Plano de Ensino

1 Código e nome da disciplina

ARA0076 SEGURANÇA CIBERNÉTICA

2 Carga horária semestral

80

3 Carga horária semanal

4h

4 Perfil docente

O docente deve preferencialmente ser graduado em Ciências da Computação, ou áreas afins e possuir Pós Graduação Lato Sensu (especialização), embora seja desejável a Pós-Graduação Stricto Sensu (Mestrado e/ou Doutorado) na área do curso ou áreas afins.

É desejável que o docente possua experiência profissional na área de Segurança da Informação, além de conhecimentos teóricos e práticos na área de segurança computacional, habilidades de comunicação em ambiente acadêmico, capacidade de interação e fluência digital para utilizar ferramentas necessárias ao desenvolvimento do processo de ensino-aprendizagem (SGC, SAVA, BdQ e SIA).

Importante, também, o conhecimento do Projeto Pedagógico dos Cursos que a disciplina faz parte na Matriz Curricular.

É necessário que o docente domine as metodologias ativas inerentes à educação por competências e ferramentas digitais que tornam a sala de aula mais interativa. A articulação entre teoria e prática deve ser o eixo direcionador das estratégias em sala de aula. Além disto, é imprescindível que o docente estimule o autoconhecimento e autoaprendizagem entre seus alunos.

5 Ementa

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA. AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP). CONTRAMEDIDAS E HARDENING. RESPOSTA À INCIDENTES E RECUPERAÇÃO (DISASTER RECOVERY).

6 Objetivos

- Classificar a informação, com base no seu valor e sua criticidade, para construir um plano de

cibersegurança alinhado às necessidades no negócio.

- Analisar vulnerabilidades e ataques, com base no estudo de diferentes tipos de ameaças, a fim de criar estratégias e contra-medidas eficazes para mitigá-las.

- Investigar as vulnerabilidades mais comuns, baseando-se nas recomendações da OWASP, para criar correções relacionadas à código inseguro.

- Projetar e configurar sistemas de proteção, com base em algoritmos e ferramentas, para garantir o funcionamento contínuo e seguro dos sistemas de TI.

- Construir um plano de resposta à incidentes e recuperação de desastres, baseando-se em normas e recomendações de segurança, para tratar incidentes, investigando, reportando e recuperando o ambiente dos danos causados.

7 Procedimentos de ensino-aprendizagem

A disciplina adotará o modelo de aprendizagem baseada em problemas.

O processo de ensino-aprendizagem iniciará por meio de uma situação- problema (problematização/pergunta geradora), previamente definida pela/pelo docente a partir dos temas de aprendizagem. Poderão ser utilizados como estratégias didáticas: exposição, discussão de filmes e documentários, estudos de casos que subsidiarão a análise de problemas, debates estruturados, fóruns de discussão, brainstormings, jogos e ferramentas digitais que tornarão o aluno protagonista de seu aprendizado. Esta abordagem prioriza o aluno, sendo este capaz de articular os temas discutidos nas aulas para responder à situação problema que abre a preleção.

É importante destacar o uso da Sala de Aula Virtual de Aprendizagem (SAVA), local em que o aluno terá acesso ao conteúdo digital da disciplina, poderá resolver questões propostas e explorar conteúdos complementares disponíveis para estudo.

O modelo de aprendizagem prevê ainda a realização da Atividade Prática Supervisionada, que são atividades práticas realizadas em laboratórios, bibliotecas e trabalhos individuais e/ou em grupo que fazem parte do ecossistema de aprendizagem global e local.

8 Temas de aprendizagem

1. PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
1.1 EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA
1.2 VALOR DA INFORMAÇÃO - ALINHAMENTO ESTRATÉGICO DA SEGURANÇA AOS NEGÓCIOS
1.3 INVESTIMENTO NECESSÁRIO PARA GARANTIR A PROTEÇÃO DOS DADOS
1.4 PLANO DE CIBERSEGURANÇA (CYBERSECURITY PLAN)

2. AMEAÇAS, VULNERABILIDADES E TIPOS DE ATAQUES
2.1 INTERCEPTAÇÃO DE TRÁFEGO & MAPEAMENTO DE REDES
2.2 ATAQUES E VULNERABILIDADES DE APLICAÇÕES WEB
2.3 CÓDIGOS MALICIOSOS
2.4 WIRELESS HACKING

