Ficha de Unidade Curricular – (Versão A3ES 2018-2023)

1. Caracterização da Unidade Curricular.

1.1. Designação da unidade curricular ***(1.000 carateres).***
Tópicos Avançados em Segurança Informática e Redes (TASIR)
Advanced Topics in Computer Security and Networking

1.2. Sigla da área científica em que se insere ***(100 carateres).***
MEIC: IC - Engenharia Informática e de Computadores;

1.3. Duração[1] ***(100 carateres).***
Semestral

1.4. Horas de trabalho[2] ***(100 carateres).***
162 h

1.5. Horas de contacto[3] ***(100 carateres).***
Total: 67,5 h; T: 45 h, TP: 22,5 h

1.6. ECTS ***(100 carateres).***
6 ECTS

1.7. Observações[4] ***(1.000 carateres).***
Unidade curricular optativa

1.7. Remarks ***(1.000 carateres).***
Elective

2. Docente responsável e respetiva carga letiva na Unidade Curricular ***(preencher o nome completo) (1.000 carateres).***
José Manuel de Campos Lages Garcia Simão (7,5)

3. Outros docentes e respetivas cargas letivas na unidade curricular ***(1.000 carateres).***
Luís Carlos Gonçalves (67,5), Vítor Jesus Sousa de Almeida (15)

4. Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes). ***(1.000 carateres).***

Os estudantes ao terminarem com sucesso esta unidade curricular serão capazes de:

1. Compreender a superfície de ataque de infraestruturas e serviços computacionais amplamente disponíveis em clouds públicas e privadas;
2. Compreender as tecnologias baseadas em livros-razão como forma de garantir tolerância e resiliência a intrusões;
3. Compreender as técnicas de engenharia social usadas por atores maliciosos;
4. Saber usar métodos e ferramentas para modelar ameaças de segurança tendo em conta os vetores de ataque e os diferentes atores maliciosos;
5. Saber usar métodos e ferramentas para resposta a incidentes e saber desenhar planos de recuperação;
6. Compreender e utilizar métodos forenses na análise de incidentes.

4. Intended learning outcomes (knowledge, skills and competences to be developed by the students). ***(1.000 characters).***

Students to successfully finish this course you will:

1. Understand the attack surface of computer infrastructure and services widely available in public and private clouds;
2. Understanding ledger-based technologies as a way to ensure tolerance and resilience to intrusions;
3. Understand the social engineering techniques used by malicious actors;
4. Know how to use methods and tools to model security threats taking into account the attack vectors and the different malicious actors;
5. Know how to use methods and tools for responding to incidents and know how to design recovery plans;
6. Understand and use forensic methods in the analysis of incidents.

5. Conteúdos programáticos ***(1.000 carateres).***

1. Segurança na Cloud
   a. Sistemas de cifra homomórfica
   b. Segurança das tecnologias de virtualização (VM e contentores)
   c. Vulnerabilidades em serviços de Cloud e matriz de mitigação de risco
2. Tolerância a intrusões com livros-razão distribuídos
   a. Arquitetura, desenho e protocolo
   b. Protocolos de consenso
   c. Segurança e privacidade
   d. Casos práticos (Blockchain, Smart contracts, Dapps)
3. Engenharia Social
   a. Análise de informação open-source (OSINT)
   b. Consciencialização em segurança: criação de campanhas; princípios de Cialdini
4. Modelação de ameaças
   a. Atores, vetores de ataque e técnicas para análise de risco
   b. Plataformas para análise de risco
5. Resposta a incidentes
   a. Métodos e ferramentas para resposta e gestão de incidentes
   b. Métodos para conter, erradicar e responder a ameaças de cibersegurança
   c. Planos de recuperação de desastres (continuidade de negócio)
6. Cibersegurança forense
   a. Técnicas de ocultação de informação e análise forense
   b. Prova digital: criação, recolha, manutenção e gestão

5. Syllabus ***(1.000 characters).***

1. Security in the Cloud
   a. Homomorphic cipher systems
   b. Security of virtualization technologies (VM and containers)
   c. Vulnerabilities in Cloud Services and risk mitigation matrices
2. Intrusion tolerance with distributed ledgers
   a. Architecture, design and protocol
   b. Consensus protocols
   c. Security and privacy
   d. Practical cases (Blockchain, Smart contracts, Dapps)
3. Social Engineering
   a. Open-source information analysis (OSINT)
   b. Security awareness: creation of campaigns; Cialdini principles
4. Threat modeling
   a. Actors, Attack Vectors and Risks
   b. Techniques for risk analysis
   c. Platforms for risk analysis
5. Incident response
   a. Incident response and management methods and tools
   b. Methods to contain, eradicate and respond to cybersecurity threats
   c. Disaster recovery plans (business continuity)
6. Forensic cybersecurity
   a. Information hiding techniques and forensic analysis
   b. Digital proof: creation, collection, maintenance, and management

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular ***(1.000 carateres).***

A evolução rápida das tecnologias de informação e comunicação (TIC), e a sua ampla dispersão em diferentes áreas das sociedades, representam riscos acrescidos pelo que o investimento em segurança é cada vez mais importante e urgente.

