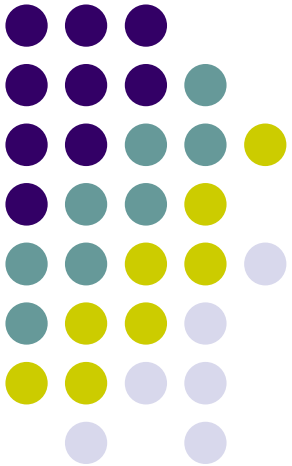
CRIPTOGRAFIA E SEGURANÇA DE DADOS
Aula Teórica 2

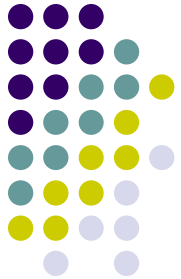
SUMÁRIO:

- O ciclo de vida de Desenvilvimento de sistemas de segurança; e
- Profissionais de segurança e Organização;
- Responsabilidade sobre dados



Docentes: J. Doho & C. Maculuve
Maputo, 2023

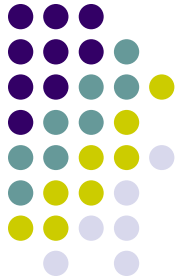
CRIPTOGRAFIA E SEGURANÇA DE DADOS



OBJECTIVOS:

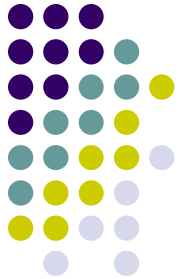
- Explicar o Ciclo de Vida de Desenvolvimento de Sistemas de Segurança (CVDSS/SecSDLC);
- Descrever as fases do CVDSS/SecSDLC);
- Identificar os profissionais de segurança de Informação e organização; e
- Distinguir as responsabilidades sobre dados

Implementação de segurança



- A implementação de sistemas de segurança nas organizações começa de algum ponto e não pode ser de dia para noite;
- É um processo incrimental que requer coordenação, tempo e paciência;
- Pode ser executada sob duas abordagens:
  - *Bottom-up*
  - *Top-down*

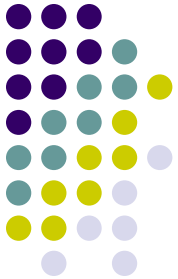
Implementação de segurança



Abordagem bottom-up:

- Os próprios administradores de sistemas tentam melhorar a segurança dos seus sistemas:
- **Vantagem:**
  - Perícia técnica dos administradores individuais
- **Desvantagem:**
  - Falta de apoio de participantes e resistência organizacional (gestores do topo), etc.

