Segurança de Ambientes com uso da TI

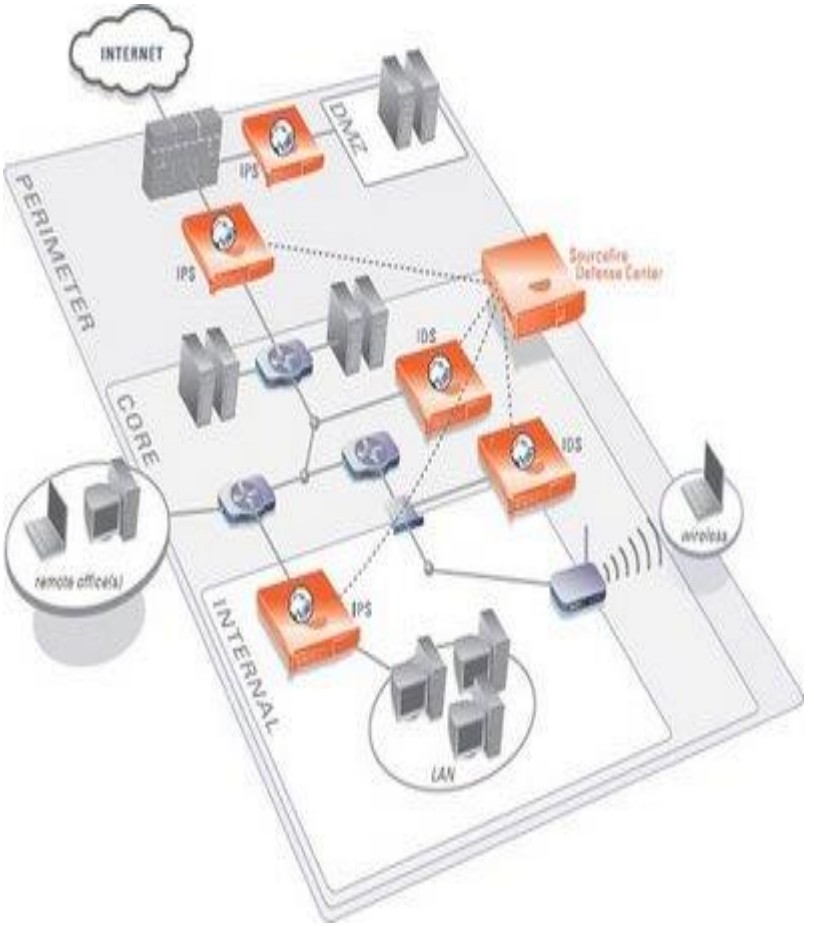
Prof. Dr. Mauricio Pitangueira

INF 025 – AUDITORIA E SEGURANÇA DE SISTEMAS

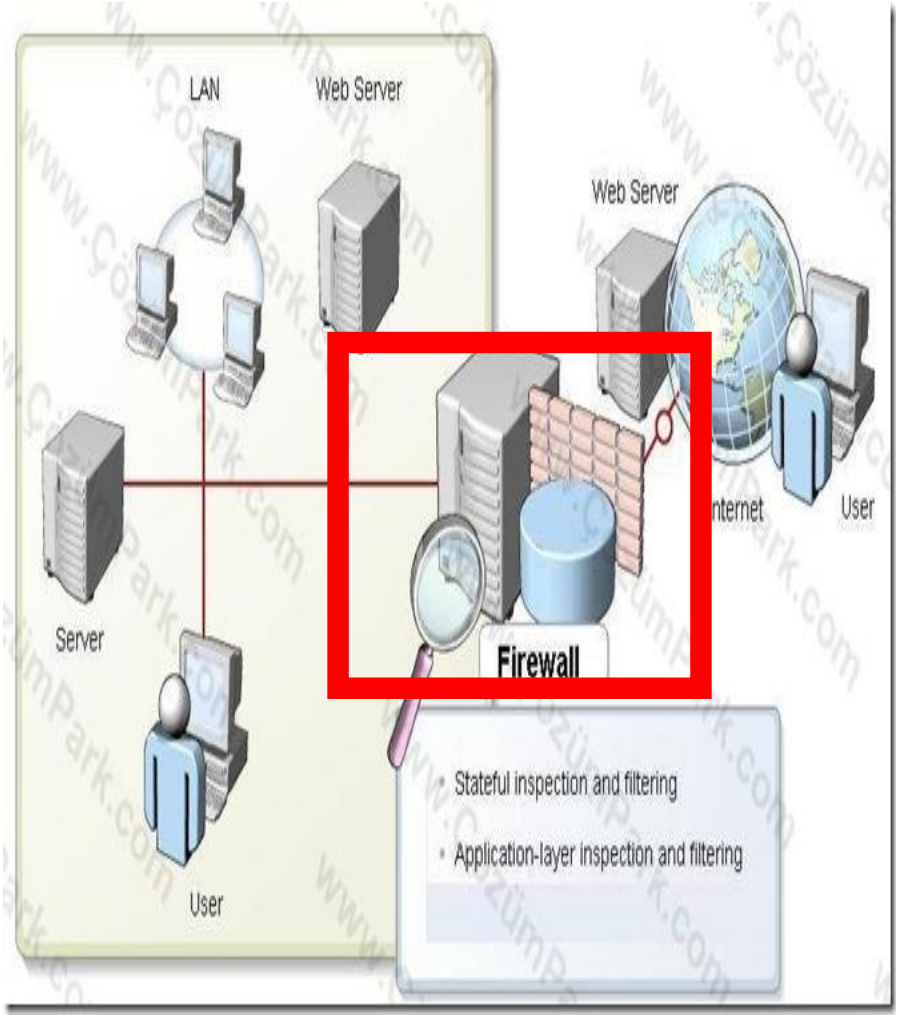
antoniomauricio@ifba.edu.br

Segurança do Ambiente Físico

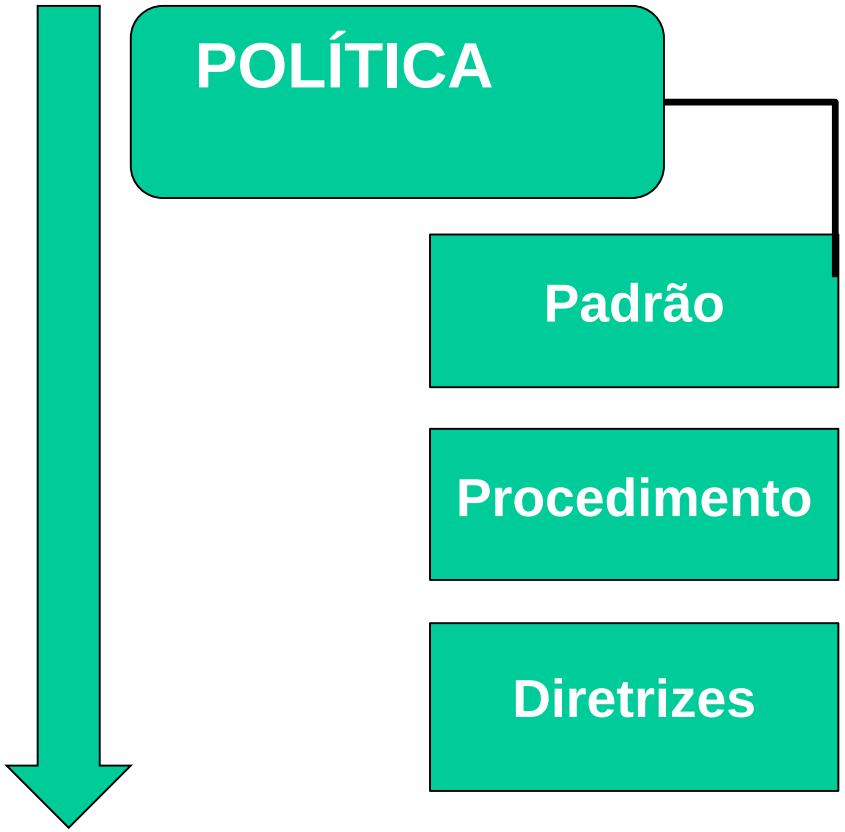
- **Perímetro de Segurança:**
  - É o **contorno ou linha imaginária** que delimita uma área ou região separada de outros espaços físicos por um conjunto qualquer de barreiras.
  - A definição clara do perímetro de segurança ajudar a estabelecer melhor os investimentos e definir que tipos de barreiras são mais adequados para a proteção do ativo da informação
  - **Perímetros a serem protegidos podem ser:**
    - Prédios;
    - Geradores;



