avaliação (EN):

1. Continuous Assessment consists of a practical audit simulation resulting from audit reports taken as auditor and auditee.
To pass, you must have at least 10 points.

2. Assessment: Normal and Appeal or Special:
The Normal Exam is 100% written and accessible only to students who did not take the continuous assessment and who were not absent.

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

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

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

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

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

1] Pfleeger, Charles P., Pfleeger, Shari L., Security in Computing?, Fourth Edition, Prentice Hall PTR, 2007.
[2] Anderson, R. J., Security Engineering: A Guide to Building Dependable Distributed Systems?, 2nd Ed., Wiley Publishing, 2008. (http://www.cl.cam.ac.uk/~rja14/book.html)
Complementar:
[3] Tarantino, Anthony, Governance, Risk, and Compliance Handbook: Technology, Finance? 1st ed.: John Wiley & Sons, Inc., 2008.
[4] ISO/IEC 27007:2020 ? Information security, cybersecurity, and privacy protection Guidelines for information security management systems auditing (third edition).
[5] ISO/IEC TS 27008:2019 Information technology Security techniques Guidelines for the assessment of information security controls (second edition)
[6] Bishop, M.,Introduction to Computer Security?. Prentice-Hall PTR, 2004.

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

[1] Pfleeger, Charles P., Pfleeger, Shari L., Security in Computing?, Fourth Edition, Prentice Hall PTR, 2007.
[2] Anderson, R. J., Security Engineering: A Guide to Building Dependable Distributed Systems?, 2nd Ed., Wiley Publishing, 2008. (http://www.cl.cam.ac.uk/~rja14/book.html)
Complementar:
[3] Tarantino, Anthony, Governance, Risk, and Compliance Handbook: Technology, Finance? 1st ed.: John Wiley & Sons, Inc., 2008.
[4] ISO/IEC 27007:2020 ? Information security, cybersecurity, and privacy protection Guidelines for information security management systems auditing (third edition).
[5] ISO/IEC TS 27008:2019 Information technology Security techniques Guidelines for the assessment of information security controls (second edition)
[6] Bishop, M.,Introduction to Computer Security?. Prentice-Hall PTR, 2004.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Cibercrime e Análise Forense Digital

4.2.1. Designação da unidade curricular (PT):

Cibercrime e Análise Forense Digital

4.2.1. Designação da unidade curricular (EN):

Cybercrime and Digital Forensics Analysis

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

CCT

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

CST

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

Semestral 2ºS

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

Semiannual 2nd S

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

162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-30.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Marco Filipe Vieira Gomes - 18.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
• Pedro Miguel Simões Pinto Carneiro - 15.0h
• Rogério Bravo - 12.0h

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A .Conhecimento das restrições éticas e legais associadas aos testes de penetração e ethical hacking
B .Domínio das etapas de desenvolvimento de testes de penetração e apresentação de resultados
C. Identificação de aplicações/tráfego malicioso na rede
D. Implementação de aplicações úteis na exploração de falhas
E. Identificar ameaças e selecionar as medidas para impedir acesso físico a equipamentos e a mitigar ataques de engenharia social
F. Aplicar as medidas corretivas adequadas à mitigação de falhas de segurança
G. Identificar e resolver problemas nas aplicações e serviços web
H. Determinar falhas de segurança em redes móveis, e para implementar soluções de segurança das comunicações
I. Reforçar as competetências relacionadas com sistemas de IDS/IPS
J. Reforçar as capacidades dos serviços de autenticação e controlo de acesso
K. Identificar vulnerabilidades de dispositivos móveis e aplicação de medidas preventivas
L. Avaliar o risco da utilização de aplicações móveis

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A. Ethical policies and legality of activities involving penetration tests
B. Domain of the stages of penetration tests and final reporting results
C. Identify the type of applications/malicious traffic, determine vulnerabilities in services and elect the most appropriate exploits
D. Implement small applications useful in fault operation
E. Identify threats and select measures to prevent physical access and social engineering attacks
F. Apply appropriate corrective measures to mitigate security breaches
G. Identify and solve problems in web applications/services
H. Determine security flaws in mobile networks and to implementation of mitigation technics
I. Strengthen the skills of planning and implementation of detection systems / prevent attacks
J. Strengthen planning capabilities and implementation of authentication, access control and traffic analysis
K. Identify vulnerabilities of mobile devices and apply preventive measures
L. Assess the risk of using mobile applications

4.2.11. Conteúdos programáticos (PT):
1. Introdução aos conceitos do Ethical hacking
2. Tipos de ameaças e ataques a redes cabladas e sem fio
3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN)
4. Fragilidades protocolares dos s istemas de comunicações móveis
5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio
6. Metodologias para testes de penetração
7. Caracterização e implementação de ataques contra redes e sistemas móveis
8. Planeamento de soluções de comunicação segura em redes e sistemas móveis
9. Identificação e deteção de vulnerabilidades nos sistemas móveis
10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis

4.2.11. Conteúdos programáticos (EN):

1. Ethical hacking concepts
2. Types of threats and attacks on wired and wireless networks
3. Protocols and security algorithms in 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN) C4. Protocol weaknesses of mobile communication systems
5. Confidentiality, privacy and availability technologies in wireless networks
6. Methodologies for the penetration tests
7. Characterization and implementation of attacks against networks and mobile systems
8. Planning of secure communication solutions in mobile networks and systems
9. Identification and detection of vulnerabilities in mobile systems
10. Implementation mechanisms and security systems for wireless networks and mobile devices

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A,B
2 – C,E
3 – E,F
4 – D
5 – K
6 – G,H
7 – K
8 –J,L
9 – K
10 - I

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A,B
2 – C,E
3 – E,F
4 – D
5 – K
6 – G,H
7 – K
8 –J,L
9 – K
10 - I

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

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

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

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

4.2.14. Avaliação (PT):

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

4.2.14. Avaliação (EN):

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

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

A metodologia de ensino teórico-prático baseia-se na transmissão de conhecimentos sobre a segurança ao nível da segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas ubíquos, redes e aplicações, com vista a dar uma visão global do processo de exploração e mitigação de falhas, tendo sempre em linha de conta as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração. Permite desenvolver nos estudantes as competências (A,B,C).
A metodologia utilizada na componente laboratorial incide, numa primeira fase, na consolidação dos conhecimentos transmitidos na componete teórico-prática atraves da realização de trabalhos laboratoriais (A,B,C) e, numa fase posterior, na realização de um projeto prático, e que contempla as seguintes fases: a) estudo do cenário proposto, b) identificação de falhas e vulnerabilidades do cenário, c) seleção de mecanismos de exploração de vulnerabilidades adequados, d) realização de testes de penetração, e) mitigação de falhas detetadas e e) escrita de relatório e e) apresentação e defesa do projeto realizado, permitem desenvolver nos estudantes os objetivos (D,E,F,G,H,I,J,K,L)

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

The methodology of theoretical and practical teaching is based on the transmission of knowledge about offensive security for assessment and mitigation of vulnerabilities in ubiquitous systems, networks and applications, in order to give an overview of the exploration and mitigation of failures, taking into account the legal and ethical constraints of activities involving a penetration test. It allows us to develop students skills (A,B,C).
The methodology used in the lab component focuses initially on consolidation of the knowledge acquired in the prevoius component through the implementation of laboratory works (A,B,C) and, at a later stage, in the implemetation of a practical project that includes the following phases: a) study of the proposed scenario, b) identification of flaws and vulnerabilities of the scenario, c) selection of the appropriate exploit mechanisms, d) conducting penetration testing e) mitigation of the detected vulnerabilities e) writing report e) presentation and defense of the implemented project, allowing the students to develop the skills (D,E,F,G,H,I,J,K,L).

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

[1] Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; 9781264268948; McGraw-Hill Education; 6 ed., 2022
[2] Hacker's Playbook: Unraveling the Tactics Behind Cyber Attacks: "Investigate the Intricacies of Cyber Warfare: Decoding the Strategies Employed in Hacker's Playbook"; Harsh Pansuriya, ISBN: 979-8872840725, Independently Published, 2023
[3] The Hacker Playbook 3: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1980901754; CreateSpace Independent Publishing Platform, 2018.
[4] Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012

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

[1] Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; 9781264268948; McGraw-Hill Education; 6 ed., 2022
[2] Hacker's Playbook: Unraveling the Tactics Behind Cyber Attacks: "Investigate the Intricacies of Cyber Warfare: Decoding the Strategies Employed in Hacker's Playbook"; Harsh Pansuriya, ISBN: 979-8872840725, Independently Published, 2023
[3] The Hacker Playbook 3: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1980901754; CreateSpace Independent Publishing Platform, 2018.
[4] Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Criptografia Aplicada

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

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

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - T-0.0; TP-11.0; PL-15.0
Síncrona a distância (SD) - T-0.0; TP-4.0

4.2.6. % Horas de contacto a distância:
13.33%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Luís Manuel Cerqueira Barreto - 30.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A. Conhecimentos. escolher que algoritmos e técnicas utilizar, seja ao nível de utilizadores, programadores ou administradores de redes e sistemas
B. Conhecimentos. Familiaridade com desafios científicos em segurança da informação
C. Conhecimentos. Entender a utilização e a operação de uma variedade de mecanismos de controle de acesso e autenticação de utilizadores.
D. Aptidões e competências: Analisar, modificar, escolher e implementar os protocolos necessários para a uma aplicação prática
E. Aptidões e competências: Implementar os algoritmos criptográficos dados.
F. Aptidões e competências: Implementar ataques aos mesmos algoritmos e protocolos.
G. Aptidões e competências: Saber aplicar provas de segurança e capacidade de pensar abstratamente sobre problemas de segurança da informação.

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

A. Knowledge: Choose which algorithms and techniques to use, whether at users, programmers or network and system administrators level.
B. Knowledge: Familiarity with scientific challenges in information security.
C. Knowledge: Understand the use and operation of a variety of user access and authentication control mechanisms
D. Skills and competences: Analyze, modify, choose and implement the protocols necessary for a practical application.
E. Skills and competences: Implement the given cryptographic algorithms.
F. Skills and competences: Implement attacks on those algorithms and protocolos.
G. Skills and competences: Know how to apply security tests and the ability to think abstractly about information security issues.

4.2.11. Conteúdos programáticos (PT):

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

4.2.11. Conteúdos programáticos (EN):

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

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – a, b, c, d, e, f, g
2 – a, c, e, f, g
3 – a, c, e, f, g
4 – a, c, d, e, f, g
5 – a, c, d, e, f, g
6 – a, c, d, e, f, g
7 – a, b
8 - a,c, d, e, f, g
9 - a, b, c, d, e, f, g

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – a, b, c, d, e, f, g
2 – a, c, e, f, g
3 – a, c, e, f, g
4 – a, c, d, e, f, g
5 – a, c, d, e, f, g
6 – a, c, d, e, f, g
7 – a, b
8 - a,c, d, e, f, g
9 - a, b, c, d, e, f, g

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

Nas aulas teórico-práticas serão apresentados os temas do programa sob a forma de apontamentos ou slides. Nas aulas práticas serão realizados trabalhos práticos que pretendem consolidar e demonstrar a aplicação dos conceitos abordados. Nas duas tipologias de aula, serão utilizadas metodologias de fomento da participação dos alunos, através do método interrogativo, da aprendizagem colaborativa e cooperativa e da utilização de case based learning.
Na componente EaD da UC serão utilizadas metodologias ativas de aprendizagem nomeadamente gamificação, problema base learning e sala de aula invertida, suportadas nas plataformas Moodle@IPVC, Genially e Quizizzz.

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

In the theoretical-practical classes the program will be presented in the form of notes or slides. In the practical classes, practical assignments will be accomplished in order to consolidate and demonstrate the application of the concepts addressed. In both types of class, methodologies will be used to encourage student participation, through the interrogative method, collaborative and cooperative learning and the use of case-based learning.
The e-learning component of the CU will use active learning methodologies such as gamification, problem-based learning and the flipped classroom, supported through the Moodle@IPVC, Genially and Quizizzz platforms.

4.2.14. Avaliação (PT):
A Classificação Global (CG) em avaliação contínua desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.4*CT +0.6*CP*
CP: Avaliação contínua obtida através da realização de trabalhos práticos e respetivos relatórios.
*CT = 0,4*T*
CT: Realização de um teste (T)
Caso o aluno não tenha aproveitamento na avaliação contínua o aluno poderá realizar um exame global no final do período letivo.

4.2.14. Avaliação (EN):
The Global Classification (GC) of this curricular unit is obtained by the average of a theoretical component (TC) and a practical component (PC) with the following weighting:
*GC= 0.4*TC + 0.6*PC*
*PC: Continuous evaluation obtained through the accomplishment of practical works and respective reports. TC= 0,4*T*
TC: Conducting a test (T)
If the student does not pass on the continuous assessment, the student may take a global exam at the end of the term.

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

4.2.15. Demonstração da coerência das metodologias de ensino e avaliação com os objetivos de aprendizagem da unidade curricular. (EN):
The profile of future graduates of this cycle of studies will lead to qualified professionals, holders of knowledge, skills and competences in their area of formation. In this sense, and with a view to the operationalization of the objectives of the Curricular Unit in question, the methodologies adopted, based on theoretical and practical classes, articulated with interrogative practices call for the participation of the students (written and oral), individually or in groups, allowing students to acquire knowledge related to the application of Cryptography and the knowledge of their fundamental theories, which allow a selection of the best models and behaviors in terms of cryptography. On the other hand, the resolution of practical cases allows students to acquire knowledge related to the implementation and knowledge of new technical notions in the scope of applied cryptography

4.2.16. Bibliografia de consulta/existência obrigatória (PT):
[1] Katz, J., & Lindell, Y. (2021). Introduction to modern cryptography. CRC Press.
[2] Boneh, D., & Shoup, V. (2023). A Graduate Course in Applied Cryptography, Stanford Press
[3] Stallings, W. (2017). Cryptography and network security: Principles and practice. Boston: Pearson Prentice Hall.
[4] Jonathan Katz and Yehuda Lindell. (2019). Introduction to Modern Cryptography, Third Edition (3rd ed.). Chapman & Hall/CRC.
[5] Bellare, M., & Goldwasser, S. (2008). Lecture Notes on Cryptography. MIT Press.

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

[1] Katz, J., & Lindell, Y. (2021). Introduction to modern cryptography. CRC Press.
[2] Boneh, D., & Shoup, V. (2023). A Graduate Course in Applied Cryptography, Stanford Press
[3] Stallings, W. (2017). Cryptography and network security: Principles and practice. Boston: Pearson Prentice Hall.
[4] Jonathan Katz and Yehuda Lindell. (2019). Introduction to Modern Cryptography, Third Edition (3rd ed.). Chapman & Hall/CRC.
[5] Bellare, M., & Goldwasser, S. (2008). Lecture Notes on Cryptography. MIT Press.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Dissertação

4.2.1. Designação da unidade curricular (PT):

Dissertação

4.2.1. Designação da unidade curricular (EN):

Dissertation

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

CCT

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

CST

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):

1,457.0

4.2.5. Horas de contacto:

Presencial (P) - OT-40.0

4.2.6. % Horas de contacto a distância:

0.00%

4.2.7. Créditos ECTS:

57.0

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

• Pedro Miguel do Vale Malheiro Ramos Coutinho - 40.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:

[sem resposta]

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

A disciplina proporcionará a integração dos conhecimentos adquiridos ao longo do CE e a transição, em alguns casos de consolidação, para o mercado de trabalho. Os trabalhos podem assumir o formato de dissertação de cariz académico. Os alunos deverão conduzir um projeto que contemple não só a aplicação dos conceitos adquiridos durante a sua formação, mas também a integração de novas técnicas e de saberes, de modo a realizar um trabalho inovador. Os regulamentos de funcionamento e avaliação encontram-se disponibilizados em www.ipvc.pt

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

The discipline will provide the integration of knowledge acquired throughout the CE and the transition, in some cases of consolidation, to the job market. The works can take the format of an academic dissertation. Students must conduct a project that includes not only the application of concepts acquired during their training, but also the integration of new techniques and knowledge, in order to carry out innovative work. The operating and evaluation regulations are available at www.ipvc.pt

4.2.11. Conteúdos programáticos (PT):

Que contemple na sua maioria os conteúdos aprendidos durante o desenvolvimento do ciclo de estudos e com a integração de novas técnicas e de saberes.

4.2.11. Conteúdos programáticos (EN):

Which mostly covers the content learned during the development of the study cycle and with the integration of new techniques and knowledge.

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

N/A

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

N/A

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

Orientação tutorial. Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

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

Tutorial guidance. After completion of the work, the public defense follows before a jury composed of three members.

4.2.14. Avaliação (PT):

Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

4.2.14. Avaliação (EN):

After completion of the work, the public defense follows before a jury composed of three members.

