MINISTÉRIO DA EDUCAÇÃO
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
DIRETORIA DE ENSINO (DIREN)
DEPARTAMENTO DE ENSINO SUPERIOR (DEPES)
DEPARTAMENTO DE INFORMÁTICA (DEPIN)
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO (BCC)

DEPARTAMENTO	PLANO DE CURSO DA DISCIPLINA
DEPIN - Departamento Acadêmico de Informática	**SEGURANÇA DA INFORMAÇÃO**

CÓDIGO	PERÍODO	ANO	SEMESTRE	PRÉ-REQUISITOS
GCC 1922	Opt	2012	2	GCC1310 Fundamentos de Redes de Computadores GCC1415 Programação de Software para Web

CRÉDITOS	AULAS/SEMANA			TOTAL DE AULAS NO SEMESTRE
	TEÓRICA	PRÁTICA	ESTÁGIO	
4	4	0	0	72

EMENTA

Conceitos básicos de Criptografia. Aplicações de Segurança de Redes. Segurança da Informação. Políticas de Segurança da Informação.

BIBLIOGRAFIA

Bibliografia básica

1. NAKAMURA, Emilio & GEUS, Paulo, Segurança de Redes em Ambientes Corporativos, Califórnia: Berkeley, 2002.
2. MARTINS, José Carlos Cordeiro, Gestão de Projetos de Segurança da Informação, Rio de Janeiro: Brasport, 2003.
3. SÊMOLA, Marcos, Gestão da Segurança da Informação – Uma Visão Executiva, Rio de Janeiro: Campus, 2003.

Bibliografia complementar

1. SCHNEIER, Bruce. Aplied Cryptography – Algorithms, Protocols and Source Code in C. . Segunda Edição. John Wiley & Sons, Inc., Toronto, 1996.
2. ULBRICH, Henrique Cesar & DELLA VALLE, James, Universidade Hacker, 2ª edição, Rio de Janeiro: Digerati, 2003.
3. KURTZ, George, SCAMBRAY, Joel & MCLURE, Stuart, Hackers Expostos, Rio de Janeiro: Campus, 2003.
4. SILVA, Gilson Marques da. Segurança da informação para leigos: como proteger seus dados, micro e familiares na internet. Rio de Janeiro: Ciência Moderna, 2011. 136 p. ISBN 9788539901197.
5. BURNETT, Steve; PAINE, Stephen. Criptografia e segurança: o guia oficial RSA. Rio de Janeiro: Elsevier, c2002. xx, 367, il. Inclui índice. ISBN 9788535210095.
6. Normas da ABNT: ABNT NBR ISO/IEC 17799/2005; ABNT NBR ISO/IEC 27001:2013; ABNT NBR

ISO/IEC 27002:2013

OBJETIVO GERAL

Apresenta uma visão geral da área de segurança no contexto de tecnologia da informação, fazendo-o compreender os riscos de segurança existentes, tanto lógicos quanto físicos, assim como as possíveis soluções para minimizar riscos nos ambientes organizacionais.

OBJETIVOS ESPECÍFICOS

- Apresentar os conceitos básicos de tolerância a falhas e situar a segurança de sistemas nessa área.
- Apresentar os conceitos básicos específicos de segurança de sistemas.
- Apresentar os tipos de vulnerabilidades existentes, destacando as mais utilizadas pelos atacantes.
- Possibilitar ao aluno a compreensão do funcionamento das técnicas e ferramentas utilizadas pelos atacantes ao conduzir um ataque.
- Apresentar os conceitos envolvidos na criptografia de informações, bem como os principais algoritmos e protocolos criptográficos incluindo a certificação digital.
- Apresentar os conceitos e ferramentas utilizados na implantação de firewalls.
- Apresentar os conceitos e ferramentas utilizados na implantação de sistemas de detecção de intrusão.
- Possibilitar ao aluno a compreensão do processo de gestão da segurança da tecnologia da informação.
- Apresentar, de forma abrangente, os conceitos e recomendações presentes nas normas ABNT NBR ISO/IEC 27001 e 27002, que abrange praticamente todos os conteúdos da disciplina.

METODOLOGIA

- Aulas expositivas com quadro branco e recursos audiovisuais.

CRITÉRIO DE AVALIAÇÃO

A avaliação semestral envolve duas provas escritas (P1 e P2). As datas das provas são agendadas entre o professor e a turma. A média parcial (MP) será calculada pelo cômputo da média aritmética simples entre a nota P1 e P2:

$$MP = (P1 + P2) / 2$$

O aluno que faltar a uma das duas provas terá direito a uma avaliação alternativa, denominada segunda chamada, versando sobre todos os tópicos abordados no curso, e cuja data também é agendada entre docente e discentes. A nota obtida nessa 2ª chamada substituirá a da avaliação P1 ou P2 onde o aluno não esteve presente. Caso ele falte às duas avaliações, terá atribuído o grau ZERO em uma delas.

Segundo o regimento do CEFET-RJ, caso o aluno obtenha média parcial inferior a 3,0 (três e zero) estará reprovado diretamente. Graus MP maiores ou iguais a 7,0 (sete e zero) aprovam diretamente o aluno. Em situações onde o aluno tenha grau MP entre 3,0 inclusive e 7,0 exclusive, terá direito a uma prova final (PF), que, juntamente com a média parcial gerará uma nova média, denominada média final (MF). Essa média é calculada da seguinte forma:

$$MF = (MP + PF) / 2$$

Para ser aprovado, o aluno deve alcançar uma MF maior ou igual a 5,0 (cinco e zero). Caso contrário, estará

reprovado, devendo repetir a componente curricular.

CHEFE DO DEPARTAMENTO	
NOME	ASSINATURA

PROFESSOR RESPONSÁVEL PELA DISCIPLINA	
NOME	ASSINATURA

PROGRAMA

1. Conceitos básicos de Criptografia
   - 1.1. Criptografia Clássica
   - 1.2. Criptoanálise
   - 1.3. Sistemas de Chave Simétrica
     - 1.3.1.AES
     - 1.3.2.DES
   - 1.4. Sistemas de Chave Pública
     - 1.4.1.RSA
   - 1.5. Infraestrutura de Chave Pública – PKI (*Public Key Infrastructure*)
   - 1.6. Assinatura e Certificação Digital
   - 1.7. Tipos de Ataques
2. Aplicações de Segurança de Redes
   - 2.1. Kerberos
   - 2.2. X.509
   - 2.3. PGP (*Pretty Good Privacy)*
   - 2.4. SET (*Security Eletronic Transaction*)
3. Segurança da Informação
   - 3.1. Conceitos e princípios de Segurança da Informação
   - 3.2. Controle de Acesso
   - 3.3. Segurança no Desenvolvimento de Software
   - 3.4. Auditoria em Sistemas de Informação
4. Políticas de Segurança da Informação
   - 4.1. ABNT NBR ISO/IEC 17.799:2005
   - 4.2. ABNT NBR ISO/IEC 27001:2013
   - 4.3. ABNT NBR ISO/IEC 27002:2013