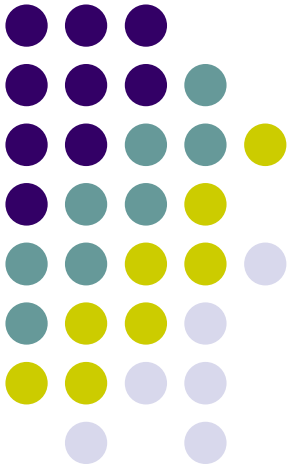
CRIPTOGRAFIA E SEGURANÇA DE DADOS
Aula Teórica 1

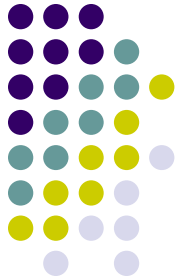
SUMÁRIO:

Introdução à Segurança de Informação



Docentes: S. Mavie & A. Covele
Maputo, 2024

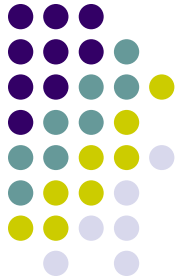
Introdução à Segurança de Informação



Obejctivos:

- Explicar o foco de segurança de informação;
- Definir segurança de informação;
- Definir os termos chaves e atributos críticos da segurança de informação;
- Enumerar os componentes de Sistemas de segurança; e
- Apresentar o modelo de segurança de informação

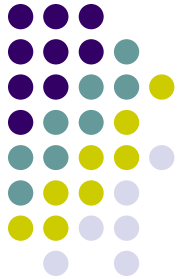
Segurança de Informação



- “A arte da guerra nos ensina a contar não só com a probabilidade do inimigo não chegar, mas com a nossa própria prontidão em recebê-lo e em tornar nossa posição inatacável”.

Sun Tzu

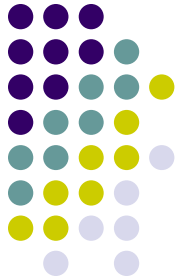
Segurança de Informação



- "*Do not figure on opponents not attacking; worry about your own lack of preparation.*".

BOOK OF THE FIVE RINGS

Segurança de Informação



Divide-se em três áreas de actividade:

1. Defesa contra catástrofes;
2. Defesa contra faltas ou falhas previsíveis; e
3. Defesa contra actividades não autorizadas.

Defesa contra catástrofes

- Visa, principalmente, conseguir que um sistema computacional, ou serviço que esse sistema presta, consiga sobreviver a catástrofes onde existam consequências a nível físico.

Defesa contra catástrofes

Catástrofe	Exemplos
Ambiental	Tremores de terra, incêndios, inundações, queda de raios, tempestades magnéticas, etc.
Política	Ataques terroristas, motins, etc.
Material	Degradação irreparável ou perda por roubo de equipamentos computacionais, como discos magnéticos, computadores portáteis, etc.

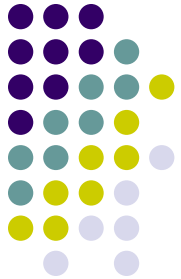
Defesa contra catástrofes

- Usa uma estratégia de sobrevivência que consiste na redundância de equipamentos ou informação:
  - Hadware (ex. RAID);
  - Equipamentos com replicação (ex. dois sistemas iguais); ou
  - Backups.

Defesa contra catástrofes

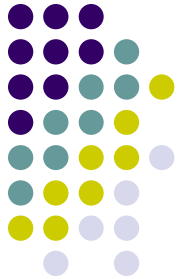
- A estratégia de sobrevivência deverá ter em conta:
  - relações custo/benefício; e
  - Possibilidade de ocorrência de catástrofes ou de dano causado pelas mesmas;

Defesa contra faltas ou falhas do sistema



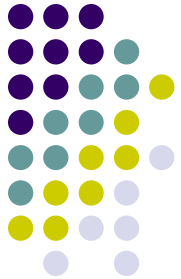
- Visa, sobretudo, minimizar o impacto de problemas que ocorrem com uma frequência maior, mas cujo impacto global é normalmente menor:
  - Queda no fornecimento de energia eléctrica ou falha na fonte de alimentação de um equipamento computacional;
  - Bloqueio de aplicações/SOs;
  - Falhas temporárias de conectividade

Defesa contra actividades não autorizadas



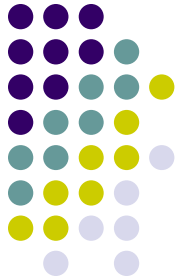
- Visa proteger os sistemas computacionais de acções tomadas por indivíduos contra o seu funcionamento normal;
- As actividades não autorizadas podem provir de dois universos populacionais distintos: **interno e externo.**

Defesa contra actividades não autorizadas



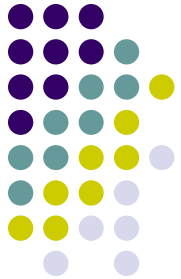
- As actividades ilícitas podem ser dividas em cinco tipos:
  1. Acesso a informação;
  2. Alteração de informação;
  3. Utilização exagerada/abusiva de recursos computacionais;
  4. Impedimento de prestação de serviços;e
  5. Vandalismo.

