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: INE410120 - Tópicos Especiais em Ciência da Computação: Infraestrutura de Chaves Públicas e Aplicações

Carga horária: 45 horas/aula – 3 créditos

Professora: Ricardo Felipe Custódio

2) Requisitos: não há.

3) Ementa:

Algoritmos Criptográficos. Modelos de ICP: X.509, PGP, IBE, Certificateless. Autoridades Certificadora (AC) e de Registro (AR). Políticas e Declaração de Práticas de Certificação. Autoridade de Gerenciamento de Políticas de Certificação. Certificados de Atributos. Carimbos do Tempo. Sistemas de Gerenciamento de Certificados Digitais. Lista de Certificados Revogados. OCSP. ICP-Brasil. Repositórios de Certificados e Lista de Serviços Confiáveis (TSL). Padrões de Assinatura Digital: CAdES, XAdES, PAdES, Padrão Brasileiro de Assinatura Digital (PBAD). Exemplos de aplicações.

4) Objetivos:

Geral: Compreender os modelos e principais componentes de uma infraestrutura de chaves públicas.

Específicos:

- Entender as técnicas criptográficas usadas em ICP
- Identificar os principais desafios na implantação de uma ICP
- Conhecer as principais normas e padrões existentes sobre ICP
- Saber implantar ICPs
- Conhecer os requisitos necessários para o uso dos serviços de ICP em aplicações

5) Conteúdo Programático:

5.1 Algoritmos Criptográficos. [2 horas]
5.2 Modelos de ICP: X.509, PGP, IBE, Certificateless. [4 horas]
5.3 Autoridades Certificadora (AC) e de Registro (AR). [2 horas]
5.4 Políticas e Declaração de Práticas de Certificação e Autoridade de Gerenciamento de Políticas de Certificação. [4 horas]
5.5 Certificados de Atributos. [2 horas]
5.6 Carimbos do Tempo. [2 horas]
5.7 Sistemas de Gerenciamento de Certificados Digitais. [4 horas]

5.8 Lista de Certificados Revogados, OCSP e outros mecanismos de verificação de status de certificados digitais. [2 horas]
ICP-Brasil. [4 horas]
Repositórios de Certificados e Lista de Serviços Confiáveis (TSL). [2 horas]
Padrões de Assinatura Digital: CAdES, XAdES, PAdES, Padrão Brasileiro de Assinatura Digital (PBAD). [4 horas]
Exemplos de aplicações. [13 horas]

6) Metodologia:

As aulas serão expositivas e dialogadas com a realização de exercícios de fixação e de avaliação e aulas práticas em laboratório.

7) Avaliação:

Haverá um conjunto de até seis trabalhos individuais (TI).

A média final (MF) será dada pela média das notas dos trabalhos individuais.

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 freqüência igual ou superior a 75% da carga horária da disciplina, obtendo os créditos equivalentes da disciplina.

8) Cronograma:

9) Bibliografia:

- **Bibliografia Básica**

- Adams, Carlisle; Loyd, Steve. Understanding PKI: Concepts, Standards, and Deplyment Considerations. 2o. Ed., 2002.
- Cooper et. Al. RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. 2008.

- **Bibliografia Complementar**

- Artigos científicos sobre o assunto, disponíveis da Capes.