**MINISTÉRIO DA EDUCAÇÃO**
**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA**
**CAMPUS CAJAZEIRAS**
**COORDENAÇÃO DO CURSO TÉCNICO EM INFORMÁTICA**

# SEGURANÇA DE DADOS

## PLANO DE DISCIPLINA

| DADOS DO COMPONENTE CURRICULAR |
|---|
| **Nome: SEGURANÇA DE DADOS** |
| **Curso: TÉCNICO EM INFORMÁTICA** |
| **Série: 4ª** |
| **Carga Horária Semestral: 66,7 h.** |

| EMENTA |
|---|
| Auditoria de sistemas. Segurança de sistemas. Metodologias de auditoria. Análise de riscos em sistemas de informação. Ferramentas de monitoramento da infraestrutura em TI. Padrões: COBIT e ITIL. Normas de Segurança: ISO 27001 e 27002. Técnicas de Criptografia e seus respectivos algoritmos e protocolos. Certificados Digitais e a Infra-estrutura de Chaves Públicas. Segurança nas redes sem fio. Detecção de vulnerabilidades em sistemas computacionais. Os riscos que rondam as organizações: Vírus, Malwares, Trojans, além da especificação de como funcionam os principais ataques aos sistemas computacionais (smurf, fraggle, etc.) e a taxonomia dos atacantes. Firewalls: arquiteturas e implementação. Recuperação de Dados. |

## OBJETIVOS

### Geral

Compreender os benefícios de um sistema seguro, para proteção da informação, bem como, fomentar o conhecimento das técnicas, ferramentas e brechas de segurança, na proteção de ambientes pessoais e corporativos, além de prover um arcabouço para o desenvolvimento e manutenção de sistemas computacionais seguros.

### Específicos

1. Explicar a importância da segurança da informação.
2. Descrever as vantagens da aplicação de metodologias de auditoria da informação.
3. Utilizar ferramentas computacionais de auditoria e monitoramento de infra-estrutura em TI.
4. Reconhecer os principais padrões de fato e de direito de segurança corporativa.
5. Descrever as técnicas, algoritmos e protocolos de criptografia.
6. Reconhecer a Infra-estrutura de Chaves Públicas (ICP) e usar os certificados digitais.
7. Descrever as técnicas, protocolos e falhas dos protocolos de segurança de Redes de Computadores sem Fio (Wireless).
8. Justificar a importância das técnicas de recuperação de dados.
9. Explicar os riscos que rondam os ambientes corporativos.
10. Identificar as principais ferramentas de análise de vulnerabilidades.
11. Descrever as principais arquiteturas de Firewall, implementando uma delas.

## CONTEÚDO PROGRAMÁTICO

1. Noções Básicas de Segurança de Dados
2. Conhecendo os Sistemas Básicos de Computação
3. Auditoria de Sistemas
4. Ferramentas de Varredura de Infra-estrutura
5. Técnicas e ferramentas de detecção de vulnerabilidades
6. Padrões de fato (COBIT e ITIL) e de direito (ISO: 27001 e 27002) de segurança corporativa
7. Noções Básicas de Criptografia
    - 7.1. Criptografia e a Infra-estrutura de Chave Pública (PKI)
    - 7.2. Criptografia Simétrica
    - 7.3. Criptografia de Chave Pública ou Assimétrica
8. Segurança em Redes sem fio
    - 8.1. Protocolos de segurança: WEP, WPA e WPA2
9. Vulnerabilidades em redes cabeadas com o uso do sniffer WireShark
10. Recuperação de Dados:
    - 10.1. Formatação Física e Lógica, Sistemas de Arquivos
    - 10.2. Estruturas lógicas, permissão de arquivos/diretórios
    - 10.3. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) e Programas de Recuperação de Dados
11. Firewall
    - 11.1. Histórico e Evolução
    - 11.2. Tipos
    - 11.3. Arquiteturas
12. Iptables (Linux Firewall)
    - 12.1. Funcionamento
    - 12.2. Políticas
    - 12.3. Implementação
13. Os riscos que rondam as organizações
14. Configuração de um servidor Web (Apache) seguro – com chave local

## METODOLOGIA DE ENSINO

Seguindo o cronograma, serão realizadas aulas expositivas utilizando recursos audiovisuais e quadro, além de aulas experimentais utilizando computadores e softwares de varredura/detecção de vulnerabilidades.

## AVALIAÇÃO DO PROCESSO DE ENSINO E APRENDIZAGEM

- Serão realizadas três avaliações, sendo duas teóricas e uma prática.

## RECURSOS NECESSÁRIOS

- Laboratório de Informática com Sistemas Operacionais: Linux e Windows instalados, além dos aplicativos necessários para o andamento da disciplina (Nagios, Wireshark, kismet, aircrack, Languard, Recuva, etc).

## BIBLIOGRAFIA

### BÁSICA


- ROCHA LYRA, MAURÍCIO. **Segurança e Auditoria em Sistemas de Informação**, 1ª edição, Ciência Moderna, 2008.
- CHAMPLAIN, J. J. **Auditing Information System**. John Wiley & Sons, 2ª edição, 2003.
- NAKAMURA, EMILIO TISSATO. **Segurança de Redes em Sistemas Cooperativos**. Editora Novatec, 2007.


### COMPLEMENTAR


- STALLINGS, WILLIAN. **Criptografia e Segurança de Redes**. Editora Prentice-Hall, 2007.
- ULBRICH, HENRIQUE CESAR; Della Valle, James. **Universidade Hacker**. Editora Digerati Books, 2009.
- DA SILVA, LINO SARLO. Public Key Infrastucture, 1ª edição, Novatec, 2004.
- MACHADO CARVALHO, ROBSON. **Certificação Digital** – Os caminhos do Documento Eletrônico no Brasil, 1ª edição, Editora Impetus, 2010.
- MARQUES, ANTÔNIO TERÊNCIO G. L. **A Prova Documental na Internet** – Validade e Eficácia do Documento Eletrônico, 1ª edição, Editora Jurua, 2005.