Campus: São José dos Campos

Curso (s): Engenharia de Computação

Unidade Curricular (UC): Segurança da Informação

Unidade Curricular (UC): *[nome da UC em inglês] Information Security*

Código da UC: 8288

Docente Responsável: Fábio Cappabianco	Contato (e-mail): *[opcional]* cappabianco@unifesp.br
Docente (s) Colaborador/a (es/as):	Contato (e-mail): [opcional]

Ano letivo: 2022	Termo: 8º	Turma (s): I
Nome do Grupo/Módulo/Eixo da UC (se houver): -		Idioma predominante em que a UC será oferecida: (X) Português ( ) English ( ) Español ( ) Français ( ) Libras ( ) Outro:
UC: (X) Fixa ( ) Eletiva ( ) Optativa	Oferecida como: (X) Disciplina ( ) Módulo ( ) Estágio ( ) Outro:	Oferta da UC: (X) Semestral ( ) Anual

Ambiente Virtual de Aprendizagem:
(X) Moodle
(X) Classroom
( ) Outro:
( ) Não se aplica

Pré-Requisito (s) - Indicar Código e Nome (s) da (s) UC: 2612/Sistemas Operacionais

Carga horária total (em horas): 36

Carga horária teórica (em horas): 24	Carga horária prática (em horas): 12	Carga horária de extensão (em horas, se houver):

Ementa:
Princípios de segurança, privacidade e integridade da informação. Leis, normas e políticas de segurança da informação. Análise forense digital. Métodos e técnicas algorítmicas de autenticação por biometria.

Conteúdo programático:

- Princípios de segurança, privacidade e integridade da informação:
  - Papeis e responsabilidades em empresas.
- Leis, normas e políticas de segurança da informação:
  - ISOs e normas ABNT
- Análise forense digital:
  - Aspectos históricos;Analise forense de documentos.
- Métodos e técnicas algorítmicas de autenticação por biometria:
  - Conceitos de processamento de imagens aplicados a falsificação de documentos e autenticação de usuários;
  - Conceitos de inteligência artificial aplicados a autenticação e proteção de usuários.

Objetivos:

Gerais:

Capacitar os discentes em boas práticas e mecanismos para prover segurança da informação diante de riscos à integridade de origem física, virtual e legal.

Específicos:

Formar alunos preparados para gerenciar práticas de segurança em sistemas computacionais diante de ataques empregando técnicas de processamento de imagens e inteligência artificial.

Metodologia de ensino:

Aulas expositivas, implementação de ferramentas em laboratório de informática.

Avaliação:

O aluno será avaliado por testes, provas, projetos e seminários.

Média = (S+T1+T2+Pv+Pr)/5

S: Seminário

T1: Testes módulo 1

T2: Testes módulo 2

Pv: Prova

Pr: Projeto

Bibliografia:

Básica:

1. Jain, Anil K.; Flynn, Patrick; Ross, Arun A. Handbook of biometrics. Springer, 2008.
2. da Silva Eleutério, Pedro Monteiro, and Marcio Pereira Machado. Desvendando a computação forense. Novatec Editora, 2011.
3. Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. BRASPORT,
2018.

Complementar:

1. Norvig, Peter; RUSSEL, Stuart J. Artificial intelligence: a modern approach. Upper Saddle River, NJ: Person, 2010.
2. Sencar, Husrev Taha, and Nasir Memon. Digital image forensics. Springer, 2013.
3. Ho, Anthony TS, and Shujun Li, eds. Handbook of digital forensics of multimedia data and devices. John Wiley & Sons, 2015.
4. ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança. Sistemas de gestão de segurança da informação – Requisitos, ABNT
5. Woods, Richard E; GONZALES, Rafael C. Digital image processing. Upper Saddle River: Pearson, 2008.

Cronograma: (Sujeito a modificações)

Semana 1: Apresentação da disciplina. Introdução a Análise Forense Digital
Semana 2: Conceitos de Imagem Digital.
Semana 3: Conceitos de Aprendizado de Máquina
Semana 4: Fonte de aquisição de imagens
Semana 5: Conceitos de Identificação de Cópia Colagem
Semana 6: Inconsistências na Aquisição
Semana 7: Conceitos de Biometria e Spoofing
Semana 8: Prova
Semana 9: Introdução a qualidade e conceitos de segurança
Semana 10: Hexagrama Parkeriano e outros conceitos de segurança
Semana 11: Políticas e organização, recursos humanos e ativos
Semana 12: Controle de acesso, criptografia
Semana 13: Segurança física e operacional
Semana 14: Segurança da comunicação e aquisição, manutenção de sistema
Semana 15: Gestão de incidentes de segurança e conformidade
Semana 16: Projeto