(CMPSEGS)

Segurança de Sistemas

Tecnologia em Análise e Desenvolvimento de Sistemas

Princípios e propriedades fundamentais para a segurança de sistemas

Prof. Me. Leonardo Arruda

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Imaginem o seguinte...

Vocês são meus sócios numa empresa gigante de dados e TI. Vamos construir toda a infraestrutura, desde o terreno até a segurança do datacenter;

Nome?

Setor para atender? (Saúde, bancos, indústria, governo, etc...)

INSTITUTO FEDERAL
São Paulo
Campus Campinas

CPD (Centro de Processamento de dados)

Qual o local?

- Definir um local físico em Campinas para montar nosso datacenter.

- Reflexão:
- O que precisamos pensar para escolher o melhor lugar?
  - Quais problemas físicos podem acontecer e que a gente não controla?
  - Campinas já teve desastres naturais? Quais?
  - Energia e internet, vocês acham que podem falhar?

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança física – Desastres Naturais

Segurança física – Desastres Naturais

Campinas está preparada para eventos climáticos extremos? Especialistas apontam gargalos e alertam para urgência de ações

Metrópole é vulnerável a temporais e, com as mudanças climáticas, pode ter chuvas fortes com mais frequência, explicaram os pesquisadores ouvidos pela reportagem.

Por João Gabriel Alvarenga, g1 Campinas e região

17/05/2024 06h55 · Atualizado há um ano

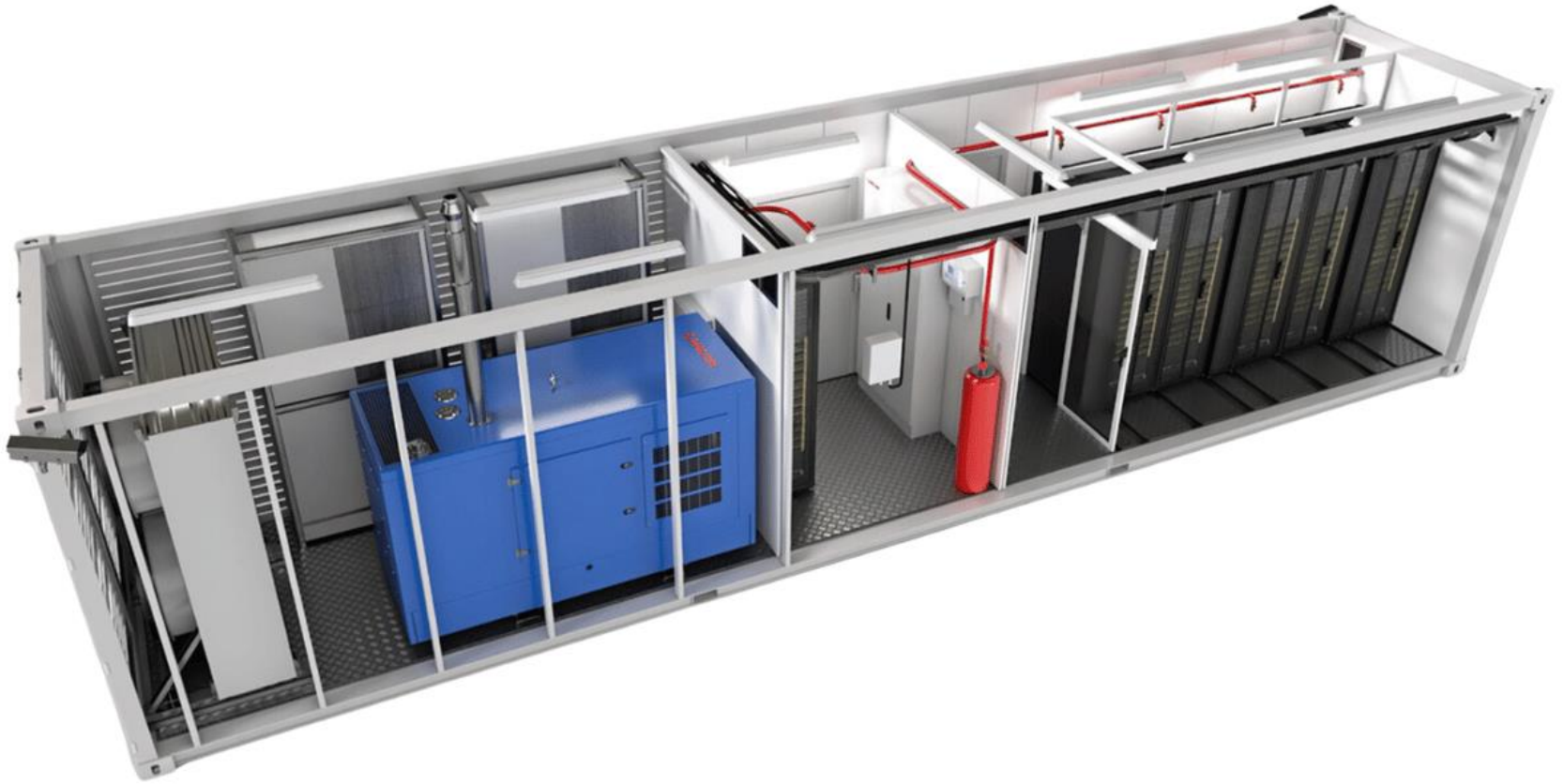
https://g1.globo.com/sp/campinas-regiao/noticia/2024/05/17/campinas-esta-preparada-para-eventos-climaticos-extremos-especialistas-apontam-vulnerabilidades-e-alertam-para-urgencia-de-acoes.ghtml