Segurança do Ambiente Lógico



Controle de Acesso



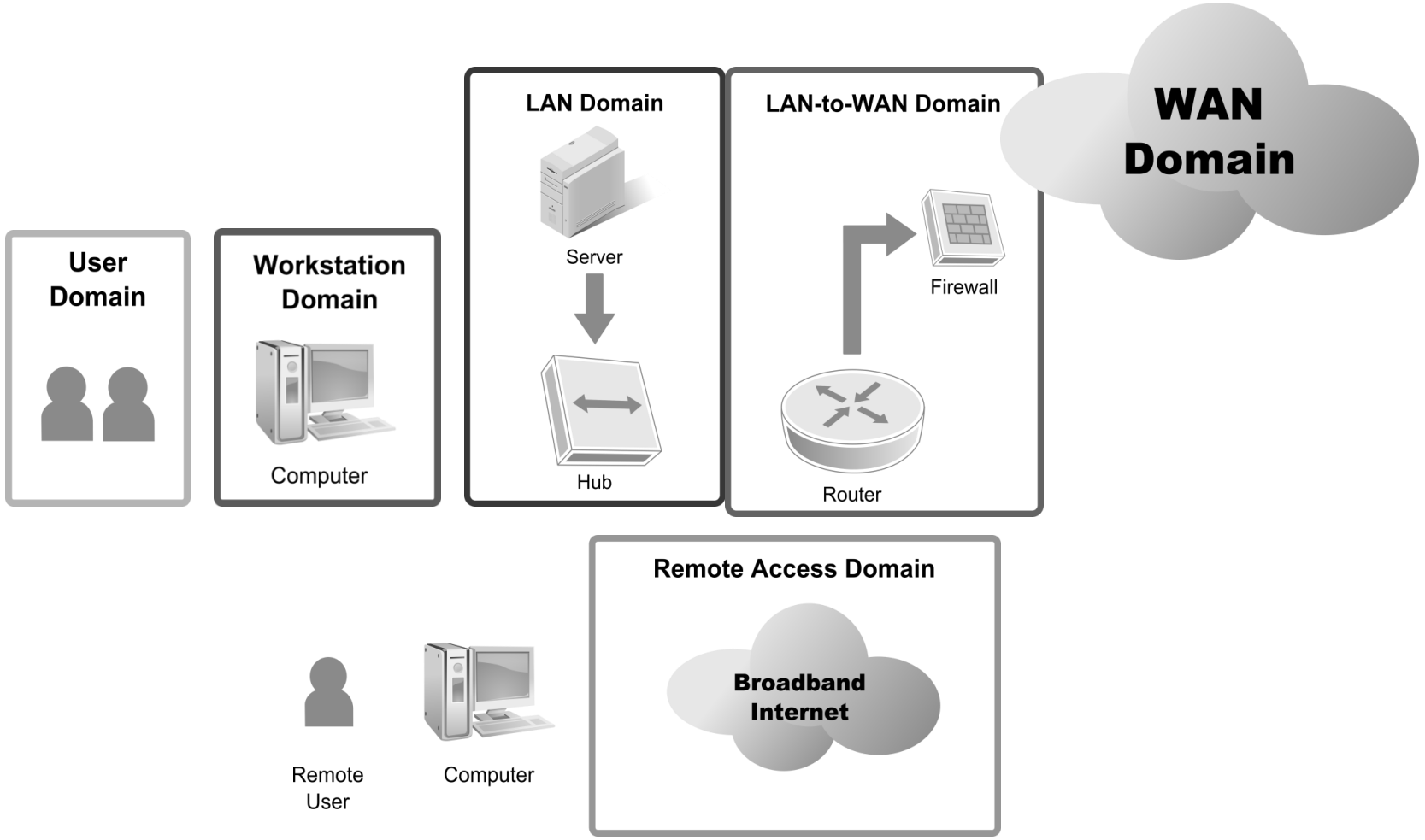
Curta declaração escrita que define um curso de ação ou direção que se aplica a toda organização

Definição escrita detalhada de como o hardware e software devem ser usados.

Instruções escritas de como usar políticas e padrões

Curso de ação sugerido para uso da política, dos padrões ou procedimentos

Domínios de uma infraestrutura de TI



Kim & Solomon,2014.

