
Ano Letivo 2022-23

Unidade Curricular SEGURANÇA INFORMÁTICA

Cursos ENGENHARIA INFORMÁTICA (2.º ciclo) (*)

(*) Curso onde a unidade curricular é opcional

Unidade Orgânica Faculdade de Ciências e Tecnologia

Código da Unidade Curricular 14741070

Área Científica CIÊNCIA DE COMPUTADORES

Sigla

Código CNAEF (3 dígitos) 481

**Contributo para os Objetivos de
Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)** 4,9,11

Línguas de Aprendizagem Inglês ou Português

Modalidade de ensino

Presencial e/ou remoto

Docente Responsável

Joel David Valente Guerreiro

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Joel David Valente Guerreiro	PL; T	T1; PL1	28T; 28PL

* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

ANO	PERÍODO DE FUNCIONAMENTO*	HORAS DE CONTACTO	HORAS TOTAIS DE TRABALHO	ECTS
1º	S2	28T; 28PL	156	6

* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Nada a assinalar.

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A unidade curricular Segurança Informática pretende contribuir para compreensão da relevância da segurança informática nas áreas da segurança de redes e sistemas, de software, de hardware e segurança física, Ciber-Segurança, criptografia e protocolos de segurança. Pretende-se também que os alunos desenvolvam competências teóricas e práticas de implementação de uma segurança informática ativa nas diferentes áreas, encontrando soluções técnicas, eliminando vulnerabilidades e assegurando a segurança física, da informação e dos sistemas. Pretende-se ainda, com a componente prática, a aquisição de conhecimentos de implementação de medidas ao nível da segurança de redes e sistemas e a aprendizagem de como efetuar uma análise forense dos sistemas informáticos após ocorrência de um ciber-ataque.

Conteúdos programáticos

1. Conceitos de Segurança Informática
 - Conceito de vulnerabilidade e segurança ativa
 - Avaliação e gestão de risco
 - Políticas e mecanismos de segurança
 - Níveis e domínios de Segurança
 - Ataques e mecanismos de defesa
 - Lei da Segurança Informática
2. Detecção e exploração de vulnerabilidades
 - Caracterização de vulnerabilidades e técnicas de exploração
 - Vulnerabilidades físicas, software, desenvolvimento e Serviços
3. Segurança de Redes e Sistemas
 - Introdução
 - Arquitetura de uma Firewall (estrutura básica, DMZ, serviços públicos, NAT e PAT, etc.)
 - Autenticação e mecanismos de autenticação
 - VPN's
 - Protocolos seguros de comunicação
 - Segurança de redes s/ fios
 - Segurança Sistemas Operativos
4. Segurança física e de Hardware
5. Ciber-Segurança
 - Introdução à Ciber-Segurança
 - Base motivacional para ciber-acidentes
 - Evolução, virtudes e perigos do ciberespaço
 - Regras essenciais Cibersegurança
 - Ataques, mecanismos e serviços de ciberespaço
6. Criptografia
7. Protocolos de Segurança

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através das aulas teóricas
- Leitura, análise e implementação de mecanismos de defesa ativa e estudos de caso (práticas laboratoriais e trabalho autónomo);
- Apresentações orais dos trabalhos de grupo
- Atendimento individual ou em grupo para esclarecimento de dúvidas
- Apoio às atividades e esclarecimento sobre funcionamento da unidade curricular.

A avaliação é contínua, com exame final e inclui:

- Teste individual para a avaliação de conhecimentos (50%)
- Trabalho de grupo com apresentação oral/discussão (50%)

Os estudantes que obtiverem uma classificação final igual ou superior a 9,5 valores em cada elemento de avaliação estão dispensados do exame final.

