Universidade Federal do Ceará
Engenharia de Computação
Sistema de Presença e Planos de Aula

Plano de Ensino

Código: QXD0069 Turma: 01 - EC Disciplina: SEGURANÇA

Período: 2022.1 Créditos: 4.0 Créditos Práticos: 2.0

Professor(a): Marcos Dantas Ortiz

Justificativa:

A disciplina de Segurança visa capacitar o profissional a lidar com as mais diversas tecnologias de segurança, habilitando-o a compreender, configurar, auditar e aplicar estas tecnologias.

Ementa:

Ameaças. Segurança como atributo qualitativo de projeto de software.
Autenticação. Autorização. Integridade. Confidencialidade. Criptografia
(chaves simétricas e assimétricas). Infraestrutura de chaves públicas brasileiras (ICP-Brasil). Certificados digitais. Assinaturas digitais. Desenvolvimento de software seguro. Noções de auditoria de sistemas. Norma NBR 27002.

Objetivos Gerais e Específicos:

Segurança em sistemas; Segurança física e lógica; Controles de acesso físico e lógico; Crimes por computador; Ferramentas de ataque; Mecanismos de segurança: Proxy, Firewall, VPN, IDS etc.; Como lidar com um ataque; Protocolos de segurança; Plano de continuidade de negócios; Aspectos especiais: vírus, fraudes, criptografia, controle de acesso; Política de segurança da informação. Realização de backup e restore.

Aula	Data	Plano de Aula
1	21/03/2022	Apresentação da Disciplina Introdução a Segurança da Informação
2	22/03/2022	Conceitos de Segurança da Informação
3	28/03/2022	Serviços ou Requisitos de Segurança
4	29/03/2022	Mecanismos de Segurança: Criptografia
5	04/04/2022	Mecanismos de Segurança: Criptografia
6	05/04/2022	Mecanismos de Segurança: Criptografia
7	11/04/2022	Mecanismos de Segurança: Assinatura e Certificado Digital
8	12/04/2022	Mecanismos de Segurança: Assinatura e Certificado Digital
9	18/04/2022	Mecanismos de Segurança: Assinatura e Certificado Digital
10	19/04/2022	Ap1
11	25/04/2022	Aplicações de Segurança de Rede: Autenticação e Autorização
12	26/04/2022	Aplicações de Segurança de Rede: Autenticação e Autorização
13	02/05/2022	Aplicações de Segurança de Rede: Segurança de Emails - PGP
14	03/05/2022	Aplicações de Segurança de Rede: Segurança na Web - SSL
15	09/05/2022	Aplicações de Segurança de Rede: VPNs
16	10/05/2022	Aplicações de Segurança de Rede: VPNs
17	16/05/2022	Aplicações de Segurança de Rede: VPNs
18	17/05/2022	Aplicações de Segurança de Rede: Firewalls
19	23/05/2022	Aplicações de Segurança de Rede: Firewalls
20	24/05/2022	Aplicações de Segurança de Rede: Firewalls
21	30/05/2022	Aplicações de Segurança de Rede: Sistemas de Detecção/Prevenção de Intrusos
22	31/05/2022	Aplicações de Segurança de Rede: Sistemas de Detecção/Prevenção de Intrusos
23	06/06/2022	Aplicações de Segurança de Rede: Sistemas de Detecção/Prevenção de Intrusos
24	07/06/2022	Tipos de Ataques - Recuperação de Informações
25	13/06/2022	Tipos de Ataques - Códigos Maliciosos

26	14/06/2022	Tipos de Ataques - Códigos Maliciosos
27	20/06/2022	Desenvolvimento de Software Seguro
28	21/06/2022	Desenvolvimento de Software Seguro
29	27/06/2022	Desenvolvimento de Software Seguro
30	28/06/2022	AP2
31	04/07/2022	Apresentação Trabalho Final
32	05/07/2022	Apresentação Trabalho Final

Data da Prova Final:

18/07/2022

Metodologia de Ensino:

* Aulas teóricas expositivas;
* Aulas práticas em laboratório;
* Desenvolvimento de projetos.

Atividades Discentes:

Exigir-se-á dos alunos as seguinte atividades:
* Uso da ferramenta Moodle
* Trabalhos individuais
* Trabalhos em grupo
* Projeto final

Avaliação:

A nota final do aluno será composta pela média aritmética de três notas:
Nota 1:
Esta nota será gerada através de 1 (uma) avaliação escrita, valendo 10 (dez) pontos.
Nota 2:
Esta nota será gerada através de 1 (uma) avaliação escrita, valendo 10 (dez) pontos.
Nota 3:
Uma nota será gerada através da entrega e da apresentação de um Trabalho Final, valendo 5 (cinco) pontos.
Outra nota será gerada através de atividades práticas, realizadas em laboratório, valendo um total de 5 (cinco) pontos.
A Nota 3 final será a soma entre os resultados das duas notas anteriores.

Bibliografia Básica:

1. IIMONIANA, Joshua Onome. . Auditoria de sistemas de informação. 2. ed São Paulo: Atlas, 2008. 201 p. ISBN 8522439443

2. BEAL, Adriana. Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005. 175 p. ISBN 8522440859

3. CARUSO, Carlos A. A; STEFFEN, Flávio Deny. Segurança em informática e de informações. 3. ed., rev. e ampl. Sao Paulo: SENAC, 2006. 416 p. ISBN 9788573590968

Bibliografia Complementar:

1. WELCH-ABERNATHY, Dameon D. Check point fire wall-1 essencial: um guia de instalação, configuração e solução de problemas. Rio de Janeiro, RJ: Campus, 2002. xvii, 537 p. ISBN 8535210350

2. STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo, SP: Pearson, 2007. 492 p. ISBN 9788576051190

3. CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. Firewalls e segurança na internet: repelindo o hacker ardiloso. 2. ed. Porto Alegre: Bookman, 2005. 400 p. (Ciência da computação. Redes) ISBN 8536304294

4. NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de redes: em ambientes cooperativos. São Paulo, SP: Novatec, c2007. 482 p. : ISBN 9788575221365

5. ULBRICH, Henrique Cesar. Universidade hacker: exercícios práticos para desvendar os segredos do submundo hacker!. 2.ed. São Paulo: Digerati Books, 2009. 381 p. ISBN 978-85-7873-096-3

Recursos Didáticos:

Recursos Didáticos:
- Notebook em sala
- Projetor multimídia
- Textos
- Livros
- Laboratório de informática