3. AS PRINCIPAIS VULNERABILIDADES COMUNS DA OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (ATIVIDADE PRÁTICA SUPERVISIONADA)
3.1 INJEÇÃO, QUEBRA DE AUTENTICAÇÃO, E EXPOSIÇÃO DE DADOS SENSÍVEIS

3.2 ENTIDADES EXTERNAS DE XML, QUEBRA DE CONTROLE DE ACESSOS, CONFIGURAÇÕES DE SEGURANÇA INCORRETAS
3.3 CROSS-SITE SCRIPTING, DESSERIALIZAÇÃO INSEGURA
3.4 REGISTRO E MONITORIZAÇÃO INSUFICIENTE

4. CONTRAMEDIDAS E HARDENING
4.1 FERRAMENTAS DE SEGURANÇA & CRIPTOGRAFIA
4.2 SEGURANÇA NOS PROTOCOLOS: IP, TCP, UDP, DNS E HTTP
4.3 HARDENING: SEGURANÇA EM AMBIENTES LINUX E WINDOWS
4.4 SEGURANÇA EM REDES SEM FIO & INTERNET DAS COISAS

5. RESPOSTA À INCIDENTES E RECUPERAÇÃO (DISASTER RECOVERY)
5.1 RESPOSTA À INCIDENTES
5.2 CORREÇÕES DE VULNERABILIDADES
5.3 FORENSE COMPUTACIONAL
5.4 DISASTER RECOVERY PLAN

9 Procedimentos de avaliação

Os procedimentos de avaliação contemplarão as competências desenvolvidas durante a disciplina, divididos da seguinte forma: AV e AVS
AV - Contemplará todos os temas abordados pela disciplina e será assim composta:
- Prova individual no formato PNI ? Prova Nacional Integrada com valor total de 5,00 (cinco) pontos;
- Atividades acadêmicas avaliativas com valor total de 5,00 (cinco) pontos.
Detalhamento das atividades que compõe os 5 pontos:
i. Aula 11 - Atividade sobre HTTPS e sua relação com a segurança de transações bancárias, valendo 2,5 (dois e meio) pontos;
ii. Aula 14 - Atividade sobre correção de vulnerabilidades, valendo 2,5 (dois e meio) pontos.
A soma de todos os instrumentos que possam vir a compor o grau final da AV não poderá ultrapassar o grau máximo de 10 (dez) pontos.

AVS - Contemplará todos os temas abordados pela disciplina. Será composta por uma prova no formato PNI - Prova Nacional Integrada, com total de 10 pontos, e substituirá a nota da AV, caso seja maior.

Para aprovação na disciplina, o aluno deverá, ainda:
- atingir nota igual ou superior a 6 (seis) na prova de AV ou AVS;
- frequentar, no mínimo, 75% das aulas ministradas.

10 Bibliografia básica

BASTA Alfred. **Segurança de Computadores e Testes de Invasão**. 2ª edição. São Paulo: Editora Trilha, 2015.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366

MACHADO, Felipe Nery Rodrigues. **Segurança da informação - princípios e controle de ameaças**. 1ª edição. São Paulo: Érica, 2014.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536531212

SCAMBRAY, Joel; McCLURE, Stuart; KURTZ, George. **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**. 4ª edição. Porto Alegre: Editora Bookman, 2014.

Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601426

11 Bibliografia complementar

AGRA, Andressa Dellay; BARBOZA, Fabrício Felipe Meleto. **Segurança de sistemas da informação**. Porto Alegre: SAGAH, 2019.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595027084

BARRETO, Jeanine dos Santos; ZANIN, Aline; MORAIS, Izabelly Soares de et al. **Fundamentos de segurança da informação**. Porto Alegre: SAGAH, 2018.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875

COMER, Douglas E. **Redes de Computadores e Internet**. Porto Alegre: Bookman, 2016.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582603734

LIGUORI, Carlos. **Direito e criptografia**. São Paulo: Saraiva, 2022.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623446

WRIGHTSON, Tyler. **Segurança de Redes sem Fio**. Porto Alegre: Editora Bookman, 2014.
Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788582601556