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança física – Incêndios

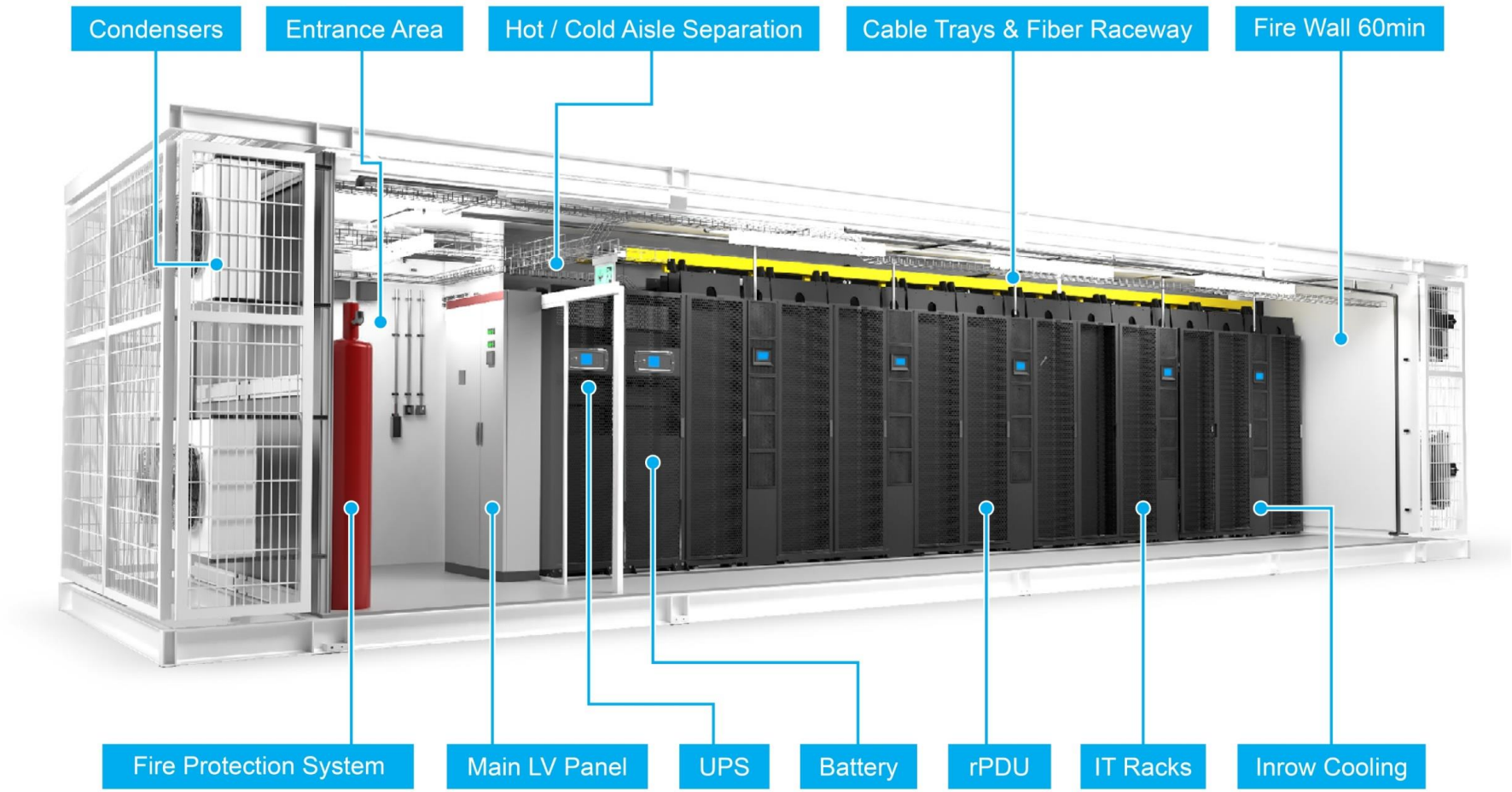
INSTITUTO FEDERAL
São Paulo
Campus Campinas

CPD (Centro de Processamento de dados)



INSTITUTO FEDERAL
São Paulo
Campus Campinas

CPD (Centro de Processamento de dados)



INSTITUTO FEDERAL
São Paulo
Campus Campinas

CPD Google

https://www.google.com/about/datacenters/inside/streetview/

https://youtu.be/zDAYZU4A3w0?t=89

INSTITUTO FEDERAL
São Paulo
Campus Campinas

CPD (Centro de Processamento de dados)

- CPD (Centro de Processamento de Dados);
  - É o coração da TI e da empresa;
  - Local onde concentram todos os dados;
  - Em empresas menores, é importante ter um sala para o CPD:
    - Bom para a segurança;
    - Não é luxo, e sim uma necessidade;
  - Toda empresa que possua qualquer tipo de informatização deveria ter um CPD;

INSTITUTO FEDERAL
São Paulo
Campus Campinas

O que vamos precisar?

Servidores

- Equipamento robustos, neles estão armazenados arquivos, bancos de dados, hospedagem páginas, gerenciam impressões, gerenciam mensagens eletrônicas, etc.
- Ex: Dell PowerEdge R760 (Pesquisem o valor, quanto custa?)

Armários, Bastidor ou Rack’s

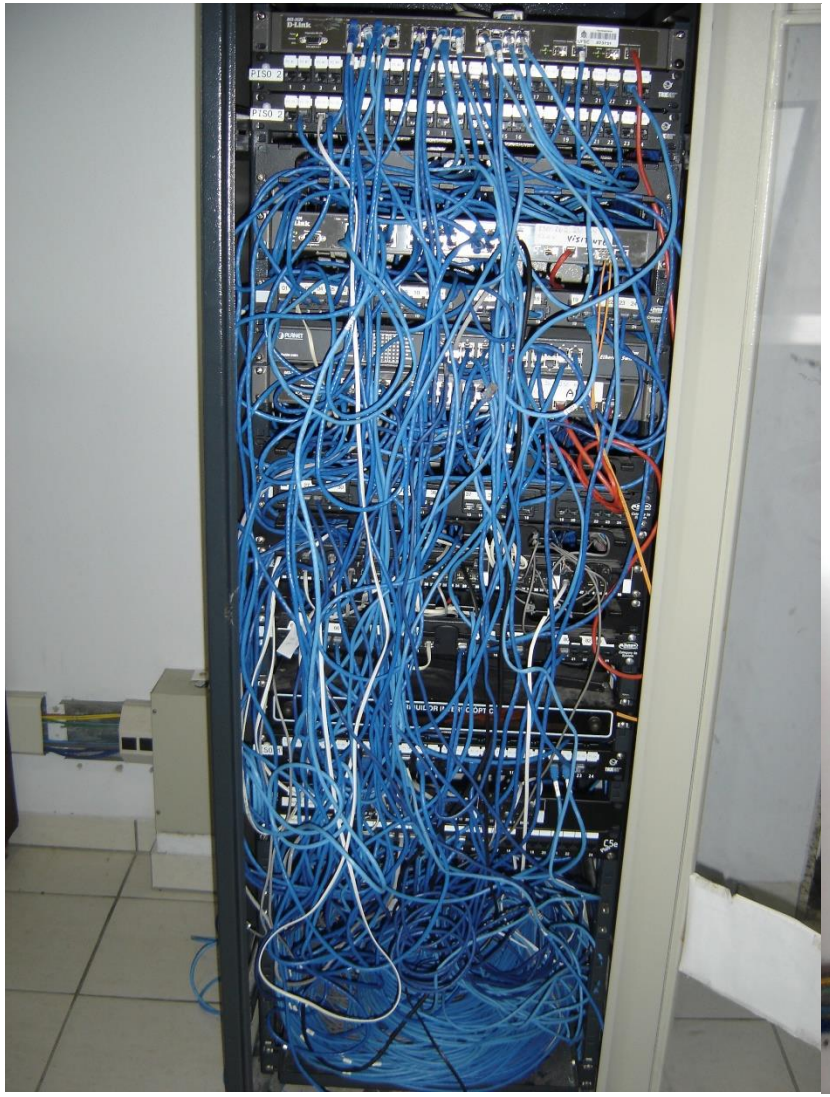
- Local onde ficam instalados os equipamentos de rede;
- Ex: Dell APC Rack NetShelter SX 24U