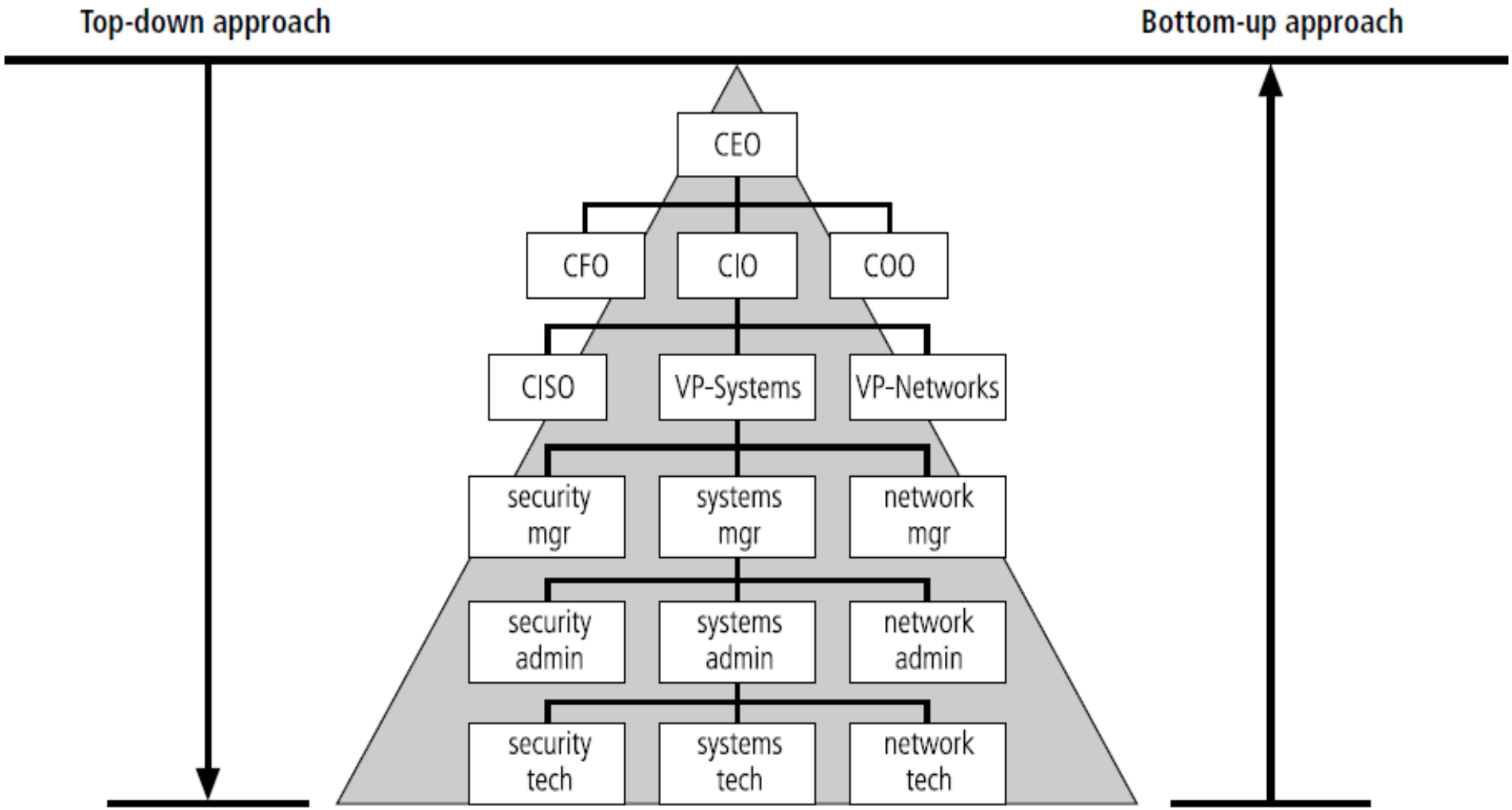
Implementação de segurança



Abordagem top-down:

- O projecto é iniciado pelos gestores de topo os quais elaboram políticas, procedimentos, determinam os objectivos e resultados esperados:
- **Vantagem:**
  - Tem maior probabilidade de sucesso;
  - Tem forte apoio dos gestores;
  - Tem um campeão e fundos dedicados;
  - Tem um processo claro de planeamento e implementação; e
  - Possui métodos de influenciar a cultura organizacional