Ameaças comuns no domínio do usuário

1. Falta de conscientização do usuário
2. Apatia dos usuários com as políticas
3. Violações de políticas de segurança
4. Usuários inserem cd/dvd/usb etc com arquivos pessoais.
5. Download de arquivos
6. Usuário descontente faz uso de sabotagem
7. Perda de interesse de funcionário
8. Chantagem ou extorsão de funcionário

9. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

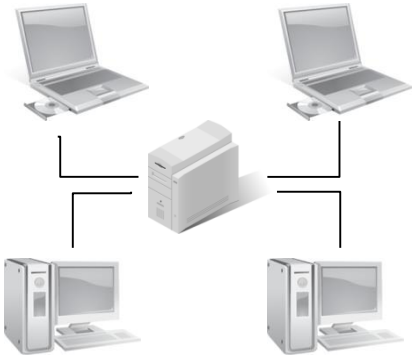
Ameaças comuns no domínio da estação de trabalho

1. Acesso não autorizado à estação de trabalho
2. Acesso não autorizado a sistemas, aplicativos e dados
3. Vulnerabilidade do SO
4. Vulnerabilidade através de atualizações de softwares
5. Infecção por vírus, código malicioso, etc.
6. Download de arquivos

7. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

Ameaças comuns no domínio da LAN

1. Acesso não autorizado à LAN
2. Acesso não autorizado a sistemas, aplicativos e dados
3. Vulnerabilidade de sistemas, softwares
4. Servidores com diferentes Hw’s, SO’s e SW
5. Confidencialidade de dados comprometida



6. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

Ameaças comuns no domínio da LAN para WAN

1. Sondagem e varredura de porta de rede sem autorização
2. Acesso não autorizado
3. Vulnerabilidade no roteador, firewall, etc..
4. Usuários locais fazem download de arquivos desconhecidos em fontes desconhecidas

1. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

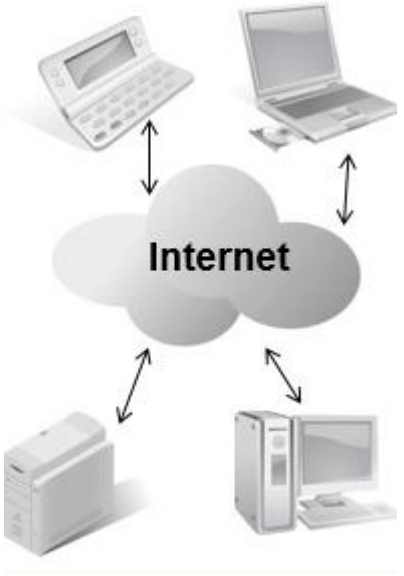
Ameaças comuns no domínio da WAN

1. Aberta, pública e acessível a qualquer um.
2. Boa parte do tráfego da internet é enviada em texto claro
3. Vulnerável a ataques maliciosos
4. Vulnerável a ataques de negação de serviços
5. Vulnerável a adulteração de dados e informação
6. Aplicativos TCP/IP são inerentemente inseguros
7. Hacker, invasores enviam livremente vírus, código malicioso, etc por e-mail.

8. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

Ameaças comuns no domínio de acesso remoto

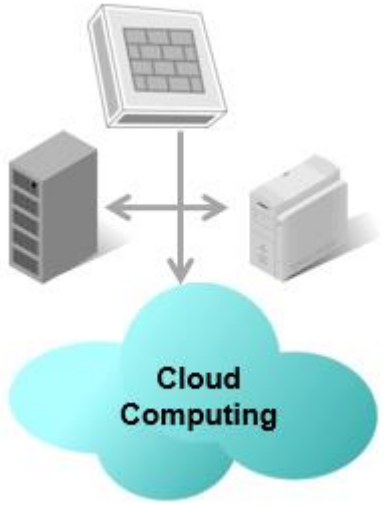
1. Ataques de ID e de senha do usuário
2. Múltiplas tentativas de acesso e ataques a controle de acesso
3. Acesso remoto não autorizado a sistemas de TI, aplicativos e dados
4. Dados confidenciais são comprometidos remotamente
5. Vazamento de dados
6. Laptop de trabalhador móvel é roubado



7. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?

Ameaças comuns no domínio de sistema/Aplicativos

1. Acesso não autorizado a data centers, sala de computadores e gabinetes de fiação
2. Dificuldade em gerenciar servidores que requerem alta disponibilidade
3. Vulnerabilidade de SO do servidor
4. Dados perdidos ou corrompidos



1. QUAIS MEDIDAS DE REDUÇÃO PODEM SER ADOTADAS?