PLANO DE DISCIPLINA
NOME DO COMPONENTE CURRICULAR: Segurança da informação (Tópicos Especiais II)
CURSO: Técnico Subsequente em Manutenção e Suporte em Informática
PERÍODO: 3º
CARGA HORÁRIA: 33,3h (2h/a semanais)
DOCENTE RESPONSÁVEL:

EMENTA

Esta disciplina desenvolve os conceitos fundamentais de segurança cibernética e como ele se relaciona com as informações e segurança de redes.

OBJETIVOS

Geral:

De maneira geral, esta disciplina apresenta aos alunos características de segurança cibernética, tenologia, procedimentos para defender uma rede.

Específicos:

- Compreender procedimentos para implementar a confidencialidade, integridade e controle de segurança em redes, dados, servidores e aplicações.
- Compreender os princípios de segurança e como desenvolver e aplicar políticas de segurança de acordo com as leis de segurança cibernéticas.
- Aplicar habilidades através de práticas usando o laboratório de informática.

CONTEÚDO PROGRAMÁTICO

- Capítulo 1 – Introdução à segurança cibernética
  - Descrever características de segurança cibernética no mundo;
  - Identificar a diferença entre os criminosos e heróis no mundo de segurança cibernética;
  - Comparar as várias ameaças de segurança cibernética e como afetam os indivíduos, empresas e organizações;
  - Compreender como as organizações somam forças para aprimorar suas técnicas e combater os crimes cibernéticos.

- Capítulo 2 – Apresentar e discutir framework para padronização e gerenciamento de informações e sistemas, ISO.
  - Descrever as três dimensões do McCumber Cube;
  - Descrever os princípios de confidencialidade, Integridade e Disponibilidade;
  - Diferenciar entre os três estados de dados;
  - Compare os tipos de contramedidas de segurança cibernética.
  - Descrever o modelo ISO de segurança cibernética.

- Capítulo 3 – Ameaças, vulnerabilidades e ataques
  - Diferenciar os tipos de malware e códigos maliciosos;
  - Descrever as táticas, técnicas e procedimentos utilizados pelos criminosos cibernéticos;
  - Comparar os diferentes métodos de engenharia social e outros ataques.

- Capítulo 4 – Criptografia, protegendo a CONFIDENCIALIDADE da informação
  - Apresentar técnicas de encriptação para proteção da confidencialidade;
  - Descrever técnicas de controle de acesso para proteção da confidencialidade;
  - Descrever conceitos de obscuridade de dados.

- Capítulo 5 – A arte de assegurar a INTEGRIDADE da informação
  - Apresentar processos utilizados para assegurar integridade;
  - Compreender o propósito de assinatura digital;
  - Compreender o propósito de certificado digital;

- Capítulo 6 – Como obter ALTA DISPONIBILIDADE
  - Apresentando o conceito de alta disponibilidade;
  - Explorando como a medição da alta disponibilidade é usado para melhorar a disponibilidade da informação;
  - Apresentar como um bom planejamento de resposta de incidentes pode aumentar a alta disponibilidade ;
  - Apresentar como a execução de uma planejamento de recuperação de desastre torna-se uma regra importante na implementação de alta disponibilidade.

- Capítulo 7 – Proteção de sistemas
  - Explicar como tecnologias, processos e procedimentos podem ser utilizados para proteção de sistemas;
  - Explicar como proteger os servidores, serviços, rede e meio físico;

- Capítulo 8 – Tornando-se um profissional em segurança cibernética
  - Apresentar os recursos disponíveis para iniciar e alavancar uma carreira em segurança cibernética;

METODOLOGIA DE ENSINO
Através de interatividade, conteúdo multimídia, atividade em laboratório e caso de estudos da industria, os estudantes constroem habilidades profissionais para o encaminhamento inicial no segmento de segurança cibernética.

AVALIAÇÃO DO PROCESSO DE ENSINO APRENDIZAGEM
• Para cada capítulo, será realizado uma avaliação de aprendizagem; • Uma avaliação de reposição, conforme dita o regimento do Instituto;

RECURSOS NECESSÁRIOS
• Laboratório de Informática com acesso à internet e sistema operacional Windows e Linux;

- Quadro, pincel, projetor multimídia e impressora;
- Técnico em informática para preparar o ambiente prático quando necessário

BIBLIOGRAFIA

Bibliografia Básica

- GEUS, Paulo Lício e NAKAMURA, Emilio Tissato. Segurança de Redes em Ambiente Corporativos. 1.ed. São Paulo: Editora Novatec, 2007.
- RAIMUNDO, Gerson e CESAR, Silvio. Backtrack Linux: Auditoria E Teste De Invasão Em Redes De Computadores. 1. ed. 2013.

Bibliografia Complementar

- CISCO CyberSecurity course – Netacad
- LONG, Johnny. Google Hacking Para Pentest, Novatec, 2016