Equipamentos de rede

- Patch Panels, Switches, Roteadores também fazer parte do CPD.

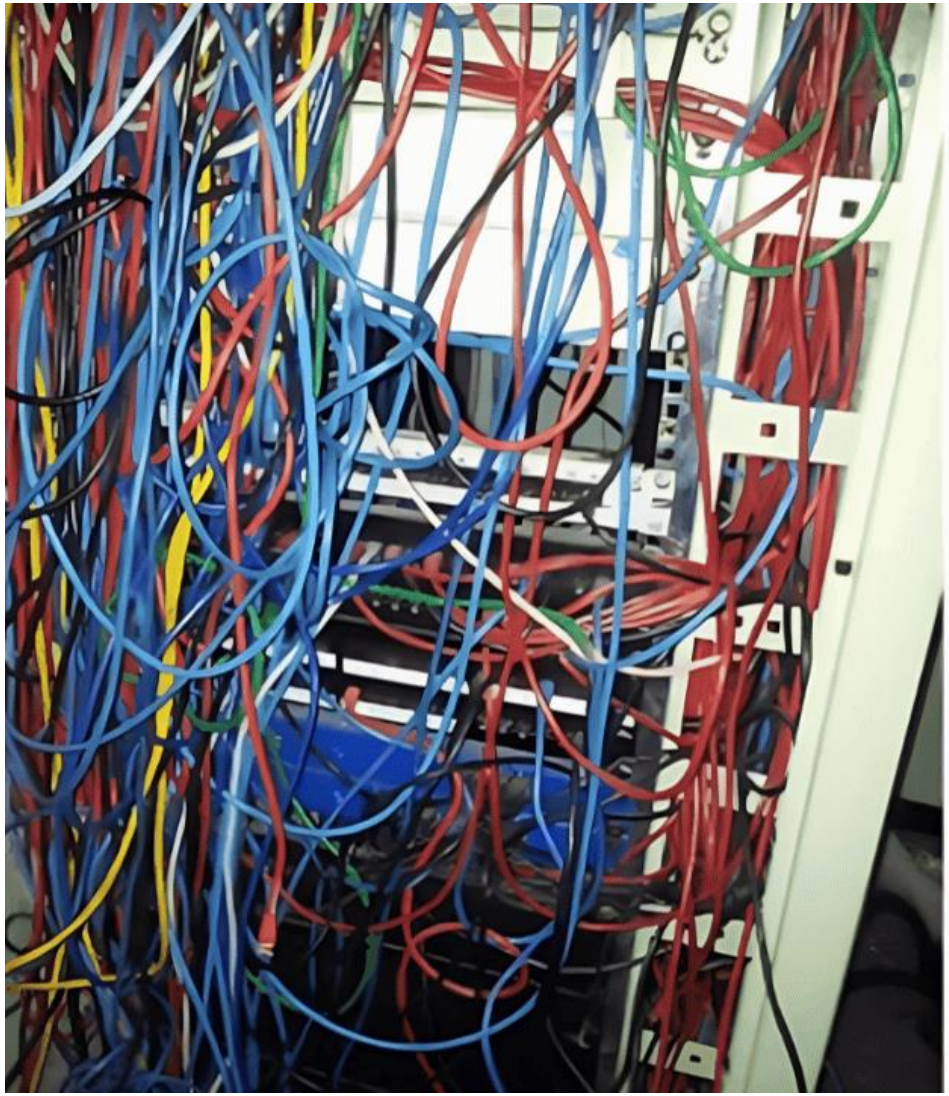
INSTITUTO FEDERAL
São Paulo
Campus Campinas