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

N/A

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

N/A

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

N/A

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

N/A

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Engenharia Social

4.2.1. Designação da unidade curricular (PT):
Engenharia Social

4.2.1. Designação da unidade curricular (EN):
Social Engineering

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 2ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 2nd S

4.2.4. Horas de trabalho (número total de horas de trabalho):
81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-7.0; PL-7.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Silvestre Lomba Malta - 14.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A - Conhecer as diferentes técnicas básicas de Engenharia Social
B - Dominar a utilização de Ferramentas de Engenharia Social
C - Conhecer as diferentes técnicas avançadas de Engenharia Social

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A - Know the different basic techniques of Social Engineering
B - Mastering the use of Social Engineering Tools
C - Know the different advanced techniques of Social Engineering

4.2.11. Conteúdos programáticos (PT):

1. Visão Geral
2. Técnicas de Influência
3. Ferramentas de Engenharia Social
4. Open Source Intelligence (OSINT)
5. Tornar-se outra pessoa
6. Conhecer o inimigo
7. Mind Tricks
8. Elicitação
9. Hacking não técnico
10. O "Lockpicker" mentiroso
11. Ultrapassando Sistemas Físicos
12. Engenharia Social Reversa

4.2.11. Conteúdos programáticos (EN):

1. Overview
2. Influence Techniques
3. Develop Your Tools
4. Open Source Intelligence (OSINT)
5. Becoming Another Person
6. Know Your Enemy
7. Mind Tricks
8. Elicitation
9. Non-Tech Hacking
10. The Lying Lockpicker
11. Getting Past Physical Systems
12. Reverse Social Engineering

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A
2 – A
3 – B
4 – B
5 – C
6 – C
7 – C
8 – C
9 – C
10 – C
11 - C
12 – C

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A
2 – A
3 – B
4 – B
5 – C
6 – C
7 – C
8 – C
9 – C
10 – C
11 - C
12 – C

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

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

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

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

4.2.14. Avaliação (PT):

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.6*CT +0.4*CP*
CP: Avaliação contínua obtida através da realização de trabalhos práticos, respectivos relatórios e ainda a avaliação do desempenho nos trabalhos em laboratório. Para aprovação à UC é necessário nota mínima de 8 valores na CP.
CT - Realização de um teste ou realização de um exame global no final do período letivo. Para aprovação à UC é necessário nota mínima de 8 valores na CT.

4.2.14. Avaliação (EN):

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

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

As metodologias de ensino estão em coerência com os objetivos da unidade curricular dado que:
1) Os métodos de ensino utilizados, ajustam-se à natureza dos conteúdos programáticos e aos objetivos a atingir em cada sessão.
2) As metodologias de ensino utilizadas procuram potenciar a participação ativa dos discentes e a transmissão metódica e rigorosa dos diferentes saberes
3) Competências complementares como sejam o trabalho de equipa, comunicação escrita e verbal serão também exploradas no âmbito da UC.

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

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

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

- Hadnagy, C. (2021). Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You. ISBN: 9780063001787, Harper Business.
- Christopher Hadnagy. 2018. Social Engineering: The Science of Human Hacking. ISBN 978-1-119-43338-5. John Wiley & Sons.
- Mitnick, K. D., & Simon, W. L. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. ISBN: 0316380504, Little, Brown, and Company.
- Kevin D. Mitnick and William L. Simon. 2005. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. John Wiley & Sons, Inc., New York, NY, USA.

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

- Hadnagy, C. (2021). Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You. ISBN: 9780063001787, Harper Business.
- Christopher Hadnagy. 2018. Social Engineering: The Science of Human Hacking. ISBN 978-1-119-43338-5. John Wiley & Sons.
- Mitnick, K. D., & Simon, W. L. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. ISBN: 0316380504, Little, Brown, and Company.
- Kevin D. Mitnick and William L. Simon. 2005. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. John Wiley & Sons, Inc., New York, NY, USA.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Estágio

4.2.1. Designação da unidade curricular (PT):

Estágio

4.2.1. Designação da unidade curricular (EN):

Internship

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

CCT

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

CST

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):

1,457.0

4.2.5. Horas de contacto:

Presencial (P) - OT-40.0

4.2.6. % Horas de contacto a distância:

0.00%

4.2.7. Créditos ECTS:

57.0

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

• Pedro Miguel do Vale Malheiro Ramos Coutinho - 40.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:

[sem resposta]

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

A disciplina proporcionará a integração dos conhecimentos adquiridos ao longo do CE e a transição para o mercado de trabalho. Os trabalhos podem assumir o formato de estágio de cariz empresarial (adequados aos alunos sem experiência na área). Os alunos deverão conduzir um projeto que contemple não só a aplicação dos conceitos adquiridos durante a sua formação, mas também a integração de novas técnicas e de saberes, de modo a realizar um trabalho inovador. Os regulamentos de funcionamento e avaliação encontram-se disponibilizados em www.ipvc.pt

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

The discipline will provide the integration of the knowledge acquired throughout the CE and the transition to the job market. The work can take the form of a business internship (suitable for students with no experience in the area). Students must conduct a project that includes not only the application of concepts acquired during their training, but also the integration of new techniques and knowledge, in order to carry out innovative work. The operating and evaluation regulations are available at www.ipvc.pt

4.2.11. Conteúdos programáticos (PT):

Que contemple na sua maioria os conteúdos aprendidos durante o desenvolvimento do ciclo de estudos e com a integração de novas técnicas e de saberes.

4.2.11. Conteúdos programáticos (EN):

Which mostly covers the content learned during the development of the study cycle and with the integration of new techniques and knowledge.

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

N/A

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

N/A

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

Orientação tutorial. Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

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

Tutorial guidance. After completion of the work, the public defense follows before a jury composed of three members.

4.2.14. Avaliação (PT):

Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

4.2.14. Avaliação (EN):

After completion of the work, the public defense follows before a jury composed of three members.

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

N/A

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

N/A

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

N/A

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

N/A

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Estratégias de Defesa na Administração de Sistemas

4.2.1. Designação da unidade curricular (PT):
Estratégias de Defesa na Administração de Sistemas

4.2.1. Designação da unidade curricular (EN):
Defense Strategies in Systems Administration

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-23.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Silvestre Lomba Malta - 38.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A - Utilização de várias técnicas para impedir que intrusos acedam a dados confidenciais
B - Impedir a instalação de malware e respetivas técnicas de deteção
C - Evitar que utilizadores do sistema acedam a dados aos quais não estão autorizados
D - Técnicas de verificação rápida na deteção serviços de rede maliciosos indevidamente instalados
E - Aprender técnicas de segurança transversais a vários sistemas operativos.

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

A - Use of various techniques to prevent intruders from accessing sensitive data
B - Prevent the installation of malware and its detection techniques
C - Prevent system users from accessing data they are not authorized to
D - Rapid scanning techniques in detecting malicious network services improperly installed
E - Learn security techniques across multiple operating systems.

4.2.11. Conteúdos programáticos (PT):

1 - Fundamentos da administração de sistemas 3.00 Horas
2 - Técnicas seguras em ambientes virtuais. 3.00 Horas
3 - Proteção de contas. Implementação e técnicas avançadas. 4.00 Horas
4 - Implementação e Configuração Avançada de Firewall e IDS. Estratégias de configuração em diversas plataformas. 5.00 Horas
5 - Encriptação e hardening. Configuração em ficheiros, diretório e partições. 5.00 Horas
6 - Controlo de acesso discricionário. Configuração e implementação de ACLs 5.00 Horas
7 – Auditoria. Sistemas de auditoria em sistemas físicos, passwords, filesystems e software instalado 5.00 Horas
8 - Processo de resposta a incidentes. Criação de processos tipo pré-incidentes, durante e pós-incidentes. Ferramentas e tecnologias associadas, SIEM, SOC 4.00 Horas
9 - Exploração de técnicas de defesa a ataques a infraestruturas 4.00 Horas

4.2.11. Conteúdos programáticos (EN):

1 - Fundamentals of System Administration 3.00 Hours
2 - Secure techniques in virtual environments. 3.00 Hours
3 - Account Protection.Implementation and advanced techniques. 4.00 Hours
4 - Firewalls and IDS Advanced Implementation and Configuration. Configuration strategies across platforms. 5.00 Hours
5 - Encryption and hardening. Configuration in files, directory and partitions. 5.00 Hours
6 - Discretionary access control. Configuration and implementation of ACL's. 5.00 Hours
7 – Audit. Audit systems in physical systems, passwords, filesystems and installed software. 5.00 Hours
8 - Incident response process. Creation of pre-incident, during and post-incident processes. Related tools and technologies, SIEM, SOC. 4.00 Hours

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A, E
2 – A, E
3 – B
4 – B
5 – C
6 – C
7 – D, E
8 – D
9 - E

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A, E
2 – A, E
3 – B
4 – B
5 – C
6 – C
7 – D, E
8 – D
9 - E

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

1 - Utilização de várias técnicas para impedir que intrusos acedam a dados confidenciais (conteúdos programáticos: 2, 3, 4, 5, 6 e 9)
2 - Impedir a instalação de malware e respetivas técnicas de deteção (conteúdos programáticos: 4, 6 e 7)
3 - Evitar que utilizadores do sistema acedam a dados aos quais não estão autorizados (conteúdos programáticos: 3 e 6)
4 - Técnicas de verificação rápida na deteção serviços de rede maliciosos indevidamente instalados (conteúdos programáticos: 7 e 8)
5 - Aprender técnicas de segurança transversais a vários sistemas operativos. (conteúdos programáticos: 8 e 9)

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

1 - Use of various techniques to prevent intruders from accessing confidential data (Syllabus: 2, 3, 4,5,6 and 9)
2 - Prevent the installation of malware and its detection techniques (Syllabus 4, 6 and 7)
3 - Prevent system users from accessing data to which they are not authorized (Syllabus 3 and 6)
4 - Rapid scanning techniques in detecting improperly installed malicious network services (Syllabus 7 and 8)
5 - Learn security techniques across multiple operating systems. (Syllabus 8 and 9)

4.2.14. Avaliação (PT):

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

A Classificação Global (CG) desta unidade curricular (UC) é obtida pela média de uma componente teórica (CT) e uma componente prática (CP) com a seguinte ponderação:
*CG = 0.5*CT +0.5*CP*

CP: Avaliação contínua obtida através da realização de trabalhos práticos e respetivos relatórios.
Para aprovação à CT - Realização de um teste ou realização de um exame global no final do período letivo.
Para aprovação à UC é necessário nota mínima de 8 valores na CT é necessário nota mínima de 8 valores na CP.

4.2.14. Avaliação (EN):

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

The Global Classification (GC) of this curricular unit is obtained by the average of a theoretical component (TC) and a practical component (PC) with the following weighting:
*CG = 0.5 * TC + 0.5 * PC*

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

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

As metodologias de ensino são coerentes com os objetivos da unidade curricular dado que:
1) a exposição teórica de conceitos e fundamentos permite preparar a realização, por parte dos alunos, de pequenos trabalhos práticos. A exposição da matéria, conjuntamente com os materiais previamente disponibilizados, permitirão aos alunos assimilarem as matérias e realizar o teste teórico da componente teórica da Unidade Curricular.
2) a elaboração de pequenos trabalhos práticos permitirá aos alunos assimilar os conceitos teóricos permitindo igualmente simular em laboratório a administração de sistemas.

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

The teaching methodologies are coherent with the curricular unit goals as:
1)The theoretical exposition of concepts allows the realization of small practical work by the students.
The exposure of the subject, together with the materials previously available, enable students to assimilate the materials and conduct the written test of the theoretical component of the curricular unit.
2) the development of small practical work will allow students to assimilate the theoretical concepts allowing also to simulate in the laboratory the system administration.

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

1 - Beyer, M. A., & Raimondo, C. (2021). Zero Trust and Security Strategies: Complete Guide for IT Security Managers and Cyber Defense Professionals. ISBN: 9781800568662, Packt Publishing.
2 Tevault, D. (2018). Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Packt.
3 Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity: Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt.
4 Brotherston, L., & Berlin, A. (2017). Defensive Security Handbook: Best Practices for Securing Infrastructure. O'Reilly.

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

1 - Beyer, M. A., & Raimondo, C. (2021). Zero Trust and Security Strategies: Complete Guide for IT Security Managers and Cyber Defense Professionals. ISBN: 9781800568662, Packt Publishing.
2 Tevault, D. (2018). Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Packt.
3 Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity: Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt.
4 Brotherston, L., & Berlin, A. (2017). Defensive Security Handbook: Best Practices for Securing Infrastructure. O'Reilly.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Gestão da Segurança da Informação

4.2.1. Designação da unidade curricular (PT):

Gestão da Segurança da Informação

4.2.1. Designação da unidade curricular (EN):

Information Security Management

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

CCT

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

CST

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-30.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Pedro Miguel Simões Pinto Carneiro - 30.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A. Desenvolver políticas de segurança, programas, e guias de implementação, de acordo com normas reconhecidas.
B. Monitorar e avaliar a eficácia dos controles de Cibersegurança adotados por uma organização, com o objetivo de garantir que proporcionem o nível de segurança desejado.
C. Delinear uma estratégia para a Cibersegurança, realçando a visão, a missão e os objetivos, e garantindo o alinhamento com o plano estratégico da organização.
D. Identificar requisitos de segurança específicos dos Sistemas de Informação organizacionais, em todas as fases do seu ciclo
E. Realizar uma avaliação de risco e delinear os controlos de segurança para mitigar os riscos identificados.

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A. Develop security policies, programs, and implementation guides in accordance with recognized standards.
B. Monitor and evaluate the effectiveness of Cybersecurity controls adopted by an organization, with the objective of ensuring that they provide the desired level of security.
C. Outline a Cybersecurity strategy, highlighting the vision, mission and objectives, and ensuring alignment with the organizations strategic plan.
D. Identify specific security requirements of organizational Information Systems, at all stages of their cycle
E. Conduct a risk assessment and outline security controls to mitigate identified risks.

4.2.11. Conteúdos programáticos (PT):

1 Conceitos e definições
-Segurança da Informação (confidencialidade, integridade e disponibilidade)
-Recursos e tipos de recursos (Informação, físicos e software)
-Valor e criticidade dos recursos críticos Organizacionais
-Ameaças e tipo de ameaças (acidentais vs. Deliberadas; internas vs. Externas)
-Vulnerabilidades e as suas categorias (fraquezas no SW, HW, físicas, pessoas e procedimentos)
-Conceito de politicas de segurança da informação
- Identidade, autenticação e privacidade
2 Conceito de SGSI.
3 Normas e standards de segurança
- A família de normas ISO/IEC 270002. NIST SP 800
4 Gestão do Risco
-Modelos de gestão de risco
-Processo da gestão do risco
-Tratamento do risco
-Objetivo dos controlos
-Avaliação quantitativa/qualitativa do impacto
-Quantificação do valor dos recursos organizacionais
5 Políticas e controlos de segurança
-Controlo de acessos dos utilizadores
-Formação e sensibilização
-Controlos de segurança técnicos
-Monitorização
-Auditoria

4.2.11. Conteúdos programáticos (EN):

1 Concepts and definitions
- Information Security (confidentiality, integrity and availability)
- Resources and types of resources (Information, physical and software)
-Value and criticality of critical Organizational resources
-Threats and type of threats (accidental vs. deliberate; internal vs. external)
-Vulnerabilities and their categories (weaknesses in SW, HW, physical, people and procedures)
-Concept of information security policies
-Identity, authentication and privacy
2 Concept of ISMS.
3 Safety norms and standards
- The ISO/IEC 270002 family of standards. NIST SP 800
4 Risk Management
-Risk Management Models
-Risk management process
Risk treatment
-Purpose of controls
-Quantitative/qualitative impact assessment
-Quantifying the value of organizational resources
5 Security Policies and Controls
-User access control
-Training and awareness
- Technical security controls
- Monitoring
- Audit

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – a, b
2 – a, b
3 – b, c
4 – d, e
5 – d, e

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – a, b
2 – a, b
3 – b, c
4 – d, e
5 – d, e

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

As aulas incluem sessões teóricas.
Nas sessões teóricas será utilizado essencialmente o método expositivo e demonstrações.
As discussões dirigidas serão orientadas para o estudo de casos. As sessões de carácter prático incluí a resolução de exercícios destinados a validar as competências adquiridas.
A maioria das atividades a desenvolver pelos alunos são supervisionadas.
Não obstante, em alguns tópicos onde existem questões em aberto, as atividades de ensino procurarão estimular a criatividade e autonomia do aluno. Estas tarefes assentarão predominantemente na leitura de artigos científicos e relatórios técnicos, complementada com produção de trabalhos de síntese.

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

In the theoretical sessions the classes will be used essentially the expository method and demonstrations. Targeted discussions will be case study oriented while practical sessions include the resolution of practical exercises designed to validate acquired skills.
Most student' activities are supervised. Nevertheless, in some topics where there are open questions, teaching activities will seek to stimulate student creativity and autonomy. These tasks will be essentially based on the reading of scientific articles and technical reports, complemented by the production of synthesis works.

4.2.14. Avaliação (PT):
Avaliação Contínua
- Avaliação (CT) obtida mediante a realização de uma prova realizada no período acadêmico. Para aprovação, é necessário ter no mínimo 7 de 20 valores na CT.
- Avaliação Prática (CP) obtida através da realização do trabalho prático indicado na avaliação contínua.
- Avaliação de Desempenho (AD): obtida através dos registos de desempenho nas aulas.
*- Classificação final (CF) = 40% * CT + 50% * CP + 10% * AD*

Avaliação: Normal e Recurso ou Especial:
Avaliação da CT: obtida através da realização de um trabalho escrito.
O Exame Normal é acessível apenas para os alunos que não realizaram a avaliação contínua e que não faltaram.
Para aprovação, é necessário ter no mínimo 7 de 20 valores na CT.
Avaliação Normal e Recurso ou Especial: Trabalho prático ou prova escrita com todos os conteúdos lecionados na UC sendo CF=100%.

4.2.14. Avaliação (EN):
*Continuous Evaluation - Evaluation (CT) obtained through the completion of a test held in the academic period. For approval, a minimum of 7 out of 20 marks is required in CT. - Practical Evaluation (PC) obtained by carrying out the practical work indicated in the continuous evaluation. - Performance Evaluation (AD): obtained through the performance records in class. - Final Classification (CF) = 40% * CT + 50% * CP + 10% * AD*

Assessment: Normal and Supplementary or Special: CT Assessment: obtained through the completion of a written work. The Normal Exam is accessible only to students who did not perform the continuous assessment and who did not miss. For approval, it is necessary to have at least 7 of 20 points in CT. Normal and Supplementary or Special Assessment: Practical work or written test with all the contents taught in the UC being CF = 100%.