Termos chaves e conceitos críticos da segurança de informação



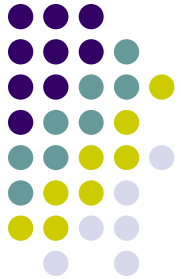
- **DEFESA** - conjunto de políticas e mecanismos desenhados, concretizados e implementados para:
  1. Diminuir as vulnerabilidades de um sistema;
  2. Detectar e contrariar/anular ataques passados ou actuais; e
  3. Minimizar os danos decorrentes de ataques bem sucedidos.

Vulnerabilidades, Ataques, Danos e Defesa



- **Defesa de perímetro –** consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes e em evitar interacções indesejáveis entre dois lados desse perímetro;
- O perímetro divide o universo de máquinas e redes em dois lados: um dos recursos e outro dos abusadores.

Vulnerabilidades, Ataques, Danos e Defesa

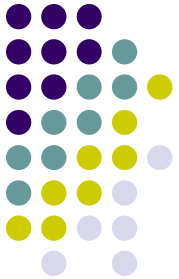


- **Defesa em profundidade –** segue uma abordagem mais complexa e quiçá mais eficaz, actuando em todos os níveis e não apenas em fronteiras entre domínios de segurança;
- Serve para detectar problemas internos em domínios de segurança que foram originados internamente, ou que passaram do mesmo originados fora.

Política *versus* Mecanismo de segurança

- **Políticas de segurança–** definem o foco da segurança e o que deve proteger;
- **Mecanismos de segurança** – são as tecnologias que permitem pôr em prática as políticas de segurança;
- **Domínio de segurança** – consiste num universo de recursos (máquinas, redes, etc.) e pessoas sujeitos à mesma política de segurança.

Definição de segurança de informação



- **Segurança de informação**:
  - É o sentido bem-informado de garantia de que os riscos e controlos de informação estão balanceados (James Anderson, citado por Whitman *et al (2012)*), ou;
- É qualidade ou estado de estar livre de perigo, ie, de adversários;
- Possui seis niveis a saber: físico, pessoal, de operações, comunicações, de rede e **de informação (CIA)**.