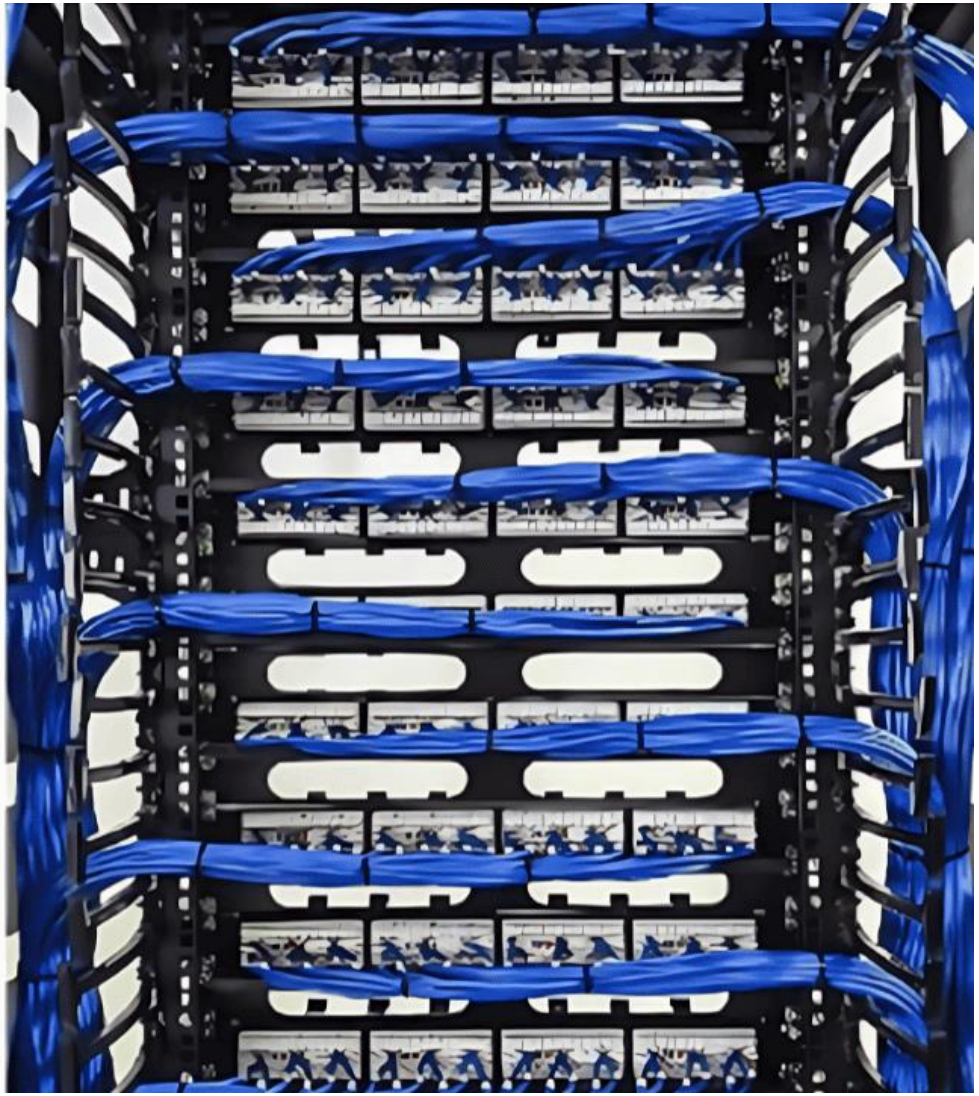
Desorganização vs. Organização



INSTITUTO FEDERAL
São Paulo
Campus Campinas

Crescimento não programado vs. Programado





INSTITUTO FEDERAL
São Paulo
Campus Campinas

Preciso de mais um ponto de rede

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Problemas frequentes

- Amplicação de novos pontos de Rede;
- Falta de restrição e de normas de acesso;
- Facilidade a acesso a HUB´s e Switch´s;
- Identificação de Cabos;
- Falta de Cabeamento Estruturado;

Outros equipamentos

- No break;
- Ar condicionado;
- Extintores de incêndio;
- Câmeras de CFTV;
- Controle de Acesso;

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Climatização

- Os computadores precisam estar em ambiente de temperatura controlada
- Mídias devem ser protegidas em local seco e arejado para evitar o mofo
- Centro de dados precisam ter temperatura controlada entre 17 a 20ºC

Climatização

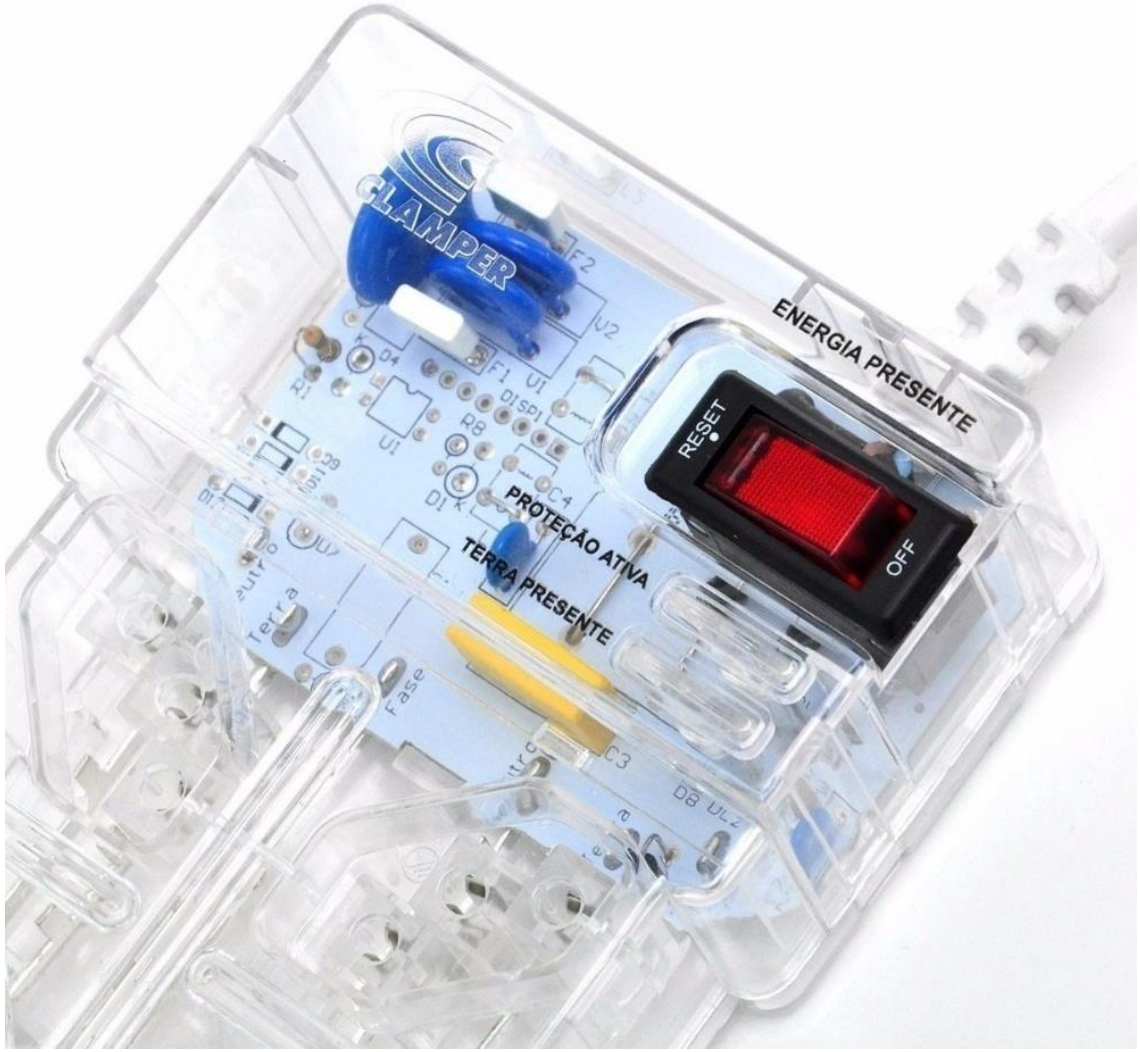
- Uma empresa que deseja ter seus sistemas informatizados precisa ter consciências dessas variáveis e saber o risco que corre por não possuir um sistema de climatização.