Bibliografia principal

- Gordon L. & Loeb M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill.
- Pfeegeer C., Pfeegeer S., Margulies J. (2015), Security in Computing. Prentice-Hall. Zúquete A. (2018). Segurança em redes informáticas (5ª Edição Atualizada). FCA Editora de Informática, Lda.
- Antunes M. & Rodrigues B. (2018). Introdução à Cibersegurança. FCA Editora de Informática.
- Herzog P. et al (2017). Security analysis essentials. ISECOM
- Stalling, W. (2006). Cryptography and Network Security: Principles and Practice. Prentice-Hall.
- Stuttard D. & Pinto M. (2011). The web application Hacker's handbook: Finding and exploring security flaws 2 Edition. John Wiley nd & Sons

Academic Year 2022-23

Course unit

Courses INFORMATICS ENGINEERING (*)
Common Branch

(*) Optional course unit for this course

Faculty / School FACULTY OF SCIENCES AND TECHNOLOGY

Main Scientific Area CIÊNCIA DE COMPUTADORES

Acronym

CNAEF code (3 digits) 481

**Contribution to Sustainable
Development Goals - SGD
(Designate up to 3 objectives)** 4,9,11

Language of instruction English or Portuguese

Teaching/Learning modality Presential and/or remote

Coordinating teacher Joel David Valente Guerreiro

Teaching staff	Type	Classes	Hours (*)
Joel David Valente Guerreiro	PL; T	T1; PL1	28T; 28PL

* For classes taught jointly, it is only accounted the workload of one.

Contact hours	T	TP	PL	TC	S	E	OT	O	Total
	28	0	28	0	0	0	0	0	156

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

Pre-requisites

no pre-requisites

Prior knowledge and skills

NA

The students intended learning outcomes (knowledge, skills and competences)

The curricular unit of Computer Security aims to contribute to better understand Computer Security's relevance in network and systems, software and hardware securities as well as cybersecurity, cryptography and security protocols. Students are expected to develop theoretical and practical competencies by implementing an active computer security in the previously mentioned areas, discovering technical solutions, eliminating vulnerabilities and assuring a physical, logical and systems security. It is also intended, with the practical component of this curricular unit, that students acquire know-how in implementing systems and network security procedures and also by a System forensic analysis after a cyber-attack.

Syllabus

1. Computer Security concepts
 - Concept of vulnerability and active security
 - Evaluation and risk assessment
 - Security policies and Mechanisms
 - Security levels and domains
 - Cyber Attacks and Defense mechanisms Computer Security legislation
2. Vulnerability detection and exploration
 - Vulnerability characterization and exploration techniques
 - Physical, software, development and services vulnerabilities
3. Network and Systems Security
 - Introduction
 - Firewall architecture (basic structure, DMZ, public services, NAT, PAT, etc.)
 - Authentication and authentication mechanisms
 - VPN's
 - Secure Communication Protocols
 - Wireless networks security
 - Operational Systems Security
4. Physical and Hardware Security
5. Cyber-security
 - Cybersecurity introduction
 - Cyberattacks motivation
 - Cyberspace evolution, virtues and dangers
 - Cybersecurity essential rules
 - Cyberspace mechanisms and service attacks
6. Cryptography
7. Security Protocols

Teaching methodologies (including evaluation)

The curricular unit combines several teaching methods:

- Exposition of the syllabus themes with theoretical classes
- Reading, analysis, and implementation of a active defence mechanisms and case studies (laboratory practice classes and autonomous work)
- Oral presentations of the group work
- Individual or group assistance to clarify doubts
- Support activities, and clarify the curricular unit functioning.

The evaluation is continuous, with a final exam, and includes:

- Individual Test for knowledge evaluation (50%)
- Group Work with Oral presentation/discussion (50%).

Students who obtain a result of 9.5 or higher grade in each element will be exempt from the final exam.

Main Bibliography

- Gordon L. & Loeb M. (2005). Managing Cybersecurity Resources: A Cost-Benefit Analysis. McGraw-Hill.
- Pfeeger C., Pfeeger S., Margulies J. (2015), Security in Computing. Prentice-Hall. Zúquete A. (2018). Segurança em redes informáticas (5ª Edição Atualizada). FCA Editora de Informática, Lda.
- Antunes M. & Rodrigues B. (2018). Introdução à Cibersegurança. FCA Editora de Informática.
- Herzog P. et al (2017). Security analysis essentials. ISECOM
- Stalling, W. (2006). Cryptography and Network Security: Principles and Practice. Prentice-Hall.
- Stuttard D. & Pinto M. (2011). The web application Hacker's handbook: Finding and exploring security flaws 2 Edition. John Wiley and Sons