Designação da Unidade Curricular (UC) / Title of Curricular Unit (CU): Segurança em Redes Informáticas / Security in Computer Networks
Área científica da UC / CU Scientific Area: Ciências Informáticas / Computer Science
Semestre / Semester: 3º
Número de créditos ECTS / Number of ECTS credits: 6
Carga horária por tipologia de horas / Workload by type of hours: TP: 45; OT: 6; O: 9
Carga letiva semanal / Weekly letive charge: 3h

Objetivos de aprendizagem (conhecimentos, aptidões e competências a desenvolver pelos estudantes):

Pretende-se que, no final do semestre, os alunos sejam capazes de:

- Definir e analisar as exigências de segurança de um sistema informático;
- Projetar e implementar uma estratégia de segurança para uma rede informática;
- Identificar vulnerabilidades de segurança em sistemas ligados por redes de computadores;
- Descrever os conceitos fundamentais de segurança de sistemas informáticos (confidencialidade, integridade, etc.);
- Propor medidas de proteção à informação armazenada e em circulação em sistemas informáticos ligados em rede local e na Internet.

Intended learning outcomes (knowledge, skills and competences to be developed by the students):

At the end of the semester, students are expected to be able to:

- Define and analyze the security requirements of a computer system;
- Design and implement a security strategy for a computer network;
- Identify security vulnerabilities in systems connected by computer networks;
- Describe the fundamental concepts of computer systems security (confidentiality, integrity, etc.);
- Propose measures to protect information stored and in circulation in computer systems connected to the local network and the Internet.

Conteúdos programáticos:

1. Introdução à segurança informática

1.1 Mecanismos e políticas de segurança
1.2 Tipos de ataques
1.3 Domínio de segurança
1.4 Principais vulnerabilidades
1.5 Ameaças externas

2. Criptografia de chave pública e privada

2.1 Algoritmos de chave simétrica

2.2 Algoritmos de chave assimétrica

2.3 Problemática da distribuição e acordo de chaves

2.4 Funções de hash

3. Gestão e utilização de chaves públicas

3.1 Infraestrutura de chave pública

3.2 Assinaturas digitais

3.3 Entidades certificadoras

4. Autenticação de utilizadores

4.1 Autenticação de utilizador de computador local

4.2 Autenticação de utilizador na rede

4.3 Configuração e administração do Active Directory

4.4 Configuração e administração do LDAP

5. Controlo de acessos

5.1 Políticas de acesso

5.2 Contas de utilizadores

5.3 Grupos

5.4 Permissões

6. Proteção de dados armazenados

6.1 Criptografia de ficheiros e diretórios (pastas)

6.2 Codificação de diretórios e ficheiros

6.3 Ficheiros e pastas escondidas

6.4 Cópias de segurança

6.5 Processo de recuperação de dados

7. Proteção da transmissão de dados

7.1 Implementação de transmissão segura de dados: Internet/LAN

7.2 Processo IPSec

7.3 Configuração do IPSec

7.4 Vulnerabilidades em aplicações Web e na Internet

Syllabus:

1. Introduction to computer security

1.1 Security mechanisms and policies

1.2 Types of attacks

1.3 Security domain

1.4 Major vulnerabilities

1.5 External Threats

2. Public and Private Key Encryption

2.1 Symmetric Key Algorithms

2.2 Asymmetric Key Algorithms

2.3 Problems of distribution and agreement of keys

2.4 Hash Functions

3. Management and use of public keys

3.1 Public Key Infrastructure

3.2 Digital Signatures

3.3 Certification bodies

4. User Authentication

4.1 Local computer user authentication

4.2 Network User Authentication

4.3 Configuring and Administering Active Directory

4.4 LDAP Configuration and Administration

5. Access control

5.1 Access policies

5.2 User Accounts

5.3 Groups

5.4 Permissions

6. Protection of stored data

6.1 Encrypting files and directories (folders)

6.2 Encoding of directories and files

6.3 Hidden files and folders

6.4 Backups

6.5 Data recovery process

7. Protection of data transmission

7.1 Implementation of secure data transmission: Internet / LAN

7.2 IPSec Process

7.3 Configuring IPSec

7.4 Vulnerabilities in Web Applications and in the Internet