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

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

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

The training profile of future Masters by this Cycle of Studies will lead to qualified professionals, holders of knowledge, skills and competences in their area of formation. In this sense, and with a view to the operationalization of the objectives of the Curricular Unit in question, the methodologies adopted, based on theoretical and practical classes, articulated with interrogative practices call for the participation of the students (written and oral), individually or in groups, allowing to students to acquire knowledge related to the application of security in networks and systems and the knowledge of their fundamental theories that allow the selection of the best models and behaviors in terms of data security and the design, implementation and experimental testing of protocols and security in computer networks and systems.

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

- Stallings, W. (2021). Effective Cybersecurity: A Guide to Using Best Practices and Standards (1nd ed.). ISBN-13: 9780137570416. Pearson.
- Calder, A. (2019). Information Security Risk Management for ISO27001/ISO27002 (3rd ed.). ISBN: 9781787781382. IT Governance Publishing.
- Vacca, John R., ed. (2013) Managing information security. ISBN-10. 0124166881. Elsevier.

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

- Stallings, W. (2021). Effective Cybersecurity: A Guide to Using Best Practices and Standards (1nd ed.). ISBN-13: 9780137570416. Pearson.
- Calder, A. (2019). Information Security Risk Management for ISO27001/ISO27002 (3rd ed.). ISBN: 9781787781382. IT Governance Publishing.
- Vacca, John R., ed. (2013) Managing information security. ISBN-10. 0124166881. Elsevier.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Gestão de Identidade Digital

4.2.1. Designação da unidade curricular (PT):

Gestão de Identidade Digital

4.2.1. Designação da unidade curricular (EN):

Digital Identity Management

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

CCT

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

CST

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

Semestral 2ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 2nd S

4.2.4. Horas de trabalho (número total de horas de trabalho):
81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-7.0; PL-7.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Ricardo Jorge da Silva Santos - 14.0h

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):
Gerais:
A. Distinguir uma identidade físicas de uma identidade digital;
B. Compreender a problemática da identidade no mundo digital, da sua gestão e do seu relacionamento com a identidade física;
C. Identificar as principais características e requisitos dos diversos tipos de aplicações de gestão de identidades e do seu relacionamento com a gestão de controle de acessos.
Específicos:
D. Especificar soluções que permitam um controle de acessos físico e lógico granular a informação, sistemas, dispositivos e instalações;
E. Identificar serviços de gestão de identidades (e.g. SSO, LDAP, AD);
F. Compreender e diferenciar sistemas de autenticação single-fator e multi-fator (e.g. fatores de autenticação, força, biometria);
G. Registar e identificar usos de identidade;
H. Identificar serviços de gestão de identidades federada (e.g. SAML, OpenID);

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
General:
A. Distinguish a physical identity from a digital identity;
B. Understand the problem of identity in the digital world, its management and its relationship with physical identity;
C. Identify the key characteristics and requirements of the various types of identity management applications and their relationship with access control management.
Specific:
D. Specify solutions that allow granular physical and logical access to the information, systems, devices and installations.
E. Identify identity management services (e.g. SSO, LDAP, AD);
F. Understand and differentiate single-factor and multi-factor authentication systems (e.g., authentication, strength, biometrics);
G. Register and identify uses of identity;
H. Identify federated identity management services (eg SAML, OpenID);

4.2.11. Conteúdos programáticos (PT):
1. Controlo do acesso fi?sico e lo?gico aos ativos
2. Gesta?o da identificac?a?o e da autenticac?a?o de pessoas e dispositivos
3. Servic?os de identidade on-premise
4. Servic?os de identidade na nuvem
5 Gesta?o da identidade e do seu ciclo de vida

4.2.11. Conteúdos programáticos (EN):

1. Control physical and logical access to assets
2. Identification management and authentication of persons and devices
3. On-premise identity services
4. Cloud identity services
5 Identity Management and its Life Cycle

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – B,D,E
2 – A,B,C,D,E
3 – C,F,H
4 – C,F,H
5 – C,F,G,H

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – B,D,E
2 – A,B,C,D,E
3 – C,F,H
4 – C,F,H
5 – C,F,G,H

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

Aulas expositivas complementadas com aulas de experimentação laboratorial, compreendendo a execução de trabalhos práticos.

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

Lectures complemented with laboratory experimentation classes, including the execution of practical works.

4.2.14. Avaliação (PT):

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

4.2.14. Avaliação (EN):

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

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

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

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

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

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

[1] Friedewald, M., Schiffner, S., & Krenn, S. (2022). Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Maribor, Slovenia, September 21–23, 2020, Revised Selected Papers. Springer International Publishing.
[2] Mahalle, P., & Railkar, P. (2022). Identity Management for Internet of Things. River Publishers.
[3] CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 7th Edition by James M. Stewart (Author); Mike Chapple (Author); Darril Gibson (Author) - ISBN-13: 978-1119042716, ISBN-10: 1119042712 (2015)
[4] Mechanics of User Identification and Authentication: Fundamentals of Identity Management 1st Edition by Dobromir Todorov (Author) - ISBN-13: 978-1420052190, ISBN-10: 1420052195 (2014)

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

[1] Friedewald, M., Schiffner, S., & Krenn, S. (2022). Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Maribor, Slovenia, September 21–23, 2020, Revised Selected Papers. Springer International Publishing.
[2] Mahalle, P., & Railkar, P. (2022). Identity Management for Internet of Things. River Publishers.
[3] CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide 7th Edition by James M. Stewart (Author); Mike Chapple (Author); Darril Gibson (Author) - ISBN-13: 978-1119042716, ISBN-10: 1119042712 (2015)
[4] Mechanics of User Identification and Authentication: Fundamentals of Identity Management 1st Edition by Dobromir Todorov (Author) - ISBN-13: 978-1420052190, ISBN-10: 1420052195 (2014)

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Hacking Ético

4.2.1. Designação da unidade curricular (PT):

Hacking Ético

4.2.1. Designação da unidade curricular (EN):

Ethical Hacking

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

CCT

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

CST

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 2ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 2nd S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-30.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Marco Filipe Vieira Gomes - 45.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A. Conhecimento das restrições éticas e legais associadas aos testes de penetração e ethical hacking
B. Domínio das etapas de desenvolvimento de testes de penetração e apresentação de resultados
C. Identificação de aplicações/tráfego malicioso na rede
D. Implementação de aplicações úteis na exploração de falhas
E. Identificar ameaças e selecionar as medidas para impedir acesso físico a equipamentos e a mitigar ataques de engenharia social
F. Aplicar as medidas corretivas adequadas à mitigação de falhas de segurança
G. Identificar e resolver problemas nas aplicações e serviços web
H. Determinar falhas de segurança em redes móveis, e para implementar soluções de segurança das comunicações
I. Reforçar as competências relacionadas com sistemas de IDS/IPS
J. Reforçar as capacidades dos serviços de autenticação e controlo de acesso
K. Identificar vulnerabilidades de dispositivos móveis e aplicação de medidas preventivas
L. Avaliar o risco da utilização de aplicações móveis

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A. Ethical policies and legality of activities involving a penetration test
B. Domain of the stages of penetration tests and final reporting results
C. Identify the type of applications/malicious traffic, determine vulnerabilities in services and elect the most appropriate exploits
D. Implement small applications useful in fault operation
E. Identify threats and select measures to prevent physical access and social engineering attacks
F. Apply appropriate corrective measures to mitigate security breaches
G. Identify and solve problems in web applications/services
H.Determine security flaws in mobile networks and implementation of mitigation technics
I. Strengthen the skills of planning and implementation of detection systems / prevent attacks
J. Strengthen planning capabilities and implementation of authentication, access control and traffic analysis
K.Identify vulnerabilities of mobile devices and apply preventive measures
L. Assess the risk of using mobile applications

4.2.11. Conteúdos programáticos (PT):

1. Introdução aos conceitos do Ethical hacking
2. Tipos de ameaças e ataques a redes cabladas e sem fio
3. Protocolos e algoritmos de segurança em redes 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN)
4. Fragilidades protocolares dos sistemas de comunicações móveis
5. Tecnologia de confidencialidade, privacidade e disponibilidade em redes sem fio
6. Metodologias para testes de penetração
7. Caracterização e implementação de ataques contra redes e sistemas móveis
8. Planeamento de soluções de comunicação segura em redes e sistemas móveis
9. Identificação e deteção de vulnerabilidades nos sistemas móveis
10. Implementação de mecanismos e sistemas de segurança em redes sem fio e dispositivos móveis

4.2.11. Conteúdos programáticos (EN):

1. Ethical hacking concepts
2. Types of threats and attacks on wired and wireless networks
3. Protocols and security algorithms in 802.11 (Wireless LAN), 802.15 (wireless PAN); 802.16 (wireless WAN) C4. Protocol weaknesses of mobile communication systems
5. Confidentiality, privacy and availability technologies in wireless networks
6. Methodologies for the penetration tests
7. Characterization and implementation of attacks against networks and mobile systems
8. Planning of secure communication solutions in mobile networks and systems
9. Identification and detection of vulnerabilities in mobile systems
10. Implementation mechanisms and security systems for wireless networks and mobile devices

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A ,B
2 – C,E
3 – E,F
4 – D
5 – K
6 – G, H
7 – K
8 – J,L
9 – K
10 - I

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A ,B
2 – C,E
3 – E,F
4 – D
5 – K
6 – G, H
7 – K
8 – J,L
9 – K
10 - I

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

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

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

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

4.2.14. Avaliação (PT):

Em avaliação contínua, a classificação global é obtida com base em:
(a) Mini teste (50%);
(b) Trabalho prático (50%);
Nas demais épocas de avaliação, a nota global é conseguida de forma similar à avaliação contínua, podendo incluir novas atividades a desenvolver pelos alunos a título individual.

4.2.14. Avaliação (EN):

The continuous evaluation comprises the final classification obtained based on:
(a) Mid-term test (50%);.
(b) Workgroup project development (50%);
In all other evaluations, the final grade comprises the same assignments of the continuous assessment with additional activities and to be carried out individually by the students.

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

A metodologia de ensino teórico-prático baseia-se na transmissão de conhecimentos sobre a segurança ao nível da segurança ofensiva para avaliação e mitigação de vulnerabilidades em sistemas ubíquos, redes e aplicações, com vista a dar uma visão global do processo de exploração e mitigação de falhas, tendo sempre em linha de conta as restrições, diretivas éticas e legalidade das atividades que envolvem um teste de penetração. Permite desenvolver nos estudantes as competências (A,B,C).

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

The methodology of theoretical and practical teaching is based on the transmission of knowledge about offensive security for assessment and mitigation of vulnerabilities in ubiquitous systems, networks and applications, in order to give an overview of the exploration and mitigation of failures, taking into account the legal and ethical constraints of activities involving a penetration test. It allows us to develop students skills (A,B,C).

The methodology used in the lab component focuses initially on consolidation of the knowledge acquired in the prevoius component through the implementation of laboratory works (A,B,C) and, at a later stage, in the implemetation of a practical project that includes the following phases: a) study of the proposed scenario, b) identification of flaws and vulnerabilities of the scenario, c) selection of the appropriate exploit mechanisms, d) conducting penetration testing e) mitigation of the detected vulnerabilities e) writing report e) presentation and defense of the implemented project, allowing the students to develop the skills (D,E,F,G,H,I,J,K,L).

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

- Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Security (6th ed.). ISBN 9781284220735, Jones & Bartlett Learning.
- Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; ISBN: 978-0071832380; McGraw-Hill Education; 4 ed., 2015
- The Hacker Playbook 2: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1512214567; CreateSpace Independent Publishing Platform, 2015.
- Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012

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

- Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Security (6th ed.). ISBN 9781284220735, Jones & Bartlett Learning.
- Gray Hat Hacking The Ethical Hacker's Handbook; Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims; ISBN: 978-0071832380; McGraw-Hill Education; 4 ed., 2015
- The Hacker Playbook 2: Practical Guide To Penetration Testing, Paperback; Peter Kim; ISBN: 978-1512214567; CreateSpace Independent Publishing Platform, 2015.
- Hacking Exposed 7; Stuart McClure, Joel Scambray; ISBN: 978-0071780285, McGraw-Hill Education; 7 ed., 2012

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Metodologias de Investigação

4.2.1. Designação da unidade curricular (PT):
Metodologias de Investigação

4.2.1. Designação da unidade curricular (EN):
Research Methodologies

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-8.0; PL-8.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
- *Silvestre Lomba Malta - 6.0h*

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
- *Carlos Abreu - 2.0h*
- *Jorge Manuel Ferreira Barbosa Ribeiro - 2.0h*
- *Luís Manuel Cerqueira Barreto - 2.0h*
- *Pedro Miguel Simões Pinto Carneiro - 2.0h*
- *Sérgio Ivan Fernandes Lopes - 2.0h*

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

A. Compreender as metodologias de investigação científica e técnicas específicas para as ciências informáticas e engenharia, com foco em cibersegurança.
B. Saber documentar e redigir dissertações, artigos científicos e relatórios técnicos de acordo com padrões e bibliografia de referência na área.
C. Desenvolver competências para gerir e coordenar projetos de investigação, incluindo a planificação, execução e avaliação.
D. Conhecer as melhores práticas para a organização de eventos científicos e divulgação de resultados, com ênfase em conferências, workshops e publicações.
E. Elaborar um estado da arte como preparação para a dissertação, aplicando metodologias de revisão sistemática.

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

A. Understand scientific research methodologies and techniques specific to computer science and engineering, with a focus on cybersecurity.
B. Know how to document and write dissertations, scientific articles and technical reports in accordance with standards and reference bibliography in the area.
C. Develop skills to manage and coordinate research projects, including planning, execution and evaluation.
D. Know the best practices for organizing scientific events and disseminating results, with an emphasis on conferences, workshops and publications.
E. Develop a state of the art in preparation for the dissertation, applying systematic review methodologies.

4.2.11. Conteúdos programáticos (PT):

1. Introdução ao Processo de Investigação
1.1 Princípios básicos da investigação científica em ciências informáticas.
1.2 Metodologias.
1.3 Ética e boas práticas na investigação.
1.4 Condução da Investigação

2. Definição de hipóteses e perguntas de investigação.
2.1 Planeamento e gestão do ciclo de vida do projeto de investigação.
2.2 Técnicas de recolha e análise de dados para cibersegurança.
2.3 Documentação e Redação Científica

3. Normas e estilos de escrita científica.
3.1 Elaboração de artigos, dissertações e relatórios técnicos.
3.2 Revisão sistemática da literatura e escrita do estado da arte.

4.Gestão de Projetos de Investigação
4.1 Monitorização do progresso e gestão de riscos.

5. Divulgação de Resultados Técnicos e Científicos
5.1 Preparação e submissão de artigos para conferências e revistas científicas.
5.2 Técnicas de apresentação).
5.3 Utilização de plataformas para repositórios e gestão de publicações.

6. Organização de uma Conferência Interna

4.2.11. Conteúdos programáticos (EN):

1. Introduction to the Research Process
1.1 Basic principles of scientific research in computer science.
1.2 Methodologies.
1.3 Ethics and good practices in research.
1.4 Conduct of the Investigation

2. Definition of hypotheses and research questions.
2.1 Planning and management of the research project life cycle.
2.2 Data collection and analysis techniques, with specific tools for cybersecurity.
2.3 Documentation and Scientific Writing

3. Scientific writing standards and styles.
3.1 Preparation of articles, dissertations and technical reports.
3.2 Systematic literature review and state-of-the-art writing.

4.Research Project Management
4.1 Progress monitoring and risk management.

5. Disclosure of Technical and Scientific Results
5.1 Preparation and submission of articles for conferences and scientific journals.
5.2 Oral and visual presentation techniques (posters, slides).
5.3 Use of platforms for repositories and publication management.

6. Organizing an Internal Conference

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A,B
2 – A,C
3 – B,E
4 – C,D
5 – C,D,E
6 – C,D,E

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A,B
2 – A,C
3 – B,E
4 – C,D
5 – C,D,E
6 – C,D,E

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

Serão apresentados os temas do programa sob a forma de apontamentos ou slides. Serão realizados exercícios com casos práticos que pretendem consolidar e demonstrar a aplicação dos conceitos abordados.

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

The program's themes will be presented in the form of notes or slides. Exercises will be carried out with practical cases that aim to consolidate and demonstrate the application of the concepts covered.