Equipamentos de proteção

- Em empresas menores ou startups, também há a possibilidade de utilização de equipamentos de proteção menos caros

- Filtros de linha com **DPS**
- Dispositivo de Proteção contra Surto

Equipamentos de proteção



Equipamentos de proteção

- **Estabilizadores**
- Tipo de proteção: Subtensões, Sobretensões, Surtos, Pico de Energia, Ruídos

- Regula a tensão de entrada.

Equipamentos de proteção

- **No-Break**
  - Tipo de proteção: Subtensões, Surto, Pico de energia, Ruído, Black-out.
  - Por possuírem baterias internas, protegem o hardware contra queda de energia;
  - Evita falhas de dispositivos do sistema como memórias, armazenamento, etc.

Gerador

- Usados para manter o fornecimento contínuo de energia
- Requer um ambiente especial
- Baseados em motores a diesel
- Ex: Procurar valor de um gerador à diesel de 72 Kva

Controle de Acesso

- O controle de acesso em locais que demandam maior grau de segurança é indispensável;

- Busca evitar o acesso de pessoas não autorizadas.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Tipos de Controle de Acesso

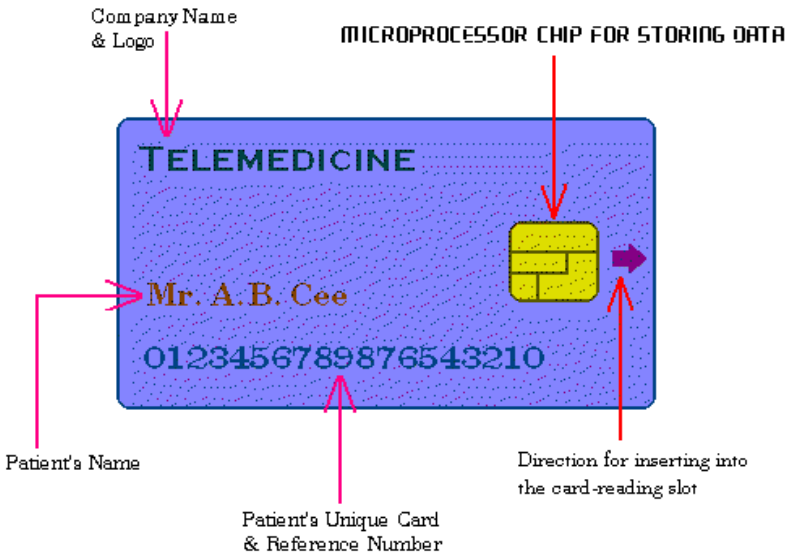
- Usuário e senha;
- Smartcard;
- Biometria (Impressão Digital, Iris, Voz)
- Token;

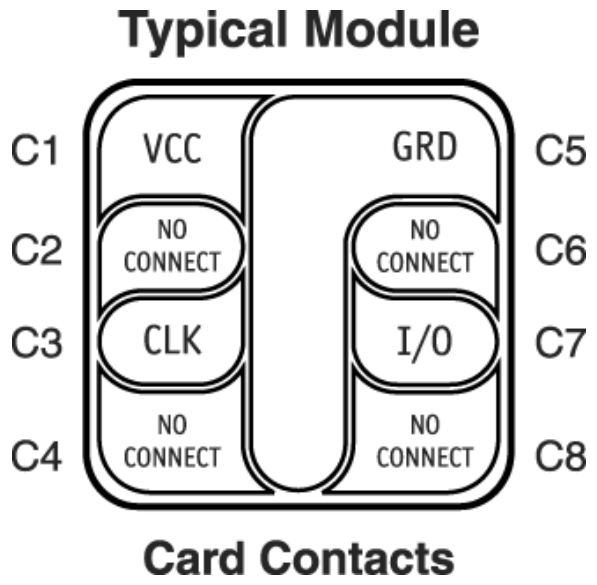
Controle de Acesso: usuário e senha

- Controle mais comum e mais aplicado;
- Responde sempre a duas das três perguntas sobre um controle de acesso;

Controle de Acesso: SmartCard

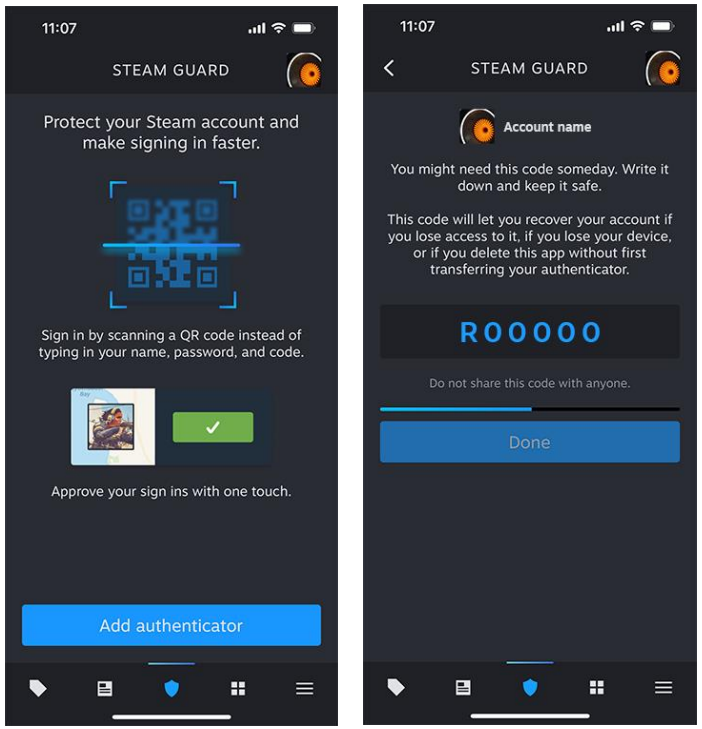
- Permitem a geração de chaves criptográficas RSA (Rivest-Shamir-Adleman) no próprio cartão, o que garante maior segurança, pois esse processo será realizado dentro de um dispositivo que já possui segurança intrínseca a ele.





