

Plano da Disciplina: Segurança Informática em Redes e Sistemas

1. Desenho da Disciplina

- **Nome:** Segurança Informática em Redes e Sistemas
 - **Curso:** Licenciatura em Engenharia Informática, Engenharia de Telecomunicações ou áreas correlatas
 - **Ano/Semestre:** 5º Ano / 1º Semestre
 - **Modalidade:** Presencial
 - **Carga Horária Semanal:** 5 horas
 - **Carga Horária Total:** 80 horas
-

2. Regime

- **Regime:** Semestral
 - **Frequência mínima:** 75% de presença nas aulas teórico-práticas
 - **Avaliação contínua** com provas, exercícios, simulações e projetos práticos
-

3. Posição no Curso

- **5º Ano, 1º Semestre**
 - Disciplina essencial para **compreensão e implementação de estratégias de segurança em redes e sistemas**
-

4. Horário Semanal

- **2 horas teóricas** (fundamentos de segurança em redes e sistemas)
 - **1 hora teórico-prática** (análise de ataques e proteção de sistemas)
 - **2 horas práticas (laboratórios)** (implementação computacional e auditoria de segurança)
-

5. Carga Horária Total

- **Total:** 80 horas
 - **Horas Teóricas:** 32h
 - **Horas Teórico-Práticas:** 16h
 - **Horas Práticas (Laboratórios):** 32h
-

6. Precedências Obrigatórias

- **Introdução à Eletrônica das Comunicações**
 - **Radiopropagação e Antenas**
-

7. Objetivos Gerais

- 1) **Ministrar, aprofundar e integrar conceitos fundamentais de segurança em redes e sistemas.**
 - 2) **Criar capacidades para análise da segurança da informação e proteção de dados.**
 - 3) **Desenvolver habilidades para implementação de políticas de segurança.**
 - 4) **Explorar sistemas de proteção como firewalls, proxies, encriptação e auditoria de segurança.**
 - 5) **Compreender a importância estratégica da segurança da informação nas organizações.**
-

8. Competências a Desenvolver

- ✓ **Identificar riscos e vulnerabilidades em redes e sistemas.**
 - ✓ **Implementar políticas de segurança, autenticação e controle de acessos.**
 - ✓ **Configurar sistemas de proteção, firewalls e monitoramento de tráfego.**
 - ✓ **Analisar mecanismos de encriptação e proteção de dados.**
 - ✓ **Aplicar auditoria de segurança e avaliação de riscos em infraestruturas de TI.**
-

9. Conteúdo Temático e Bibliografia

Unidade 1: A Necessidade de Segurança (10h)

Computer Security Basics – Russell, Debby and Gangemi, G. T., O'Reilly

- **Noções de Segurança Empresarial**
- **Segurança nos Sistemas de Informação**
- **O papel da Auditoria Informática**

Laboratório: Análise de vulnerabilidades em redes corporativas

Unidade 2: Políticas de Segurança (10h)

Auditoria dos Sistemas de Informação – Carneiro, Alberto, FCA-Editora de Informática

- **Fundamentos: Confidencialidade, Integridade e Disponibilidade (CIA)**
- **Funções de Segurança: autenticação, autorização, auditoria e integridade de dados**

- Elaboração e implementação de um plano de segurança

Laboratório: Implementação de uma política de segurança corporativa

Unidade 3: Segurança Física e Lógica (10h)

A Segurança em Informática e em Redes Locais – Caruso, Carlos A., LTC

- Aspectos físicos: pessoal, instalações, equipamentos e manutenção
- Identificação e autenticação de usuários
- Sistemas de encriptação: chave única e chave pública

Laboratório: Implementação de encriptação em comunicações seguras

Unidade 4: Segurança em Redes (15h)

Computer Networks – Peterson, Larry L. and Davie, Bruce S., Academic Press

- Segurança em Sistemas Distribuídos
- Segurança da Informação em Redes
- Perigos da Segurança: ameaças e ataques

Laboratório: Simulação de ataques e implementação de defesas

Unidade 5: Sistemas de Proteção e Firewalls (10h)

Building Internet Firewalls – Zwicky, Elizabeth D., Cooper, Simon and Chapman, D. Brent, O'Reilly

- Conceito e funcionamento de firewalls
- Proxies e gateways de segurança
- Auditoria de segurança em redes

Laboratório: Configuração de firewalls e proxies

Unidade 6: Segurança em Intranets e Ambientes Corporativos (10h)

Firewalls and Internet Security – Cheswick, William R. and Bellovin, Steven M., Addison Wesley

- Segurança em redes internas (LAN e WLAN)
- Identificação e autenticação em sistemas empresariais
- Técnicas de isolamento de ameaças

Laboratório: Implementação de segurança para redes corporativas

Unidade 7: Auditoria e Gestão de Segurança (10h)

Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios - Schiffman, Mike, McGraw-Hill Osborne Media

- Áreas da auditoria de segurança
- Avaliação de riscos e compliance
- Fases da auditoria de segurança física e lógica

Laboratório: Simulação de um processo de auditoria de segurança

Unidade 8: Projeto Final Integrado (10h)

Baseado nas competências adquiridas ao longo do semestre

- Desenvolvimento de um **projeto prático envolvendo análise e proteção de redes e sistemas**
- Aplicação dos conceitos estudados para garantir segurança da informação

Laboratório: Implementação e defesa do projeto final

10. Metodologia de Trabalho

Aulas teóricas para introdução aos conceitos fundamentais de segurança informática

Exercícios práticos para reforço da proteção e auditoria de sistemas

Laboratórios computacionais para simulação de ataques e implementação de defesas

Projetos individuais e em grupo para aplicação prática dos conteúdos estudados

11. Critério de Avaliação

✓ **40% - Trabalhos práticos e implementação de segurança em redes e sistemas**

✓ **30% - Projeto Final Integrado**

✓ **20% - Participação e atividades complementares**

✓ **10% - Prova escrita/técnica**

12. Bibliografia Básica

Russell, Debby & Gangemi, G. T. - *Computer Security Basics*, O'Reilly

Caruso, Carlos A. - *A Segurança em Informática e em Redes Locais*, LTC

Zwicky, Elizabeth D. et al. - *Building Internet Firewalls*, O'Reilly

Cheswick, William R. & Bellovin, Steven M. - *Firewalls and Internet Security*, Addison Wesley

Schiffman, Mike - *Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios*, McGraw-Hill Osborne Media

