

**Unidade Curricular: Gestão e Segurança de Redes Informáticas**

**Curso:** Engenharia Informática

**Ano:** 3º ano

**Regime:** Semestral ( 5º)

**Ano Lectivo:** 2011/2012

**Carga Horária Total:**

**Horas de Contacto:** (TP: 28; PL: 42; OT: 5; O:5)

**Créditos:** 6 ECTS

**Docentes:** Luís Miguel Lopes de Oliveira (Assistente do 2º Triénio); Renato Eduardo Silva Panda (Assistente convidado)

**Objectivos:**

Aprendizagem de conceitos fundamentais sobre:

- Conhecer e saber aplicar as novas metodologias usadas na gestão e manutenção de redes informáticas.
- Identificar serviços críticos de uma infraestruturas, propondo soluções e estratégias que minimizem a sua inoperacionalidade;
- Usar aplicações de gestão de redes e de sistemas informáticos;
- Usar os protocolos e os mecanismos de segurança na concepção de redes seguras;

**Programa:**

1. Gestão de redes e sistemas informáticos

- Introdução à Gestão Integrada
- Arquitectura dum sistema de gestão
- Evolução da Arquitectura de Gestão Internet
- A Arquitectura de Gestão SNMP
- Evolução da arquitectura de Gestão Internet
- Arquitectura de Gestão OSI
- A Rede de Gestão de Telecomunicações
- Ferramentas de Gestão e Plataformas de Gestão

2. Segurança em redes informáticas:

- Conceitos fundamentais e terminologia.
  - Necessidade de proteger as redes e os sistemas informáticos.
  - Definição de segurança Propriedades e serviços de segurança
  - Estruturação do estudo dos suportes de segurança.

- Princípios e Fundamentos dos métodos criptográficos.
- Princípios de criptografia computacional
  - Princípios do funcionamento dos métodos criptográficos
  - Métodos e algoritmos de criptografia simétrica
  - Métodos e algoritmos de criptografia de chave pública
  - Infra-estruturas de Chave Pública.
  - Funções de Hashing e Message Digests.
  - Assinaturas digitais e sua utilização.
  - Certificados digitais.
  - Caso de estudo – Pretty Good Privacy (PGP).
- Sistemas de autenticação, certificação e controlo de acessos.
  - Kerberos V4/V5
  - Serviços de autenticação com certificação X.509
  - Sistemas de autenticação centralizada (Sistemas SingleSignOn).
  - Sistemas e infra-estruturas de gestão de chaves públicas (PKIs).
- Firewalls e sistemas de detecção de intrusão
  - Tipos de Firewalls.
  - Sistemas de detecção de intrusão (IDS).
- Segurança em redes Wireless 802.11.
- Mecanismos de Network Access Control.
- Planeamento de redes seguras.

### **Métodos de Avaliação:**

A avaliação é composta por trabalhos laboratoriais com o peso total de 40% e uma frequência ou exame individual com o peso de 60%.

#### **Avaliação prática:**

Os trabalhos práticos são realizados individualmente ou em grupos de dois alunos. Todos os trabalhos são sujeitos a discussão. Nota mínima **10 valores (0 a 20 valores)**.

É obrigatória a presença nas aulas práticas de acordo com o art. 12 do Regulamento de Académico.

#### **Avaliação teórica:**

Só são admitidos à prova escrita os alunos que tenham obtido **10 valores** na componente prática. A prova escrita é composta por uma frequência ou exame escrito sem consulta. Nota mínima da prova escrita **8 valores (0 a 20 valores)**.

### **Bibliografia:**

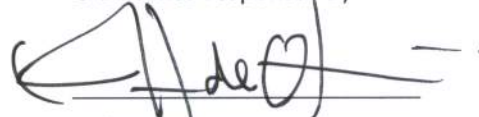
André Zúquete.: "Segurança em Redes Informáticas". FCA, 2006.

Stallings William, "Network Security Essentials, Prentice Hall, 2000.

Stallings William, "Cryptography and Network Security: Principles and Practice", Prentice Hall, Second Edition, 1998.

Edmundo Monteiro e Fernando Boavida.: "Engenharia de Redes Informáticas". FCA, 2000.

O Docente responsável,



Luís Miguel Lopes de Oliveira