

PLANO DA DISCIPLINA - SEGURANÇA INFORMÁTICA EM REDES E SISTEMAS

1. IDENTIFICAÇÃO DA DISCIPLINA

- **Nome:** Segurança Informática em Redes e Sistemas
- **Curso:** Informática e Sistemas de Informação
- **Regime:** Semestral
- **Ano/Semestre:** 5º ano, 2º semestre
- **Carga Horária Total:** 80 horas
- **Horas Semanais:** 5 horas (2 teóricas, 2 teórico-práticas, 1 prática)
- **Precedência Obrigatória:** Redes de Computadores e Sistemas Operativos II

2. OBJETIVOS GERAIS

- Ministar, aprofundar e integrar conhecimentos sobre segurança em sistemas informáticos e redes.
- Desenvolver capacidades para análise de riscos e ameaças em sistemas de informação.
- Implementar estratégias e técnicas de proteção de dados e infraestrutura computacional.
- Conhecer e aplicar políticas de segurança e auditoria de sistemas.

3. COMPETÊNCIAS A DESENVOLVER

- Identificação e mitigação de ameaças e ataques informáticos.
- Aplicação de políticas e técnicas de segurança.
- Implementação de mecanismos de proteção, autenticação e criptografia.
- Auditoria e avaliação de riscos em sistemas de informação.
- Configuração de firewalls, proxies e protocolos de segurança.

4. CONTEÚDO PROGRAMÁTICO

UNIDADE 1: A Necessidade de Segurança em Sistemas de Informação (15h)

- Noções de segurança empresarial.
- Segurança nos sistemas de informação.
- O papel da auditoria informática.

UNIDADE 2: Políticas e Estratégias de Segurança (20h)

- Fundamentos: confidencialidade, integridade e disponibilidade.
- Autenticação, autorização e auditoria de contas.
- Desenvolvimento e implementação de um plano de segurança.

UNIDADE 3: Segurança Física e Lógica (20h)

- Aspectos físicos: instalações, equipamentos e manutenção.
- Identificação e autenticação de utilizadores.
- Sistemas de encriptação: chave única e chave dupla.
- Uso de smart cards e normas de controlo de acessos.

UNIDADE 4: Segurança em Redes e Infraestruturas (15h)

- Segurança em sistemas distribuídos.
- Segurança da informação em redes corporativas.
- Ameaças e ataques: phishing, malware, DDoS.
- Serviços e mecanismos de segurança (SSO, LDAP, Kerberos, Sesame).
- Firewalls, proxies e auditoria de segurança em redes.

UNIDADE 5: Auditoria e Benefícios Estratégicos da Segurança (10h)

- Áreas e fases da auditoria de segurança.
- Avaliação de riscos em infraestruturas informáticas.
- Segurança como fator estratégico para organizações.

5. METODOLOGIA DE ENSINO

- Aulas expositivas e interativas.
- Estudo de casos reais de ataques e soluções de mitigação.
- Simulações práticas de segurança em redes e sistemas.
- Configuração e utilização de ferramentas de auditoria e segurança.

6. CRITÉRIOS DE AVALIAÇÃO

- **Trabalhos práticos e projetos:** 30%
- **Testes intermediários:** 30%
- **Exame final:** 40%
- **Frequência mínima:** 75% nas aulas práticas.

7. BIBLIOGRAFIA

Bibliografia Básica

- Marques, Ana Margarida et al. – *101 Perguntas e Respostas do Direito da Internet e da Informática*, Centro Atlântico.
- Caruso, Carlos A. – *A Segurança em Informática e em Redes Locais*, LTC.
- Carneiro, Alberto – *Auditoria dos Sistemas de Informação*, FCA.
- Zwicky, Elizabeth et al. – *Building Internet Firewalls*, O'Reilly.

Bibliografia Complementar

- Cheswick, William R. & Bellovin, Steven M. – *Firewalls and Internet Security*, Addison Wesley.
- Peterson, Larry & Davie, Bruce – *Computer Networks*, Academic Press.
- Russell, Debby & Gangemi, G. T. – *Computer Security Basics*, O'Reilly.
- Schiffman, Mike – *Hacker's Challenge: Test Your Incident Response Skills*, McGraw-Hill.
- Silva, Pedro T. et al. – *Segurança dos Sistemas de Informação*, Centro Atlântico.