Nesta unidade curricular os estudantes ficam a conhecer os conceitos principais referentes à segurança aplicada a tecnologias em grande expansão como é o caso de *cloud computing* e *blockchain*, ponto 1 e 2 dos conteúdos programáticos, que concretizam os pontos 1 e 2 dos objetivos de aprendizagem. Os conteúdos programáticos incluem também a análise de ferramentas e métodos para modelação de ameaças, resposta a incidentes e planos de recuperação, correspondente aos pontos 3, 4 e 5 dos objetivos de aprendizagem. Com o aumento de ciberataques é importante o conhecimento de técnicas forenses para analisar, preservar e recuperar evidências, cobrindo assim o objetivo de aprendizagem 6.

6. Evidence of the syllabus coherence with the curricular unit's intended learning outcomes ***(1.000 characters).***

The rapid evolution of information and communication technologies (ICT), and their wide dispersion in different areas of society, represent increased risks, making investment in security increasingly important and urgent. In this curricular unit, students get to know the main concepts related to security applied to technologies in great expansion, such as cloud computing and blockchain, points 1 and 2 of the syllabus, which concretize points 1 and 2 of the learning objectives. The syllabus also includes the analysis of tools and methods for threat modeling, incident response and recovery plans, corresponding to points 3, 4 and 5 of the learning objectives. With the increase in cyber-attacks, it is important to know forensic techniques to analyze, preserve and recover evidence, thus covering the learning objective 6.

7. Metodologias de ensino (avaliação incluída) ***(1.000 carateres).***

Ensino teórico-prático, estando previstas 30 aulas a que correspondem 67,5 horas de contacto. O tempo total de trabalho estimado para o estudante é de cerca de 162 horas. As aulas de caracter teórico destinam-se à exposição e discussão dos principais conteúdos programáticos, incentivando a interatividade e colocação de questões. Os tópicos principais são ainda explorados ao longo do semestre através da realização, em grupo, de até 3 séries de exercícios (P). Os resultados de aprendizagem são avaliados individualmente através de exame final (T).

A classificação final é obtida ponderando 50% da classificação da componente teórica (T) e 50% da classificação da componente prática (P). Ambas as componentes são pedagogicamente fundamentais.

7. **Teaching methodologies (including assessment)** ***(1.000 characters).***

Theoretical-practical teaching, with 30 classes planned, corresponding to 67,5 hours of contact. The total estimated working time for the student is about 162 hours. Theoretical classes are designed to expose and discuss the main syllabus, encouraging interactivity during lectures. The main topics are further explored through practical work carried out in groups, in up to 3 series of exercices (P). Learning outcomes are assessed individually through a final exam (T).

The final classification is obtained by weighting 50% of the classification of the theoretical component (T) and 50% of the classification of the practical component (P). Both components are pedagogically fundamental.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular ***(3.000 carateres).***

Os objetivos da unidade curricular são atingidos através de aulas teóricas e respetivos elementos de apoio (*slides*) e bibliografia, da realização de exercícios práticos e de casos de estudo selecionados pelos docentes.
A componente teórica dos resultados de aprendizagem são avaliados através de teste escrito e da análise crítica de artigos selecionados. A componente prática dos resultados de aprendizagem são avaliados através de pequenos trabalhos ou projetos.

Nas aulas são apresentadas as bases teóricas dos conteúdos programáticos, privilegiando-se uma forma de apresentação interativa e enfatizando-se as competências de compreensão. Nestas aulas, são também apresentadas as consequências práticas e as formas de aplicação destes conteúdos. O trabalho fora da aula é guiado pelos problemas e projectos, com o objetivo de consolidar as competências de escolha e utilização dos conteúdos programáticos.

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

(3.000 characters).

The objectives of the curricular unit are achieved through theoretical classes and respective support elements (slides) and bibliography, by carrying out practical exercises and case studies selected by the teachers.
The theoretical component of the learning results is assessed through written test and critical analysis of selected articles. The practical component of learning outcomes is assessed through small assignments or projects.

In class, the theoretical bases of the syllabus are presented, favoring an interactive presentation, and emphasizing comprehension skills. In these classes, the practical consequences and ways of applying these contents are also presented. The work outside the classroom is guided by the problems and projects, with the objective of consolidating the competences of choosing and using the syllabus.

9. Bibliografia de consulta/existência obrigatória *(1.000 carateres).*

- "*Cloud Computing: Theory and Practice"* (2ª edição), Dan Marinescu, Morgan Kaufmann (2017) [Capítulos 10 e 11]
- "*Container Security: Fundamental Technology Concepts that Protect Containerized Applications"* (1ª edição), Liz Rice, O'Reilly Media (2020)
- "*Mastering Blockchain"* (2ª edição), Imran Bashir, Packt Publishing (2018)
- "*Operating Systems Forensics"* (1ª edição), Ric Messier, Syngress (2015)
- "*Effective Cybersecurity : A Guide to Using Best Practices and Standards"* (1ª edição), William Stallings, Addison Wesley (2018)
- Legislação portuguesa, União Europeia e Americana

---

[1] Anual, semestral, trimestral, …

[2] Número total de horas de trabalho.

[3] Discriminadas por tipo de metodologia adotado (T - Ensino teórico; TP - Ensino teórico-prático; PL - Ensino prático e laboratorial; TC - Trabalho de campo; S - Seminário; E - Estágio; OT - Orientação tutorial; O - Outro).

[4] Assinalar sempre que a unidade curricular seja optativa.