

Plano de Ensino

1) Identificação

Disciplina: INE5680 - Segurança da Informação e de Redes
Turma(s): 07238
Carga horária: 72 horas-aula Teóricas: 44 Práticas: 28
Período: 1º semestre de 2023

2) Cursos

- Sistemas de Informação (238)

3) Requisitos

- Sistemas de Informação (238) (currículo: 20001)
 - INE5625 - Computação Distribuída
- Sistemas de Informação (238) (currículo: 20111)
 - INE5615 - Redes de Computadores
 - INE5645 - Programação Paralela e Distribuída

4) Professores

- Carla Merkle Westphall (carla.merkle.westphall@ufsc.br)
- Ricardo Felipe Custodio (ricardo.custodio@ufsc.br)
- Jean Everson Martina (jean.martina@ufsc.br)
- Wyllian Bezerra da Silva (wyllian.bs@ufsc.br)
- Bobiquins Estêvão de Mello (estevao.mello@ufsc.br)

5) Ementa

Introdução à Segurança. Conceitos básicos. Técnicas clássicas de criptografia. Criptografia Simétrica. Acordo de chave de Diffie-Hellman. Criptografia de Chave Pública. Gerenciamento de chaves públicas. Funções Hash. Assinaturas Digitais. Certificação Digital. Protocolos de Autenticação. Protocolos Criptográficos. Segurança de aplicações. Redes Privadas Virtuais. Tecnologias disponíveis para defesa. Gestão da Segurança da Informação.

6) Objetivos

Geral: Apresentar os principais desafios, abordagens e técnicas para implementar, desenvolver e manter a segurança da informação nos sistemas e redes.

Específicos:

- Conhecer fatos e problemas sobre segurança computacional.
- Conhecer os fundamentos para gestão de segurança da informação.
- Compreender conceitos, princípios, mecanismos e métodos para segurança.
- Aplicar algoritmos de criptografia.
- Especificar protocolos criptográficos básicos.
- Empregar ferramentas que servem de suporte à segurança computacional.

7) Conteúdo Programático

7.1) Introdução [4 horas-aula]

- Conceitos Básicos
 - Propriedades Fundamentais
 - Vulnerabilidades, Ameaças, Riscos, Ataques
- Segurança nas Organizações
 - Políticas de Segurança
 - Normas de Segurança

7.2) Criptografia Simétrica [8 horas-aula]

- Princípios básicos
- Algoritmos de Fluxo
- Algoritmos de Bloco

- Modos de Operação
- 7.3) Funções Hash, MAC, Criptografia Autenticada, Derivação de Chaves [6 horas-aula]
 - Hash sem chave
 - Hash com chave (MAC - Message Authentication Code)
 - Tipos de MAC
 - Criptografia Autenticada
 - Modos e Padrões de Criptografia Autenticada
 - Derivação de chaves
- 7.4) Criptografia Assimétrica [10 horas-aula]
 - Princípios básicos
 - Certificados digitais
 - Padrão X.509
 - Algoritmos assimétricos
 - Assinatura Digital
 - Infra-estrutura de chaves públicas
- 7.5) Gerenciamento e Distribuição de Chaves [4 horas-aula]
 - Protocolo Diffie-Hellman
 - Distribuição de Chaves usando Criptografia Simétrica
 - Kerberos
 - Distribuição de Chaves usando Criptografia Assimétrica
- 7.6) Protocolos criptográficos [4 horas-aula]
 - Princípios básicos
 - Protocolos básicos
 - Protocolos de troca de chaves
 - Protocolos de autenticação
 - TLS (Transport Layer Security)/SSL (Secure Socket Layer)
- 7.7) Autenticação [4 horas-aula]
 - Princípios
 - Mecanismos de autenticação
 - Protocolos com criptografia simétrica
 - Protocolos com criptografia assimétrica
 - Gerenciamento de identidades
- 7.8) Segurança da Rede e de Sistemas [4 horas-aula]
 - Tipos de Ataques
 - Varredura de Portas e Serviços
 - Análise de Vulnerabilidades em Serviços
 - Segurança de Servidor Web
 - Segurança de Redes Sem Fio
 - Segurança de Email
 - Firewall
 - Redes Privadas Virtuais
- 7.9) Atividades práticas [28 horas-aula]

8) Metodologia

As aulas serão expositivas, intercaladas por aulas de laboratório, onde os alunos realizarão atividades práticas individuais ou em grupos. Algumas aulas teóricas, expositivas serão gravadas e disponibilizadas via Moodle aos alunos. Algumas aulas práticas serão feitas remotamente caso os laboratórios de informática não apresentem condições de trabalho, mas com a entrega via Moodle de relatórios das atividades. Além disso, para cada tema relevante, será solicitado um trabalho individual, que terá uma parte teórica e outra prática a ser feita pelo aluno. Também haverá um trabalho a ser realizado em grupos de 2 ou 3 alunos sobre um tema atual de segurança em computação, procurando manter o grupo e a turma cientes do estado da arte da área.

A disciplina será acompanhada por estagiário de docência, que é aluno de mestrado regularmente matriculado no PPGCC da UFSC

9) Avaliação

Serão aplicadas duas provas teóricas P1 e P2, um conjunto entre 3 e 6 trabalhos individuais cuja média forma a nota TI, e um trabalho em grupo TG. A média final será dada por $MF = (P1 + P2 + TI + TG)/4$. Os requisitos e critérios de avaliação dos trabalhos individuais serão postados no Moodle.

Conforme parágrafo 2º do artigo 70 da Resolução 17/CUn/97, o aluno com frequência suficiente (FS) e média final no período (**MF**) entre 3,0 e 5,5 terá direito a uma nova avaliação ao final do semestre (**REC**), sendo a nota final (**NF**) calculada conforme parágrafo 3º do artigo 71 desta resolução, ou seja: $NF = (MF + REC) / 2$.

10) Cronograma

A primeira prova teórica será aplicada após a finalização do conteúdo de Identidade e Certificação Digital. A segunda prova antes o início do trabalho em grupo. As datas para entregas dos trabalhos individuais e do trabalho em grupo serão postadas no Moodle. A prova de recuperação será na última semana de aula.

11) Bibliografia Básica

- B. Preneel, C. Paar, and J. Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer, 2009. (Disponível online no link: <http://link.springer.com/book/10.1007%2F978-3-642-04101-3>)
- Svetlin Nakov. Practical Cryptography for Developers. 2018. ISBN: 978-619-00-0870-5 (9786190008705). (Disponível online no link: <https://cryptobook.nakov.com/>)

12) Bibliografia Complementar

- Criptografia e Segurança de Redes, William Stallings, 4 Edição, Prentice-Hall, 2008.
- A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, October 1996. (Disponível online no link: <http://cacr.uwaterloo.ca/hac/index.html>)
- Ivo de Carvalho Peixinho; Francisco Marmo da Fonseca; Francisco Marcelo Lima. Segurança de Redes e Sistemas. RNP/ESR, 2013. (Disponível online no link: <http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas>)