**DADOS DO COMPONENTE CURRICULAR: SEGURANÇA DA INFORMAÇÃO**

**CURSO: TÉCNICO EM INFORMÁTICA**

**SÉRIE: 3ºANO**

**CARGA HORÁRIA: 33 h.r**

**DOCENTE RESPONSÁVEL: NARALLYNNE MACIEL DE ARAÚJO**

## Ementa

Apresentar os pilares da segurança da informação, seus princípios e importância; Conceituar os princípios da gerência de risco, acesso à dados, ataques e ameaças; Demonstrar os conceitos de Engenharia Social, seus tipos de ataques e técnicas utilizadas, bem como meios de prevenção e segurança; Princípios básicos de Criptologia; Demonstrações de análise de tráfego e gestão da Segurança da Informação.

## Objetivos de Ensino

**Geral:**
Conhecer os conceitos de segurança da informação, reconhecendo o seu valor para organizações e indivíduos.
**Específicos:**
• Reconhecer e relacionar os principais riscos envolvidos no ambiente de informações;
• Descrever e explicar ferramentas e procedimentos com relação à segurança da informação - nos aspectos de segurança lógica, física e ambiental;
• Descrever e montar uma Política de Segurança da Informação;
• Reconhecer e relacionar os diferentes tipos de códigos maliciosos, bem como meios de defesa pessoal e organizacional;
• Identificar ataques de Engenharia Social e meios de defesa de dados pessoais e organizacionais relacionados a essa técnica;
• Entender os princípios de criptologia, conhecendo o uso de diferentes ferramentas de cifragem e decifragem de dados;
• Reconhecer e relacionar diferentes tipos de interferências de dados aos meios relacionados à Segurança da Informação;
• Descrever e explicar a segurança de redes, reconhecendo técnicas e o uso de diferentes ferramentas.

## Conteúdo Programático

**UNIDADE I**

1.1Introdução à segurança da Informação

1.2Controles de acesso físico e lógico.

1.3NBR ISO/IEC 17799:2005

**UNIDADE II**

2.1Gerência de Riscos

2.2Tratamento de incidentes e problemas.

2.3Vírus de computador e outros malware cavalos de tróia, adware, spyware, backdoors, keyloggers, worms, bots, botnets, rootkits

2.4Engenharia Social

**UNIDADE III**

3.1Ataques e proteções relativos a hardware, software, sistemas operacionais, aplicações, bancos de dados, redes, pessoas e ambiente físico.

3.2Segurança de Redes.

3.3Criptologia

3.4Autenticação de usuários, Senhas.

**UNIDADE IV**

4.1Monitoramento de tráfego.

4.2Sniffer de rede.

4.3Interpretação de pacotes.

4.4Detecção e prevenção de ataques (IDS e IPS).

4.5Ataques e ameaças da Internet e de redes sem fio (phishing/scam, spoofing, DoS, flood).

**Metodologia de Ensino**

Aulas teóricas expositivas e dialogadas, explanando conceitos básicos sobre o conteúdo com auxílio de mídias projetoras, internet, quadro branco e computadores com software específicos.

Aulas práticas com roteiros de atividades, pesquisas e seminários.

Visitas técnicas e elaboração de relatórios.

**Avaliação do Processo de Ensino e Aprendizagem**

Avaliação de forma contínua com exercícios teóricos e práticos.

Apresentação de seminários.

Provas escritas e práticas, a fim de verificar as especificidades individuais de cada educando.

**Sistema de Acompanhamento Para a Recuperação da Aprendizagem**

O acompanhamento para a recuperação da aprendizagem ocorrerá, nos Núcleos de Aprendizagem, por meio de atividades que possibilitem ao estudante a apreensão efetiva dos conteúdos, de acordo com o previsto na LDB e nas Normas Didáticas dos Cursos Técnicos Integrado ao Médio do IFPB (item 2.3, artigos 28 a 30).

**Recursos Didáticos Necessários**

Serão utilizados, como recursos didáticos: data show, quadro branco, pincel atômico e computadores com softwares específicos

| Bibliografia |
| --- |
| **Básica:** |
| JAMES, K.; KEITH, R. Redes de Computadores e a Internet: Uma abordagem top-down. Pearson Addison Wesley, 2005.<br>MORAES, Alexandre Fernandes de. Segurança em redes: fundamentos. São Paulo: Érica, 2010. |
| **Complementar:** |
| PEIXOTO, Mário César Pintaudi. Engenharia social e segurança da informação na gestão corporativa. Brasport, 2006.<br>Estatísticas Mantidas pelo CERT.br. Disponível em http://www.cert.br/stats |