Ministério da Educação
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
Campus Pato Branco

PLANO DE ENSINO

CURSO	195 - Engenharia de Computação	MATRIZ	535

FUNDAMENTAÇÃO LEGAL	Resoluções n°89/08- COEPP - n°153/09- COEPP - n°158/10- COEPP

DISCIPLINA/UNIDADE CURRICULAR	CÓDIGO	PERÍODO	CARGA HORÁRIA (aulas)					
			AT	AP	APS	AD	APCC	Total
Segurança Computacional	SC28CP	9º	51	17	04	00	00	72

AT: Atividades Teóricas, AP: Atividades Práticas, APS: Atividades Práticas Supervisionadas, AD: Atividades a Distância, APCC: Atividades Práticas como Componente Curricular.

PRÉ-REQUISITO	Redes de Computadores 1
EQUIVALÊNCIA	

OBJETIVOS
Compreender os mecanismos de ameaças aos sistemas computacionais. Identificar e aplicar mecanismos de prevenção contra falhas e possíveis ataques. Compreender conceitos e mecanismo de segurança como: criptografia, autenticação, assinatura digital e firewall. Gerenciar a segurança em sistemas computacionais.

EMENTA
Segurança lógica, física e ambiental; políticas de segurança; vulnerabilidade; mecanismos de segurança: autenticação, assinatura digital, firewall, criptografia; ameaças e contramedidas em um sistema computacional; aplicação de solução de segurança em estudo de caso.

CONTEÚDO PROGRAMÁTICO

ITEM	EMENTA	CONTEÚDO
1	Segurança lógica, física e ambiental	Mecanismos de proteção baseados em software para proteção de dados, programas e sistemas, contra tentativas de acessos não autorizados. Proteção das vias de acesso ao ambiente e equipamentos, contra usuários não autorizados. Prevenção de danos por causas naturais.
2	Políticas de segurança	Definição, planejamento e pontos importantes a serem tratados sobre política de segurança. Política para senhas, firewall e acesso remoto. Política de segurança em ambientes cooperativos.
3	Vulnerabilidade	Definição de Vulnerabilidade. Análise de vulnerabilidades em sistemas.
4	Mecanismos de segurança: criptografia, autenticação, assinatura digital, firewall;	O Papel da Criptografia, Criptografia de Chave Simétrica, Criptografia de Chave Pública e gerenciamento de Chaves. Autenticação de mensagens, funções de autenticação. Assinatura Digital e protocolos de autenticação: autenticação mútua e autenticação unidirecional. Princípios de projeto de Firewall, arquiteturas de Firewall.
5	Ameaças e contramedidas em um sistema computacional	Definição de ameaças e contramedidas. Utilização de contramedidas para diminuição de riscos e ameaças.
6	Aplicação de solução de segurança em estudo de caso.	Avaliar e aplicar ferramentas e mecanismos de segurança em sistemas de informações.

PROCEDIMENTOS DE ENSINO

AULAS TEÓRICAS

Aulas ministradas em sala de aula, nas quais a ênfase está em explicações conceituais.

AULAS PRÁTICAS

Aulas centradas na realização de atividades práticas pelos alunos com supervisão, orientação e auxílio do professor; aulas em que o professor realiza a resolução tutorada de exercícios (o professor conduz a resolução que é acompanhada pelos alunos); aulas em que o professor exemplifica a resolução de exercícios. As aulas práticas incluem aulas de laboratório que são realizadas em ambientes específicos em que há uso de equipamentos e materiais que permitem a experimentação.

ATIVIDADES PRÁTICAS SUPERVISIONADAS

Atividades acadêmicas desenvolvidas sob a orientação, supervisão e avaliação de docentes e realizadas pelos discentes em horários diferentes daqueles destinados às atividades presenciais (aulas teóricas e aulas práticas). Estas atividades incluem: estudos dirigidos, trabalhos individuais, trabalhos em grupo, desenvolvimento de projetos, atividades em laboratório, atividades de campo, oficinas, pesquisas, estudos de casos, seminários, desenvolvimento de trabalhos acadêmicos, dentre outras. Deverá ser dada ênfase à realização de atividades em grupo que envolva pesquisa e seja interdisciplinar.

PROCEDIMENTOS DE AVALIAÇÃO

Considerar-se-á aprovado na disciplina, o aluno que tiver frequência igual ou superior a 75% (setenta e cinco por cento) e Nota Final igual ou superior a 6,0 (seis), consideradas todas as avaliações previstas no início do semestre.
No caso do aluno perder alguma avaliação presencial e escrita, por motivo de doença ou força maior, poderá requerer uma única segunda chamada por avaliação, no período letivo. O requerimento deve ser protocolado no Departamento de Registros Acadêmicos dentro do prazo estabelecido pelo regulamento da UTFPR, a prova será aplicada após o deferimento. Para a prova de segunda chamada o professor definirá os conteúdos e a data da avaliação.

REFERÊNCIAS

Referencias Básicas:

- STALLINGS, WILLIAM. **Criptografia e segurança de redes:** princípios e práticas. 4. ed. São Paulo, SP: Pearson Prentice Hall, 2008.
- NAKAMURA, Emilio T. ; GEUS, Paulo L. **Segurança de Redes em ambientes cooperativos.** São Paulo, SP: Novatec Editora, 2007.
- COULOURIS, George F.; DOLLIMORE, Jean; KINDBERG, Tim. **Sistemas distribuídos: conceitos e projeto.** 4. ed. Porto Alegre: Bookman, 2007

Referências Complementares:

- BISHOP, Matt. **Computer Security: art and science**. Boston: Addison-Wesley, 2003.
- GOLLMANN, Dieter. **Computer Security.** 3. Ed. United Kingdom, UK: John Wiley & Sons, 2011.
- SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital.** Rio de Janeiro: Campus, 2001.
- MELO, Sandro; TRIGO, Clodonil, H.. **Projeto de Segurança em Software Livre.** Rio de Janeiro: Alta Books, 2004
- LUCCHESI, Claudio L.. **Introdução à criptografia computacional.** Campinas: Papirus, 1986.

ORIENTAÇÕES GERAIS

As datas das avaliações, exceto as de segunda chamada, serão estabelecidas em sala de aula no início do semestre. O uso de aparelhos celulares deve ser feito somente fora de sala de aula. A utilização de notebook apenas em caso de necessidade em atividades da disciplina.

Assinatura do Professor

Assinatura do Coordenador do Curso