

DADOS DO COMPONENTE CURRICULAR
<b>Nome:</b> Segurança
<b>Série/Período:</b> 4º semestre
<b>Carga Horária:</b> 33 h/r (40 aulas)
<b>Docente Responsável:</b>
EMENTA
Políticas de segurança. Responsabilidades e controle em sistemas de informação. Controle de acesso e senhas. Criptografia simétrica e assimétrica. Certificados digitais. Aspectos de segurança em redes sem fio. Recuperação de dados. Tipos de ataques. Ferramentas de ataque aos sistemas Computacionais e suas respectivas defesas. Brechas de segurança em sistemas computacionais.
OBJETIVOS
<p><b>Geral</b></p> <ul style="list-style-type: none"> <li>• Apresentar os benefícios de um sistema seguro, para proteção da informação, bem como fomentar o conhecimento das técnicas, ferramentas e brechas de segurança, na proteção de ambientes pessoais e corporativos;</li> <li>• Prover um arcabouço para o desenvolvimento e manutenção de sistemas computacionais seguros.</li> </ul> <p><b>Específicos</b></p> <ul style="list-style-type: none"> <li>• Mostrar a importância da segurança da informação;</li> <li>• Estimular as vantagens da aplicação de metodologias de auditoria da informação;</li> <li>• Apresentar as técnicas de criptografia;</li> <li>• Apresentar os certificados digitais;</li> <li>• Conhecer técnicas de segurança de redes de computadores sem fio (wireless);</li> <li>• Apresentar e aplicar ferramentas de intrusão, varredura e de busca de falhas de segurança;</li> </ul>
CONTEÚDO PROGRAMÁTICO
<ol style="list-style-type: none"> <li>1) Políticas de segurança. <ol style="list-style-type: none"> <li>a) Noções básicas de segurança de dados</li> <li>b) Responsabilidades e controle em sistemas de informação.</li> <li>c) Controle de acesso e senhas</li> <li>d) Auditoria.</li> </ol> </li> <li>2) Criptografia simétrica e assimétrica. <ol style="list-style-type: none"> <li>a) Criptografia e a infraestrutura de chave pública (PKI)</li> <li>b) Criptografia simétrica</li> <li>c) Criptografia de chave pública ou assimétrica</li> <li>d) Funções de hash</li> </ol> </li> <li>3) Certificados digitais.</li> <li>4) Aspectos de segurança em redes sem fio. <ol style="list-style-type: none"> <li>a) Protocolos de segurança: WEP, WPA e WPA2</li> <li>b) Ferramentas de busca de vulnerabilidades</li> </ol> </li> <li>5) Recuperação de dados.</li> <li>6) Ataques <ol style="list-style-type: none"> <li>a) Tipos de ataques.</li> <li>b) Ferramentas de ataque aos sistemas Computacionais e suas respectivas defesas. Brechas de segurança em sistemas computacionais.</li> </ol> </li> </ol>
METODOLOGIA DE ENSINO

Aulas expositivas e dialogadas;  
Aulas experimentais utilizando computadores e softwares de varredura/detecção de vulnerabilidades.

#### **AVALIAÇÃO DO PROCESSO DE ENSINO E APRENDIZAGEM**

Provas Escritas  
Seminários

#### **RECURSOS NECESSÁRIOS**

Quadro branco;  
Marcadores para quadro branco;  
Projetor de dados multimídia.

#### **PRÉ-REQUISITOS**

21 – Banco de Dados  
24 – Redes de computadores  
35 – Desenvolvimento de Aplicações Web I

#### **BIBLIOGRAFIA**

##### ***Básica***

NAKAMURA, E. T. **Segurança de redes em sistemas cooperativos**. Editora Novatec, 2007;  
GOODRICH, M. T.; TAMASSIA, R. **Introdução à Segurança de Computadores**. Bookman, 1ª edição, 2013.

##### ***Complementar***

ULBRICH, H. C.; DELLA VALLE, J. **Universidade Hacker**. Editora Digerati Books, 2009;  
SHOKRANIAN, S. **Criptografia para iniciantes**. Ciência Moderna, 2ª edição, 2012.