4.2.14. Avaliação (PT):

A avaliação incidirá sobre o desempenho de cada aluno na escrita de um artigo científico (item Publicação) e no envolvimento na organização do evento científico (item Gestão).
Itens avaliados na componente "Publicação" (60%)
- Submissão de Artigo (20%)
- Reviews realizadas (15%)
- Update do Artigo (Camera ready) (5%)
- Apresentação na conferência (20%)
Itens avaliados na componente "Gestão" (40%)
- Desempenho nas sessões de acompanhamento (5%)
- Posição e Organização geral (15%)
- Comunicação (Página Web, Emails) (10%)
- Configuração Plataforma de Gestão (10%)

4.2.14. Avaliação (EN):

The evaluation will focus on the performance of each student in the writing of a scientific article and in the involvement in the organization of the scientific event.
Items evaluated in the "Publication" component (60%)
- Article Submission (20%)
- Reviews (15%)
- Article Update (Camera ready) (5%)
- Presentation at the conference (20%)
Items evaluated in the "Management" component (40%)
- Performance in follow-up sessions(5%)
- Role and general organization (15%)
- Communication (Web page, Emails) (10%)
- Management Platform Configuration (10%)

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

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

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

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

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

- Flick, U. (2022). An Introduction to Qualitative Research (7th ed.). ISBN 1529783542. SAGE Publications.
- Justin Zobel. 2015. Writing for Computer Science (3rd ed.). Springer Publishing Company, Incorporated.
- Martha Davis, Kaaron Joann Davis, and Marion Dunagan. 2012. Scientific Papers and Presentations: Navigating Scientific Communication in Today's World (3 ed.). Academic Press, Inc., Orlando, FL, USA.
- Luís Adriano Oliveira. 2011. Dissertação e tese em Ciência e Tecnologia: Segundo Bolonha (Guia de boas práticas) 3ª Ed. Lidel - Edições Técnicas. ISBN 978-972-757-742-2

4.2.16. Bibliografia de consulta/existência obrigatória (EN):
- Flick, U. (2022). An Introduction to Qualitative Research (7th ed.). ISBN 1529783542. SAGE Publications.
- Justin Zobel. 2015. Writing for Computer Science (3rd ed.). Springer Publishing Company, Incorporated.
- Martha Davis, Kaaron Joann Davis, and Marion Dunagan. 2012. Scientific Papers and Presentations: Navigating Scientific Communication in Today's World (3 ed.). Academic Press, Inc., Orlando, FL, USA.
- Luís Adriano Oliveira. 2011. Dissertação e tese em Ciência e Tecnologia: Segundo Bolonha (Guia de boas práticas) 3ª Ed. Lidel - Edições Técnicas. ISBN 978-972-757-742-2

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Privacidade e Proteção de Dados

4.2.1. Designação da unidade curricular (PT):
Privacidade e Proteção de Dados

4.2.1. Designação da unidade curricular (EN):
Privacy and Data Protection

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 2ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 2nd S

4.2.4. Horas de trabalho (número total de horas de trabalho):
81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-14.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Pedro Miguel Simões Pinto Carneiro - 14.0h

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

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

A - Sensibilizar e estar consciente da importância da privacidade e proteção de dados pessoais em todo o espectro digital da cadeia de negócio.
B - Recomendar tecnologia que garanta a segurança adequada ao cumprimento da conformidade legal aplicável aos vários tipos de dados.
C - Reconhecer potencialidades e limitações da tecnologia a desenvolver e implementar num programa de privacidade para conduzir à avaliação dos dados.
D - Implementar um plano de resposta a incidentes de privacidade.

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

A - Raise awareness and be aware of the importance of privacy and protection of personal data across the digital spectrum of the business chain.
B - Recommend technology that guarantees adequate security to comply with the legal compliance applicable to the various types of data.
C - Recognize the potential and limitations of the technology to be developed and implemented in a privacy program to conduct data evaluation.
D - Implement privacy incidents response plan

4.2.11. Conteúdos programáticos (PT):

1 INTRODUÇÃO
Cenários críticos para a proteção de dados
Proteção de dados em tecnologias emergentes
Recolha e transferência de informação

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

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

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

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

4.2.11. Conteúdos programáticos (EN):

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

2 DATA EVALUATION, SYSTEMS AND PROCESSES
Mapping and classification of data types at enterprise information systems.
Cloud Computing Strategies.
Technological standards for safeguarding information (datacenters, physical access, data destruction and sanitization, forensic devices).
Due diligence and technological risk assessment in mergers, acquisitions and divestitures

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

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

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

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – A ,D
2 – A, B, D
3 – A, C, D
4 – A, C, D
5 – A, C, D

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – A ,D
2 – A, B, D
3 – A, C, D
4 – A, C, D
5 – A, C, D

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

As aulas incluem sessões teóricas, discussões dirigidas e sessões de carácter prático com demonstração de casos temáticos.
- Nas sessões teóricas será utilizado o método expositivo.
- As discussões dirigidas serão orientadas para o estudo de casos.
- As sessões de carácter prático incluem a resolução de casos práticos destinados a permitir validar as competências adquiridas.

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

This curricular unit include theoretical sessions, guided discussions and practical sessions for demonstration of thematic cases.
- In theoretical sessions we'll use the expository method.
- Targeted discussions will focus on case studies.
- Practical sessions include the resolution of practical cases to enable the skills acquired to be validated.

4.2.14. Avaliação (PT):

Avaliação contínua:
100% prático em formato de Report /Artigo/Prova de conceito.
Exame final: Exame teórico-prático (100%)

4.2.14. Avaliação (EN):

Continuous evaluation:
100% practical in Report / Article / Proof of concept format.
Final exam: Theoretical-practical exam (100%)

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

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

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

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

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

[1] Leenes,R. , van Brakel,R. , Gutwirth,S. , Hert, P. (2018). Data Protection and Privacy: The Internet of Bodies. United Kingdom: Hart Publishing.
[2] Regulamento Geral sobre a Proteção de Dados 2016/679 - General Data Protection Regulation 2016/679
[3] Stalla-Bourdillon, S., Phillips, J., & Ryan, M. D. (2014). Privacy vs security. (Springer Briefs in Cybersecurity). London, GB: Springer.

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

[1] Leenes,R. , van Brakel,R. , Gutwirth,S. , Hert, P. (2018). Data Protection and Privacy: The Internet of Bodies. United Kingdom: Hart Publishing.
[2] Regulamento Geral sobre a Proteção de Dados 2016/679 - General Data Protection Regulation 2016/679
[3] Stalla-Bourdillon, S., Phillips, J., & Ryan, M. D. (2014). Privacy vs security. (Springer Briefs in Cybersecurity). London, GB: Springer.

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Projeto

4.2.1. Designação da unidade curricular (PT):
Projeto

4.2.1. Designação da unidade curricular (EN):
Project

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

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

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):
1,457.0

4.2.5. Horas de contacto:
Presencial (P) - OT-40.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
57.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Pedro Miguel do Vale Malheiro Ramos Coutinho - 40.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A disciplina proporcionará a integração dos conhecimentos adquiridos ao longo do CE e a transição, em alguns casos de consolidação, para o mercado de trabalho. Os trabalhos podem assumir o formato de projeto integrado num contexto empresarial. Os alunos deverão conduzir um projeto que contemple não só a aplicação dos conceitos adquiridos durante a sua formação, mas também a integração de novas técnicas e de saberes, de modo a realizar um trabalho inovador. Os regulamentos de funcionamento e avaliação encontram-se disponibilizados em www.ipvc.pt

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
The discipline will provide the integration of knowledge acquired throughout the CE and the transition, in some cases of consolidation, to the job market. Work can take the form of an integrated project in a business context. Students must conduct a project that includes not only the application of concepts acquired during their training, but also the integration of new techniques and knowledge, in order to carry out innovative work. The operating and evaluation regulations are available at www.ipvc.pt

4.2.11. Conteúdos programáticos (PT):
Variável consoante a temática do projeto mas que contemple na sua maioria os conteúdos aprendidos durante o desenvolvimento do ciclo de estudos e com a a integração de novas técnicas e de saberes.

4.2.11. Conteúdos programáticos (EN):
Variable depending on the theme of the project but mostly covering the content learned during the development of the study cycle and with the integration of new techniques and knowledge.

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

N/A

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

N/A

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

Orientação tutorial. Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

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

Tutorial guidance. After completion of the work, the public defense follows before a jury composed of three members.

4.2.14. Avaliação (PT):
Após a conclusão do trabalho segue-se a defesa pública perante um júri constituído por três membros.

4.2.14. Avaliação (EN):
After completion of the work, the public defense follows before a jury composed of three members.

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

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

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

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

4.2.17. Observações (PT):
[sem resposta]

4.2.17. Observações (EN):
[sem resposta]

Mapa III - Segurança de Redes e Sistemas

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

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

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-15.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Silvestre Lomba Malta - 30.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A Conhecer tipos de ataques simples e complexos a redes e sistemas
B. Conhecer o modo de funcionamento dos Worms e ataques DDoS
C. Dominar o funcionamento fundamental dos protocolos de segurança e serviços em redes IP
D. Conhecer o funcionamento fundamental de sistemas de firewall e IDS

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A. Know types of simple and complex attacks on networks and systems
B. Know how Worms and DDoS attacks work
C. Master the fundamental functioning of security protocols and services in IP networks
D. Know the fundamental functioning of firewall and IDS systems

4.2.11. Conteúdos programáticos (PT):
1 Ataques e Vulnerabilidades em Redes e Sistemas
2 Vírus e Worms
3 Ataques DoS (Denial of Service) e DDoS (Distributed Denial of Service)
4 Protocolos de segurança e serviços de segurança em Redes IP
5 Firewalls
6 Sistemas de Deteção de Intrusão (IDS)

4.2.11. Conteúdos programáticos (EN):
1 Attacks and Vulnerabilities in Networks and Systems
2 Virus and Worm
3 DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks
4 Security Protocols and Security Services in IP Networks
5 Firewalls
6 Intrusion Detection Systems (IDS)

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – a
2 – b
3 – c
4 – c
5 – d
6 – d

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – a
2 – b
3 – c
4 – c
5 – d
6 – d

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

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

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

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

4.2.14. Avaliação (PT):

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

4.2.14. Avaliação (EN):

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

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

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

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

The training profile of future Masters by this Cycle of Studies will lead to qualified professionals, holders of knowledge, skills and competences in their area of formation. In this sense, and with a view to the operationalization of the objectives of the Curricular Unit in question, the methodologies adopted, based on theoretical and practical classes, articulated with interrogative practices call for the participation of the students (written and oral), individually or in groups, allowing to students to acquire knowledge related to the application of security in networks and systems and the knowledge of their fundamental theories that allow the selection of the best models and behaviors in terms of data security and the design, implementation and experimental testing of protocols and security in computer networks and systems.

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

- *Kurose, J. F., & Ross, K. W. (2020). Computer Networking: A Top-Down Approach (8th ed.). Pearson. ISBN-13: 9780135928615.*
- *Stallings, W. (2021). Network Security Essentials: Applications and Standards (6th ed.). Pearson. ISBN-13: 9780137561650.*
- *Stallings, W., & Brown, L. (2017). Computer Security: Principles and Practice, Global Edition (4th ed.). Harlow, England: Pearson.*
- *Gollmann, D. (2011). Computer Security (3rd ed.). Wiley & Sons. ISBN 0470741155.*

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

- *Kurose, J. F., & Ross, K. W. (2020). Computer Networking: A Top-Down Approach (8th ed.). Pearson. ISBN-13: 9780135928615.*
- *Stallings, W. (2021). Network Security Essentials: Applications and Standards (6th ed.). Pearson. ISBN-13: 9780137561650.*
- *Stallings, W., & Brown, L. (2017). Computer Security: Principles and Practice, Global Edition (4th ed.). Harlow, England: Pearson.*
- *Gollmann, D. (2011). Computer Security (3rd ed.). Wiley & Sons. ISBN 0470741155.*

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Segurança de Sistemas Ciberfísicos

4.2.1. Designação da unidade curricular (PT):

Segurança de Sistemas Ciberfísicos

4.2.1. Designação da unidade curricular (EN):

Cyber-Physical Systems Security

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

CCT

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

CST

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

Semestral 1ºS

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

Semiannual 1st S

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

81.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-7.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
3.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Sérgio Ivan Fernandes Lopes - 22.0h

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

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A - Perceber o que é um sistema ciber-físico e identificar quais as suas maiores vulnerabilidades
B - Reconhecer os principais blocos funcionais de um sistema embebido e a sua importância no desenho de sistemas ciber-físicos seguros
C - Identificar os recursos físicos mais vulneráveis a um ataque e entender os problemas críticos associados à sua utilização, e.g. microprocessadores, interfaces de comunicações, etc
D - Identificar os recursos não-físicos mais vulneráveis a um ataque e entender os problemas críticos associados à sua utilização, e.g. sistemas distribuidos, sistemas operativos e protocolos de comunicações
E - Aplicar boas práticas para o desenho e concepção de sistemas ciber-físicos seguros

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A - Understand what is a Cyber-Physical System (CPS) and identify its biggest vulnerabilities
B - Recognize the main functional blocks of an embedded system and its importance in the design of safe CPSs
C - Identify the most vulnerable physical resources to an attack and understand the critical problems associated with their use, e.g. microprocessors, communications interfaces, etc
D - Identify the non-physical resources most vulnerable to an attack and understand the critical issues associated with their use, e.g. distributed systems, operating systems, and communications protocols
E - Apply good practices for the design of safe CPSs

4.2.11. Conteúdos programáticos (PT):
1 Introdução à Segurança em Sistemas Ciber-Físicos (SCFs)
1.1 Fundamentos e arquiteturas de SCFs
1.2 Redes de comunicações, Segurança da informação e Sistemas de controlo
1.3 Tendências de segurança em SCFs
1.4 Ameaças e ataques comuns em SCFs
2 Considerações sobre Sistemas Embebidos (SE)
2.2 O microprocessador e as suas vulnerabilidades
2.3 Requisitos principais de segurança de um SE
2.4 Desenvolvimento de Software seguro para SE
2.5 O papel do Sistema Operativo e suas vulnerabilidades num SE
3 Redes e aplicações industriais de SCFs (Industria 4.0)
3.1 Arquiteturas típicas e protocolos comuns
3.2 Introdução aos Sistemas de Controlo Industrial, e.g. ICS/SCADA
3.3 Segurança e Privacidade em SCFs Industriais
3.4 Ameaças e ataques comuns em aplicações industriais
4 Segurança em aplicações específicas de SCFs: IoT
4.1 A (in)segurança da Internet das Coisas (IoT)
4.2 Ameaças e ataques comuns em aplicações IoT
4.3 Aspetos legais e de privacidade
4.4 Gestão e mitigação de Risco em SCFs

4.2.11. Conteúdos programáticos (EN):

1 Introduction to Security in Cyber-Physical Systems (CPSs)
1.1 CPS Fundamentals and Architectures
1.2 Communications networks, Information security, and Control systems
1.3 Security Trends in CPSs
1.4 Common Threats and Attacks on CPSs
2 Considerations on Embedded Systems (ES)
2.2 The microprocessor and its vulnerabilities
2.3 Main security requirements of an ES
2.4 Secure Software Development for ES
2.5 The role of the Operating System and its vulnerabilities in an ES
3 Industrial Networks and Applications of CPSs (Industry 4.0)
3.1 Typical architectures and common protocols
3.2 Introduction to Industrial Control Systems, e.g. ICS/SCADA
3.3 Security and Privacy in Industrial CPSs
3.4 Common Threats and Attacks in Industrial Applications
4 Security in specific applications of CPSs: IoT
4.1 The (in) security of the Internet of Things (IoT)
4.2 Common threats and attacks in IoT applications
4.3 Legal and privacy aspects
4.4 Risk management and mitigation in CPSs

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – a
2 – b, c
3 – b, c, d
4 – d, e

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – a
2 – b, c
3 – b, c, d
4 – d, e

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

metodologia de ensino assenta numa primeira exposição dos conceitos e problemáticas a que os alunos devem estar atentos e seguidamente na consolidação dos mesmos através da aplicação prática num trabalho. Privilegia-se a aprendizagem com recurso à experiência prática

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

The teaching methodology is based on a first exposition of the concepts and problems to which the students must be attentive and then in the consolidation of the same through the practical application in a work. Learning is privileged by practical experience.

4.2.14. Avaliação (PT):

- Tarefa: Investigação sobre IoT Hacks
Atividade Individual/Grupo 10%
Avaliação Escrita 20%
Apresentação/Discussão 20%

- Exame Final 50%

4.2.14. Avaliação (EN):

methodology will focus on the problem-based learning paradigm. This will enable the student to apply the knowledge in the context of real applications by means of practical examples and therefore provide to the students the most important concepts in secure Cyber-Physical Systems.

- Assignment 1: Research on IoT Hacks
Individual/Group Activity 10%
Written Recension 20%
Presentation/Discussion 20%

- Final Exam 50%

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

Sendo uma disciplina com conteúdos essencialmente práticos, é nosso entender que, após a exposição inicial dos conceitos, deve haver um grande cariz prático e por isso a metodologia privilegia que os alunos façam para aprender. São por isso dados trabalhos práticos que permitam que o aluno aplique os conhecimentos e que no final resulte uma aplicação completa que demonstre aos alunos como é que os vários conceitos aprendidos de facto são empregues numa aplicação real.

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

Being this a course with considerable practical content, it is our understanding that, after the initial presentation of the concepts, the course will focus on practical aspects and therefore the methodology will focus the problem-based learning paradigm. This will enable the student to apply the knowledge in the context of real applications by means of practical examples and therefore provide to the students the most important concepts in secure Cyber-Physical Systems.