Controle de Acesso: Token

- Senha gerada no instante da utilização
- Usuário completa com números impressos num cartão ou aparelho.

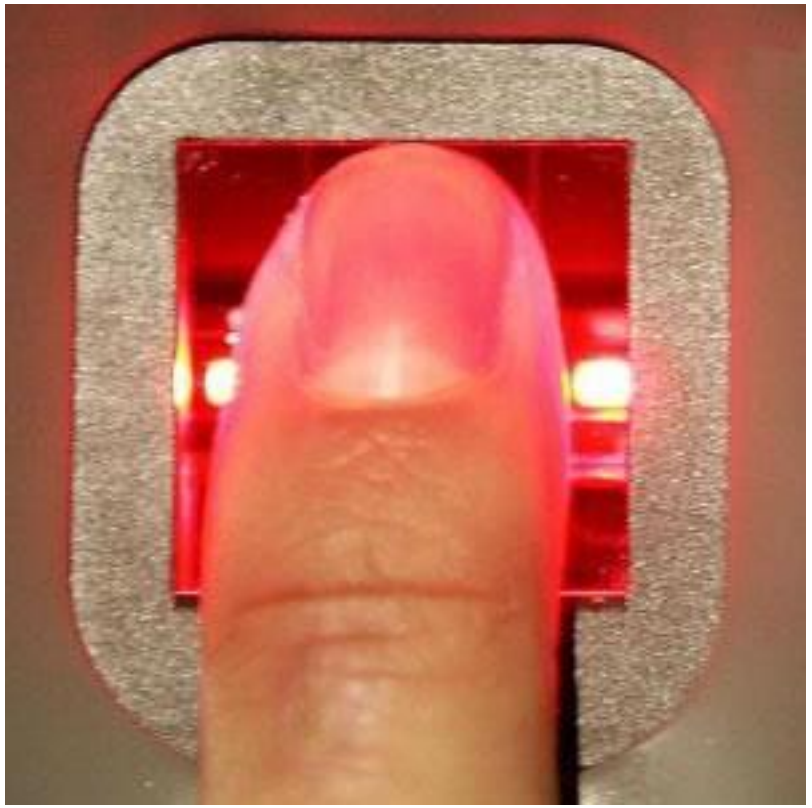


Controle de Acesso: Biometria

- É a medição de parâmetros biológico com o objetivo de identificar e autenticar pessoas
- Os sinais biológicos mais usados são:
  - Impressão Digital
  - Características da Iris
  - Características da Retina
  - Reconhecimento da Voz
  - Reconhecimento da Face
  - Reconhecimento da Assinatura

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Controle de Acesso: Biometria



INSTITUTO FEDERAL
São Paulo
Campus Campinas

Controle de Acesso: Biometria

Controle de Acesso: CFTV

- Sistema de TV que distribui sinais provenientes de câmeras localizadas em locais específicos, para um ou mais pontos de visualização.

- O sistema de CFTV é na sua versão mais simples constituído por câmera(s)

- O fato de ser um Circuito Fechado e a captura e transmissão das imagens ser de acordo com os conceitos e formatos da televisão analógica conduziu à sigla CFTV.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Controle de Acesso: CFTV

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança física: Vulnerabilidades

- Construção de CPD em área de inundação;
- Falta de controle de acesso;
- Servidor sendo usado com estação de trabalho;
- Falta de sistemas de climatização e manutenção de energia.
- Controle dos Backups e seus sistemas de gerenciamento

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança física: Ameaças

- Remoção de material não autorizado (Roubo);
- Arrombamento;
- Acesso ilegítimo a pontos de rede;
- Enchentes;
- Incêndios;
- Engenharia Social;

Políticas de Segurança Física

- Objetivo
  - Proporcionar segurança para o ambiente de TI em todos os componentes da Informação
- Foco da Segurança Física está na
  - Proteção de servidores
  - Proteção de concentradores
  - Manutenção do Link de Dados
  - Controle de Acesso aos ambientes de TI
  - Controle de Temperatura
  - Manutenção da energia elétrica
  - Elaboração de planos de contigência

Políticas de Segurança Física

- Algumas ações
  - Acesso restringido a todos os usuários
  - Material etiquetado e contabilizado
  - Sala Específica para Dados
  - Sistemas de Controle de Temperatura
  - Controle de Acesso
    - Humano de entradas e saídas
    - Controle de entrada/saída de material do edifício
  - Códigos de Acesso
  - Tarefas vigiadas por câmeras

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança da Informação

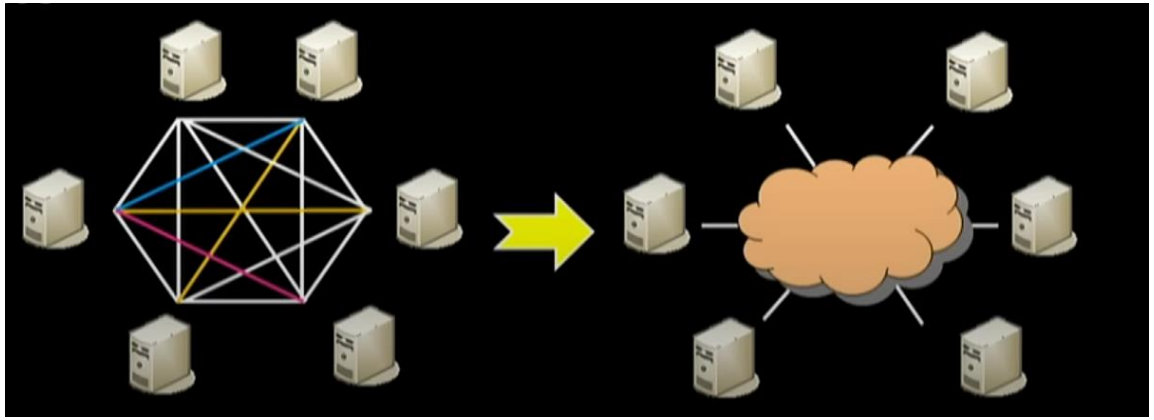
Economia na Internet

Pré-Internet:

- Redes privativas, soluções proprietárias e recursos individualizados (acesso controlado, mas custo elevado); pouco computadores, isolados.

