



Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística
Programa de Pós-Graduação em Ciência da Computação



Plano de Ensino

1) Identificação

Disciplina: INE 6608000 – Segurança em Sistemas Distribuídos

Carga horária: 45 horas/aula

Professora: Carla Merkle Westphall

2) Requisitos: não há.

3) Ementa:

Conceitos básicos de sistemas distribuídos e segurança. Normas de segurança relacionadas. Vulnerabilidades de softwares. Requisitos para construção de sistemas seguros. Estudos de caso: segurança em ambientes distribuídos.

4) Objetivos:

Geral: Compreender os principais problemas existentes e possíveis soluções para a segurança de sistemas distribuídos.

Específicos:

- Compreender os conceitos básicos de sistemas distribuídos e segurança;
- Identificar os principais problemas e desafios de segurança;
- Conhecer aspectos de normas de segurança relacionadas para identificar requisitos exigidos;
- Entender os requisitos para construção de sistemas distribuídos seguros;

Observar a concretização dos requisitos em alguns estudos de caso.

5) 1. Conteúdo Programático:

- 1.1. Conceitos básicos de sistemas distribuídos e segurança
 - 1.1.1. Conceito de sistemas distribuídos
 - 1.1.2. Conceito de segurança
 - 1.1.3. Questões de Segurança
 - 1.1.3.1. Confidencialidade
 - 1.1.3.2. Integridade
 - 1.1.3.3. Disponibilidade
 - 1.1.3.4. Autenticação
 - 1.1.3.5. Autorização
 - 1.1.3.6. Confiança
 - 1.1.3.7. Privacidade
 - 1.1.3.8. Gerenciamento de Identidades
 - 1.1.4. Mecanismos Comuns
 - 1.1.4.1. Criptografia

- 1.1.4.2. Assinatura Digital
- 1.1.4.3. Mecanismos de autenticação
- 1.1.4.4. Mecanismos de controle de acesso
- 1.1.4.5. Firewalls e Sistemas de Detecção de Intrusão
- 1.1.5. Desafios de segurança em sistemas distribuídos

- 1.2. Normas de segurança relacionadas
 - 1.2.1. Norma ISO/IEC 15408

- 1.3. Vulnerabilidades existentes em aplicações
 - 1.3.1. Problemas de ambientes Web

- 1.4. Requisitos para construção de sistemas distribuídos seguros
 - 1.4.1. Segurança da comunicação (criptografia)
 - 1.4.2. Autenticação
 - 1.4.3. Autorização – Modelos de Segurança
 - 1.4.4. Delegação de privilégios, Auditoria, Não-Repudiação

- 1.5. Estudos de caso: segurança em ambientes distribuídos

6) Metodologia:

As aulas serão expositivas e dialogadas com a realização de exercícios de fixação e de avaliação. Alguns exercícios serão práticos. Também serão feitas leituras de textos e artigos científicos, com discussões em sala de aula.

7) Avaliação:

A avaliação dos alunos será baseada:

- na realização de exercícios para verificação do aprendizado;
- na apresentação de seminários sobre o estado da arte de algum dos assuntos da ementa da disciplina;
- na elaboração e apresentação de um artigo final sobre segurança.

Nos seminários, os critérios de avaliação a serem utilizados serão: (i) a clareza da apresentação, (ii) a habilidade na exposição dos conteúdos; (iii) a qualidade do material elaborado; e (iv) a capacidade de argumentação e discussão oral.

A avaliação do artigo utilizará como critérios: (i) a clareza e a coerência do texto; (ii) a correção gramatical; (iii) a correção dos conceitos apresentados; (iv) o encadeamento lógico da redação; e (v) a capacidade de interpretação e discussão, todos os itens com o mesmo peso.

A média final (MF) será dada por: $MF = (N1 + N2 + N3) / 3$

Onde:

- N1: média aritmética dos exercícios de verificação
- N2: média dos seminários
- N3: nota do artigo

O conceito do aluno na disciplina será definido a partir da média final utilizando-se da tabela de equivalência abaixo:

Conceito	Significado	Nota
A	Excelente	9,0 – 10,0
B	Bom	8,0 – 8,9
C	Regular	7,0 – 7,9
D	Insuficiente	< 7,0
I	Incompleto	---

Será considerado aprovado o aluno que obtiver conceito final igual ou superior a “C” e frequência igual ou superior a 75% da carga horária da disciplina, obtendo os créditos equivalentes da disciplina.

8) Cronograma:

9) Bibliografia:

- **Bibliografia Básica**

- BELAPURKAR, A; et al. Distributed Systems Security: Issues, Processes and Solutions. Wiley, 2009.
- COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; BLAIR, Gordon. Distributed Systems: Concepts and Design. Fifth edition. Addison-Wesley, 2011.
- GOLLMANN, Dieter. Computer Security. John Wiley and Sons, Third edition, 2011.
- HARRIS, Shon. CISSP Certification All-in-One Exam Guide. Sixth Edition. McGraw-Hill/Osborne, 2012.

- **Bibliografia Complementar**

- OWASP. Projeto OWASP (The Open Web Application Security Project). Disponível em <http://www.owasp.org>
- Artigos científicos sobre o assunto, disponíveis no portal da IEEE: <http://www.computer.org>