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

- Security and Resilience of Cyber Physical Systems, Chapman & Hall/CRC Cyber-Physical Systems, (2022) (1nd Edition), by Krishan Kumar, Sunny Behal, Abhinav Bhandari, Sajal Bhatia. ISBN 1032028564
- Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), by Eric D. Knapp and Joel Thomas Langill, ISBN: 978-0124201149
- Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure (1st Edition), by Eric D. Knapp and Raj Samani, ISBN: 978-1597499989
- David Kleidermacher Mike Kleidermacher, "Embedded Systems Security - Practical Methods for Safe and Secure Software and Systems Development", 1st Edition, ISBN: 9780123868862, March 2012

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

- Security and Resilience of Cyber Physical Systems, Chapman & Hall/CRC Cyber-Physical Systems, (2022) (1nd Edition), by Krishan Kumar, Sunny Behal, Abhinav Bhandari, Sajal Bhatia. ISBN 1032028564
- Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), by Eric D. Knapp and Joel Thomas Langill, ISBN: 978-0124201149
- Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure (1st Edition), by Eric D. Knapp and Raj Samani, ISBN: 978-1597499989
- David Kleidermacher Mike Kleidermacher, "Embedded Systems Security - Practical Methods for Safe and Secure Software and Systems Development", 1st Edition, ISBN: 9780123868862, March 2012

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

Mapa III - Segurança no Software

4.2.1. Designação da unidade curricular (PT):

Segurança no Software

4.2.1. Designação da unidade curricular (EN):

Software Security

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

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

4.2.3. Duração (anual, semestral ou trimestral) (PT):
Semestral 1ºS

4.2.3. Duração (anual, semestral ou trimestral) (EN):
Semiannual 1st S

4.2.4. Horas de trabalho (número total de horas de trabalho):
162.0

4.2.5. Horas de contacto:
Presencial (P) - TP-15.0; PL-15.0
Síncrona a distância (SD) - TP-0.0

4.2.6. % Horas de contacto a distância:
0.00%

4.2.7. Créditos ECTS:
6.0

4.2.8. Docente responsável e respetiva carga letiva na Unidade Curricular:
• Pedro Miguel do Vale Malheiro Ramos Coutinho - 16.0h

4.2.9. Outros docentes e respetivas cargas letivas na unidade curricular:
• Pedro Miguel Simões Pinto Carneiro - 14.0h

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (PT):
A - Ser eficaz na identificação de pontos de entrada (entry points) aquando da programação de software reconhecendo habitualmente as entradas mais desejadas e facilitadoras do ponto de vista de um atacante.
B - Conhecer as principais considerações OWASP (Open Web Application Security Project) no desenvolvimento de aplicações seguras.
C - Programar uma aplicação com as técnicas de segurança aprendidas
D - Ser autónomo no desenho de um modelo de análise de ameaças num cenário de caso
E - Identificar, enumerar e priorizar, com sucesso, as potenciais vulnerabilidades sob um hipotético ponto de vista de um hacker
F - Conhecer os principais ataques que podem ser feitos a aplicações móveis

4.2.10. Objetivos de aprendizagem e a sua compatibilidade com o método de ensino (conhecimentos, aptidões e competências a desenvolver pelos estudantes). (EN):
A - Be effective in identifying entry points (entry points) when programming software, usually recognizing the most desired and facilitating entries from an attacker's point of view.
B - Apply OWASP (Open Web Application Security Project) considerations in the development of secure applications.
C - Program a software application with learned techniques that are secure related
D - Be autonomous in the design of a threat analysis model in a case scenario
E - Identify, enumerate and prioritize, successfully, potential vulnerabilities under a hypothetical point of view of a hacker
F - Understand the main attacks that can be made against mobile apps

4.2.11. Conteúdos programáticos (PT):

1 – CONCEITOS
2 - MODELOS DE ANÁLISE DE AMEAÇAS
3 - SEGURANÇA E DESENVOLVIMENTO DE SOFTWARE
3.1 processos de desenvolvimento de software seguro
3.1.1 modelo cascata e modelo espiral
3.1.2 microsoft security development lifecycle
3.1.3 segurança no desenvolvimento ágil
3.1.4 verificação e validação - norma IEEE 1012-2012
3.1.5 building security in maturity model
3.1.6 segurança aplicacional - norma ISO/IEC 27034
3.2 segurança durante o projeto
3.2.1 segurança nas linguagens de programação
3.2.2 sandboxes
4. VULNERABILIDADES
4.1 Buffers overflow
4.2 Race conditions
4.3 Validação de entradas
4.4 Ficheiros de inclusão local/remota
5. APLICAÇÕES WEB
5.1 top 10 OWASP
5.2 Análise de vulnerabilidades e mitigação
6. APLICAÇÕES MÓVEIS
6.1 top 10 de vulnerabilidades em aplicações móveis
6.2 Técnicas de análise de vulnerabilidades e de mitigação
6.3 Conceitos básicos e fundamentais de desenvolvimento
6.4 Laboratório prático de inserir código malicioso numa app

4.2.11. Conteúdos programáticos (EN):

1 – CONCEPTS
2 - THREAT ANALYSIS MODELS
3 - SECURITY AND SOFTWARE DEVELOPMENT
3.1 secure software development processes
3.1.1 waterfall model and spiral model
3.1.2 Microsoft Security Development Lifecycle
3.1.3 security in agile development
3.1.4 verification and validation - IEEE 1012-2012 standard
3.1.5 building security in maturity model
3.1.6 application security - ISO/IEC 27034
3.2 safety during the project
3.2.1 security in programming languages
3.2.2 sandboxes
4. VULNERABILITIES
4.1 Buffer overflow
4.2 Race conditions
4.3 Validation of inputs
4.4 Local/remote include files
5. WEB APPLICATIONS
5.1 top 10 OWASP
5.2 Vulnerability analysis and mitigation
6. MOBILE APPLICATIONS
6.1 top 10 vulnerabilities in mobile applications
6.2 Vulnerability analysis and mitigation techniques
6.3 Basic and fundamental development concepts
6.4 Practical laboratory for inserting malicious code into an app

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

Os conteúdos programáticos expostos foram delineados de forma a serem o mais coerente possível com os objetivos da unidade curricular. Nas secções anteriores os objetivos e competências estão identificados por letras e o conteúdo está devidamente numerado. À semelhança de uma matriz de alinhamento poderá assim observar-se para que competência é que os conteúdos programáticos contribuem:
1 – a, d
2 – d
3 – c, d
4 – e
5 – b
6 – f

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

In the previous sections the objectives and skills are identified by letters and the content is properly numbered. Like an array of alignment, can thus be noted to what skill each part of the syllabus is contributing to:
1 – a, d
2 – d
3 – c, d
4 – e
5 – b
6 – f

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

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

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

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

4.2.14. Avaliação (PT):
Avaliação contínua:
Módulo 1 - um trabalho prático ou artigo científico (50%)
Módulo 2 - um trabalho prático ou artigo científico (50%)

Exame final, recurso e especial: mantém-se os mesmos elementos de avaliação.

4.2.14. Avaliação (EN):
Continuous evaluation:
Module 1 - one practical work or scientific paper (50%)
Module 2 - one practical work or scientific paper (50%)

Final exam and all other exam seasons: same evaluation elements.

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

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

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

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

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

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

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

4.2.17. Observações (PT):

[sem resposta]

4.2.17. Observações (EN):

[sem resposta]

4.3. Unidades Curriculares (opções)

Mapa IV - Opção 1

4.3.1. Designação da unidade curricular (PT):

Opção 1

4.3.1. Designação da unidade curricular (EN):

Option 1

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

CCT

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

CST

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):
1,547.0

4.3.5. Horas de contacto:
Presencial (P) - OT-40.0

4.3.6. % Horas de contacto a distância:
0.00%

4.3.7. Créditos ECTS:
57.0

4.3.8. Unidades Curriculares filhas:
- *Dissertação - 57.0 ECTS*
- *Estágio - 57.0 ECTS*
- *Projeto - 57.0 ECTS*

4.3.9. Observações (PT):
[sem resposta]

4.3.9. Observações (EN):
[sem resposta]

4.4. Plano de Estudos

Mapa V - Percurso Geral - 1

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

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

4.4.2. Ano curricular:

1

4.4.3. Plano de Estudos

Unidade Curricular	Área Científica	Duração	Horas Trabalho	Horas Contacto	% HC a distância	Tipo	Opcional	ECTS
Criptografia Aplicada	CCT	Semestral 1ºS	162.0	P: PL-15.0; T-0.0; TP-11.0 SD: T-0.0; TP-4.0	13.33%		Não	6.0
Estratégias de Defesa na Administração de Sistemas	CCT	Semestral 1ºS	162.0	P: PL-23.0; TP-15.0 SD: TP-0.0	0.00%		Não	6.0
Gestão da Segurança da Informação	CCT	Semestral 1ºS	81.0	P: TP-30.0 SD: TP-0.0	0.00%		Não	3.0
Segurança de Redes e Sistemas	CCT	Semestral 1ºS	162.0	P: PL-15.0; TP-15.0 SD: TP-0.0	0.00%		Não	6.0

Segurança de Sistemas Ciberfísicos	CCT	Semestral 1ºS	81.0	P: PL-7.0; TP-15.0 SD: TP-0.0	0.00%		Não	3.0
Segurança no Software	CCT	Semestral 1ºS	162.0	P: PL-15.0; TP-15.0 SD: TP-0.0	0.00%		Não	6.0
Análise de Dados e Ciberinteligência	CCT	Semestral 2ºS	162.0	P: PL-15.0; TP-11.0 SD: TP-4.0	13.33%		Não	6.0
Auditoria e Conformidade em Cibersegurança	CCT	Semestral 2ºS	81.0	P: T-0.0; TP-21.0 SD: TP-0.0	0.00%		Não	3.0
Cibercrime e Análise Forense Digital	CCT	Semestral 2ºS	162.0	P: PL-30.0; TP-15.0 SD: TP-0.0	0.00%		Não	6.0
Engenharia Social	CCT	Semestral 2ºS	81.0	P: PL-7.0; TP-7.0 SD: TP-0.0	0.00%		Não	3.0
Gestão de Identidade Digital	CCT	Semestral 2ºS	81.0	P: PL-7.0; TP-7.0 SD: TP-0.0	0.00%		Não	3.0
Hacking Ético	CCT	Semestral 2ºS	162.0	P: PL-30.0; TP-15.0 SD: TP-0.0	0.00%		Não	6.0
Privacidade e Proteção de Dados	CCT	Semestral 2ºS	81.0	P: TP-14.0 SD: TP-0.0	0.00%		Não	3.0
Total: 13								

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
Opção 1	CCT	Anual	1,547.0	P: OT-40.0	0.00%	UC de Opção	Não	57.0
Metodologias de Investigação	CCT	Semestral 1ºS	81.0	P: PL-8.0; TP-8.0 SD: TP-0.0	0.00%		Não	3.0
Total: 2								

4.5. Percentagem de ECTS à distância

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

0.0

4.6. Observações Reestruturação curricular

4.6. Observações. (PT)

Em alinhamento com as diretrizes pedagógicas do projeto Línea e com as exigências atuais do mercado, apresentamos as propostas de atualização da estrutura curricular do Mestrado em Cibersegurança.
O projeto Línea tem como objetivo o desenvolvimento e implementação de um quadro de linhas orientadoras para um modelo pedagógico inovador,
que abrange toda a oferta formativa do Instituto Politécnico de Viana do Castelo (IPVC).
Este modelo valoriza práticas pedagógicas ativas, centradas no/a estudante e baseadas em projeto, proporcionando percursos de formação flexíveis.
Adicionalmente, incorpora experiências de imersão em contextos de prática profissional, de investigação e de internacionalização, incentivando a aprendizagem autorregulada e colaborativa.
O enfoque deste modelo está na formação orientada para os desafios societais do futuro e na promoção da empregabilidade.

1. Ajuste de Horas Letivas e Créditos ECTS
As horas letivas de cada unidade curricular foram ajustadas para semestres de 15 semanas, promovendo uma distribuição equilibrada entre o tempo de contacto e o estudo independente. Os créditos ECTS foram reorganizados em múltiplos de 3, facilitando a flexibilidade e a transferência de créditos entre instituições.
Esta reorganização resultou numa redução das horas de contacto em algumas unidades curriculares, exigindo um maior empenho em trabalho autónomo.
Contudo, unidades curriculares com igual número de créditos, mas maior componente prática, mantêm um número superior de horas de contacto
para refletir o seu carácter laboratorial.

2. Revisão da Bibliografia de Referência
A bibliografia foi revista e atualizada para incorporar as mais recentes tendências e avanços na área de Cibersegurança, garantindo a pertinência e atualidade dos conteúdos abordados.

3. Integração de Ensino Não Presencial
A nova estrutura curricular prevê a inclusão de momentos de ensino não presencial, até ao limite de 15% da carga horária total por unidade curricular. Esta abordagem visa introduzir flexibilidade adicional e refletir as práticas modernas de ensino.

4. ECTS obtidos por via alternativa
O Modelo Pedagógico do IPVC estabelece que até um total de 9 ECTS possam ser realizado, opcionalmente e por iniciativa do/a estudante, através das seguintes vias alternativas:
i) realização de UC de outros cursos do IPVC;
ii) e obtenção de microcreditações através da realização de formações de curta duração creditadas (com mínimo de nível 7).
As UCs realizáveis (substituíveis) através de vias alternativas são propostas previamente pela Comissão de Curso, com intervenção do CTC e das Comissões de Creditação, e não põem em causa a componente da(s) área(s) fundamentais do curso, nem as condições para certificação profissional onde esta é requerida.

Estas mudanças visam tornar o curso mais adaptado às necessidades do mercado, ao mesmo tempo que promovem uma abordagem pedagógica mais eficaz
e alinhada com padrões internacionais.

4.6. Observações. (EN)

In alignment with the pedagogical guidelines of the Línea project and current market demands,
we present the proposals to update the curricular structure of the Master in Cybersecurity.
The Línea project aims to develop and implement a framework of guidelines for an innovative pedagogical model,
which covers the entire training offer of the Polytechnic Institute of Viana do Castelo (IPVC).
This model values active, student-centered and project-based pedagogical practices, providing flexible training paths.
Additionally, it incorporates immersion experiences in contexts of professional practice, research and internationalization,
encouraging self-regulated and collaborative learning.
The focus of this model is on training aimed at the societal challenges of the future and promoting employability.

1. Adjustment of Teaching Hours and ECTS Credits
The teaching hours for each subject were adjusted to 15-week semesters, promoting a balanced distribution between contact time and independent study.
The ECTS credits have been reorganized into multiples of 3, facilitating flexibility and transfer of credits between institutions.
This reorganization resulted in a reduction in contact hours in some curricular units, requiring greater commitment to independent work.
However, curricular units with the same number of credits, but a greater practical component, maintain a higher number of contact hours
to reflect its laboratory character.

2. Review of the Reference Bibliography
The bibliography has been revised and updated to incorporate the latest trends and advances in the area of Cyber Security,
ensuring the relevance and timeliness of the content covered.

3. Integration of Non-In-Person Teaching
The new curricular structure provides for the inclusion of non-face-to-face teaching moments, up to a limit of 15% of the total workload
per curricular unit. This approach aims to introduce additional flexibility and reflect modern teaching practices.

4. ECTS obtained by alternative means
The IPVC Pedagogical Model establishes that up to a total of 9 ECTS can be completed, optionally and at the student's initiative, through the following alternative routes:
i) completion of UC from other IPVC courses;
ii) and obtaining micro-credits through carrying out credited short-term training (with a minimum of level 7).
UCs that can be achieved (replaceable) through alternative routes are previously proposed by the Course Committee, with the intervention of the CTC and the Crediting Committees, and do not put at risk the component of the fundamental area(s) of the course course, nor the conditions for professional certification where this is required.

These changes aim to make the course more adapted to market needs, while promoting a more effective pedagogical approach and aligned with international standards.

