Ficha de Unidade Curricular A3ES
Segurança Informática
Licenciatura em Engenharia Informática e de Computadores
2024-25

1. Caracterização da Unidade Curricular

1.1 Designação
[3094] Segurança Informática / Computer Security

1.2 Sigla da área científica em que se insere
IC

1.3 Duração
Unidade Curricular Semestral

1.4 Horas de trabalho
162h 00m

1.5 Horas de contacto
Total: 67h 30m das quais TP: 67h 30m

1.6 ECTS
6

1.7 Observações
Unidade Curricular Obrigatória
Unidade Curricular comum ao(s) curso(s) de LEIRT

2. Docente responsável	[1551] José Manuel de Campos Lages Garcia Simão

3. Docentes e respetivas cargas letivas na unidade curricular	[1551] José Manuel de Campos Lages Garcia Simão | Horas Previstas: 67.5 horas [2086] Diego Gimenez Passos | Horas Previstas: 67.5 horas [2108] Fernanda Gonçalves de Oliveira Passos | Horas Previstas: 67.5 horas [2136] João Pedro Borges Pereira Faria Vitorino | Horas Previstas: 67.5 horas

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

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

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.

5. Conteúdos programáticos

a. Introdução à criptografia e aos protocolos criptográficos

1. Esquemas simétricos e assimétricos. Esquemas criptográficos para garantir confidencialidade e autenticidade.
2. Infraestruturas de chave pública.
3. Protocolos criptográficos e métodos de gestão de chaves.
4. Utilização de biblioteca criptográfica.

b. Autenticação e autorização

1. Vulnerabilidades e ataques à informação de autenticação (e.g., passwords) e métodos de mitigação.
2. Protocolos para gestão de identidade e autorização em aplicações Web (OpenID Connect e OAuth2).
3. 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").

5. Syllabus

a. Introduction to Cryptography and Cryptographic Protocols

1. Symmetrical and asymmetrical schemes. Cryptographic schemes to ensure confidentiality and authenticity.
2. Public key infrastructures.
3. Cryptographic protocols and key management methods.
4. Use of cryptographic library.

b. Authentication and authorization

1. Vulnerabilities and attacks on authentication information (e.g., passwords) and mitigation methods.
2. Protocols for identity management and authorization in Web applications (OpenID Connect and OAuth2).
3. Models and mechanisms for access control ? reference monitor; access control matrix, access control lists and capabilities; RBAC ("Role Based Access Control") models.

6. Demonstração da coerência dos conteúdos programáticos com os objetivos de aprendizagem da unidade curricular

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 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

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.
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)

Ensino teórico-prático e avaliação distribuída com exame final. As aulas interativas destinam-se à apresentação dos diferentes conceitos e de exemplos práticos de aplicação.

Os tópicos principais são explorados através de dois trabalhos práticos onde os alunos realizam experiências para consolidação dos conceitos apresentados em aula teórica, usando horas de trabalho autónomo e horas de contacto com o docente. As aulas práticas servem para acompanhar a realização dos trabalhos assegurando o correto desenvolvimento das competências dos estudantes.

A avaliação global é feita com base em: prova global escrita em época de exames para validar a componente teórica dos objetivos de aprendizagem (60%), primeiro trabalho (20%) e segundo trabalho (20%). Todas as componentes são pedagogicamente fundamentais.

7. Teaching methodologies (including assessment)

Theoretical-practical teaching and distributed assessment with final exam. The interactive classes are intended to present different concepts and practical examples of application.

The main topics are explored through two practical assignments where students carry out experiments to consolidate the concepts presented in theoretical class, using hours of independent work and hours of contact with the teacher. Practical classes serve to monitor the completion of work, ensuring the correct development of students' skills.

The overall assessment is based on: written global test during exam time to validate the theoretical component of the learning objectives (60%), first assignment (20%) and second assignment (20%). All components are pedagogically fundamental.

8. Demonstração da coerência das metodologias de ensino com os objetivos de aprendizagem da unidade curricular

A componente teórica dos resultados de aprendizagem, ?compreender? e ?escolher?, são avaliados através de teste escrito e dois trabalhos práticos. 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 dos dois trabalhos, 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

The theoretical component of the learning outcomes, ?understand? and ?choose?, are assessed through a written test and two practical assignments. The practical component of the learning outcomes, ?use?, are assessed through small assignments or projects.

In classes, the theoretical bases of the syllabus are presented, favoring an interactive form of presentation and emphasizing comprehension skills. In these classes, the practical consequences and ways of applying these syllabuses are also presented.

Extra-class work is guided by the problems and projects of the two works, with the aim of consolidating skills in choosing and using syllabus content.

9. Bibliografia de consulta/existência obrigatória

- 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

10. Data de aprovação em CTC 2024-07-17 2024-07-17

11. Data de aprovação em CP 2024-06-26 2024-06-26