Internet:

- Compartilhamento de recursos (economia de escala) e adoção de padrões abertos de comunicação; muitos computadores conectados.



INSTITUTO FEDERAL
São Paulo
Campus Campinas

O problema de segurança

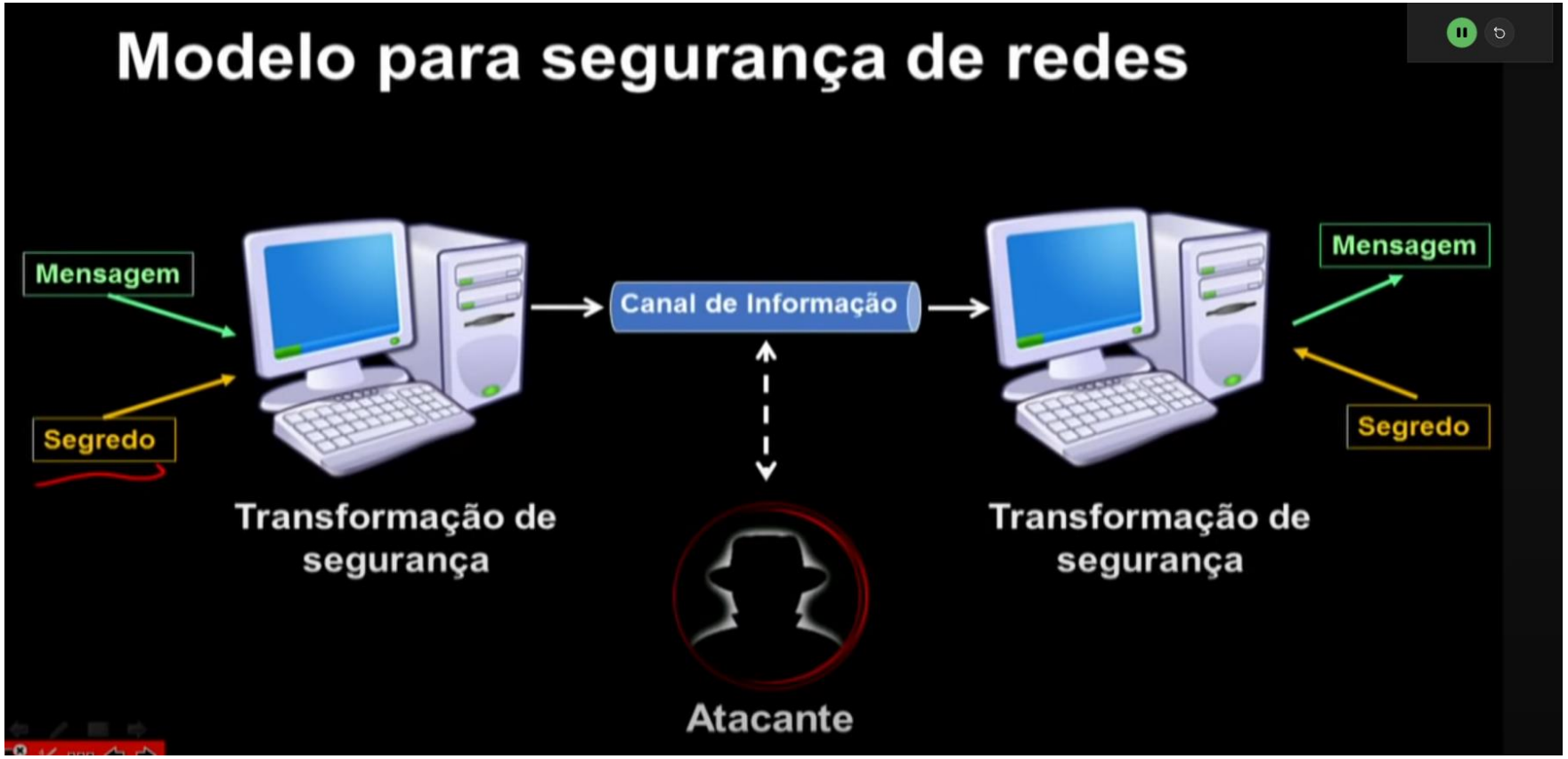
- **Dados que circulam** na internet passam por **equipamentos de terceiros** sem grande controle dos donos destes dados.
- **Dados armazenados** em computadores conectados contêm várias informações potencialmente valiosas.

- Diversos tipos de **atacantes**:
  - Motivados por fama, curiosidade, poder, desafios. Casos famosos: Adrian Lamo, Kevin Mitnick e Kevin Poulsen.
  - “Crackers”: objetivos maliciosos, como ganho financeiro (ex.: Wannacry/2017) ou espionagem (ex: NSA).

