Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino

DISCIPLINA: Segurança da Informação	
Vigência: a partir de 2020/1	**Período letivo:** 4º ano
Carga horária total: 60h	**Código:** CH.INF.074
Ementa: 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 aspectos de segurança para desenvolvimento de sistemas web; estudo dos mecanismos para implementação de controle de acesso; estudo dos mecanismos para imposição de segurança em redes de computadores; análise do funcionamento do softwares maliciosos.	

Conteúdos

UNIDADE I – Introdução à Segurança da Informação
- 1.1 Modelos de controle de acesso
- 1.2 Conceitos de criptografia
- 1.3 Questões de força de proteção e complexidade computacional

UNIDADE II – Dimensões e Terminologia da Segurança da Informação
- 2.1 As quatro dimensões da segurança
- 2.2 Terminologia empregada na segurança da informação
- 2.3 Boas práticas para o desenvolvimento de software seguro

UNIDADE III – Criptografia Simétrica
- 3.1 Tipos de criptografia e suas aplicações
- 3.2 Criptografia simétrica
- 3.3 Conceito de chave, texto plano e cifrado
- 3.4 Criptoanálise
- 3.5 DES, 3-DES, AES e Hash
- 3.6 Estudo de caso da máquina Enigma

UNIDADE IV – Criptografia Assimétrica
- 4.1 Chaves públicas e privadas
- 4.2 Vantagens, desvantagens e características
- 4.3 O algoritmo RSA
- 4.4 Criptoanálise para criptografia assimétrica

UNIDADE V – Segurança WEB
- 5.1 Ataques a clientes
- 5.2 Ataques a servidores
- 5.3 Principais mecanismos de proteção

UNIDADE VI – Autenticação e Controle de Acesso
- 6.1 Métodos de autenticação
- 6.2 Implementação de controle de acesso
- 6.3 Assinaturas digitais

UNIDADE VII – Segurança em Redes
- 7.1 Principais ataques
- 7.2 IDS
- 7.3 IPS
- 7.4 Firewall

UNIDADE VIII – Softwares Maliciosos
- 8.1 Cavalos de tróia, backdoors, keyloggers e outras ameaças
- 8.2 Mecanismos de defesa para softwares maliciosos

Bibliografia básica

BAARS, Hans. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.
GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores.** São Paulo: Bookman, 2013.
STALLINGS, William; BROWN, Lawrie. **Segurança de Computadores** – princípios e práticas. Rio de Janeiro: Elsevier, 2014.

Bibliografia complementar

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