Universidade Federal da Fronteira Sul

Plano de Ensino

1. Dados de Identificação

Curso: Ciência da Computação
Turno: Diurno
Componente Curricular: Segurança e auditoria de sistemas
Fase: Oitava
Ano/Semestre: 2013.2
Numero de Créditos: 4
Carga horária - Horas Aula: 72
Carga horária - Horas Relógio: 60
Professor: Emílio Wuerges

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, infraestrutura de chaves públicas e aplicações, e protocolos criptográficos.

4. Justificativa

5. Objetivo

5.1. 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.

5.2 Específicos

Prover uma visão geral da Criptografia Convencional: técnicas clássicas e modernas;

1. Mostrar os conceitos básicos de Criptografia por Chave Pública e Funções em Hash;
2. Descrever aspectos de Segurança em redes de computadores: Assinatura Digital e Protocolos de Autenticação;
3. Apresentar a Infraestrutura de Chaves Públicas;
4. Mostrar como utilizar as técnicas de criptografia e protocolos para propiciar a Segurança de Sistemas: E-mail, IP e Web seguros. Intrusos, vírus e vermes. Firewalls.

6. Cronograma e Conteúdo Programático

Total Parc.	Encontro	Assunto
20	1 a 8	Exame detalhado da criptografia convencional e princípios de projeto, incluindo o uso desta para confidencialidade. Introdução a criptografia clássica e moderna. Introdução a criptografia assimétrica e infraestrutura de chaves públicas.
30	9 a 12	Criptografia por chaves públicas • Teoria de Números • Autenticação • Funções Hash
35	13 e 14	Protocolos de Autenticação
40	15 e 16	Assinatura Digital
55	17 a 22	Autenticação de Aplicações • Kerberos • X.509
65	23 a 26	E-mail seguro [12 horas-aula] • PGP • S/MIME • IP seguro • Web seguro (SSL e SET)
70	27 e 28	Intrusão e programas maliciosos
72	29	Filtros de Pacotes

Obs.: O plano e cronograma podem ser alterados ao longo do semestre. O aluno deve consultar as atualizações, periodicamente, através do ambiente *Moodle*.

7. Procedimentos Metodológicos

Conduzir a disciplina com aulas expositivas enquanto discutidos os itens de cunho teórico, evoluindo em tópicos específicos para exercícios práticos, demonstrações, contextualização baseada em publicações atualizadas. Uso de atividades em laboratórios com o objetivo de apresentar/exercitar os conceitos estudados.

8. Avaliação do Processo Ensino-Aprendizagem

Uso de abordagens tais como: avaliações teóricas e trabalhos de implementação.

As avaliações serão agrupadas em dois momentos (conforme instrução normativa No. 001/Prograd/2010). Notas Parciais 1 e 2 ($\mathbf{NP_1}$ e $\mathbf{NP_2}$, respectivamente).

Cada uma das notas parciais (NP_k) será **n** trabalhos escritos ($\mathbf{T_n}$). A recuperação dos trabalhos se dará através da apresentação da correção do trabalho em questão. A nota do trabalho corrigido irá substituir a nota do trabalho em recuperação. O peso de cada trabalho ($\mathbf{w_n}$) será definido de acordo com o esforço exigido por cada trabalho.

Cada uma das duas Notas Parciais será calculada da seguinte forma:

$$NP_k = \frac{\sum_{i=1}^{n} w_i T_n}{\sum_{i=1}^{n} w_i}$$

A média final (MF) será calculada como $MF = \frac{NP1 + NP2}{2}$

Em caso de se identificar plágio e/ou "cola", o aluno recebe nota zero no trabalho ou prova.

Para os trabalhos, o uso de conteúdo externo (*e.g.*, *Internet*, livros, consulta a colegas) é permitido desde que a fonte seja citada. Contudo, a nota do trabalho será proporcional ao conteúdo original.

9. Atendimento ao aluno

Horário: Quartas-feiras, das 14:00 às 15:30 (eventuais cancelamentos serão comunicados via sistema *moodle*).
Local: Sala dos professores
Fora desse horário, o(a) aluno(a) deve agendar através do e-mail: *emilio.wuerges@uffs.edu.br*

10. Referências

10.1 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.

10.2 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.