5. Pessoal Docente

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

• Pedro Miguel do Vale Malheiro Ramos Coutinho

5.2. Pessoal docente do ciclo de estudos

Nome	Categoria	Grau	Vínculo	Especialista	Regime de tempo	Informação
Luís Manuel Cerqueira Barreto	Professor Coordenador ou equivalente	Doutor Engenharia Eletrotécnica	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID

Nome	Categoria	Grau	Vínculo	Especialista	Regime de tempo	Informação
Pedro Miguel do Vale Malheiro Ramos Coutinho	Professor Adjunto ou equivalente	Doutor Tecnologias e Sistemas de Informação	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Sérgio Ivan Fernandes Lopes	Professor Adjunto ou equivalente	Doutor Engenharia Eletrotécnica	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Marco Filipe Vieira Gomes	Equiparado a Professor Adjunto ou equivalente	Doutor Desenvolvimento e análise de software e aplicações informáticas	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		30	Ficha Submetida CienciaVitae OrcID
Ricardo Jorge da Silva Santos	Professor Coordenador ou equivalente	Doutor FÍSICA - ENGENHARIA ELETROTÉCNICA E ENGENHARIA INFORMÁTICA - SISTEMAS INTELIGENTES, INTERAÇÃO E MULTIMÉDIA - INFORMÁTICA	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		20	Ficha Submetida CienciaVitae OrcID
Jorge Manuel Ferreira Barbosa Ribeiro	Professor Adjunto ou equivalente	Doutor Ciências de Engenharia Informática	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Carlos Abreu	Professor Adjunto ou equivalente	Doutor Engenharia Biomédica	Docente de Carreira (Art. 3º, alínea k) do DL-74/2006, na redação fixada pelo DL-65/2018		100	Ficha Submetida CienciaVitae OrcID
Silvestre Lomba Malta	Professor Adjunto ou equivalente	Doutor Ciências da computação	Outro vínculo		100	Ficha Submetida CienciaVitae OrcID
Pedro Miguel Simões Pinto Carneiro	Professor Adjunto ou equivalente	Mestre Novas Tecnologias	Outro vínculo	Sim 481	50	Ficha Submetida CienciaVitae OrcID
Rogério Bravo	Professor Associado convidado ou equivalente	Licenciado Direito	Outro vínculo	Sim Direito	20	Ficha Submetida CienciaVitae OrcID
					Total: 720	

5.2.1. Ficha curricular do docente

5.2.1.1. Dados Pessoais - Luís Manuel Cerqueira Barreto

Vínculo com a IES

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

Categoria

Professor Coordenador ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Engenharia Eletrotécnica

Área científica deste grau académico (EN)

Electrical Engineering

Ano em que foi obtido este grau académico

2012

Instituição que conferiu este grau académico

Universidade de Aveiro

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

100

CienciaVitae

9A19-DB13-11E0

Orcid

0000-0001-6173-433X

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Luís Manuel Cerqueira Barreto

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)	Outro	

5.2.1.3. Outros graus académicos ou títulos - Luís Manuel Cerqueira Barreto

Ano	Grau ou Título	Área	Instituição	Classificação
1995	Licenciatura em Engenharia Eletrotécnica	Engenharia Eletrotécnica	Faculdade de Engenharia da Universidade do Porto	12
2005	Mestrado em Informática-Ramo Segurança Informática	Informática	Faculdade de Ciências da Universidade do Porto	Muito Bom

5.2.1.4. Formação pedagógica - Luís Manuel Cerqueira Barreto

Formação pedagógica relevante para a docência
Gamificação (2 horas)
Conceção de Atividades/UC em E/B-lerning (6 ECTS) 30horas
Aula Invertida (3 horas)

5.2.1.5. Distribuição do serviço docente - Luís Manuel Cerqueira Barreto

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Criptografia Aplicada	Mestrado em Cibersegurança	32.0	0.0	16.0	16.0					
Metodologias de Investigação e Gestão de Projetos	Mestrado em Cibersegurança	2.0			2.0					
Tecnologias e Redes de Comunicação Veicular	Mestrado em Eletrónica e Eletrificação Automóvel	6.0		6.0						

5.2.1.1. Dados Pessoais - Pedro Miguel do Vale Malheiro Ramos 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 Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Tecnologias e Sistemas de Informação

Área científica deste grau académico (EN)

Information Systems and Technology

Ano em que foi obtido este grau académico

2020

Instituição que conferiu este grau académico

Universidade do Minho

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

100

CienciaVitae

0C11-0619-2E71

Orcid

0000-0002-1804-9406

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Pedro Miguel do Vale Malheiro Ramos Coutinho

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Investigação ALGORITMI (ALGORITMI)	Muito Bom	Universidade do Minho (UM)		

5.2.1.3. Outros graus académicos ou títulos - Pedro Miguel do Vale Malheiro Ramos Coutinho

Ano	Grau ou Título	Área	Instituição	Classificação
1992	Engenharia de Sistemas e Informática	Informática	Universidade do Minho	14
1998	Mestrado em Informática	Informática	Universidade do Minho	Muito Bom
2020	Doutoramento em Tecnologias e Sistemas de Informação	Tecnologias e Sistemas de Informação	Universidade do Minho	Muito Bom

5.2.1.4. Formação pedagógica - Pedro Miguel do Vale Malheiro Ramos Coutinho

Formação pedagógica relevante para a docência
2021, Curso de Formação Profissional de Aprendizagem com base em Processos de Co-criação, Instituto Politécnico de Bragança / Programa de formação de desenvolvimento profissional em facilitação da cocriação Demola (8 ECTS), Universidade de Ciências Aplicadas de Kajaani, Finlândia, com duração de 344 horas
2023, Ação de Formação sobre Gamificação – Carlos Renato Zacharias (UNESP). ESE-IPVC
2023, Ação de Formação sobre Aula Invertida – Carlos Renato Zacharias (UNESP). ESE-IPVC
2024, "RUN.EU Future Skills - O Conceito 50+10 na dinamização de aprendizagens ativas", I Jornadas de Excelência Pedagógica e Inovação em Cocriação (EPIC)
2024, "Boas práticas curriculares em contexto de Ensino Superior: recursos para a promoção do sucesso académico", I Jornadas de Excelência Pedagógica e Inovação em Cocriação (EPIC)
2024, "Estudantes ativamente envolvidos nas aulas com os seus telemóveis: estratégias de utilização de Audience Response Systems (ARS)", I Jornadas de Excelência Pedagógica e Inovação em Cocriação (EPIC)

5.2.1.5. Distribuição do serviço docente - Pedro Miguel do Vale Malheiro Ramos Coutinho

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Introdução à Programação	Curso Técnico Superior Profissional em Desenvolvimento Web e Multimédia	24.0	24.0							
Algoritmos e Estruturas de Dados	Licenciatura em Engenharia de Redes e Sistemas de Computadores	40.0		40.0						
Algoritmos e Estruturas de Dados	Licenciatura em Engenharia Informática	80.0		80.0						
Segurança no Software	Mestrado em Cibersegurança	16.0		8.0	8.0					
Programação 2	Licenciatura em Engenharia de Redes e Sistemas de Computadores	88.0		24.0	64.0					
Programação 1	Licenciatura em Engenharia de Redes e Sistemas de Computadores	32.0		32.0						
Algoritmia e Programação	Licenciatura em Engenharia da Computação Gráfica e Multimédia	64.0		32.0	32.0					
Estágio	Curso Técnico Superior Profissional em Desenvolvimento Web e Multimédia	1.0						1.0		
Projecto IV	Licenciatura em Engenharia Informática	6.0			6.0					

5.2.1.1. Dados Pessoais - Sérgio Ivan Fernandes Lopes

Vínculo com a IES

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

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Engenharia Eletrotécnica

Área científica deste grau académico (EN)

Electrical Engineering

Ano em que foi obtido este grau académico

2014

Instituição que conferiu este grau académico

Universidade de Aveiro

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

100

CienciaVitae

8B1B-F6F5-B218

Orcid

0000-0001-6944-7757

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Sérgio Ivan Fernandes Lopes

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)		

5.2.1.3. Outros graus académicos ou títulos - Sérgio Ivan Fernandes Lopes

Ano	Grau ou Título	Área	Instituição	Classificação
2004	Licenciatura	Engenharia Eletrónica e Telecomunicações	Universidade de Aveiro	13
2009	Mestrado	Engenharia Biomédica	Universidade de Aveiro	Aprovado
2017	Pós Graduação	Gestão de Projetos	Porto Business School/Universidade do Porto	16

5.2.1.4. Formação pedagógica - Sérgio Ivan Fernandes Lopes

Formação pedagógica relevante para a docência
Webinar Interno IPVC (120 min), sessão de informação e formação sobre a operacional- ização na ESTG do plano de contingência relativo às atividades letivas não-presenciais (EaD): Orientações; Plataformas Recomendadas; Mecanismos de Assiduidade / Estatísticas de Participação; Ferramentas e Mecanismos de Suporte; Zoom Colibri - Demonstração e Boas Práticas; Testes no Moodle com o "Safe Exam Browser"; Partilha de Experiências, 18 de Março de 2020.
Ação de Sensibilização - Regulamento Geral sobre a Proteção de Dados, promovida pela SGS Portugal e com duração de 3 horas, Escola Superior de Tecnologias e Gestão do Instituto Politécnico de Viana do Castelo, 16 de abril de 2018, entre as 09h00 e as 12h00.
Metodologia de Ensino e Aprendizagem - Designing Student Centered Learning Experiences, formação promovida pelo Gabinete de Avaliação e Qualidade, Instituto Politécnico de Viana do Castelo, 23 de Maio, 2018.
Metodologia de Ensino e Aprendizagem - Student Centered Learning, formação promovida pelo Gabinete de Avaliação e Qualidade, Instituto Politécnico de Viana do Castelo, 22 de Maio, 2018.
Formação de Curta Duração - Inteligência Artificial Generativa na Educação, pro- movida pelo Instituto Politécnico de Viana do Castelo, no âmbito do projeto LIneA IPVC Skills4PosCovid, com duração de 4 horas, ocorrido nos dias 7 e 14 de junho de 2023.

5.2.1.5. Distribuição do serviço docente - Sérgio Ivan Fernandes Lopes

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Análise e Processamento de Sinal	Licenciatura em Engenharia de Redes e Sistemas de Computadores	32.0		32.0						
Sistemas Ciber-Físicos	Licenciatura em Engenharia de Redes e Sistemas de Computadores	32.0		32.0						
Projecto 2	Licenciatura em Engenharia de Redes e Sistemas de Computadores	24.0			24.0					
Projeto Final ou Estágio	Licenciatura em Engenharia Mecatrónica	4.0							4.0	
Projeto 1	Licenciatura em Engenharia de Redes e Sistemas de Computadores	6.0		6.0						
Segurança de Sistemas Ciber-Físicos	Mestrado em Cibersegurança	24.0		16.0	8.0					
Metodologias de Investigação e Gestão de Projetos	Mestrado em Cibersegurança	2.0			2.0					
Circuitos e Sistemas de Aquisição de Dados	Mestrado em Eletrónica e Eletrificação Automóvel	6.0		6.0						
Sistemas Ciber-Físicos e Indústria 4.0	Mestrado em Eletrónica e Eletrificação Automóvel	10.0		10.0						
Seminários	Mestrado em Engenharia Informática	2.0		2.0						
Computação Móvel e Multisensorial	Mestrado em Engenharia informática	10.0		4.0	6.0					

5.2.1.1. Dados Pessoais - Marco Filipe Vieira Gomes

Vínculo com a IES

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

Categoria

Equiparado a Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Desenvolvimento e análise de software e aplicações informáticas

Área científica deste grau académico (EN)

Engenharia Eletrotécnica e Engenharia Informática - Engenharia de Software e Sistemas de Informação

Ano em que foi obtido este grau académico

2011

Instituição que conferiu este grau académico

Universidade do Minho

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

30

CienciaVitae

BD14-4019-9EAB

Orcid

0000-0001-6370-9955

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Marco Filipe Vieira Gomes

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação (CIICESI)	Bom	Instituto Politécnico do Porto (IPP)		Sim

5.2.1.3. Outros graus académicos ou títulos - Marco Filipe Vieira Gomes

Ano	Grau ou Título	Área	Instituição	Classificação
2010	Licenciatura	Ciências da Computação	Universidade do Minho	12
2012	Mestrado	Informática	Universidade do Minho	17

5.2.1.4. Formação pedagógica - Marco Filipe Vieira Gomes

Formação pedagógica relevante para a docência
Plataforma Moodle

5.2.1.5. Distribuição do serviço docente - Marco Filipe Vieira Gomes

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Cibercrime e Análise Forense Digital	Mestrado em Cibersegurança	16.0			16.0					
Hacking Ético	Mestrado em Cibersegurança	48.0	20.0		28.0					

5.2.1.1. Dados Pessoais - Ricardo Jorge da Silva Santos

Vínculo com a IES

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

Categoria

Professor Coordenador ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

FÍSICA - ENGENHARIA ELETROTÉCNICA E ENGENHARIA INFORMÁTICA - SISTEMAS INTELIGENTES, INTERAÇÃO E MULTIMÉDIA - INFORMÁTICA

Área científica deste grau académico (EN)

Informatics

Ano em que foi obtido este grau académico

2010

Instituição que conferiu este grau académico

UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

20

CienciaVitae

B119-1A2A-58BF

Orcid

0000-0002-2139-5414

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Ricardo Jorge da Silva Santos

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação (CIICESI)	Bom	Instituto Politécnico do Porto (IPP)	Institucional	Sim

5.2.1.3. Outros graus académicos ou títulos - Ricardo Jorge da Silva Santos

Ano	Grau ou Título	Área	Instituição	Classificação
2010	PhD In Informatics	Informática	Universidade de Trás-os-Montes e Alto Douro	Aprovado com Mérito e Distinção
2005	Licenciatura em Engenharia Informática	ELETRÓNICA E AUTOMAÇÃO - ENGENHARIA ELETROTÉCNICA E ENGENHARIA INFORMÁTICA - CIÊNCIA E TECNOLOGIA DA PROGRAMAÇÃO - Informática	Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto	17

5.2.1.4. Formação pedagógica - Ricardo Jorge da Silva Santos

Formação pedagógica relevante para a docência
Inquirir na e com a Comunidade: Desafios e Implicações
Inovar as Apresentações com o Mentimeter
Metodologias ativas & ChatGPT: uma Parceria de Sucesso

5.2.1.5. Distribuição do serviço docente - Ricardo Jorge da Silva Santos

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Análise de Dados e CiberInteligência	Mestrado em Cibersegurança	8.0		8.0						
Gestão de Identidade Digital	Mestrado em Cibersegurança	8.0		8.0						

5.2.1.1. Dados Pessoais - Jorge Manuel Ferreira Barbosa Ribeiro

Vínculo com a IES

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

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Ciências de Engenharia Informática

Área científica deste grau académico (EN)

Computer Engineering Sciences

Ano em que foi obtido este grau académico

2011

Instituição que conferiu este grau académico

Universidade de Santiago de Compostela

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

1310-2CF4-C108

Orcid

0000-0003-1874-7340

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Jorge Manuel Ferreira Barbosa Ribeiro

5.2.1.3. Outros graus académicos ou títulos - Jorge Manuel Ferreira Barbosa Ribeiro

Ano	Grau ou Título	Área	Instituição	Classificação
2007	Mestrado	Ciências de Engenharia Informática	Universidade do Minho	Muito Bom
2001	Licenciatura (5 ano curriculares)	Ciências de Engenharia Informática	Universidade do Minho	14

5.2.1.4. Formação pedagógica - Jorge Manuel Ferreira Barbosa Ribeiro

Formação pedagógica relevante para a docência
2023, Conceção de atividades/Unidades curriculares em e/B-learning (6 ECTS), Centro de Inovação Pedagógica do Instituto Politécnico do Porto, 12 de outubro a 21 de dezembro de 2022, com a duração de 30 horas.
2018, Ação de formação, Regulamento Geral de Proteção de Dados, IPVC, 12 de julho.
2017, Desenho de Experiências de Aprendizagem Centradas no Aluno - Coordenador: Olin Collaboratory 2017 Summer Institute - Olin College of Engineering em Boston, EUA. 5 a 9 de junho.
2013, Curso de Formação sobre “A nova norma de auditorias e Sistemas de Gestão – ISO 19001:2011”, APCER – Associação Portuguesa de Certificação, 2 de janeiro de 2013.
2009, Curso de Qualificação de Auditores Internos da Qualidade. 22, 23, 27, 28 e 29 Julho de 2009. Formação com um total de 40 horas ministrada pela entidade SGS Portugal (http://www.pt.sgs.com). Certificado n.º PT09/03301.

5.2.1.5. Distribuição do serviço docente - Jorge Manuel Ferreira Barbosa Ribeiro

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Integração de Sistemas	Licenciatura em Engenharia Informática	32.0		32.0						
Metodologias de Investigação e Gestão de Projetos	Mestrado em Cibersegurança	2.0		2.0						
Projeto IV	Licenciatura em Engenharia Informática	30.0			30.0					
Inteligência Artificial	Licenciatura em Engenharia Informática	112.0		64.0	48.0					
Business Analytics e Mineração de Dados	Mestrado em Engenharia Informática	16.0		8.0	8.0					
Análise de Dados e CiberInteligência	Mestrado em Cibersegurança	16.0		8.0	8.0					
Projeto III	Licenciatura em Engenharia Informática	30.0	0.0	8.0	22.0					
Aprendizagem Organizacional - Opção II	Ciências de Engenharia Informática	74.0		32.0	42.0					

5.2.1.1. Dados Pessoais - Carlos Abreu

Vínculo com a IES

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

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Engenharia Biomédica

Área científica deste grau académico (EN)

Biomedical Engineering

Ano em que foi obtido este grau académico

2014

Instituição que conferiu este grau académico

Universidade do Minho

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

Não

Área científica do título de especialista (PT)

[sem resposta]

Área científica do título de especialista (EN)

[no answer]

Ano em que foi obtido o título de especialista

-

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

100

CienciaVitae

911A-2C18-106F

Orcid

0000-0001-9005-9599

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 Abreu

Unidades de Investigação	Classificação FCT	Instituição de ensino superior (IES)	Tipo unidade investigação	Docente Integrado
Unidade de Investigação em Microssistemas Eletromecânicos (CMEMS-UMinho)	Excelente	Universidade do Minho (UM)		

5.2.1.3. Outros graus académicos ou títulos - Carlos Abreu

Ano	Grau ou Título	Área	Instituição	Classificação
2008	Mestrado	Engenharia Biomédica	Universidade de Aveiro	Aprovado
2005	Licenciatura	Electrónica e Telecomunicações	Universidade de Aveiro	14

5.2.1.4. Formação pedagógica - Carlos Abreu

Formação pedagógica relevante para a docência
Demola International Project Studies

5.2.1.5. Distribuição do serviço docente - Carlos Abreu

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Sistemas Embebidos	Licenciatura em Engenharia de Redes e Sistemas de Computadores	72.0	0.0	24.0	48.0					
Metodologias de Investigação e Gestão de Projetos	Mestrado em Cibersegurança	2.0		2.0						
Sistemas Embebidos	Licenciatura em Engenharia Mecatrónica	64.0		32.0	32.0					
Sistemas Digitais e Microcontroladores	Licenciatura em Engenharia Mecatrónica	72.0		32.0	40.0					
Microcontroladores	Curso Técnico Superior Profissional em Sistemas Eletrónicos e Computadores	30.0		16.0	14.0					
Projeto 1	Licenciatura em Engenharia de Redes e Sistemas de Computadores	6.0		6.0						
Projeto 2	Licenciatura em Engenharia de Redes e Sistemas de Computadores	14.0		14.0						
Eletrónica	Licenciatura em Engenharia Mecatrónica	64.0		32.0	32.0					
Sistemas Distribuídos	Licenciatura em Engenharia Mecatrónica	64.0		32.0	32.0					
Estágio	Curso Técnico Superior Profissional em Sistemas Eletrónicos e Computadores	3.0						3.0		