Definição de segurança de informação

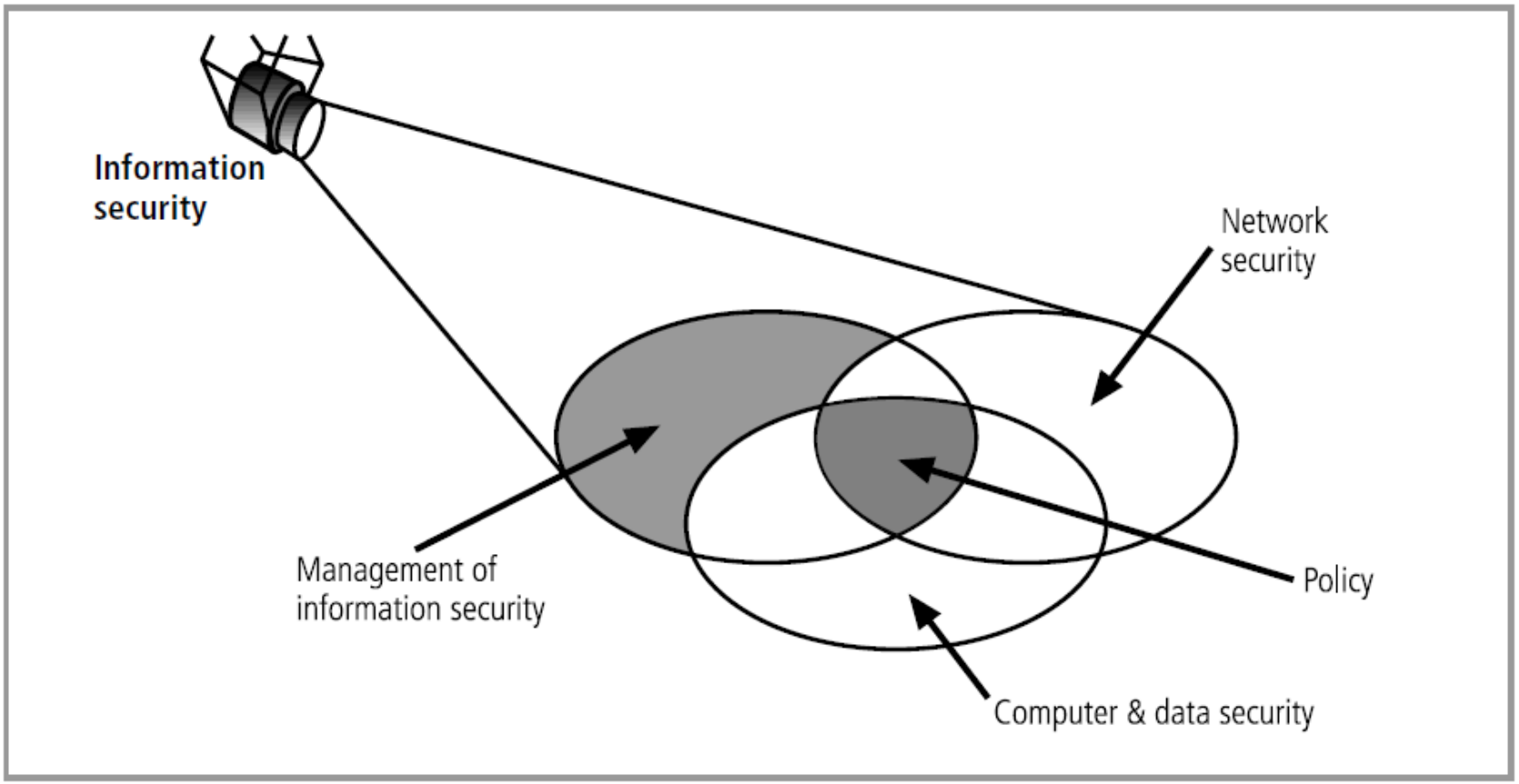


Figura 1: Componentes de Segurança de Informação (Infosec)

Fonte: Whitman et al (2012:9)

Modelo de segurança de informação

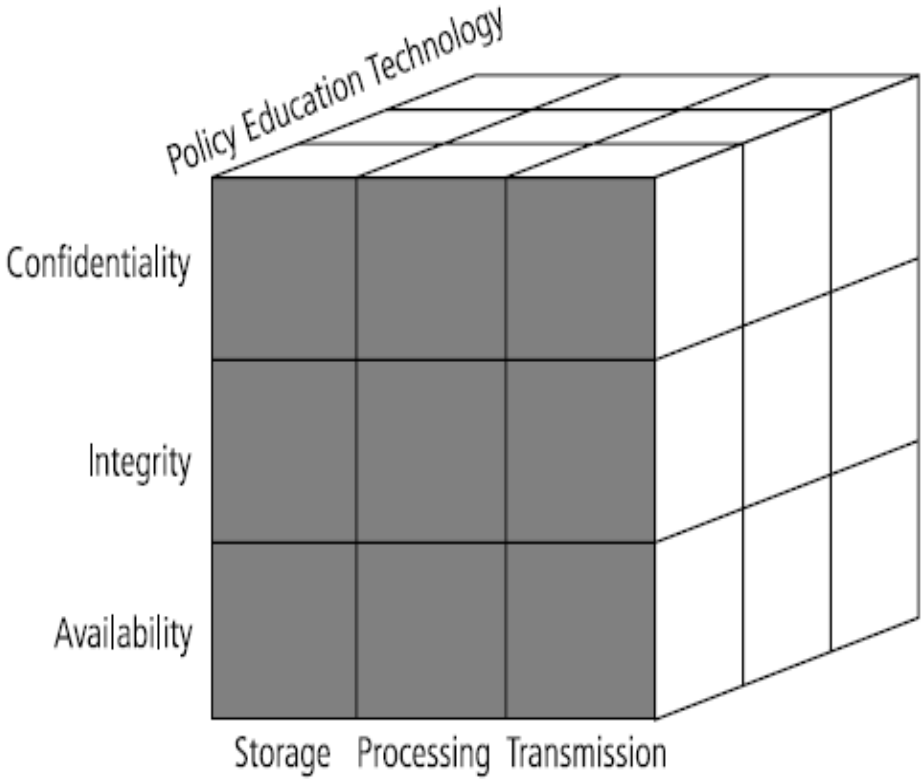
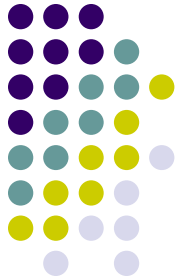


Figura 2: Modelo Infosec McCumber Cube

Fonte: Whitman et al (2012:16)

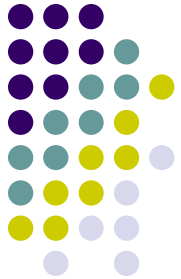
Segurança de Informação



Atitudes realistas:

- Não existe segurança a 100%;
- A segurança efectiva é cara;
- O retorno do investimento é difícil de avaliar;
- A segurança contrasta com a disponibilidade.

TPC



- História de Segurança de Informação
- Padrão ISO 27001
- Segurança pela ocultação;

Obrigado!