Fundamentos de Segurança Informática

LEI

2025/2026

Apresentação

Jorge Granjal
University of Coimbra

Sumário

Organização

Aulas T e PL

Jorge Granjal

Gab D3.22

jgranjal@dei.uc.pt

Aulas PL

Rogério Costa

Gab D3.5

rogcosta@dei.uc.pt

Conteúdos programáticos

- Conceitos fundamentais de segurança (confidencialidade, privacidade, ..)
- Algoritmos de encriptação simétrica e assimétrica (3DES, AES, RSA)
- Mecanismos de integridade de dados
- Autoridades de certificação digital e PKI
- Mecanismos de autenticação e gestão de chaves (KDM, Kerberos, DH)
- Ataques e estratégias de defesa em aplicações web (SQLi, XSS, etc.)
- Segurança na camada de transporte e de rede (SSL/TLS, IPSec)
- Firewalls de rede (filtros de pacotes, proxies de aplicação) e sistemas de deteção/prevenção de intrusões
- Segurança em redes sem fios (WPA, IEEE 802.11i)
- Segurança em ambientes de cloud
- Arquitetura e Design de Software Seguro
- Computação Multipartidária Segura e Privacidade de Dados

Planeamento

Semana	Teórica (3a)	PL (Materials)		
		2a	3a	5a
		PL5; PL6	PL2;PL3;PL4	PL1
9 Fev 2026	Fundamental security concepts	Ficha 00 - Setup VMs	Ficha 00 - Setup VMs + Ficha 01 - Email security using PGP	Ficha 00 - Setup VMs
16 Fev 2026	Carnaval	Ficha 01 - Email security using PGP	Carnaval	Ficha 01 - Email security using PGP
23 Fev 2026	Firewalls and intrusion detection	Ficha 02 - Firewalls with IPTables (system)	Ficha 02 - Firewalls with IPTables (system)	Ficha 02 - Firewalls with IPTables (system)
2 Março 2026	Data integrity mechanisms	Ficha 03 - Firewalls with IPTables (network)	Ficha 03 - Firewalls with IPTables (network)	Ficha 03 - Firewalls with IPTables (network)
9 Março 2026	Symmetric Encryption (1)	Ficha 04 - Intrusion detection with suricata	Ficha 04 - Intrusion detection with suricata	Ficha 04 - Intrusion detection with suricata
16 Março 2026	Symmetric Encryption (2)	Practical Assignment 1 (support)	Practical Assignment 1 (support)	Practical Assignment 1 (support)
23 Março 2026	Asymmetric Encryption	Practical Assignment 1 (defenses)	Practical Assignment 1 (defenses)	Practical Assignment 1 (defenses)
30 Março 2026	Páscoa	Páscoa	Páscoa	Páscoa
6 Abril 2026	Digital Certification Authorities and PKI	Páscoa	Ficha 05 - Certification authorities using OpenSSL	Ficha 05 - Certification authorities using OpenSSL
13 Abril 2026	Web and Transport Layer Security	Ficha 05 - Certification authorities using OpenSSL	Ficha 06 - OpenVPN	Ficha 06 - OpenVPN
20 Abril 2026	Network layer security using IPSec	Ficha 06 - OpenVPN	Practical Assignment 2 (support)	Practical Assignment 2 (support)
27 Abril 2026	Authentication and key management	Practical Assignment 2 (support)	Practical Assignment 2 (support)	Practical Assignment 2 (support)
4 Maio 2026	Web application security (attacks)	Ficha 07 - Web application attacks	Ficha 07 - Web application attacks	Ficha 07 - Web application attacks
11 Maio 2026	Web application security (application firewalls)	Ficha 08 - Web application Firewalls	Ficha 08 - Web application Firewalls	Ficha 08 - Web application Firewalls
18 Maio 2026	Wireless security	Practical Assignment 3 (support)	Practical Assignment 3 (support)	Practical Assignment 3 (support)
25 Maio 2026	*Queima das Fitas*	*Queima das Fitas*	*Queima das Fitas*	*Queima das Fitas*
2-Jun-2026		Practical Assignment 3 (defenses)	Practical Assignment 3 (defenses)	Practical Assignment 3 (defenses)

Avaliação

Exame: 11 valores

Trabalhos Práticos: 9 valores

- Três (3) projetos a realizar individualmente ou em grupos de 2 estudantes
- Apresentados e defendidos nas aulas práticas
- O plágio implica a exclusão da unidade curricular (“Não Admitido”)
- Mínimo de 40% em cada componente (total dos 3 trabalhos, exame)

Bibliografia

William Stallings, Cryptography and Network Security: Principles and Practice (7th edition), Prentice Hall, 2017

Jorge Granjal, Segurança Prática em Sistemas e Redes (com Linux), FCA Editora 2017

Segurança em Redes Informáticas, André Zúquete, FCA, 2006

Security in Computing. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J.. , Prentice Hall.

J. Viega and G. McGraw, Building secure software: how to avoid security problems the right way. Addison-Wesley, 2001.

M. Howard and S. Lipner, The security development lifecycle. O'Reilly Media, Incorporated, 2009