**Universidade Federal da Fronteira Sul**

# Plano de Ensino

## 1. Dados de Identificação

Curso: Ciência da Computação Turno: Noturno
Componente Curricular: Segurança e Auditoria de Sistemas
Fase: 9a
Ano/Semestre: 2014/2
Numero de Créditos: 4
Carga horária - Hora Aula: 72
Carga horária - Hora Relógio: 60
Professor: Emílio Wuerges
Atendimento ao aluno: segundas-feiras das 18:00h às 19:00h e terças-feiras das 18:00h às 19:00h.

## 2. Objetivo Geral do Curso

O curso tem por objetivo a formação integral de novos cientistas e profissionais da computação, os quais deverão possuir conhecimentos técnicos e científicos e serem capazes de aplicar estes conhecimentos, de forma inovadora e transformadora, nas diferentes áreas de conhecimento da Computação. Adicionalmente, os egressos do curso deverão ser capazes de adaptar-se às constantes mudanças tecnológicas e sociais, e ter uma formação ao mesmo tempo cidadã, interdisciplinar e profissional.

## 3. Ementa

Segurança em aplicações: programação segura, detecção de falhas, códigos maliciosos (malware). Segurança em sistemas operacionais: princípios de controle de acesso, sistemas confiáveis. Segurança em redes de computadores: ataques e defesas. Princípios de criptografia: criptografia simétrica e assimétrica, integridade de dados. Protocolos de autenticação: princípios, infra-estrutura de chaves públicas e aplicações, e protocolos criptográficos.

## 4. Objetivo

### 4.1 Geral

- Reconhecer e relacionar os principais riscos envolvidos no ambiente de informações e os principais pontos de controle de auditoria da tecnologia da informação no que se refere à auditoria do desenvolvimento e manutenção de sistemas, administração de dados, administração de banco de dados, e administração de redes de computadores.

### 4.2 Específicos

- Conhecer os principais mecanismos de criptografia clássica.
- Conhecer criptoanálise de criptografia clássica.
- Conhecer as principais técnicas de criptografia moderna: Funções hash, Criptografia de chave simétrica e criptografia de chave assimétrica.
- Conhecer técnicas de programação e ataques de buffer overflow.

## 5. Cronograma e Conteúdo Programático

| Horas Aula Totais | Conteúdo |
|---|---|
| 8 | Cifra de César |
| 16 | Cifra de Vigenére |
| 24 | Aritmética Modular |
| 32 | BigInt |
| 40 | AES |
| 48 | Diffie Hellmann |
| 56 | RSA |
| 64 | Buffer Overflow |
| 72 | Revisão |

## 6. Procedimentos Metodológicos (estratégias de ensino, equipamentos, entre outros)

Conduzir a disciplina através de exercícios práticos de implementação. Discutir as implicações práticas dos resultados teóricos conhecidos através de avaliação construtiva.
Reuso de código de terceiros é incentivado, entretanto a nota será proporcional ao conteúdo original.

## 7. Avaliação do Processo Ensino-Aprendizagem

Avaliação construtiva dos trabalhos de implementação. Serão feitos 9 trabalhos de implementação e 2 seminários. A média final será a média aritmética de todos os trabalhos e dos seminários.

### 7.1 Recuperação: novas oportunidades de aprendizagem e avaliação

A recuperação será feita através do retrabalho da tarefa a ser recuperada. A nota da tarefa retrabalhada substituirá a nota da tarefa original.

## 8. Referências

### 8.1 Básicas

SCHMIDT, Paulo; ARIMA, Carlos Hideo; SANTOS, José Luiz dos. Fundamentos de Auditoria de Sistemas. São Paulo: Atlas, 2006.
ONOME, J. Auditoria de Sistemas de Informação. Rio de Janeiro: Editora Atlas, 2005.
GREG, Hoglund; GARY, Macgraw. Como quebrar códigos – a arte de explorar e proteger software. São Paulo: Makron Books, 2006.
GIL, A. Auditoria de Computadores. São Paulo: Atlas 2000.

### 8.2 Complementares

MELLO, Sandro. Computação forense com software livre – conceitos, técnicas, ferramentas e estudos de casos. São Paulo: Atlas, 2009.
CARUSO, Carlos A. A.; STEFFEN, Flávio D. Segurança em Informática e de Informações. 2. ed. São Paulo: Senac, 1999.
GIL, A. L. Fraudes Informatizadas. São Paulo: Atlas, 1999.
DIAS, C. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Editora Axcel Books, 2000.
SCHMIDT, P. Fundamentos de Auditoria de Sistemas. São Paulo: Editora Atlas, 2006.