# INSTITUTO POLITÉCNICO DE BEJA
# ESCOLA SUPERIOR DE TECNOLOGIAS E GESTÃO

CURRICULUM DO CURSO DE ENGENHARIA INFORMÁTICA

**DESCRITOR DE UNIDADE CURRICULAR**

| |
|---|
| **DESIGNAÇÃO:** Segurança em Redes de Comunicação |

| | | | |
|---|---|---|---|
| **ANO:** 3 | **SEMESTRE:** 2 | **ÁREA CNAEF:** 481 | **CRÉDITOS:** 7,0 |

**TEMPO DE TRABALHO DO ESTUDANTE EM HORAS:**

| **Total:** | **Contacto:** 60 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Teóricas** | **Teórico Práticas** | **Práticas e Laboratório** | **Trabalho de Campo** | **Seminário** | **Estágio** | **Orientação Tutória** | **Outras*** |
| 189 | | 30 | 30 | | | | | |

**DESCRIÇÃO RESUMIDA DA UNIDADE CURRICULAR:**

Esta unidade curricular irá proporcionar aos alunos os fundamentos basilares de segurança em redes de computadores incluindo a componente de Criptografia e de Networking. No que respeita à componente de Criptografia incluem-se a as técnicas clássicas e modernas, criptografia de chave simétrica e de chave pública, técnicas de autenticação de mensagens e funções de hash, protocolos de autenticação e assinatura digital, e servidores de autenticação. Esta unidade curricular irá ainda abordar uma outra vertente relativa às redes sem fios, com especial enfoque par as questões de segurança e integração com redes com fios de forma segura recorrendo a servidores de autenticação. Os alunos terão a possibilidade de instalar e configurar as matérias abordadas em equipamento existente num laboratório específico de redes de computadores.

**TEMAS PROGRAMÁTICOS:**

- Segurança: Introdução à Segurança; Criptografia Convencional; Criptografia de Chaves Públicas; Autenticação de Mensagens e Funções de *Hash*; Protocolos de Autenticação e Assinatura Digital; Servidores de Autenticação;
- Redes Sem Fios: Introdução às Redes de Dados Sem Fios; Segurança em Redes de Dados Sem Fios; Implementação de Redes de Dados Sem Fios; Implementação de politicas de segurança em ambientes envolvendo redes sem fios.

**BIBLIOGRAFIA DE BASE:**


- Stallings, William (2005) Cryptography and Network Security, Principles and Practices, 4th Edition. Prentice Hall.
- Spillman, Richard J. (2005) Classical and Contemporary Cryptology. Prentice Hall.
- Buchman, Johannes A. (2004) Introduction to Cryptography, 2nd Edition. Springer.
- Scheneier, Bruce (1996) Applied Cryptography, 2nd Edition. John Wiley & Sons.
- Edney, Jon, Arbaugh, William A. (2004)Real 802.11 Security Wi-Fi Protected Access and 802.11i. Addison Wesley.
- Flickenger, Rob. (2003) Building Wireless Community Networks, 2nd Edition. O'Reilly.

**OBJECTIVOS EDUCACIONAIS:**

Para obter sucesso nesta unidade curricular o estudante demonstrará que é capaz de:

- Aplicabilidade de Algoritmos de Criptografia Convencional, Criptografia de Chaves Públicas, Funções de *Hash* e Códigos MAC;
- Desenvolvimento de Aplicações para Implementação de Serviços de Segurança;
- Projecto, Instalação e Configuração de Redes Sem Fios;
- Projecto e Implementação de Soluções de Segurança para Redes de Dados com e Sem Fios recorrendo às Tecnologias Existentes;
- Desenvolvimento de Aplicações de Criptanálise.

**ESTRATÉGIAS DE ENSINO / APRENDIZAGEM:**

- Aulas expositivas;
- Desenvolvimento de exercícios práticos;
- Desenvolvimento de laboratórios.

**AVALIAÇÃO:**

- Teste ou exame escrito;
- Trabalho prático autónomo;
- Relatório escrito;
- Projecto em Grupo com Defesa.