| **DISCIPLINA:** Segurança da Informação | |
|---|---|
| **Vigência:** a partir de 2023/1 | **Período letivo:** 5º semestre |
| **Carga horária total:** 45h | **Código:** CH_SUP.131 |
| **Ementa:** Introdução aos principais conceitos da segurança da informação; estudo dos fundamentos dos algoritmos de criptografia; estudo dos aspectos de complexidade computacional da segurança da informação; análise das dimensões da segurança; definição da terminologia empregada em segurança da informação; estudo das técnicas de criptografia simétrica; estudo das técnicas de criptografia assimétrica; estudo dos mecanismos para implementação autenticação e controle de acesso; estudo dos mecanismos para imposição de segurança em redes de computadores e sistemas; aprofundamento prático dos conceitos apresentados por meio de estudos de caso. | |

**Conteúdos**

UNIDADE I – INTRODUÇÃO E PRINCIPAIS CONCEITOS

1.1 Modelos de controle de acesso

1.2 Conceitos de criptografia

1.3 Questões de força de proteção e complexidade computacional

1.4 As quatro dimensões da segurança

1.5 Terminologia empregada na segurança da informação

1.6 Cavalos de tróia, backdoors, keyloggers e outras ameaças

1.7 Principais mecanismos de defesa

UNIDADE II – CRIPTOGRAFIA SIMÉTRICA

2.1 Aplicações da criptografia simétrica

2.2 Conceito de chave, texto plano e cifrado

2.3 Criptoanálise

2.4 DES, 3-DES, AES

2.5 Hash e funções one-way

2.6 Estudo de caso: Enigma

UNIDADE III – CRIPTOGRAFIA ASSIMÉTRICA

3.1 Chaves públicas e privadas

3.2 Vantagens, desvantagens e características

3.3 O algoritmo RSA

3.4 Criptoanálise para criptografia assimétrica

UNIDADE IV – AUTENTICAÇÃO E CONTROLE DE ACESSO

4.1 Principais métodos de autenticação

4.2 Implementação de controle de acesso

4.3 Assinaturas digitais

UNIDADE V – SEGURANÇA EM REDES E SISTEMAS

5.1 Principais ataques via rede

5.2 IDS, IPS e Firewall

5.3 Principais ataques via sistemas

5.4 Mecanismos de proteção do sistema operacional

5.5 Desenvolvimento de software seguro
UNIDADE VI – ESTUDOS DE CASO
6.1 Desenvolvimento de um sistema seguro de login e recuperação de senha
6.2 Implementação de um servidor web seguro

**Bibliografia básica**

STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores – Princípios e Práticas**. Rio de Janeiro: Elsevier, 2014.
GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. São Paulo: Bookman, 2013.
STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 4. ed. São Paulo, SP: Pearson, 2008.

**Bibliografia complementar**

BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.
MITNICK, Kevin D.; SIMON, William L. **A arte de Invadir**. São Paulo: Person Prentice Hall, 2005.
ZWICK, Elizabeth D.; COOPER, Simon; CHAPMAN, Brent. **Construindo Firewalls para Internet.** Rio de Janeiro: Campus, 2000.
IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. São Paulo: Atlas, 2016.
FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.
SÊMOLA, Marcos. **Gestão da segurança da informação**. Rio de Janeiro: Elsevier Brasil, 2014.