



Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino

DISCIPLINA: Fundamentos de Segurança de Sistemas Computacionais	
Vigência: a partir de 2025/1	Período letivo: 4º semestre
Carga horária total: 45 h	Código: SUP.2661
Ementa: Estudo das definições e dos conceitos introdutórios de segurança da informação e de sistemas computacionais. Compreensão dos fundamentos da criptografia.	

Conteúdos

UNIDADE I – Definições e Conceitos

- 1.1 Definições
- 1.2 Conceitos
 - 1.2.1 Integridade, Disponibilidade e Confidencialidade
 - 1.2.2 Autenticação, Autorização e Auditabilidade
 - 1.2.3 Irretratabilidade
 - 1.2.4 Ativo, Ameaça, Ataque, Vulnerabilidade, Risco, Contramedida
- 1.3 Princípios de segurança

UNIDADE II – Fundamentos de Criptografia

- 2.1 Criptografia Clássica
- 2.2 Chaves simétricas
- 2.3 Chaves assimétricas
- 2.4 Código de Autenticação de Mensagem (MAC)

Bibliografia básica

BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro, RJ: Brasport, 2018. *E-book*. Disponível em <https://plataforma.bvirtual.com.br>. Acesso em: 05 jan. 2025.

ZOCHIO, Marcelo. **Introdução à Criptografia**. São Paulo, SP: Novatec, 2016.

DA SILVA, Michel. **Cibersegurança:** uma visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro, RJ: Freitas Bastos, 2023. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 05 jan. 2025.

Bibliografia complementar

MITANI, Masaaki; SATO, Shinichi; HINOKI, Idero; CORP., Verte. **The Manga Guide to Cryptography**. São Francisco, CA, EUA: No Starch Press, 2018.



Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino

CONKLIN, Wm Arthur; SHOEMAKER, Daniel Paul. **CSSLP Certified Secure Software Lifecycle Professional All-In-One Exam Guide**. 3.ed. New York City, NY, EUA: McGraw-Hill, 2022.

FREIRE, Alexandre, SANTOS, Alfredo; MUNIZ, Antonio; PIMENTA, Cristiano. **Jornada segurança da informação**: unindo visão executiva e técnica para estratégia, comportamento, inovação e tendências. Rio de Janeiro: Brasport, 2024. *E-book*. Disponível em <https://plataforma.bvirtual.com.br>. Acesso em: 05 jan. 2025.

STALLINGS, William; VIEIRA, Daniel. **Criptografia e segurança de redes: princípios e práticas**. 6.ed. Londres, Reino Unido: Pearson, 2015. *E-book*. Disponível em: <https://plataforma.bvirtual.com.br>. Acesso em: 05 jan. 2025.