

# Aspectos de Governança da Segurança

A **Governança da Segurança** é o conjunto de práticas, processos, regulamentos e instituições que regulam a gestão da segurança da informação e dos sistemas de computação. Este é um contexto extremamente amplo, que demandaria uma carga horária significativa para seu estudo.

Para prover uma visão geral (embora superficial) da área, esta aula consiste em um conjunto de seminários preparados pelos alunos sobre alguns de seus aspectos mais relevantes:

- Domínios da ISO/IEC 27001 (27002, 27003, ...):
  - Security policy (management direction)
  - Organization of information security (governance of information security)
  - Asset management (inventory and classification of information assets)
  - Human resources security (security aspects for employees joining, moving and leaving an organization)
  - Physical and environmental security (protection of the computer facilities)
  - Communications and operations management (management of technical security controls in systems and networks)
  - Access control (restriction of access rights to networks, systems, applications, functions and data)
  - Information systems acquisition, development and maintenance (building security into applications)
  - Information security incident management (anticipating and responding appropriately to information security breaches)
  - Business continuity management (protecting, maintaining and recovering business-critical processes and systems)
  - Compliance (ensuring conformance with information security policies, standards, laws and regulations)
- COBIT BMIS - Business Model for Information Security (\$ pago)
- ITIL-Security Management
- SAMM - Software Assurance Maturity Model
- OSSTMM - Open Source Security Testing Methodology Manual
- OCTAVE—Operationally Critical Threat, Asset, and Vulnerability Evaluation
- OWASP - Open Web Application Security Project
- CC - Common Criteria (ISO/IEC 15408)
- CPA - Commercial Product Assurance
- PCI-DSS—Payment Card Industry Data Security Standard

Outros tópicos relacionados:

- CISSP - Certified Information Systems Security Professional
- CSIRT - Computer Security Incident Response Team

Cada aluno deve produzir **e enviar ao professor**:

- Artigo PDF com 4-6 páginas sobre o tema designado
- Apresentação de 15-20 minutos sobre o tema (com slides)

From:  
<https://wiki.inf.ufpr.br/maziero/> - Prof. Carlos Maziero

Permanent link:  
[https://wiki.inf.ufpr.br/maziero/doku.php?id=sas:aspectos\\_de\\_governanca\\_da\\_seguranca](https://wiki.inf.ufpr.br/maziero/doku.php?id=sas:aspectos_de_governanca_da_seguranca)

Last update: **2013/11/01 17:31**

