



UNIVERSIDADE LUSÍADA DE LISBOA

## Programa de Unidade Curricular

- Ano Lectivo 2007/2008 -

### **Faculdade**

Ciências da Economia e da Empresa

### **Licenciatura**

Informática

### **Unidade Curricular**

Instalação, Administração e Segurança de Redes

**Ano:** 3º

**Tipo:** 2º Semestre

**Nº ECTS:** 6

### **Regente**

Mestre Eng. Joaquim Mesquita da Cunha Viana

### **Assistente**

-

### **Carga Horária Lectiva Semanal**

Aulas Teóricas: -

Aulas Teórico-práticas: 2

Orientação Tutorial: 1

### **Língua de Ensino**

Português

### **Objectivos Gerais**

Introdução ao conceito de Segurança na Comunicação de Dados entre computadores inseridos numa rede. Análise das principais vulnerabilidades, ameaças e acções susceptíveis de as minimizar

### **Objectivos Específicos**

Esta disciplina fornece uma introdução à segurança no contexto das redes de computadores. Os objectivos do curso consistem na transmissão das bases que permitam aos estudantes identificar, analisar, e eventualmente resolver problemas relacionados com redes de computadores. Cobre os conceitos fundamentais de teoria dos números, autenticação e tecnologias de encriptação, bem como os problemas práticos que precisam ser resolvidos num ambiente de Internet.



UNIVERSIDADE LUSÍADA DE LISBOA

### Competências a adquirir

- Qual a importância das políticas de segurança;
- Ameaças à segurança dos ambientes de rede e contramedidas;
- Bases da encriptação por chave privada e pública, incluindo os fundamentos de teoria dos números;
- Princípios de autenticação;
- Análise das vulnerabilidades dos protocolos de segurança.

### Metodologia de Ensino (até 250 caracteres)

O ensino basear-se-á na transmissão oral de informação relacionada com os temas em estudo, seguida da resolução de exercícios adequados aos problemas em estudo e de práticas laboratoriais sobre o equipamento Omniswitch da Alcatel.

### Programa da Unidade Curricular / Conteúdo programático

1. INTRODUÇÃO
  - a) Vulnerabilidades
  - b) Ameaças
  - c) Medidas de protecção
2. CRIPTOGRAFIA
  - a) Introdução
  - b) Algoritmos de chave secreta
  - c) Modos de operação
  - d) Hashes e Message Digests
  - e) Algoritmos de chave pública
3. AUTENTICAÇÃO
  - a) Generalidades
  - b) Autenticação de pessoas
  - c) Vulnerabilidades na autenticação
4. STANDARDS
  - a) Kerberos
  - b) PKI (Public Key Infrastructure)
  - c) IPsec
  - d) SSL/TLS
5. CORREIO ELECTRÓNICO
  - a) PEM & S/MIME
  - b) PGP (Pretty Good Privacy)
6. TIPOS DE INTRUSÕES
7. DETECÇÃO DE INTRUSÕES
  - a) Firewalls
  - b) Sistemas de detecção de intrusões (IDS's)



UNIVERSIDADE LUSÍADA DE LISBOA

### **Bibliografia Principal**

#### **Autor(es)**

Kaufman, Perlman, Speciner

#### **Título**

Network Security: Private Communication in a Public World

#### **Edição**

2ª

#### **Local**

#### **Editora**

Prentice Hall

#### **Ano**

2002

#### **Autor(es)**

William Stallings

#### **Título**

Network Security Essentials: Applications and Standards

#### **Edição**

2ª

#### **Local**

#### **Editora**

Prentice Hall

#### **Ano**

2003

### **Bibliografia Complementar**

#### **Autor(es)**

Bruce Schneier



UNIVERSIDADE LUSÍADA DE LISBOA

**Título**

Applied Cryptography

**Edição**

1ª

**Local**

**Editora**

Wiley

**Ano**

1996

**Autor(es)**

Chuck Easttom

**Título**

Computer Security Fundamentals

**Edição**

1ª

**Local**

**Editora**

Prentice Hall

**Ano**

**Metodologia de Avaliação Contínua / Elementos relevantes**

De acordo com os regulamentos internos da escola, a avaliação terá uma componente contínua e uma frequência. A componente contínua será composta pelas seguintes parcelas,

Assiduidade, Participação e Trabalhos práticos

com os pesos estipulados pelo Regulamento de Avaliações.

A nota final será apenas a nota da frequência, caso o aluno seja por isso beneficiado, ou, em caso contrário, a média das notas da frequência e da nota de avaliação contínua.



UNIVERSIDADE LUSÍADA DE LISBOA

### Recursos Didáticos

### Palavras-chave

Comunicações, Redes, Internet, Protocolos

*João R. A. Lima*