Abordagens top-down vs bottom-up



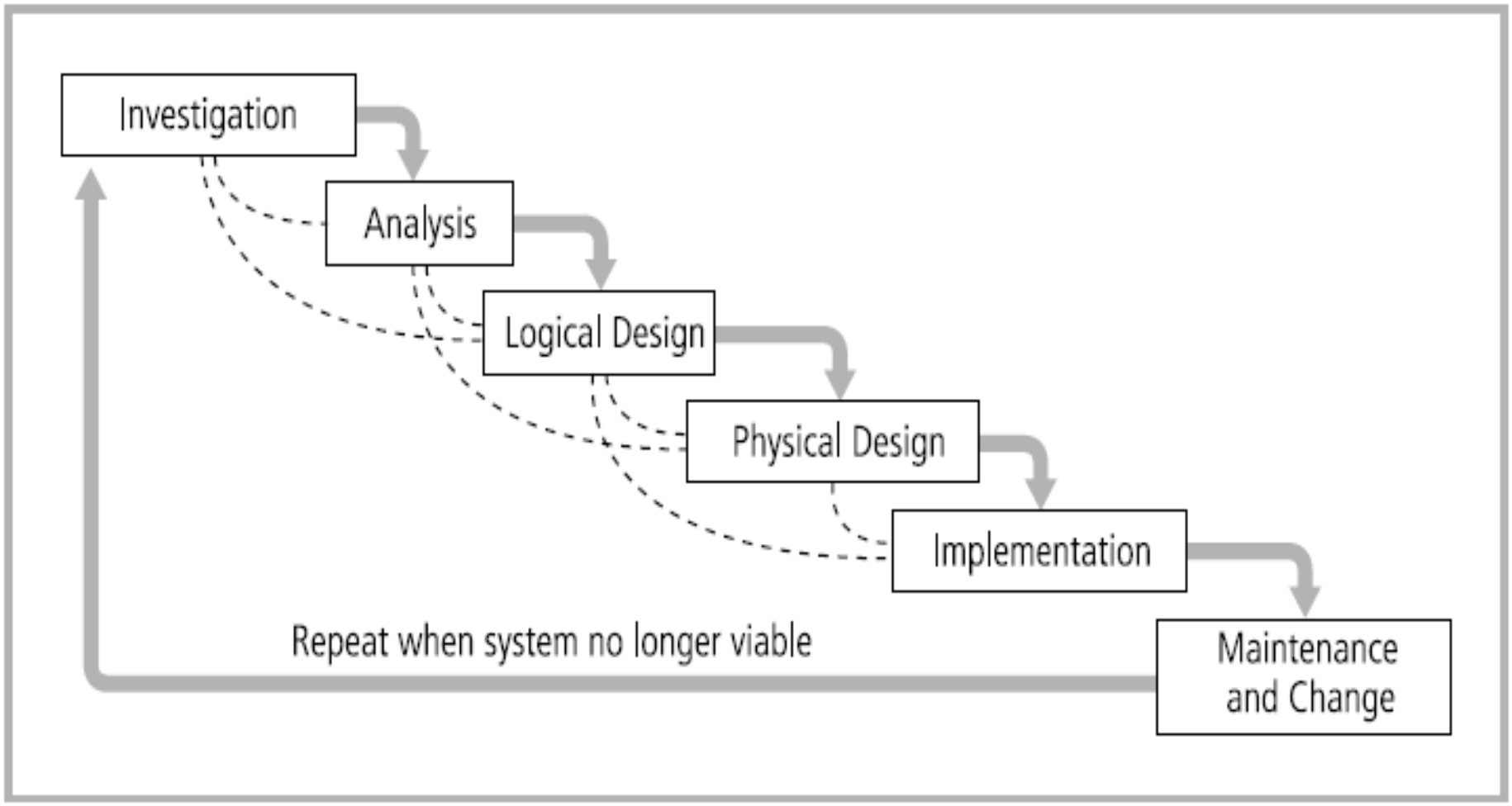
Ciclo de Vida de Desenvolvimento de Sistemas

- O CVDS (ou SDLC, em inglês) é uma **metodologia** de desenho e implementação de um sistema de informação;
- Metodologia é uma abordagem formal de resolução de problemas por meio de uma sequência estruturada de procedimentos;
- Garante um processo rigoroso com definição de objectivos claros e aumenta a probabilidade de sucesso.

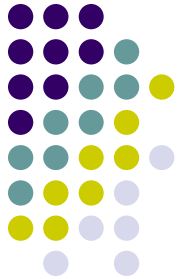
Ciclo de Vida de Desenvolvimento de Sistemas (cont.)

- O CVDS/SDLC tradicional consiste em seis fases organizadas em um modelo em cascata;
- O modelo em cascata implica que cada fase inicia com os resultados e informação obtidas na fase anterior;
- No final de cada fase faz-se uma revisão estruturada ou verificação da realidade e se determina se continua, descontinua, terciariza-se, adia-se ou retorna-se à fase anterior.

