Plano de Ensino

DISCIPLINA: Segurança da Informação

CURSO: Bacharelado em Tecnologia da Informação

CARGA HORÁRIA: 80 horas

CÓDIGO DA DISCIPLINA: COM440

EMENTA

Confidencialidade, integridade, disponibilidade e autenticidade; privacidade; políticas de segurança; monitoramento e backups (locais e remotos); permissões de acesso padrão e estendidas, controle de privilégios POSIX (*capabilities*); autenticação e autorização; fatores de autenticação e autorização (saber algo, ter algo, ser algo); autenticação e autorização com múltiplos fatores; programas maliciosos e spam; noções de uso de protocolos de criptografia simétrica e assimétrica: pgp/gpg, ssh; HTTPS, certificados, autoridades certificadoras e Let's Encrypt; hashes criptográficos e assinaturas digitais; gestão de senhas; segurança em redes: firewalls, prevenção e detecção de invasões (IPS e IDS), VPNs, vulnerabilidades e atualizações de software; segurança em dispositivos e sistemas IoT.

OBJETIVOS DA DISCIPLINA

Apresentar os conceitos básicos e ferramentas de segurança da informação.

CONTEÚDO PROGRAMÁTICO

1. Segurança da Informação
2. Confidencialidade
3. Códigos de Autenticação de Mensagens e Funções Hash
4. Criptografia Assimétrica e Certificados Digitais
5. Mecanismos de Autenticação e Softwares Maliciosos
6. Aspectos Relacionados à Invasão de Sistemas e Medidas de Segurança
7. Segurança em Nuvens Computacionais e em Internet das Coisas
8. Revisão

BIBLIOGRAFIA

Bibliografia Básica:

BOSWORTH S., KABAY E. M., WHYNE E. **Computer Security Handbook**. 5. ed. New York: Willey .2014.

BRANQUINHO, M. A. *et al*. **Segurança de Automação Industrial e SCADA**. Rio de Janeiro: Elsevier, 2014.

STALLINGS W., BROWN, L. **Computer Security**: Principles and Practices. 3. ed. London: Pearson, 2016.

Bibliografia Complementar:

BEJTLICH, R. **The Practice of Network Security Monitoring**. San Francisco: No Starch Press, 2013.

BOLLINGER, J., ENRIGHT, B., VALITES, M. **Crafting the InfoSec Playbook**: Security Monitoring and Incident Response Master Plan. Sebastopol: O'Reilly Media, 2015.

FERGUSON, F., SCHNEIER, B., KOHNO, T. **Cryptography Engineering**: Design Principles and Practical Applications. New York: Wiley, 2010.

LUTTGENS, J., PEPE, M., MANDIA, K. **Incident Response & Computer Forensics**. 3. ed. New York: MacGraw Hill, 2014.

SHOSTACK, A. **Threat Modeling**: Designing for Security. New York: Wiley 2014.

STAMP, M. **Information Security**: Principles and Practice. 2. ed. New York: Willey, 2011.

PRÉ-REQUISITOS

Não possui.

CRITÉRIOS DE AVALIAÇÃO

A avaliação da disciplina é formativa* e somativa**. Os alunos devem entregar as resoluções de atividades e/ou exercícios no Ambiente Virtual de Aprendizagem semanalmente e realizar, ao final do período letivo, uma prova presencial aplicada nos polos Univesp.

**A avaliação formativa ocorre quando há o acompanhamento dos alunos, passo a passo, nas atividades e trabalhos desenvolvidos, de modo a verificar suas facilidades e dificuldades no processo de aprendizagem e, se necessário, adequar alguns aspectos do curso de acordo com as necessidades identificadas.*

***A avaliação somativa é geralmente aplicada no final de um curso ou período letivo. Esse tipo de avaliação busca quantificar o que o aluno aprendeu em relação aos objetivos de aprendizagem do curso. Ou seja, a avaliação somativa quer comprovar se a meta educacional proposta e definida foi alcançada pelo aluno.*

DOCENTE RESPONSÁVEL

Prof. Dr. Julio Cezar Estrella

Professor Associado no Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (ICMC/USP) e Livre-Docente pela mesma instituição. Possui Doutorado e Mestrado em Ciências de Computação e Matemática Computacional pela Universidade de São Paulo (USP) e Graduação em Ciência de Computação pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (Unesp). Suas linhas de pesquisa incluem: Provisionamento Dinâmico de Recursos Computacionais em Sistemas Distribuídos, com destaque para aplicações no contexto de: Internet das Coisas, *Smart Cities* e *Smart Building*, *Cloud Computing*, Virtualização, *Micro Services* e SOA. Desenvolve também pesquisa com foco na otimização de aplicações distribuídas e em processamento de alto desempenho.