5.2.1.1. Dados Pessoais - Rogério Bravo

Vínculo com a IES

Outro vínculo

Categoria

Professor Associado convidado ou equivalente

Grau Associado

Sim

Grau

Licenciatura - 1º ciclo

Área científica deste grau académico (PT)

Direito

Área científica deste grau académico (EN)

Law

Ano em que foi obtido este grau académico

2006

Instituição que conferiu este grau académico

Universidade Autónoma 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)

Sim

Área científica do título de especialista (PT)

Direito

Área científica do título de especialista (EN)

Law

Ano em que foi obtido o título de especialista

2020

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

20

CienciaVitae

5012-7B2A-9918

Orcid

0000-0002-0165-5071

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Rogério Bravo

5.2.1.3. Outros graus académicos ou títulos - Rogério Bravo

Ano	Grau ou Título	Área	Instituição	Classificação
2009	Pós-Graduação em Direito, em Ciências Jurídico-Processuais	Ciências Jurídico-Processuais	Universidade Autónoma de Lisboa	16
2009	Curso de Especialização com reconhecimento académico	“Competitive Intelligence”	ISCSP	17
2010	Pós-Graduação	Guerra de Informação	Academia Militar	15

5.2.1.4. Formação pedagógica - Rogério Bravo

Formação pedagógica relevante para a docência
equivalência por lei baseado em docência desde 2010

5.2.1.5. Distribuição do serviço docente - Rogério Bravo

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Cibercrime e Análise Forense Digital	2.º Ciclo Mestrado	12.0		12.0						

5.2.1.1. Dados Pessoais - Pedro Miguel Simões Pinto Carneiro

Vínculo com a IES

Outro vínculo

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Mestrado - 2º ciclo

Área científica deste grau académico (PT)

Novas Tecnologias

Área científica deste grau académico (EN)

New Technologies

Ano em que foi obtido este grau académico

2008

Instituição que conferiu este grau académico

Instituto Universitário de pós-grado

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)

Sim

Área científica do título de especialista (PT)

481

Área científica do título de especialista (EN)

Ciências Informáticas

Ano em que foi obtido o título de especialista

2021

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

50

CienciaVitae

651A-A317-A101

Orcid

0000-0003-1557-4181

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Pedro Miguel Simões Pinto Carneiro

5.2.1.3. Outros graus académicos ou títulos - Pedro Miguel Simões Pinto Carneiro

5.2.1.4. Formação pedagógica - Pedro Miguel Simões Pinto Carneiro

Formação pedagógica relevante para a docência
Profissionalização em serviço Informática
Certificado de competências Pedagógicas

5.2.1.5. Distribuição do serviço docente - Pedro Miguel Simões Pinto Carneiro

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Metodologias de Investigação e Gestão de Projetos	Mestrado	2.0		2.0						
Segurança no Software	Mestrado	16.0	8.0	8.0						
Gestão da Segurança da Informação	Mestrado	32.0		32.0						
Auditoria e Conformidade em Cibersegurança	Mestrado	24.0		24.0						
Privacidade e Proteção de Dados	Mestrado	16.0		16.0						
Cibercrime e Análise Forense Digital	Mestrado	12.0		12.0						

5.2.1.1. Dados Pessoais - Silvestre Lomba Malta

Vínculo com a IES

Outro vínculo

Categoria

Professor Adjunto ou equivalente

Grau Associado

Sim

Grau

Doutoramento - 3º ciclo

Área científica deste grau académico (PT)

Ciências da computação

Área científica deste grau académico (EN)

Computer science

Ano em que foi obtido este grau académico

2024

Instituição que conferiu este grau académico

Universidade de Vigo, Espanha

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

5D1C-FC16-564D

Orcid

0000-0002-5274-3733

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

Sim

5.2.1.2. Filiação Unidades de Investigação - Silvestre Lomba Malta

5.2.1.3. Outros graus académicos ou títulos - Silvestre Lomba Malta

Ano	Grau ou Título	Área	Instituição	Classificação
2013	Mestrado	Ciencias da computação	ESTG - Instituto Politécnico de Viana do Castelo	16
2005	Licenciado	Ciências da computação	ESTG - instituto Politécnico de Viana do Castelo	13

5.2.1.4. Formação pedagógica - Silvestre Lomba Malta

Formação pedagógica relevante para a docência
CCP - Certificado de Competências Pedagógicas - 04/02/2010 - Certificado nº EDF 521588/2010 DN

5.2.1.5. Distribuição do serviço docente - Silvestre Lomba Malta

Unidade Curricular	Ciclo de estudos	Total horas contacto	T	TP	PL	TC	S	E	OT	O
Tópicos Avançados de Redes	Licenciatura	96.0		32.0	64.0					
Redes e Serviços de Comunicação	Licenciatura	88.0		24.0	64.0					
Redes e Serviços Multimédia	Licenciatura	64.0		32.0	32.0					
Projeto 1	Licenciatura	4.0		4.0						
Projeto 2	Licenciatura	16.0			16.0					
Segurança de Redes e Sistemas	Licenciatura	32.0		32.0						
Segurança de Redes e Sistemas	Mestrado	32.0		16.0	16.0					
Estratégias de Defesa na Administração de Sistemas	Mestrado	40.0		16.0	24.0					
Metodologias de Investigação e Gestão de Projetos	Mestrado	6.0		2.0	4.0					
Engenharia Social	Mestrado	16.0		8.0	8.0					

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

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

5.3.1.1. Número total de docentes.

10

5.3.1.2. Número total de ETI.

7.20

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	76.39%
Investigador de Carreira (Art. 3º, alínea l) do DL-74/2006, na redação fixada pelo DL-65/2018	0.00%
Outro vínculo	23.61%

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)	650	90.28%

5.3.4. Corpo docente especializado

Corpo docente especializado	ETI	Percentagem*
Doutorados especializados na(s) área(s) fundamental(is) do CE (% total ETI)	6.5	90.28%
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)	0.5	6.94%
% de docentes com título de especialista ou doutores especializados, na(s) área(s) fundamental(is) do ciclo de estudos (% total ETI)		97.22%

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	6.0	83.33%
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

5.4. Observações. (PT)

[sem resposta]

5.4. Observações. (EN)

[sem resposta]

Observações (PDF)

[sem resposta]

6. Pessoal técnico, administrativo e de gestão (se aplicável)

6.1. Número e regime de dedicação do pessoal técnico, administrativo e de gestão afeto à lecionação do ciclo de estudos. (PT)

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

Apoio aos Laboratórios - 3 funcionários (tempo inteiro)
Secretariado dos Conselhos Técnico-Científico e Pedagógico - 2 funcionário (tempo inteiro)
Biblioteca da ESTG - 3 funcionários (tempo inteiro)
Serviços Académicos - 4 funcionários (tempo inteiro)

Neste contexto, existem muitos outros serviços e unidades que por razões de pertinência não estão aqui colocados.

6.1. Número e regime de dedicação do pessoal técnico, administrativo e de gestão afeto à lecionação do ciclo de estudos. (EN)

The number of non-teaching people in the areas most relevant to the support of the study cycle are:

Support to Laboratories - 3 employees (full time)
Secretariat of the Technical-Scientific and Pedagogical Councils - 2 official (full time)
ESTG Library - 3 employees (full time)
Academic Services - 4 employees (full time)

In this context, there are many other services and units that for reasons of relevance are not placed here.

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

A maior parte do pessoal não docente possui o 12º ano ou o grau de licenciado nas mais diversas áreas.

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

Most of the non teaching staff has a 12th grade or a bachelor's degree in several areas.

7. Instalações, parcerias e estruturas de apoio aos processos de ensino e aprendizagem (se aplicável)

7.1. Registaram-se alterações significativas quanto a instalações e equipamentos desde o anterior processo de avaliação?

[X] Sim [ ] Não

7.1.1. Em caso afirmativo, apresentar uma breve explanação e fundamentação das alterações efetuadas. (PT)

O IPVC efetuou um forte investimento em equipamentos digitais para o ensino, com instalação em muitas salas com equipamentos para o desenvolvimento da investigação sobre práticas pedagógicas, adquirindo vários softwares, incluído de antiplágio e outros mais específicos. A nível da Unidade Orgânica (UO) onde o Ciclo de Estudos é lecionado, foi substituída toda a cobertura que utilizava amianto. Foram instalados novos sistemas de aquecimento, e climatização e ventilação do auditório principal. Foram instaladas cortinas de corte de luz solar direta. Foi instalado um parque fotovoltaico que garante à UO operar em autossuficiência energética numa % muito significativa do consumo. Foi requalificado o auditório principal com novos meios audiovisuais. Foram instaladas 20 salas com capacidade de vídeo conferência e instaladas 12 salas com ecrãs interativos. Foi requalificado o mobiliário e pisos (eliminação de alcatifas) em sala e gabinetes. Foram atualizados meios computacionais (HW e SW)

7.1.1. Em caso afirmativo, apresentar uma breve explanação e fundamentação das alterações efetuadas. (EN)

IPVC made a strong investment in digital equipment for teaching, installing equipment in many rooms for carrying out research on pedagogical practices, acquiring various software, including anti-plagiarism and other more specific software. In terms of the Organic Unit (OU) where the Study Cycle is taught, all the covering that used asbestos was replaced. New heating, air conditioning and ventilation systems were installed in the main auditorium. Curtains cutting out direct sunlight have been installed. A photovoltaic park was installed that guarantees the OU operates in energy self-sufficiency in a very significant % of consumption. The main auditorium was renovated with new audiovisual equipment. 20 rooms with video conferencing capacity were installed and 12 rooms with interactive screens were installed. The furniture and floors were renovated (elimination of carpets) in the living room and offices. Computational means (HW and SW) have been updated

7.2. Registaram-se alterações significativas quanto a parcerias nacionais e internacionais no âmbito do ciclo de estudos desde o anterior processo de avaliação?

[X] Sim [ ] Não

7.2.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (PT)

Parcerias Internacionais:
Para intensificar a internacionalização do Mestrado em Cibersegurança, foi firmado um acordo de dupla titulação entre o IPVC e o Instituto Federal de Santa Catarina (IFSC), no Brasil. Esse acordo tem como objetivo proporcionar dupla titulação para os estudantes do Mestrado em Cibersegurança do IPVC e para a graduação em Ciência da Computação do Campus Lages do IFSC. Adicionalmente, está em fase final um acordo de dupla titulação do Mestrado em Cibersegurança com o Mestrado em "Applied Computer Science" da Universidade de Østfold, na Noruega. Este acordo permitirá que estudantes do Mestrado em Cibersegurança possam sejam selecionados para o Mestrado em "Applied Computer Science", e vice-versa.
Parcerias Nacionais:
Com a Polícia Judiciária, o inspetor Rogério Bravo é docente convidado, e com o Instituto Politécnico do Porto com os docentes convidados Ricardo Santos e Marco Gomes.

7.2.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (EN)

International Partnerships:
To intensify the internationalization of the Master's Degree in Cybersecurity, a double degree agreement was signed between IPVC and the Federal Institute of Santa Catarina (IFSC), in Brazil. This agreement aims to provide double degrees for students of the Master's in Cybersecurity at IPVC and for the undergraduate degree in Computer Science at the Lages Campus of IFSC. Additionally, a double degree agreement for the Master in Cyber ??Security with the Master in "Applied Computer Science" at the University of Østfold, in Norway, is in the final stages. This agreement will allow students from the Master's in Cybersecurity to be selected for the Master's in "Applied Computer Science", and vice versa.
National Partnerships:
With the Judiciary Police, inspector Rogério Bravo is a guest professor, and with the Porto Polytechnic Institute with guest professors Ricardo Santos and Marco Gomes.

7.3. Registaram-se alterações significativas quanto a estruturas de apoio aos processos de ensino e aprendizagem desde o anterior processo de avaliação?

[X] Sim [ ] Não

7.3.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (PT)

O IPVC criou a Pró-Presidência para a Inovação Pedagógica e a Unidade de Ensino Digital e a Distância (UE2D) do IPVC com a missão de fomentar a inovação pedagógica no ensino digital e a distância, assim como o Modelo Pedagógico com as linhas orientadoras atualizadas para as novas práticas de ensino, nomeadamente o ensino à distância.

O IPVC disponibiliza a plataforma ON.IPVC que permite Gestão Documental; Gestão da atividade letiva; Gestão de Indicadores no Observatório IPVC; Pedidos de Suporte de Serviços.

São disponibilizadas ainda outras plataformas de apoio, com interoperabilidade com a ON.IPVC: E-learning Moodle que integra o Sistema de Deteção de Plágio; Serviços Académicos; Digitalis de gestão académica; SAS-SOCIAL-IPVC e a APP My IPVC; Microsoft, Office365 (correio eletrónico, Onedrive, Microsoft TEAMS, etc.; Plataforma de Serviços RCTS (Zoom, Educast, Filesender, B-On; Repositório Científico IPVC.

7.3.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (EN)

IPVC created the Pro-Presidency for Pedagogical Innovation and the IPVC Digital and Distance Learning Unit (UE2D) with the mission of promoting pedagogical innovation in digital and distance learning, as well as the Pedagogical Model with updated guidelines for new teaching practices, namely distance learning.

IPVC provides the ON.IPVC platform that allows Document Management; Management of teaching activities; Management of Indicators at the IPVC Observatory; Service Support Requests.

Other support platforms are also available, with interoperability with ON.IPVC: E-learning Moodle that integrates the Plagiarism Detection System; Academic Services; Academic management digitalis; SAS-SOCIAL-IPVC and the My IPVC APP; Microsoft, Office365 (email, Onedrive, Microsoft TEAMS, etc.; RCTS Services Platform (Zoom, Educast, Filesender, B-On; IPVC Scientific Repository.

7.4. Registaram-se alterações significativas quanto a locais de estágio e/ou formação em serviço, protocolos com as respetivas entidades e garantia de acompanhamento efetivo dos estudantes durante o estágio desde o anterior processo de avaliação?

[ ] Sim [X] Não

7.4.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (PT)

[sem resposta]

7.4.1. Em caso afirmativo, apresentar uma síntese das alterações ocorridas. (EN)

[sem resposta]

8. Parâmetros de avaliação do Ciclo de Estudos.

8.1. Estudantes inscritos no ciclo de estudos no ano letivo em curso.

8.1.1. Total de estudantes inscritos.

49.0

8.1.2. Caracterização por Género.

Género	Percentagem
Masculino	89.8
Feminino	10.2

8.1.3. Estudantes inscritos por ano curricular.

Ano curricular	Estudantes inscritos
1º ano curricular	28
2º ano curricular	21

8.1.4. Eventual informação adicional sobre a caracterização dos estudantes. (PT)

[sem resposta]

[sem resposta]

8.2. Procura do ciclo de estudos - Estudantes

Parâmetro	Penúltimo ano	Último ano	Ano corrente
N.º de vagas / No. of openings	30	25	25
N.º de candidatos / No. of candidates	68	63	65
N.º de admitidos / No. of admissions	33	23	27
N.º de inscritos no 1º ano, 1ª vez / No. of enrolments in 1st year 1st time	33	23	27

8.2. Procura do ciclo de estudos - Classificações

Parâmetro	Penúltimo ano	Último ano	Ano corrente
Nota de candidatura do último colocado / Grade of the last candidate to be admitted			
Nota média de entrada / Average entry grade			

8.3. Resultados Académicos.

8.3.1. Eficiência formativa.

Indicador	Antepenúltimo ano	Penúltimo ano	Último ano
N.º de graduados / No. of graduates	3	8	1
N.º de graduados em N anos / No. of graduates in N years	1	7	0
N.º de graduados em N+1 anos / No. of graduates in N+1 years	2	1	1
N.º de graduados em N+2 anos / No. of graduates in N+2 years	0	0	0
N.º de graduados em mais de N+2 anos / No. of graduates in more than N+2 years	0	0	0

8.3.2. Apresentar relação de teses defendidas nos três últimos anos, indicando, para cada uma, o título, o ano de conclusão e o resultado final (PT)

N/A

8.3.2. Apresentar relação de teses defendidas nos três últimos anos, indicando, para cada uma, o título, o ano de conclusão e o resultado final (EN)

N/A

8.3.3. Dados sobre desemprego dos diplomados do ciclo de estudos (PT)

Sem dados.

8.3.3. Dados sobre desemprego dos diplomados do ciclo de estudos (EN)

Sem dados.

8.4. Resultados de internacionalização.

8.4.1. Mobilidade de estudantes, docentes e pessoal técnico, administrativo e de gestão.

Indicador	Antepenúltimo ano	Penúltimo ano	Último ano
Alunos estrangeiros matriculados no ciclo de estudos / Foreign students enrolled in the study programme	19.14	20	16.66
Alunos em programas internacionais de mobilidade (in) / Students in international mobility programs (in)			
Alunos em programas internacionais de mobilidade (out) / Students in international mobility programs (out)			
Docentes estrangeiros (in) / Foreign teaching staff (in)			
Docentes (out) / Teaching staff (out)		8.3	30
Pessoal técnico, administrativo e de gestão estrangeiro (in) / Foreign technical, administrative and management staff (in)			
Pessoal técnico, administrativo e de gestão (out) / Technical, administrative and management staff (out)			

8.4.2. Participação em redes internacionais com relevância para o ciclo de estudos (PT)

Participação do IPVC como parceiro na Rede Europeia de Universidades SUNRISE - "Smaller (strategic) Universities Network for Regional Innovation and Sustainable Evolution", composto por oito parceiros de seis países europeus, https://sites.google.com/view/sunrise-alliance/home.