Fases do CVDSS/SecSDLC



1ª Fase – Investigação

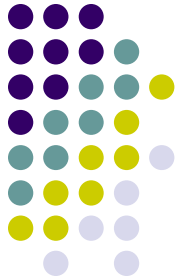


1. A Investigação começa com elaboração de um plano chamado EISP *(Enterprise Information System Policy)* no qual se determinam:
    1. Objectivos,
    2. Metas;
    3. Orçamento;
    4. Directiva para o arranque do processo; e
    5. Outras restrições

1ª Fase – Investigação (cont.)

2. Organização da equipa de gestores responsáveis, empregados e empreiteiro;
3. Análise de problemas que originaram o processo;
4. Definição do escopo do projecto, os objectivos específicos, as metas e as restrições adicionais não cobertas no EISP;
5. Análise da viabilidade organizacional para aferir se a organização tem ou não recursos e compromisso para conduzir uma análise de segurança bem sucedida.

2ª Fase – Análise



- Esta fase consiste primariamente na avaliação da organização, os seus sistemas existentes e a sua capacidade para suportar os sistemas propostos;
- Os analistas começam por determinar o que se espera que o novo sistema faça e como ele irá interagir com os sistemas existentes; e
- Termina com a documentação das descobertas e uma actualização da análise de viabilidade.

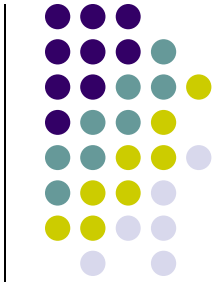
2ª Fase – Análise

1. Estudo dos documentos da fase anterior;
2. Análise preliminar de políticas ou programas de segurança existentes juntamente com as actuais ameaças e os controlos associados documentados;
3. Análise de questões legais;
4. Início de gestão de risco (identificação, classificação e avaliação dos níveis de risco das ameaças sobre a segurança da organização e da informação armazenada e processada).

3ª Fase – Desenho lógico

- Utiliza a informação obtida da fase de análise para começar a criar os sistemas solução para um problema de negócio;
- Em quaisquer sistemas solução, é imperativo que o primeiro e factor determinante seja a necessidade empresarial;
- Baseado na necessidade empresarial, são seleccionadas aplicações para prover serviços necessários, e então escolhidos os suportes de dados e estruturas capazes de prover os inputs necessários.

3ª Fase – Desenho lógico

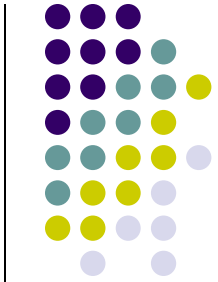


1. Criação e desenvolvimento de modelos/esquemas para a segurança de informação;
2. Exame e implementação de políticas chave que influenciarão as decisões futuras;
3. Planificação de acções de resposta aos incidentes:
    1. Como o negócio irá continuar em caso de perda?
    2. Que passos são executados quando ocorre um ataque?
    3. Que será feito para restaurar informação/sistemas?

4ª Fase – Desenho Físico

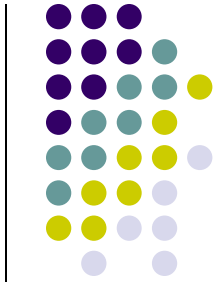
1. Avaliação de tecnologias de segurança de informação necessárias para executar os planos da fase de desenho lógico, gerando soluções alternativas e determinando o desenho final;
2. Revisão do plano do desenho lógico para estar alinhado com as alterações quando o desenho físico estiver terminado;

4ª Fase – Desenho Físico



3. Preparação de critérios para a definição de soluções bem sucedidas;
4. Desenho de medidas de segurança física para complementar as soluções tecnológicas;
5. Estudo de viabilidade para determnar a prontidão da organização para o projecto proposto;
6. Apresentação do desenho ao campeão e os patrocinadores.

