de dezembro de 2020.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores**: princípios e práticas. 2. ed. Rio de Janeiro: Campus, 2014.

STALLINGS, William; **Criptografia e segurança de redes:** princípios e práticas. 4. ed. São Paulo: Prentice-Hall, 2008. Disponível em <http://bvu.ifce.edu.br/>. Acesso em 7 de dezembro de 2020.

TERADA, Routo. **Segurança de dados: criptografia em rede de computador**. 2. ed. São Paulo: Edgard Blucher, 2008.

Disciplina:	Segurança da Informação
Código:	msi34
Carga Horária	80
Número de créditos	4
Código pré-requisito:	-
Semestre:	3º
Nível:	Técnico

Ementa:

Introdução a segurança. Criptografia. Engenharia social. Mensagem e função hash. Assinatura Digital. Autenticação de entidades. Gerenciamento de chaves.

Objetivos:

Capacitar o alunos a utilizar os conceitos de segurança da informação e proteção ao conhecimento; identificar as diferentes modelos e técnicas de segurança da informação; contribuir para o desenvolvimento de planos de proteção ao conhecimento e segurança da informação.

Programa:

1. Introdução a segurança
   - 1.1. Segurança de computador
   - 1.2. Segurança de rede
   - 1.3. Estatísticas
   - 1.4. Arquitetura de segurança OSI
     - 1.4.1. Ataques ativos
     - 1.4.2. Ataques passivos
   - 1.5. Serviços de segurança
   - 1.6. Mecanismos de Segurança
2. Criptografia

2.1. Criptografia de chave simétrica
2.1.1. Cifras modernas
2.1.2. Cifras cíclicas
2.2. Criptografia de chave assimétrica
2.2.1. RSA
2.2.2. Diffe-Hellman
3. Engenharia social
3.1. Fator Humano x Segurança
3.2. Ferramentas utilizadas
3.3. Ataques
3.4. Engenharia social reversa
3.5. Evitando ataque de engenharia social
4. Mensagem e função hash
4.1. Confidencialidade de mensagem
4.2. Integridade de mensagem
4.3. Autenticação de mensagem
5. Assinatura Digital
5.1. Comparação Assinatura convencional x Assinatura digital
5.2. Obtendo assinatura digital
5.3. Serviços
6. Autenticação de entidades
6.1. Tipos de autenticação
6.2. Senha fixa
6.3. Confrontação resposta
7. Gerenciamento de chaves
7.1. Distribuição de chaves simétrica
7.2. Centro de distribuição de chaves
7.3. Chave de sessão
7.4. Distribuição de chaves pública
7.5. Autoridade de certificação
7.6. Identificação de sites seguros
7.7. Visualização de informações de certificados
7.8. Inserindo autoridades certificadoras em navegadores

Metodologia de Ensino:

Aulas teóricas expositivas e participativas, com uso de recursos audiovisuais. Aulas práticas em laboratório. Atividades de pesquisa. Resolução de exercícios. Visitas técnicas.

Avaliação:

A avaliação do aluno será processual e contínua, através da participação de atividades em sala de aula e de avaliações teóricas e práticas (trabalhos, dinâmicas e seminários).

Bibliografia básica

ORGANIZADORA MICHELE DA COSTA GALVÃO. **Fundamentos em Segurança da Informação.** [S.l.]: Pearson. 128 p. ISBN 9788543009452.

KUROSE, James F.; ZUCCHI, Wagner Luiz. **Redes de computadores e a internet:** uma abordagem top-down. Tradução de Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2013. 634 p., il. ISBN 9788581436777.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008. 492 p., il. ISBN 9788576051190.

Bibliografia complementar:

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores.** Porto Alegre: Bookman, 2006.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre: Bookman, 2013. 550 p., il. ISBN 9788540701922.

TERADA, Routo. **Segurança de dados: criptografia em redes de computadores.** 2. ed. rev. e ampl. São Paulo: Blucher, 305 p., il. ISBN 9788521204398, 2014.