Participação do IPVC no programa Erasmus+International Credit Mobility, envolvendo as instituições: Agricultural University of Tirana (Albânia), University of Kragujevac, Faculty of Education in Jagodina (Sérvia), UBT Pristina (Kosovo), University of Tuzla, University of Mostar e University of Sarajevo (Bósnia e Herzegovina)

8.4.2. Participação em redes internacionais com relevância para o ciclo de estudos (EN)

Participation of IPVC in the European University Network SUNRISE - "Smaller (strategic) Universities Network for Regional Innovation and Sustainable Evolution", which comprises eight partners from six European countries. For more information, visit: SUNRISE Alliance.

Participation of IPVC in the Erasmus+ International Credit Mobility Program, collaborating with the following institutions: Agricultural University of Tirana (Albania)
University of Kragujevac, Faculty of Education in Jagodina (Serbia), UBT Pristina (Kosovo) and University of Tuzla, University of Mostar, and University of Sarajevo (Bosnia and Herzegovina).

8.5. Resultados das atividades de investigação e desenvolvimento e/ou de formação avançada e desenvolvimento profissional de alto nível

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

Unidade de investigação	Classificação (FCT)	IES	Tipos de Unidade de Investigação	N.º de docentes do ciclo de estudos integrados
Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação (CIICESI)	Bom	Instituto Politécnico do Porto (IPP)		1
Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação (CIICESI)	Bom	Instituto Politécnico do Porto (IPP)	Institucional	1
Centro de Investigação ALGORITMI (ALGORITMI)	Muito Bom	Universidade do Minho (UM)		1
Instituto de Telecomunicações (IT)	Muito Bom	Instituto de Telecomunicações (IT)		1
Instituto de Telecomunicações (IT)	Muito Bom	Instituto de Telecomunicações (IT)	Outro	1
Unidade de Investigação em Microssistemas Eletromecânicos (CMEMS-UMinho)	Excelente	Universidade do Minho (UM)		1

8.5.2. Lista dos principais projetos e/ou parcerias nacionais e internacionais em que se integram as atividades científicas, tecnológicas, culturais e artísticas desenvolvidas na área do ciclo de estudos incluindo, quando aplicável, indicação dos principais projetos financiados e do volume de financiamento envolvido. (PT).

O Ciclo de Estudos (CE) está associado ao centro de investigação ADiT-Lab - Applied -Digital Transformation Laboratory no ambito do qual são realizados diversos projetos de Investigação e Desenvolvimento, bem como prestação de serviços à comunidade. Além da relação com o centro de investigação sediado no IPVC, os docentes do CE estão envolvidos noutros projetos de investigação na qual a área da Cibersegurança desempenha um papel relevante.
De entre esses projetos destacam-se:

1-Projetos com bolsas de I&D, envolvendo alunos do CE:
-Be@t-Medida 1: Investigação & desenvolvimento de mecanismo para assegurar a qualidade dos dados submetidos a plataforma de rastreabilidade e Medida 2: Investigação & desenvolvimento de jogo didático sobre sustentabilidade ambiental e engagement do consumidor na economia circular do setor têxtil e do Vestuário-IPVC Budget: 308 723,29 €

2-Projetos I&D, envolvendo docentes do CE:
- COMENERG, 0052_COM ENERG_1_E, Budget: €200,207.53, from 2023-07-01 to 2026-06-30
- PRR TEXP@CT, Budget: €1,489,225.62, from 2022-07-01 to 2025-12-31
- PRR BE@T, 02/C12-i01.01/2022.P1, Budget: €308,723.29, from 2022-05-25 to 2025-12-31
- PAT.TECH, POCI-01-0 246-FEDER-181306-PAT.TECH, Budget: €485,318.00, from 2021-10-01 to 2023-06-30
- PRR - Drivolution, 02/C05-i01.02/2022.PC644913740-00000022, Budget: €1,303,454.57, from 2021-10-01 to 2025-12-31
- TECH, NORTE-01-0145-FEDER-000043, Budget: €1,656,726, from 2020-10 to 2023-09
- STVgoDIGITAL, POCI-01-0247-FEDER-046086, Budget: €5,991,865, from 2020-07 to 2023-06
- Refill H2O IPVC, PROJECT 10_SGS#1, Budget: €175,437, from 2021-01 to 2022-06
- CoViS, POCI-01-02B7-FEDER-070090, Budget: €379,197, from 2020-10 to 2021-12
- RnMonitor, POCI-01-0145-FEDER-023997, Budget: €132,300, from 2017-09 to 2020-01

8.5.2. Lista dos principais projetos e/ou parcerias nacionais e internacionais em que se integram as atividades científicas, tecnológicas, culturais e artísticas desenvolvidas na área do ciclo de estudos incluindo, quando aplicável, indicação dos principais projetos financiados e do volume de financiamento envolvido. (EN)

The Study Cycle (CE) is associated with the research center ADiT-Lab - Applied -Digital Transformation Laboratory, within which several Research and Development projects are carried out, as well as the provision of services to the community. In addition to the relationship with the research center based at IPVC, CE professors are involved in other research projects in which the area of ??Cybersecurity plays a relevant role.

Among these projects, the following stand out:
1-Projects with R&D grants, involving CE students:
-Be@t-Measure 1: Research & development of a mechanism to ensure the quality of data submitted to the traceability platform and Measure 2: Research & development of a didactic game on environmental sustainability and consumer engagement in the circular economy of the textile and clothing sector - ADiT-Lab – Grang - IPVC Budget: 308 723.29 €

2-R&D projects, involving CE teachers:
- COMENERG, 0052_COM ENERG_1_E, Budget: €200,207.53, from 2023-07-01 to 2026-06-30
- PRR TEXP@CT, Budget: €1,489,225.62, from 2022-07-01 to 2025-12-31
- PRR BE@T, 02/C12-i01.01/2022.P1, Budget: €308,723.29, from 2022-05-25 to 2025-12-31
- PAT.TECH, POCI-01-0 246-FEDER-181306-PAT.TECH, Budget: €485,318.00, from 2021-10-01 to 2023-06-30
- PRR - Drivolution, 02/C05-i01.02/2022.PC644913740-00000022, Budget: €1,303,454.57, from 2021-10-01 to 2025-12-31
- TECH, NORTE-01-0145-FEDER-000043, Budget: €1,656,726, from 2020-10 to 2023-09
- STVgoDIGITAL, POCI-01-0247-FEDER-046086, Budget: €5,991,865, from 2020-07 to 2023-06
- Refill H2O IPVC, PROJECT 10_SGS#1, Budget: €175,437, from 2021-01 to 2022-06
- CoViS, POCI-01-02B7-FEDER-070090, Budget: €379,197, from 2020-10 to 2021-12
- RnMonitor, POCI-01-0145-FEDER-023997, Budget: €132,300, from 2017-09 to 2020-01

8.5.4. Atividades de desenvolvimento tecnológico e artístico, prestação de serviços à comunidade e formação avançada na(s) área(s) científica(s) fundamental(ais) do ciclo de estudos, e seu contributo real para o desenvolvimento nacional, regional e local, a cultura científica e a ação cultural, desportiva e artística. (PT)

N/A

N/A

8.6. Relatório de autoavaliação do ciclo de estudo elaborado no âmbito do sistema interno de garantia da qualidade.

RAC - Cibersegurança - 2022-23.pdf | PDF | 74.1 Kb

9. Análise SWOT do ciclo de estudos e proposta de ações de melhoria.

9.1. Análise SWOT global do ciclo de estudos.

9.1.1. Forças. (PT)

- Objetivos adequados à realidade do mercado e necessidades globais;
- Plano curricular orientado para a aplicação prática dos conhecimentos;
- Corpo docente especializado e com experiência diversificada nas áreas/UCs do Mestrado;
- Experiência de lecionação adquirida com os anteriores 5 anos letivos;
- Realização de várias edições de um seminário técnico-científico em Cibersegurança
http://mciber.estg.ipvc.pt/cybersec/21/
http://mciber.estg.ipvc.pt/cybersec/22/
http://mciber.estg.ipvc.pt/cybersec/23/
http://mciber.estg.ipvc.pt/cybersec/24/;
- Reputação bem estabelecida do IPVC, quer a jusante junto de potenciais formandos, quer a montante junto das empresas;
- A capacidade científica instalada do corpo docente, validada pelas publicações na área científica do CE;
- A qualidade e diversidade dos recursos existentes, incluindo instalações, equipamentos e serviços (Biblioteca, Laboratórios de Informática, Serviços de Ação Social);
- Existência de parcerias de colaboração com outras Instituições no âmbito de formações na mesma área (ex. parceria com a Polícia Judiciária, IPP, e outras empresas da área);
- Alinhamento com segundos ciclos similares em universidades reconhecidas na Europa;
- Quadro de docentes único no IPVC, e não por Escola, o que permite uma maior flexibilidade na gestão do pessoal docente;
- Acordos de dupla titulação com universidade Brasileira e Norueguesa;
- IPVC conta com Sistema de Gestão da Qualidade desde março de 2009 e, em 2022, obteve a certificação do novo sistema integrador - Qualidade, Responsabilidade Social e Conciliação;
- Oferta formativa alinhada com as necessidades de empresas locais/regionais e nacionais;
- Existência de uma cultura de avaliação à qualidade de ensino.

9.1.1. Forças. (EN)

- Objectives suited to market reality and global needs;
- Curriculum plan oriented towards the practical application of knowledge;
- Specialized teaching staff with diverse experience in the Master's areas/UCs;
- Teaching experience acquired over the previous 5 academic years;
- Carrying out several editions of technical-scientific seminars on Cyber ??Security
http://mciber.estg.ipvc.pt/cybersec/21/
http://mciber.estg.ipvc.pt/cybersec/22/
http://mciber.estg.ipvc.pt/cybersec/23/
http://mciber.estg.ipvc.pt/cybersec/24/;
- IPVC's well-established reputation, whether downstream with potential trainees or upstream with companies;
- The installed scientific capacity of the teaching staff, validated by publications in the scientific area of ??the CE;
- The quality and diversity of existing resources, including facilities, equipment and services (Library, IT Laboratories, Social Action Services);
- Existence of collaborative partnerships with other Institutions within the scope of training in the same area (e.g. partnership with the Judiciary Police, IPP, and other companies in the area);
- Alignment with similar second cycles at recognized universities in Europe;
- Single teaching staff at IPVC, and not per School, which allows greater flexibility in the management of teaching staff;
- Dual degree agreements with Brazilian and Norwegian universities.
- IPVC has had a Quality Management System since March 2009 and, in 2022, obtained certification of the new integrating system - Quality, Social Responsibility and Conciliation;
- Training offer aligned to the needs of local/regional and national companies;
- Existence of a culture of evaluating teaching quality.

9.1.2. Fraquezas. (PT)

- Poucas empresas especializadas neste domínio na Região (designadamente Consultoras de Segurança Informática);
- Ainda alguma falta de conhecimento do que é a CiberSegurança por parte de muitas das empresas da Região, nomeadamente das Pequenas e Médias Empresas;
- A existência de uma linha de Investigação no IPVC orientada para a área específica da CiberSegurança com a contribuição de vários docentes é relativamente recente;
- Apesar da existência de docentes especialistas, a realidade é que os títulos de especialista que detêm, não são na área de Cibersegurança;
- Lacunas na formação de base dos alunos;
- Dificuldade no acompanhamento continuado do processo de ensino por parte dos alunos.

9.1.2. Fraquezas. (EN)

- Few companies specialized in this field in the Region (notably IT Security Consultants);
- There is still a lack of knowledge of what Cybersecurity is on the part of many companies in the Region, particularly Small and Medium-sized Companies;
- The existence of a line of Research at IPVC focused on the specific area of ??Cybersecurity with the contribution of several professors is relatively recent;
- Despite the existence of specialist teachers, the reality is that the specialist titles they hold are not in the area of ??Cybersecurity;
- Gaps in students' basic training;
- Difficulty in continued monitoring of the teaching process by students.

9.1.3. Oportunidades. (PT)

- Oferta inovadora e diferenciada na área geográfica;
- Conhecimentos adquiridos no ciclo de estudos cada vez mais cruciais num mundo globalizado e da informação;
- Necessidade, na região, de quadros de empresa capazes de inovar e de criar valor pela qualidade e pela diferença;
- Necessidade de requalificação profissional e valorização da aprendizagem ao longo da vida;
- A Cibersegurança está elencada como uma área estratégica nacional, C-Academy - CNCS, CNCS - C-Network e CNCS - Diretiva SRI 2 (NIS 2)
- Proximidade ao mercado espanhol, sem oferta formativa nesta área;
- Reforço de parcerias/colaborações externas, e procura de novos parceiros no desenvolvimento de projetos técnicos e de investigação;
- Estabilização do corpo docente;
- Novas abordagens pedagógicas (modelo de inovação pedagógica do IPVC);
- Políticas (europeias/nacionais) de incentivo à formação ao longo da vida;
- Integração do IPVC na Universidades Europeia SUNRISE;
- A integração bem sucedida de docentes especialistas no CE pode ser extendida a novos docentes especialistas na área da Cibersegurança;
- Parcerias ao nível dos projetos científicos, prestação de serviços e projetos pedagógicos com os parceiros internacionais do CE.

9.1.3. Oportunidades. (EN)

- Innovative and differentiated offer in the geographic area;
- Knowledge acquired in the cycle of studies that are increasingly crucial in a globalized and information world;
- Need, in the region, for company staff capable of innovating and creating value through quality and difference;
- Need for professional requalification and appreciation of lifelong learning;
- Cybersecurity is listed as a national strategic area, C-Academy - CNCS, CNCS - C-Network and CNCS - SRI Directive 2 (NIS 2)
- Proximity to the Spanish market, no training offered in this area;
- Strengthening external partnerships/collaborations, and searching for new partners in the development of technical and research projects;
- Stabilization of the teaching staff;
- New pedagogical approaches (IPVC pedagogical innovation model);
- Policies (European/national) to encourage lifelong training;
- Integration of IPVC into SUNRISE European Universities;
- The successful integration of specialist teachers in the SC can be extended to new specialist teachers in the area of ??Cybersecurity;
- Partnerships in terms of scientific projects, provision of services and pedagogical projects with SC's international partners.

9.1.4. Ameaças. (PT)

- Incertezas nas perspetivas de evolução nas políticas de financiamento do sistema científico e tecnológico nacional;
- Reduzido apoio financeiro para a investigação dos docentes;
- Incumprimento do pagamento de propinas devido a dificuldades económicas dos estudantes.
- Abandono escolar no 2º ano curricular, alguns alunos pretendem apenas aprender os conceitos lecionados no 1º ano curricular, e não estão interessados em desenvolver uma dissertação/projeto/estágio;
- Contexto económico adverso, desfavorável ao crescimento das empresas da região e ao investimento na formação dos seus RH.

9.1.4. Ameaças. (EN)

- Uncertainties in the prospects for evolution in financing policies for the national scientific and technological system;
- Reduced financial support for faculty research;
- Failure to pay monthly fees due to students' economic difficulties.
- Dropping out of school in the 2nd curricular year, some students only intend to learn the concepts taught in the 1st curricular year, and are not interested in developing a dissertation/project/internship.
- Adverse economic context, unfavorable to the growth of companies in the region and investment in training their HR.

9.2. Proposta de ações de melhoria.

9.2.1. Ação de melhoria. (PT)

1- Reforçar a formação de docentes na área de educação digital EaD e metodologias de ensino inovadoras: Intensificar a produção científica na área fundamental do CE.
2- Desenvolver atividades promotoras da aproximação do CE aos stakeholders (jornadas abertas, master classes de empresas, demonstrações, etc.)
3 - Reforçar o acompanhamento dos estudantes do segundo ano, através da realização de um encontro de apresentação e discussão de trabalhos em curso, com a participação dos orientadores.
4 - Expandir parcerias com empresas nacionais e internacionais, especialmente na área de cibersegurança, para fortalecer a componente prática e de investigação.

9.2.1. Ação de melhoria. (EN)

1- Strengthen teacher training in the area of ??distance learning digital education and innovative teaching methodologies: Intensify scientific production in the fundamental area of ??CE.
2- Develop activities that promote bringing the CE closer to stakeholders (open days, company master classes, demonstrations, etc.)
3 - Strengthen the monitoring of second-year students, by holding a meeting to present and discuss work in progress, with the participation of supervisors.
4 - Expand partnerships with national and international companies, especially in the area of ??cybersecurity, to strengthen the practical and research component.

9.2.2. Prioridade (alta, média, baixa) e tempo de implementação da ação. (PT)

1 - Média – 3 anos;
2 - Alta – 1 ano;
3 - Alta – 1 ano.
4 - Média – 3 anos;

9.2.2. Prioridade (alta, média, baixa) e tempo de implementação da ação. (EN)

1 - Average – 3 years;
2 - High – 1 year;
3 - High – 1 year.
4 - Average – 3 years;

9.2.3. Indicador(es) de implementação. (PT)

1- N.º de ações de formação e de docentes que participam
2- N.º de eventos/ações
3- N.º de mestrandos participantes no encontro de apresentação de trabalhos do segundo ano, n.º de abandono.
4 - Nº de novas parcerias formalizadas anualmente e Nº de pojetos de investigação conjuntos desenvolvidos.

9.2.3. Indicador(es) de implementação. (EN)

1- Number of training actions and teachers who participate
2- Number of events/actions
3- Number of master's students participating in the meeting to present second year works, number of dropouts.
4 - Number of new partnerships formalized annually and Number of joint research projects developed.