



UNIVERSIDADE FEDERAL DE UBERLÂNDIA



## FICHA DE COMPONENTE CURRICULAR

|  |  |                              |
|--|--|------------------------------|
| <b>CÓDIGO:</b><br>GSI536                                       | <b>COMPONENTE CURRICULAR:</b><br>Auditoria e Segurança da Informação |                              |
| <b>UNIDADE ACADÊMICA OFERTANTE:</b><br>Faculdade de Computação |  | <b>SIGLA:</b><br>FACOM       |
| <b>CH TOTAL TEÓRICA:</b><br>60 horas                           | <b>CH TOTAL PRÁTICA:</b><br>00 horas                                 | <b>CH TOTAL:</b><br>60 horas |

1. **OBJETIVOS**

**Geral:** O objetivo geral é tornar o aluno apto a propor ações necessárias para dotar os sistemas de informação de mecanismos de segurança que permitam garantir a integridade e recuperação de informações armazenadas em meio eletrônico.

**Específicos:**

- Alcançar conhecimentos dos fundamentos de auditoria de sistemas e TIC (Tecnologia da Informação e Comunicação);
- Adquirir conceitos e metodologias para planejar e realizar atividades regulares de mensuração e avaliação de processos, dados, sistemas, infra-estrutura e projetos de TIC;
- Capacidade de fundamentar e apresentar conclusões em relatórios concisos e objetivos de auditoria;
- Capacidade de observar responsabilidades, atitudes e requisitos de ética e conduta do auditor de sistemas.

2. **EMENTA**

Introdução à segurança da informação e à segurança de redes; ataques e principais recursos aos sistemas de informação; princípios de criptografia; autenticação e controle de acesso; políticas de segurança; introdução à auditoria de sistemas e suas metodologias; tópicos especiais em segurança da informação e auditoria de sistemas.

3. **PROGRAMA**

1. Introdução à segurança da informação
  1. Segurança da Informação: passado, presente e futuro
  2. Fundamentos da Segurança da Informação
  3. Segurança da informação nas organizações

2. Introdução à segurança de redes
  1. Invasões técnicas
  2. Engenharia Social
  3. Potenciais atacantes
  4. Planejamento de ataques
3. Ataques aos sistemas de informação
  1. Ataques de negação de serviços
  2. Ataques no nível de aplicação
  3. Combinação de ataques técnicos e engenharia social
4. Principais recursos para proteção da informação
  1. Firewall
  2. Sistemas de Detecção de Intrusão
5. Princípios de criptografia
  1. História e conceitos básicos
  2. Criptografia simétrica
  3. Criptografia assimétrica
  4. Modelo híbrido de criptografia
6. Autenticação e controle de acesso
  1. Hash
  2. Assinatura digital
  3. Secure Socket Layer (SSL) e Transport Layer Security (TLS)
7. Políticas de segurança
  1. Relação da política de segurança com a segurança da informação
  2. Legislação e normas de segurança da informação
  3. Exemplos de políticas de segurança
8. Introdução à auditoria de sistemas
  1. Princípios gerais
  2. Auditoria e controles internos
  3. Controles externos
  4. Relação da auditoria com a política de segurança
  5. Auditoria e perícia forense computacional
9. Metodologias de auditoria
  1. Tipos de auditoria
  2. Metodologia de auditoria de sistemas de informação
  3. Metodologia de auditoria de segurança da informação
  4. Normas e procedimentos de auditoria de sistemas
  5. Auditoria seguindo a tradição contábil
10. Tópicos especiais em Segurança da Informação e Auditoria de Sistemas
  1. Estado da arte e atualidades

## 2. Perspectivas futuras

### 4. BIBLIOGRAFIA BÁSICA

IMONIANA, Joshua O. **Auditoria de sistemas de informação**. 2. ed. São Paulo: Atlas, 2008.

LYRA, Maurício R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

WHEELER, Evan. **Security Risk Management: building an information security risk management program from the ground up**. Waltham: Syngress, 2011.

### 5. BIBLIOGRAFIA COMPLEMENTAR

ANDRESS, Jason. **The basics of Information security: understanding the fundamentals of infosec in theory and practice**. Boston: Syngress, 2011.

GARFINKEL, Simson; SPAFFORD, Gene; SCHWARTZ, Alan. **Practical Unix & internet security**. 3rd. ed. Beijing: O'Reilly, 2003.

HOOG, Andre. **Android forensics: investigation, analysis, and mobile security for Google Android**. Waltham: Syngress, 2011.

KNAPP, Eric. **Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems**. Waltham: Syngress, 2011.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2015.

### 6. APROVAÇÃO

Prof. Dr. Rafael Dias Araújo  
Coordenador do Curso de Sistemas de Informação  
Campus Monte Carmelo

Prof. Dr. Mauricio Cunha Escarpinati  
Diretor da Faculdade de Computação



Documento assinado eletronicamente por **Rafael Dias Araújo, Coordenador(a)**, em 25/01/2023, às 22:13, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Mauricio Cunha Escarpinati, Diretor(a)**, em 26/01/2023, às 17:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://www.sei.ufu.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **4063978** e o código CRC **E418C2FE**.