PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE GRADUAÇÃO
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO

PLANO DE ENSINO

Disciplina: Segurança da Informação			
Curso: Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas			
Professor/Responsável: Ana Flávia Marinho de Lima Garrote			
Código	**Nº de Créditos**	**Pré-requisitos:**	**Co-requisito**
CMP1025	04		

EMENTA

Estudo dos aspectos de segurança e auditoria de sistemas de informação, análise de riscos, planos de contingencia e procedimentos de segurança e proteção de sistemas de informação

OBJETIVOS GERAIS

- Visão geral de segurança e auditoria de sistemas de informação (riscos, planos de contingência e outros). Autenticação, autorização, integridade e confidencialidade. Criptografia. Chave pública. Certificado digital. Assinatura digital. Protocolos. Segurança de banco de dados. Detecção e prevenção de sistemas intrusos

OBJETIVOS ESPECÍFICOS

- Conhecer os conceitos básicos de auditoria de banco de dados e auditoria computacional;
- Aprofundar o estudo na administração de serviços de redes;
- Definir estratégias para segurança de banco de dados;
- Identificar os conceitos e práticas de segurança correntes.

CONTEÚDO PROGRAMÁTICO

- Segurança computacional básica;
- Política de segurança: conceitos básicos: ameaças, ataques, vulnerabilidades, contra ataques;
- Serviços básicos: identificação, autenticação, autorização, criptografia, auditoria;
- Mecanismos de proteção: ataques comuns. Proteção: conceitos e modelos de firewall e IDS;
- Segurança em redes sem fio e experimentação;
- Implantação de uma estrutura PKI;
- Plataforma de gerenciamentos NMS;
- Backup;
- Segurança de banco de dados;
- Estratégias de defesa em BD;
- Detecção e prevenção de sistema intrusos;
- Auditoria em banco de dados;
- Auditoria computacional;
- Auditoria: legislação;
- Auditoria aplicada a computação.

METODOLOGIA

- Conteúdo expositivo;
- Resolução de exercícios;
- Desenvolvimento de projetos e trabalhos.

AVALIAÇÃO

A nota final (**NF**) da disciplina será resultante da média ponderada de dois conjuntos de notas – **N1** e **N2** – conforme a expressão **NF** = 0,4***N1**+ 0,6* **N2**, sendo que, tanto **N1** quanto **N2** serão compostas por no mínimo

duas notas resultantes de: (a) uma avaliação individual, e (b) uma ou mais atividades definidas pelo professor, sendo uma delas a AED (Atividades Externas da Disciplina) com valor de 1,0 ponto.
A **N1** e a **N2** serão calculadas conforme a expressão:

N1 = Avaliação*0,6 + Atividades*0,4
N2 = Avaliação*0,5 + Atividades*0,4 + AED *0,1

A **N2** final será composta pela **N2** resultante da expressão anterior e da nota da Avaliação Interdisciplinar (**AI**) seguindo o critério estipulado pela PROGRAD, conforme a expressão:

$N2_{FINAL}$ = **N2** * 0,9 + AI

Será considerado aprovado na disciplina o aluno que obtiver a frequência mínima de 75% e a Nota Final (**NF**) igual ou superior a 5 (cinco).

ATIVIDADE EXTERNA DA DISCIPLINA

a. Objetivo da atividade:

Aplicação prática do conteúdo visto na disciplina abrangendo Fundamentos de Segurança da Informação, Criptografia e Certificação Digital

b. Descrição da Atividade:

Instalação e configuração de um servidor Web Apache com acesso seguro (HTTPS), utilizando a ferramenta OpenSSL para criar um certificado digital auto assinado. A implementação deve ser feita em máquina virtual (VirtualBox), devendo ser gerada a documentação dos procedimentos realizados.

c. Cronograma:

Inicio: 01/11/2017

Término: 09/12/2017

d. Forma de Registro:

Elaboração de um relatório com a descrição detalhada de todo o desenvolvimento do trabalho e entregar em arquivo digital.

OBS: O trabalho será feito em grupos de até 4 componentes.

BIBLIOGRAFIA BÁSICA

1. SILBERSCHATZ, Abraham. Sistema de banco de dados. 3. ed. São Paulo: Makron, 1999. 778 p
2. STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008. 792 p
3. TANENBAUM, Andrew S. Computer networks. 4. ed. New Jersey: Prentice Hall, 2003. 891 p

BIBLIOGRAFIA COMPLEMENTAR

1. ALBUQUERQUE, Ricardo. Segurança no desenvolvimento de software. Rio de Janeiro: Campus, 2002
2. ALVES, Gustavo A. Segurança da informação: uma visão inovadora da Gestão. 1. ed. Ciência Moderna. 2005
3. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: NBR ISO/IEC 27001. Tecnologia da informação: Técnicas de segurança, sistemas de gestão de segurança da informação, requisitos

4. BURGESS, Mark. Princípios de administração de redes e sistemas. 2. ed. Rio de Janeiro: LTC, c2006. 455 p

5. NORTHCUTT, Stephen. Desvendando segurança em redes. Rio de Janeiro: Campus, 2002. 650 p

4. KUROSE, Janes; ROSS, Keith. Computer Networking: a top-down approach. 6. ed. New York: Addison Wesley, 2012

5. NEMETH, E.; SNYDER, G.; HEIN, T. Manual de administração do Linux. 2. ed. São Paulo: Prentice Hall, 2007.

CRONOGRAMA

Encontro	Data	Conteúdos/Atividades/Avaliações
1	09/08	Apresentação do Plano de Ensino
2	12/08	Conceitos iniciais de segurança da informação
3	16/08	Vulnerabilidades, ameaças e ataques
4	19/08	Vulnerabilidades, ameaças e ataques (continuação)
5	23/08	Ferramentas para detecção de vulnerabilidades
6	26/08	Políticas de segurança
7	30/08	Políticas de segurança
8	02/09	Elaboração de política de segurança
9	06/09	Elaboração de política de segurança
10	13/09	Norma ISO 27002
11	16/09	Norma ISO 27002
12	20/09	Aplicando a Norma ISO 27002 na gestão de SI
13	23/09	Criptografia - Definições e conceitos
14	27/09	Criptografia Simétrica - Definições e conceitos
15	30/09	Exercícios
16	**04/10**	**N1**
17	07/10	Algoritmos de criptografia simétrica
18	11/10	Criptografia Assimétrica - Definições e conceitos
19	**18/10**	**III Congresso de Ciência e Tecnologia da PUC Goiás**
20	21/10	Algoritmos de criptografia assimétrica
21	25/10	Hashing - Conceitos e Aplicações
22	28/10	Início da AED
23	01/11	Assinaturas Digitais
24	08/11	Certificados Digitais
25	11/11	PKI - Public Key Infrastructure
26	18/11	Vulnerabilidades em aplicações Web
27	22/11	Segurança de bancos de dados
28	**25/11**	**II Jornada Científica da ECEC – JCECEC**
29	29/11	Melhores práticas para configurações seguras de SGBD
30	02/12	Detecção e prevenção de sistema intrusos
31	06/12	Auditoria
32	09/12	Auditoria - Entrega da AED
33	13/12	Exercícios
34	**16/12**	**N2**
35	20/12	Entrega dos resultados
36 - 40	AED – (10h)	

MATERIAL DE APOIO

www.cert.br
www.sans.org
www.owasp.org