



Plano de Ensino

1) Identificação:

Disciplina: INE xx – Segurança da Informação e de Redes I

Carga horária: 45 h/a (**atividades não presenciais síncronas**)

Créditos: 3 créditos

Professor(a): Carla Merkle Westphall (carla.merkle.westphall@ufsc.br)

Período: 2º semestre de 2021

Horário da disciplina: 5ª feira (18:30h-20:10h) e 6ª feira (20:20h-22:00h).

Esta disciplina é ministrada em conjunto com a disciplina INE5680, Segurança da Informação e de Redes, do Bacharelado de Sistemas de Informação da UFSC.

2) Requisitos:

Esta disciplina requer que o aluno tenha conhecimentos de programação pois serão realizados trabalhos práticos de desenvolvimento usando biblioteca criptográfica.

3) Ementa:

Introdução à Segurança. Conceitos básicos. Segurança de aplicações. Técnicas clássicas de criptografia. Criptografia Simétrica. Funções Hash. Derivação de chaves. Autenticação.

4) 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;
- Compreender conceitos, princípios, mecanismos e métodos básicos de segurança;
- Aplicar algoritmos de criptografia;
- Empregar ferramentas que servem de suporte à segurança computacional;
- Pesquisar temas relevantes de pesquisa na área.

5) Conteúdo Programático

1. Introdução [6 horas-aula]

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

2. Criptografia Simétrica [8 horas-aula]

- Princípios básicos
- Algoritmos de Fluxo
- Algoritmos de Bloco
- Modos de Operação

3. Funções Hash, MAC, Criptografia Autenticada, Derivação de Chaves [8 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

4. Autenticação [4 horas-aula]

- Princípios
- Mecanismos de autenticação
- Gerenciamento de identidades

5. 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

6. Desenvolvimento de experimentos práticos e estudos de caso [15 horas-aula]

6) Metodologia

Será utilizado o ambiente virtual do Moodle (ou Google Meet parceria da UFSC) para atividades síncronas online. As atividades síncronas podem ser aulas via webconferência (Moodle ou Google Meet), apresentação de trabalhos via webconferência, discussão via chat, webinar ao vivo. Nas aulas síncronas via webconferência serão apresentados os tópicos do conteúdo programático usando os slides que são disponibilizados no moodle. Também serão feitas demonstrações práticas de exemplos e exercícios. As aulas síncronas podem ser usadas para resolução de exercícios e de dúvidas. Também estão previstas atividades assíncronas que podem ser trabalhos em grupo a distância ou individuais, visualização de webinar gravado ou visualização de vídeo aula gravada. A comunicação com os alunos será feita usando o email, o fórum da disciplina no Moodle e o momento das aulas síncronas. Todo o material da disciplina como os slides, referências, definições de trabalhos e links para consulta serão disponibilizados no Moodle. As aulas síncronas via webconferência, sempre que possível, serão gravadas e disponibilizadas aos alunos. Caso o professor tenha problemas de conexão com a Internet ou queda de energia durante as atividades síncronas, será combinada uma forma de reposição: através de gravação de conteúdo a ser disponibilizado aos alunos ou através de atividade assíncrona no moodle.

Controle de frequência

O controle de frequência será realizado pelo professor em todas as aulas síncronas. Será exigido o mínimo de 75% de frequência nas aulas síncronas. A presença das aulas síncronas via webconferência será computada no moodle (registro de presença). A presença nas aulas síncronas

também poderá ser computada com a entrega de eventual atividade no moodle. Nas atividades assíncronas a presença será computada pela entrega de atividades definidas.

7) Avaliação

Os alunos serão avaliados através dos seguintes Instrumentos de Avaliação:

- Prova (peso 4)
- Tarefa prática sobre segurança da rede e de aplicações (peso 2)
- Tarefa prática de implementação com biblioteca criptográfica (peso 2)
- Seminário (peso 2)

8) Bibliografia

1. 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>)
2. David Hook and Jon Eaves. Java Cryptography: Tools and Techniques. 2020, Lean Publishing.
3. 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>)
4. Svetlin Nakov. Practical Cryptography for Developers. 2018. ISBN: 978-619-00-0870-5 (9786190008705). (Disponível online no link: <https://cryptobook.nakov.com/>)
5. William Stallings, Cryptography and Network Security – Principles and Practices. 7th edition, Pearson Education Limited, 2017.