English version at the end of this document

Ano Letivo	2023-24
Unidade Curricular	SEGURANÇA EM REDES INFORMÁTICAS, SEM FIOS E MÓVEIS
Cursos	CIBERSEGURANÇA
Unidade Orgânica	Faculdade de Ciências e Tecnologia
Código da Unidade Curricular	19381003
Área Científica	
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

Modalidade de ensino

B-Learning

Docente Responsável Luís Manuel Pisco Rodrigues

DOCENTE	TIPO DE AULA	TURMAS	TOTAL HORAS DE CONTACTO (*)
Luís Manuel Pisco Rodrigues	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	S1	28T; 28PL	156	6

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

Precedências

Sem precedências

Conhecimentos Prévios recomendados

Não aplicável

Objetivos de aprendizagem (conhecimentos, aptidões e competências)

A Segurança em Redes Informáticas, sem fios e Móveis pretende dotar o estudante com conhecimentos que lhe permita conceptualizar, desenhar e implementar redes informáticas seguras. É ainda objetivo desenvolver a capacidade do estudante para conhecer os ataques a redes informáticas mais vulgares e preveni-los, implementar mecanismos de autenticação, autorização, registo (AAA) e controlo de acesso. Pretende ainda dotar o estudante de conhecimento das ferramentas e técnicas de isolamento com routers e firewalls e configurar redes sem fios com recurso a encriptação assim como a configuração segura de equipamentos móveis.

Conteúdos programáticos

- Conceção, desenho e implementação de redes informáticas seguras;
- Implementação de segurança ativa em redes informáticas;
- Implementar mecanismos de AAA com recurso a serviços de Radius, Tacacs e 802.1X;
- Aplicar técnicas de isolamento de redes informáticas;
- Virtual Private Networks (VPN);
- Configurar redes sem fios seguras com recursos a protocolos de encriptação na comunicação;
- Segurança em equipamentos móveis.

Metodologias de ensino (avaliação incluída)

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através da componente teórica
- Prática laboratorial de redes informáticas com simuladores e equipamentos de redes;
- 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

. Michael Stewart and Denise Kinsey (2020), Network Security, Firewalls, and VPN?s, Jones & Bartlett Learning 3rd edition.

Ross Anderson (2020), Security Engineering: A Guide to building Dependable Distributed Systems, Wiley, 3rd Edition, ISBN-10: 1119642787

Richard Bejtlich (2013), The Practice of Network Monitoring: Understanding Incident Detection and Response, No Starch Press, ISBN-10: 1593275099

William Stallings (2016), Network Security Essentials: Applications and Standards, Pearson, ISBN-10: 9780134527338

Evan Gilman and Doug Barth (2017), Zero Trust Networks: Building Secure Systems in Untrusted Networks, O?Reilly, ISBN-10: 9781491962190

Aditya Mukherjee (2020), Network Security Strategies: Protect your Network and Enterprise against advanced Cibersecurity Attacks and Threats, Packt Publishing.

Academic Year	2023-24
Course unit	COMPUTER NETWORKS, WIRELESS AND MOBILE SECURITY
Courses	CIBERSECURITY
Faculty / School	FACULTY OF SCIENCES AND TECHNOLOGY
Main Scientific Area	
Acronym	
CNAEF code (3 digits)	481
Contribution to Sustainable Development Goals - SGD (Designate up to 3 objectives)	4,9,11
Language of instruction	English
Teaching/Learning modality	B-Learning

Coordinating teacher Luís Manuel Pisco Rodrigues

Teaching staff	Type	Classes	Hours (*)
Luís Manuel Pisco Rodrigues	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

Not applicable

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

The Informatic network Security, wireless and mobile aims to provide students with knowledge that allows them to conceptualize, design and implement secure computer networks. It also aims to develop the student's ability to know the most common attacks on the computer networks and prevent them, implement authentication, authorization, accounting (AAA) and access control mechanisms. It also intends to provide the student with knowledge of isolation tools and techniques with routers and firewalls and configure wireless networks using encryption as well as the secure configuration of mobile equipment.

Syllabus

- Conception, design and implementation of secure computer networks;
- Implementation of active security in computer networks;
- Implement AAA mechanisms using Radius, Tacacs and 802.1X services;
- Apply computer network isolation techniques;
- Virtual Private Networks (VPN);
- Configure secure wireless networks using communication encryption protocols;
- Security in mobile equipment.

Teaching methodologies (including evaluation)

This course unit combines several teaching methods:

- Exposition of the syllabus, through the theoretical component
- Laboratory practice of computer networks with simulators and network equipment.
- Oral presentations of group work.
- Individual or group service to clarify doubts.
- Support for activities and clarification on the functioning of the curricular unit

Evaluation is continuous, with a final exam and includes:

- Individual test to assess knowledge (50%).
- Group work with oral presentation/discussion (50%).

Students who obtain a final grade equal to or greater than 9.5 in each evaluation element are exempt from the final exam.

Main Bibliography

J. Michael Stewart and Denise Kinsey (2020), Network Security, Firewalls, and VPN?s, Jones & Bartlett Learning 3rd edition.

Ross Anderson (2020), Security Engineering: A Guide to building Dependable Distributed Systems, Wiley, 3rd Edition, ISBN-10: 1119642787

Richard Bejtlich (2013), The Practice of Network Monitoring: Understanding Incident Detection and Response, No Starch Press, ISBN-10: 1593275099

William Stallings (2016), Network Security Essentials: Applications and Standards, Pearson, ISBN-10: 9780134527338

Evan Gilman and Doug Barth (2017), Zero Trust Networks: Building Secure Systems in Untrusted Networks, O?Reilly, ISBN-10: 9781491962190

Aditya Mukherjee (2020), Network Security Strategies: Protect your Network and Enterprise against advanced Cibersecurity Attacks and Threats, Packt Publishing.