P R O G R A M A D E D I S C I P L I N A

DEPARTAMENTO: Sistemas de Informação

DISCIPLINA: Introdução à Segurança da Informação	**SIGLA:** 7ISE002

CARGA HORÁRIA TOTAL: 72h	**TEORIA:** 54h	**PRÁTICA:** 18h

CURSO: Bacharelado em Sistemas de Informação

PRÉ-REQUISITOS: 5REC202

EMENTA: Conceitos e terminologia de segurança em computação: criptografia simétrica e criptografia assimétrica; Assinatura digital: infraestrutura de chave pública; Segurança de sistemas.

PROGRAMA

1. Introdução
1.1. Apresentação da disciplina;
1.2. Metodologia de ensino utilizada;
1.3. Avaliações;
1.4. Cronograma das aulas.

2. Introdução à Segurança da Informação
2.1. Conceitos básicos de Segurança da Informação;
2.2. Ataques à segurança e ameaças;
2.3. Serviços e mecanismos de segurança;
2.4. Conceitos básicos de criptografia;
2.5. Criptoanálise e modelo de segurança baseado em criptografia;
2.6. Criptografia simétrica e assimétrica.

3. Aplicações de criptografia assimétrica
3.1. Autenticação de mensagem e funções Hash;
3.2. Assinatura digital;
3.3. O problema do gerenciamento de chaves públicas (PKI);
3.4. Autoridades de certificação;
3.5. Padronização e políticas para controle de riscos.

4. Segurança em camadas de redes
4.1. Protocolos e serviços de segurança para redes;
4.2. Segurança de IP;
4.3. Segurança de serviços (email, web e ftp) – camada de transporte e aplicação;
4.4. Introdução a software malicioso;
4.5. Sistemas de detecção de intrusão;

4.6. Firewalls.

5. Trabalho final
5.1. Temas diversos sobre tecnologias relacionadas a Segurança da Informação

Bibliografia Básica

STALLINGS, William. **Criptografia e segurança de redes - Princípios e práticas**. 4a ed. Ed. Prentice Hall, São Paulo, 2008.

TERADA, Routo. **Segurança de dados: criptografia em redes de computador**. 2a ed., São Paulo: Ed. Blucher, 2008.

NAKAMURA, Emilio; GEUS, Paulo. **Segurança de Redes em Ambientes Corporativos**. Novatec, 2007.

Bibliografia Complementar

KUROSE, James F; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down**. 3a ed. São Paulo: Makron Books, 2006.

BURNET, Steve; PAINE, Stephen. **Criptografia e Segurança – O Guia Oficial RSA**. Campus/Elsevier. 4a. Ed, 2002.

VIANA, Eliseu R. C. **Virtualização de servidores Linux para redes corporativas**. Rio de Janeiro: Ciência Moderna, 2008. 230p.

MORAES, Alexandre F. **Redes sem fio: instalação, configuração e segurança – fundamentos**. São Paulo: Érica, 2010 284 p.

TANENBAUM, Andrew S; STEEN, Maarten Van. **Sistemas distribuídos: princípios e paradigmas**. 2. ed. São Paulo: Prentice Hall, c2008. 402 p.