



**Ciências  
ULisboa**

## Segurança e Confiabilidade

Código: 26749

ECTS: 6

Ano Letivo: 2015/16

Carga horária: T: 2:00 h; TP: 1:30 h; OT: 2:00 h;

Departamento: Informática

Área Científica: Informática;

### Objetivos da Unidade Curricular

A cadeira de Segurança pretende abordar a problemática da segurança e confiabilidade nos sistemas computacionais abertos, incluindo computadores e redes de comunicação, isto é, numa óptica de sistemas distribuídos. Como bases, espera-se que os alunos possuam já noções introdutórias sobre: sistemas computacionais e redes de computadores; sistemas operativos e sistemas distribuídos; sistemas de informação e transaccionais.

### Pré-requisitos

- Redes de Computadores (26704)
- Sistemas Distribuídos (26730)

### Conteúdos

O Problema da (In)Segurança Informática Hoje em Dia

Conceitos Fundamentais de Segurança

Conceitos Fundamentais de Confiabilidade

Paradigmas da Segurança e Confiabilidade

Modelos de Computação Segura Distribuída

Modelos de Computação Tolerante a Falhas

Sistemas e Plataformas Seguras e Confiáveis

### Descrição detalhada dos conteúdos programáticos

#### Componente Teórica

Conceitos e propriedades da segurança; elementos de criptografia, incluindo cifra, síntese, síntese autenticada (MAC) e assinaturas digitais; gestão de chaves simétricas e públicas; infraestrutura de chave pública; autenticação local e distribuída; princípios para a comunicação segura; anteparas de segurança e sistemas de deteção de intrusões; conceitos ligados à confiabilidade; deteção e tolerância a falhas através de redundância de dados (e.g., códigos de Hamming; RAID); checkpointing; replicação por primário-secundários e replicação ativa.

## Componente Teórica-Prática

Máquina virtual do Java e mecanismos para assegurar a segurança; API do Java para segurança (incluindo, cifra, sínteses, MACs, assinaturas, certificados, e TLS)

## Componente Prática

-

## Bibliografia

### Recomendada

- William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, Pearson, 2014
- Scott Oaks, Java Security, 2nd edition, O'Reilly 2001

### Outros elementos de estudo

- @DI-FCUL, Guião de Segurança Informática – Acetatos das Aulas Teóricas, FCUL 2015.
- @DI-FCUL, Guião de Segurança Informática – Acetatos das Aulas Teórico-Práticas, FCUL 2015.

## Métodos de Avaliação

Regras de classificação:

40% Projecto, incluindo impressões da participação nas aulas

60% Exame final

- Eliminatório: Exame, Projecto

\* Projecto:

- Projecto em várias fases, distribuídas pelo semestre

- Participação activa e a contribuição para os debates estão previstos e serão consideradas

\* Exame Final: exame de 2 horas e abrangente

## Língua de ensino

Português