5ª Fase – Implementação

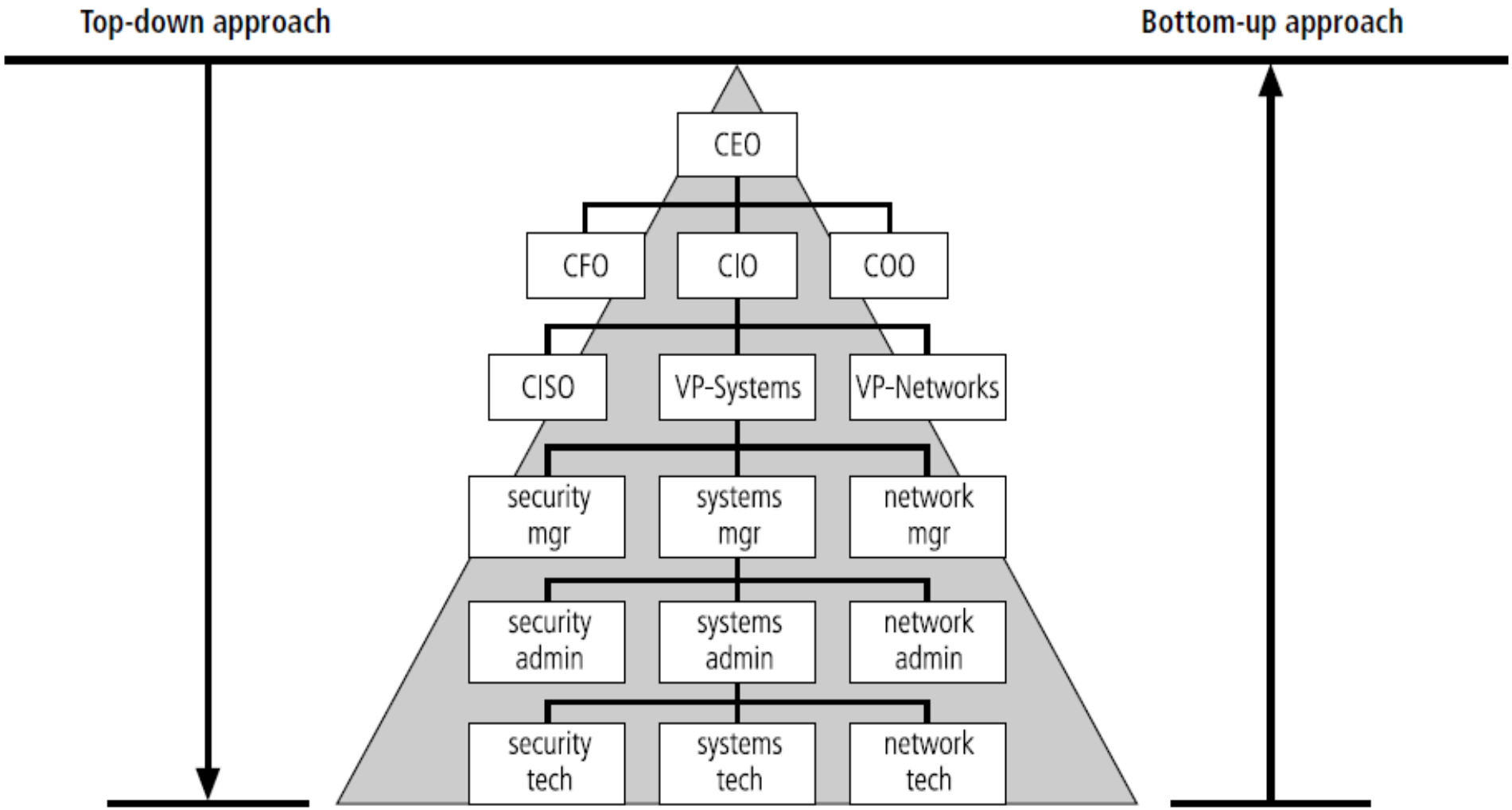


1. Aquisição (construção ou compra), teste, implementação e novo teste das soluções de segurança;
2. Avaliação das competências técnicas das pessoas e condução de treinamento específico ou programas de formação;
3. O pacote inteiro testado é apresentado à gestão suprior para aprovação final.

