UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FICHA DE COMPONENTE CURRICULAR

CÓDIGO:	**COMPONENTE CURRICULAR:**
FEELT39017D	TÓPICOS ESPECIAIS EM ENGENHARIA DE COMPUTAÇÃO II – SEGURANÇA DE SISTEMAS COMPUTACIONAIS

UNIDADE ACADÊMICA OFERTANTE:	**SIGLA**:
FACULDADE DE ENGENHARIA ELÉTRICA	FEELT

CH TOTAL TEÓRICA:	**CH TOTAL PRÁTICA:**	**CH TOTAL:**
60 horas	-	60 horas

OBJETIVOS

O curso capacita o discente a efetuar análise dos sistemas computacionais sob a perspectiva da integridade, disponibilidade e confidencialidade dos dados armazenados e daqueles que trafegam através das redes heterogêneas de dados. Portanto, deve fomentar a aquisição das seguintes habilidades:

• Capacidade de reconhecer os riscos existentes e as diversas formas de tratamento dos mesmos.
• Capacidade de aplicar os diversos métodos, técnicas e tecnologias com a finalidade de garantir a confidencialidade, disponibilidade, integridade, autenticidade e irretratabilidade dos dados e transações.
• Capacidade de adquirir e analisar evidencias e auditar sistemas computacionais dentro do arcabouço legal vigente.
• Entendimento dos limitantes éticos e legais relativos ao desenvolvimento das atividades de perícia computacional.

EMENTA

Fundamentos legais. Fundamentos da Gestão de Risco. Política de Segurança, Planejamento de Continuidade de Negócio e Recuperação de Desastre. Propriedades da Informação. Introdução a Criptografia. Segurança de Redes. Segurança de Sistemas. Seguranca em Aplicações. Auditoria de Segurança e Teste de Penetração. Forense Computacional. Certificações. Computação forense em ambiente de nuvem.

PROGRAMA

1) **Conceitos Básicos**
   a) Ameaças nos Sistemas de Informação
   b) Propriedades da Informação
   c) Gestão de Risco – Impacto, Vulnerabilidades e Tratamento
   d) Política de Segurança de Informação
   e) Plano de Continuidade / Recuperação de Desastre

2) **Fundamentos Legais**

3) **Introdução à Criptografia**
   a) Cifradores Clássicos
   b) Ataques
   c) Cifradores Modernos
   d) Funções de hashing
   e) Cifradores Assimétricos
   f) Protocolos Criptográficos

4) **Segurança de Redes**
   a) Firewall
   b) Ataques comuns – DDoS, Ataques Voltados à SSL e DNS, BotNets e Backdoors
   c) Ataques à Redes Wireless
   d) Sistemas de Detecção e Prevenção de Intrusão (IPS/IDS)
   e) Exemplos de Uso de Ferramentas Importantes - NMAP, Wireshark, Snort

5) **Segurança de Sistemas**
   a) Mecanismos de Autenticação
   b) Atualização de Sistemas

6) **Desenvolvimento de Aplicações**
   a) Tratamento de Entrada (SQL Injection)
   b) Ataques comuns:
      i) Buffer Overflow
      ii) Cross Site Scripting
      iii) Insecure Direct Object References
      iv) Sensitive Data Exposure

7) **Auditoria e Teste de Penetração**
   a) Técnicas de Scanning
   b) Técnicas de Enumeração / Reconhecimento
   c) Ferramentas de Escaneamento de Vulnerabilidades

8) Computação Forense

a) Iniciando a Aquisição de Evidência – Boas Práticas e Cadeia de Custódia
b) Recuperação de Artefatos da Memória Volátil e Não Volátil
c) Sistemas de Arquivos e Recuperação de Dados
d) Computação Forense em Ambiente de Nuvem

BIBLIOGRAFIA BÁSICA

1. MERKOW, Mark S.; BREITHAUPT, Jim. **Information security: Principles and practices**. Pearson Education, 2014.
2. ALTHEIDE, Cory; CARVEY, Harlan. **Digital forensics with open source tools**. Elsevier, 2011.
3. BEJTLICH, Richard. **The practice of network security monitoring: understanding incident detection and response.** No Starch Press, 2013.

BIBLIOGRAFIA COMPLEMENTAR

1. HOWARD, Michael; LEBLANC, David; VIEGA, John. 24 **Deadly Sins of Software Security. Programming Flaws and How to Fix Them**. McGraw-Hill, 2010.
2. O'GORMAN, Jim; KEARNS, Devon; AHARONI, Mati. Metasploit: **The penetration tester's guide**. No Starch Press, 2011.
3. LIGH, Michael Hale et al. **The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory**. John Wiley & Sons, 2014.
4. SIKORSKI, Michael; HONIG, Andrew. **Practical malware analysis: the hands-on guide to dissecting malicious software**. No Starch Press, 2012.
5. RAMACHANDRAN, Vivek. BackTrack 5 **Wireless Penetration Testing: Beginner's Guide**. Packt Publishing Ltd, 2011.
6. LYON, Gordon Fyodor**. Nmap network scanning: The official Nmap project guide to network discovery and security scanning**. Insecure, 2009.

APROVAÇÃO

_____ /_____/ _____

_____

Carimbo e assinatura do Coordenador do Curso

_____/ _____ / _____

_____

Carimbo e assinatura do Diretor da Unidade Acadêmica