

| CÓDIGO DO CURSO | CURSO                                 |
|-----------------|---------------------------------------|
| GSISNF          | BACHARELADO EM SISTEMAS DE INFORMAÇÃO |

| CÓDIGO DA DISCIPLINA | NOME DA DISCIPLINA                | ANO/SEMESTRE |
|----------------------|-----------------------------------|--------------|
| GS19602NF            | SEGURANÇA E AUDITORIA DE SISTEMAS | 2022/1       |

| CARGA HORÁRIA        | CRÉDITOS | AULAS/SEMANA |         |         |                | PERÍODO |
|----------------------|----------|--------------|---------|---------|----------------|---------|
| 75 horas<br>(90 h-a) | 4        | TEÓRICA      | PRÁTICA | ESTÁGIO | NÃO PRESENCIAL | 6º      |
|                      |          | 3            | 2       | 0       | 0              |         |

| PRÉ - REQUISITO (S)                                       | CORREQUISITO (S) |
|-----------------------------------------------------------|------------------|
| Administração de Redes<br>Administração de Banco de Dados | -----            |

| EMENTA                                                                     |
|----------------------------------------------------------------------------|
| Criptografia. Firewall. Segurança nas Comunicações. Auditoria de Sistemas. |

| BIBLIOGRAFIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BIBLIOGRAFIA BÁSICA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <ol style="list-style-type: none"> <li>1. KIM, David. <b>Fundamentos de segurança de sistemas de informação</b>. Rio de Janeiro: LTC, 2014. xxi, 386p., il., 28 cm. Bibliografia: p. 375-377. ISBN 9788521625070 (broch.).</li> <li>2. GALVÃO, Ricardo Kléber M. <b>Introdução à análise forense em redes de computadores: conceitos, técnicas e ferramentas para 'grampos digitais'</b>. 1.ed. São Paulo: Novatec, 2013. 152 p. ISBN 9788575223079.</li> <li>3. SILVA, Gilson Marques da. <b>Segurança da informação para leigos: como proteger seus dados, micro e familiares na internet</b>. Rio de Janeiro: Ciência Moderna, 2011. 136 p. ISBN 9788539901197:(broch.).</li> </ol>                                                                                           |
| BIBLIOGRAFIA COMPLEMENTAR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <ol style="list-style-type: none"> <li>1. BROAD, James; BINDNER, Andrew. <b>Hacking com Kali Linux: técnicas práticas para testes de invasão</b>. 1.ed. São Paulo: Novatec, 2014. 283 p. ISBN 9788575223956.</li> <li>2. FOROUZAN, Behrouz A. <b>Comunicação de dados e redes de computadores</b>. Colaboração de Sophia Chung Fegan. 4. ed. São Paulo: McGraw-Hill, 2008. xxxiv, 1134 p., il. (algumas color.). ISBN 9788586804885 (Broch.).</li> <li>3. GIAVAROTO, Sílvio César Roxo. <b>Backtrack linux: auditoria e teste de invasão em redes de computadores</b>. Rio de Janeiro: Ciência Moderna, 2013. 232 p. ISBN 9788539903740 (broch.).</li> <li>4. TANENBAUM, Andrew S., 1944-. <b>Redes de computadores</b>. Rio de Janeiro: Elsevier: Campus, c2003. xx,</li> </ol> |

945 p., il. ISBN 8535211853 (broch.).

5. ENGBRETSON, Patrick. **Introdução ao hacking e aos testes de invasão: facilitando o hacking ético e os testes de invasão**. Revisão de David Kennedy. 1.ed. São Paulo: Novatec, 2014. 302 p. ISBN 9788575223901.

### OBJETIVOS GERAIS

1. Conhecer os princípios de segurança de sistemas de informação;
2. Proteger uma rede local de computadores;
3. Conhecer e implementar mecanismos de auditoria de sistemas.

### METODOLOGIA

Aulas expositivas, dialogadas e práticas, ilustradas, com o auxílio de recursos audiovisuais. Para obter melhor aprofundamento do conteúdo, poderão ser propostos seminários e/ou atividades de pesquisa. Todas as aulas serão realizadas em laboratório devidamente equipado com ferramentas de apoio.

### CRITÉRIO DE AVALIAÇÃO

Trabalhos de pesquisa e/ou seminários.

### PROGRAMA

1. Segurança de Sistemas de Informação
  - 1.1. Princípios de Segurança de Sistemas de Informação
  - 1.2. Domínios de uma infraestrutura típica de TI
  - 1.3. Políticas de Segurança de TI
  - 1.4. Legislação em Segurança de Sistemas de Informação
2. Proteção de Dados
  - 2.1. Criptografia Clássica
  - 2.2. Algoritmos criptográficos de chave simétrica
  - 2.3. Algoritmos criptográficos de chave assimétrica
  - 2.4. Assinatura digital
  - 2.5. Hash
3. Proteção de Sistemas
  - 3.1. Firewall
  - 3.2. Teste de penetração
  - 3.3. Sniffing
  - 3.4. Ataques maliciosos
  - 3.5. Ameaças
  - 3.6. Vulnerabilidades
4. Segurança nas Comunicações
  - 4.1. VPN
  - 4.2. SSL/TLS
  - 4.3. PGP
  - 4.4. HTTPS

5. Auditoria de Sistemas  
5.1. Forense computacional  
5.2. Logs e registros de acesso

**PROFESSOR RESPONSÁVEL**

**NOME - SIAPE** Nilson Mori Lazarin – 2888838

**ASSINATURA**

**COORDENADOR DO CURSO**

**NOME - SIAPE** Rodrigo Reis Gomes – 1644791

**ASSINATURA**

**LOCAL E DATA**

Nova Friburgo, 19 de novembro de 2021.