MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE _____

Coordenação do Curso de ou Departamento de_____

Ficha 2 (variável)

Disciplina: **Segurança de Sistemas Computacionais**	Código: **DEE345**
Natureza: (x) Obrigatória ( ) Optativa	(x) Semestral ( ) Anual ( ) Modular
Pré-requisito:	Co-requisito:	Modalidade: ( ) Totalmente Presencial (x) Totalmente EAD ( ) Parcialmente EAD: _____ *CH

CH Total: 30 CH Semanal: 2	Padrão (PD): 30	Laboratório (LB):	Campo (CP):	Estágio (ES):	Orientada (OR):	Prática Específica (PE):	Estágio de Formação Pedagógica (EFP):
Prática como Componente Curricular (PCC): Atividade Curricular de Extensão (ACE):							

Indicar a carga horária semestral (em PD-LB-CP-ES-OR-PE-EFP-EXT-PCC)

*indicar a carga horária que será à distância.

EMENTA

Visão geral sobre auditoria de sistemas. Segurança de sistemas. Políticas de segurança. Privacidade na era digital. Análise de riscos em sistemas de informação. Aspectos especiais: vírus, criptografia, acesso não autorizado, ataques. Implementar mecanismos de garantia de segurança. Firewall, mecanismos de criptografia: simétrica e assimétrica, assinatura digital, certificados digitais. Plano de contingência organizacional. Metodologias de auditoria. Técnicas de avaliação de sistemas.

PROGRAMA

1. Conceitos básicos: princípios e propriedades fundamentais para segurança computacional; ameaças, vulnerabilidades e ataques; base de computação confiável;

2. Introdução à criptografia: cifragem simétrica e assimétrica; hashes; assinaturas digitais; certificados; infraestruturas de chaves públicas;

3. Autenticação: local; em rede; distribuída;

4. Controle de acesso: políticas; modelos; mecanismos;

5. Segurança de sistemas e aplicações: ataques contra sistemas e mecanismos de defesa; segurança de sistemas; segurança em aplicações Web; desenvolvimento seguro;

6. Segurança em redes: filtragem de pacotes; firewalls; DMZ; ataques contra redes; protocolos de segurança;

7. Auditoria: logs; testes de invasão; detecção de intrusão; antivírus; análise de malware;

8. Gestão da segurança: normas e padrões; gerenciamento de vulnerabilidades; ética em segurança.

Aula 1: Apresentação da disciplina,ficha 1 e 2 turma

Aula 2: Introdução

Aula 3: Fundamentos de Segurança

Aula 4: Criptografia

Aula 5: Autenticação

Aula 6: Trabalho prático

Aula 7: controle de acesso

Aula 8: Pesquisa

Aula 9: Ferramentas livres de segurança

Aula 10: Ataque e Defesa

Aula 11: Firewall, DMZ, filtragem de pacotes

Aula 12: Logs e detecção

Aula 13: Normas

Aula 14: Seminário

Aula 15: Palestra de encerramento

OBJETIVO GERAL

O aluno deve ser capaz de pensar criticamente sobre os problemas de segurança a que um sistema ou rede estão suscetíveis e soluções possíveis para mitigá-los. Deve também ser capaz de buscar formas de identificar ameaças e vulnerabilidades, planejar a implementação de soluções para defesa e gerenciar o processo de manutenção de segurança.

OBJETIVO ESPECÍFICO

1. Entender o que é segurança computacional e os princípios fundamentais que norteiam a área;

2. Identificar ameaças, vulnerabilidades e ataques contra sistemas, redes e informação;

3. Aprender conceitos introdutórios sobre criptografia, mecanismos que a implementam e suas aplicações em segurança;

4. Compreender os mecanismos utilizados para prover autenticação e controle de acesso em sistemas e redes;

5. Estudar ataques clássicos e modernos de forma a entender como são feitos, que vulnerabilidades exploram e por que funcionam;

6. Conhecer o funcionamento dos mecanismos de defesa utilizados em sistemas e redes;

7. Instalar e configurar mecanismos de defesa tradicionais para analisar sua eficácia, eficiência e limitações;

8. Implementar ferramentas para varredura de vulnerabilidades, automatização de ataques e/ou detecção de ameaças;

9. Utilizar ferramentas (defensivas e ofensivas) para gerenciamento de vulnerabilidades em um sistema/rede: configuração, instalação, execução, atualização, monitoramento;

10. Conhecer as normas e padrões que regem a segurança da informação e estudar conceitos éticos sobre pesquisa, desenvolvimento e atuação na área.

PROCEDIMENTOS DIDÁTICOS

A disciplina será desenvolvida mediante aulas expositivas para apresentação dos conteúdos curriculares teóricos ou demonstrações feitas pelo professor, e através de atividades de laboratório nas quais as ferramentas e mecanismos serão implementados ou instalados, bem como avaliados na prática em ambiente controlado. Serão utilizados quadro branco, computador e projetor multimídia, computadores com sistema operacional GNU/Linux e ferramentas livres específicas para estudar cada conceito aplicável em laboratório

FORMAS DE AVALIAÇÃO

Parte Teórica:

N_aval = AVAL1 + AVAL2

Onde

Aval1 = Nota obtida na avaliação 1

Aval2 = Nota obtida na avaliação 2

N_aval = Média das nota obtidas nas avaliações teóricas 1 e 2;

Parte Prática:

A avaliação será composta pelos trabalhos desenvolvidos e apresentados durante as aulas.

Sendo entre eles, desenvolvido uma pesquisa, um trabalho escrito e uma apresentação oral do trabalho.

Nota final: Nf=

Onde NF= Nota final obtida na disciplina

N_Aval = Nota da Parte Teórica

N_prat = Nota da Parte Prática

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

GOODRICH, Michael T.; TAMASSIA, Roberto. Introdução à segurança de computadores. Bookman, 2013.

FONTES, Edison. Políticas e Normas para a Segurança da Informação. Brasport, 2012.

TANENBAUM, Andrew S. Redes de computadores. São Paulo: Pearson, [2011]. xvi, 581 p., il., grafs., tabs. Inclui bibliografia e índice.

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

REZENDE, Pedro Antonio Dourado. Criptografia e segurança na informática. Apostila-Capítulos, v. 1, n. 2, p. 3, 1998.

ESCOLA SUPERIOR DE REDES. Administração de Sistemas Linux: redes e segurança. 1.ed. rev Rio de Janeiro: RNP/ESR, 2013. 228p.,

CASSARRO, Antonio Carlos. Controles internos e segurança de sistemas: prevenindo fraudes e tornando auditáveis os sistemas. São Paulo: LTr, 1997. 196 p.

KIM, David. Fundamentos de segurança de sistemas de informação. Rio de Janeiro: LTC, 2014. 386p

Documento assinado eletronicamente por **JEFER BENEDETT DORR**, **PROFESSOR DO MAGISTERIO SUPERIOR**, em 29/11/2021, às 15:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **4073929** e o código CRC **CDF12883**.