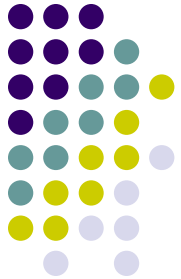
6ª Fase – Manutenção e alteração

1. Assistir e modificar o sistema durante a sua vida útil;
2. Testar periodicamente o sistema para responder as necessidades do negócio;
3. Modernizar e remendar se necessário.
4. Constatemente monitorar, testar, modificar, actualizar e reparar para adeguar às alterações das ameaças.

Profissionais de Segurança e Organização



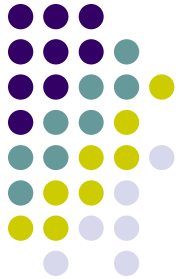
Profissionais de Segurança e Organização



Podemos encontrar dois grupos de profissionais de segurança de informação dentro de uma organização, nomeadamente:

- Gestão Sénior; e
- Equipa do projecto do sistema de segurança.

Gestão sénior

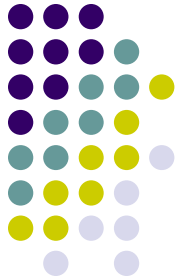


- **Chief Information Officer (CIO)** – é responsável por aconselhar o presidente executivo (CEO), presidente, ou dono da empresa na planificação estratégica que afecta a gestão de segurança de informação;
- **Chief Information Security Officer (CISO)** – é primariamente responsável por avaliar, gerir e implementar a segurança de informação na organização.

Equipa do Projecto de Segurança de Informação

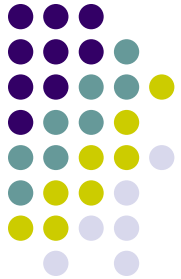
- **Campeão/*champion*** – executivo sénior que promove o projecto e garante o seu apoio, quer financeira ou administrativamente, nos níveis mais altos da organização;
- **Líder da equipa/Team leader** – um gestor de projectos, que pode ser do nível hierárquico departamental ou gestor da unidade do staff.

Equipa do Projecto de Segurança de Informação



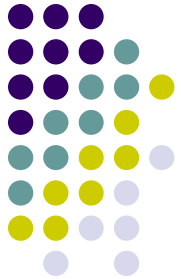
- **Desenvolvedores de política de segurança** – pessoas que entendem a cultura da organização, políticas existentes e requisitos para o desenvolvimento e implementação de políticas de éxito;
- **Especialista de avaliação de risco** – pessoa que entende técnicas de avaliação de risco financeiro, o valor dos activos da organização, e os métodos de segurança a serem usados.

Equipa do Projecto de Segurança de Informação



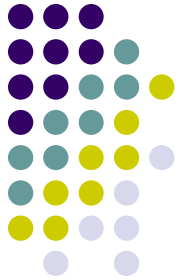
- **Profissionais de segurança** – especialistas dedicados, treinados e bem educados em todos os aspectos de segurança de informação quer de ponto de vista técnico ou não técnico;
- **Administradores de sistemas** – pessoas cuja responsabilidade primária é a administração dos sistemas que hospedam a informação utilizada pela organização.

Equipa do Projecto de Segurança de Informação



- **Utilizadores finais** – aqueles que o novo sistema irá afectar directamente.
- Idealmente, devem fazer parte da equipa usuários de vários departamentos, níveis e graus de conhecimento técnico para permitir o foco na aplicação de controlos realísticos de tal maneira que não perturbem as actividades de negócio essenciais que procuram proteger.

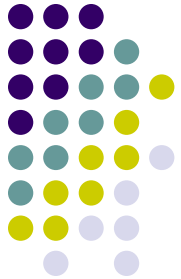
Responsabilidades sobre dados



- Proprietários de dados/*Data owners*
- Guardiões de dados/*Data custodians*
- Utilizadores de Dados/*Data users*

Bibliografia

- WHITMAN, M. & MATTORD, H (2012). *Principles of Information Security*, 4ª Ed. Boston:Course Technology.



Obrigado!