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

1. Caracterização da Unidade Curricular.

1.1. Designação da unidade curricular ***(1.000 carateres).***
Segurança Informática / Computer Security

1.2. Sigla da área científica em que se insere ***(100 carateres).***
IC

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 - 55,5 h
PL – 12 h

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

1.7. Observações[4] ***(1.000 carateres).***
Comum com outros cursos.

1.7. Remarks ***(1.000 carateres).***
Common with other courses.

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

3. Outros docentes e respetivas cargas letivas na unidade curricular ***(1.000 carateres).***

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

a. Compreender os principais tipos de ameaças à segurança de sistemas informáticos;
b. Compreender, escolher e utilizar mecanismos e protocolos criptográficos, incluindo aspetos da gestão de chaves;
c. Compreender, escolher e utilizar modelos e mecanismos para autorização e controlo de acesso;
d. Identificar vulnerabilidades existentes em programas e usar técnicas adequadas à sua correção.

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

a. Understand the main threats to the security of computer systems.
b. Understand, choose and use cryptographic mechanisms and protocols, including the key management issues.
c. Understand, choose and use authorization and access control models and mechanisms.
d. Identity vulnerabilities in software systems and use adequate protection measures.

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

a. Esquemas e protocolos criptográficos e métodos de gestão de chaves: esquemas de cifra simétrica e assimétrica, esquemas MAC e de assinatura digital; protocolos de autenticação e estabelecimento de chaves; infraestruturas de chave pública.

b. Autenticação e autorização: Vulnerabilidades e ataques à informação de autenticação (e.g., *passwords*) e

métodos de mitigação. Modelos e mecanismos para controlo de acessos – monitor de referência; matriz de controlo de acessos, listas de controlo de acessos e "*capabilities*"; modelos RBAC ("Role Based Access Control"); Protocolos para gestão de identidade e autorização em aplicações Web;

c. Escrita de código seguro: vulnerabilidades típicas, técnicas de proteção e metodologias de desenho e desenvolvimento.

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

a. Cryptographic schemes and key management schemes: symmetric and asymmetric cipher schemes, MAC schemes and digital signature; authentication and key establishment protocols; public-key infrastructures.

b. Authentication and authorization: Vulnerabilities and attacks on authentication information (e.g., passwords) and mitigation methods. Models and mechanisms for access control - reference monitor; access control matrix, access control lists and capabilities; RBAC (Role Based Access Control) models; Protocols for identity and authorization management in Web applications;

c. Safe code writing: typical vulnerabilities, protection techniques, design and development technologies.

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

As competências para compreender, escolher e utilizar mecanismos criptográficos (objetivo a.) são fornecidas pela primeira parte do conteúdo programático, nomeadamente a apresentação, discussão e utilização de esquemas e protocolos criptográficos.

A capacidade de escolha e utilização de modelos e mecanismos de controlo de acesso está associada ao ponto b. do conteúdo programático, onde são analisadas e usadas técnicas e tecnologias para gestão de identidade e modelos de controlo de acesso, incluindo os modelos baseados em papeis.

A identificação de vulnerabilidades no software e a seleção de técnicas adequadas à sua correção é fornecida no último ponto do programa.

A compreensão dos principais tipos de ameaças à segurança dos sistemas informáticos é exercitada de forma transversal, em todos os pontos do programa.

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

The skills to understand, choose and use cryptographic mechanisms (objective a.) are provided by the first part of the programmatic content, namely the presentation, discussion and use of cryptographic schemes and protocols.

The ability to choose and use access control models and mechanisms is associated with point b. of programmatic content, where identity management techniques and technologies and access control models, including role-based models, are analysed and used.

The identification of vulnerabilities in the software and the selection of suitable techniques for its correction is provided in the last point of the program.

Understanding the main types of threats to the security of computer systems is exercised across the board at all points of the program.

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

Ensino teórico-prático, estando previstas 30 aulas a que correspondem 67,5 horas de contacto (15 aulas de 3 horas e 15 de 1,5 horas). As aulas interativas destinam-se à apresentação dos diferentes conceitos e de exemplos práticos de aplicação (aprendizagem baseada em casos).

Os tópicos principais são ainda explorados através da realização de trabalhos práticos baseados em computador (aprendizagem baseada na resolução de problemas). A realização dos trabalhos é acompanhada pelo docente, em laboratório, para assegurar o correto desenvolvimento dos conhecimentos e das competências dos

estudantes. As soluções apresentas pelos alunos nos exercícios são ainda alvo de discussão oral.

A avaliação global é feita com base numa prova escrita (60%) e discussão oral dos trabalhos realizados ao longo do semestre (40%).

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

Teaching theory and practice, with 30 classes corresponding to 67.5 hours of contact (15 lessons of 3 hours and 15 of 1.5 hours). The interactive classes are designed to present different concepts and practical examples of application (case-based learning).

Key topics are further explored through the execution of computer-based practical work (problem-based learning). The work is carried out by the teacher in the laboratory to ensure the correct development of the students' knowledge and skills. The solutions presented by the students in the exercises are still the subject of oral discussion.

The overall assessment is based on a written exam (60%) and oral discussion of the work carried out during the semester (40%).

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

A componente teórica dos resultados de aprendizagem, “compreender” e “escolher”, são avaliados através de teste escrito e três séries de exercícios. A componente prática dos resultados de aprendizagem, “utilizar”, 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 programáticos. O trabalho extra aula é guiado pelos problemas e Projectos das séries de exercícios, com o objetivo de consolidar as competências de escolha e utilização dos conteúdos programáticos.

As formas de avaliação, maioritariamente teóricas, refletem a ênfase nas competências analíticas fornecidas por esta unidade curricular.

8. Evidence of the teaching methodologies coherence with the curricular unit’s intended learning outcomes ***(3.000 characters).***

The theoretical component of learning outcomes, "understand" and "choose", are evaluated through written test and three sets of exercises. The practical component of learning outcomes, "to use", are evaluated through small work or projects.

Lectures present the theoretical bases of the programmatic contents, privileging a form of interactive presentation and emphasizing the skills of understanding. In these classes, the practical consequences and the forms of application of these programmatic contents are also presented. The extra class work is guided by the problems and projects of the series of exercises, with the purpose of consolidating the competences of choice and use of the programmatic contents.

The forms of evaluation, mostly theoretical, reflect the emphasis on the analytical skills provided by this curricular unit.

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

D. Gollmann, *Computer Security*, 3rd Edition, Willey, 2011. ISBN 9780470741153
W. Du, *Computer Security: A Hands-on Approach*, CreateSpace Independent Publishing Platform, 2017. ISBN 9781548367947

---

[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.