INSTITUTO FEDERAL
São Paulo
Campus Campinas

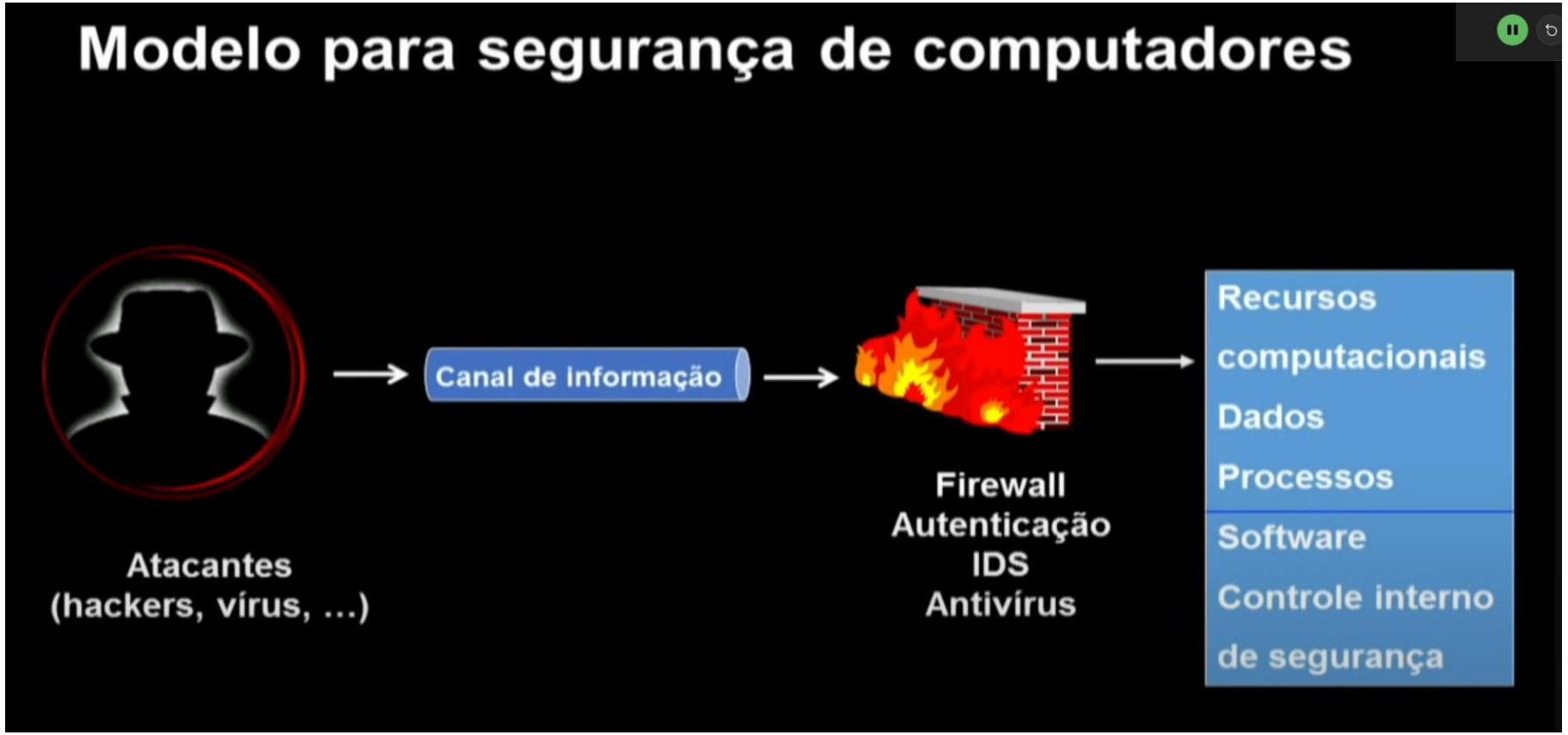
O problema de segurança

Modelo para seguranças de redes (mais fácil de executar)



O problema de segurança

Modelo para seguranças de computadores (mais complicado de garantir)



Segurança da Informação

- Visa proteger a informação das ameaças que têm impacto sobre a continuidade do negócio e, em última instância maximizar o retorno sobre investimentos e oportunidades de negócios (DA VEIGA; MARTINS, 2015; ISO/IEC 27002, 2013).

DA VEIGA, Adéle; MARTINS, Nico. *Information security culture and information protection culture: A validated assessment instrument*. ***Computer Law & Security Review***, [S.l.], v. 31, n. 2, p.243-256, abr. 2015.
ISO/IEC 27002:2022. *Information technology – Security techniques – Code of practice for information security management*. 2022.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

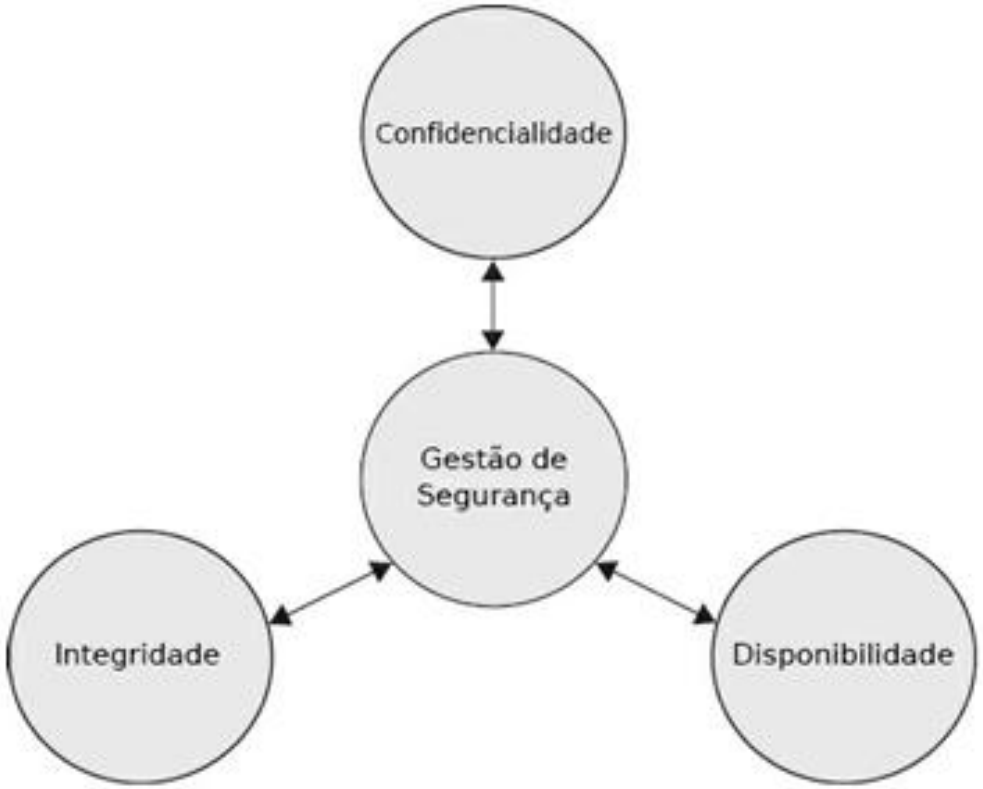
Segurança da Informação

A segurança da informação trata da **proteção** dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados à **informação**, preservando:

Princípios da Segurança da Informação

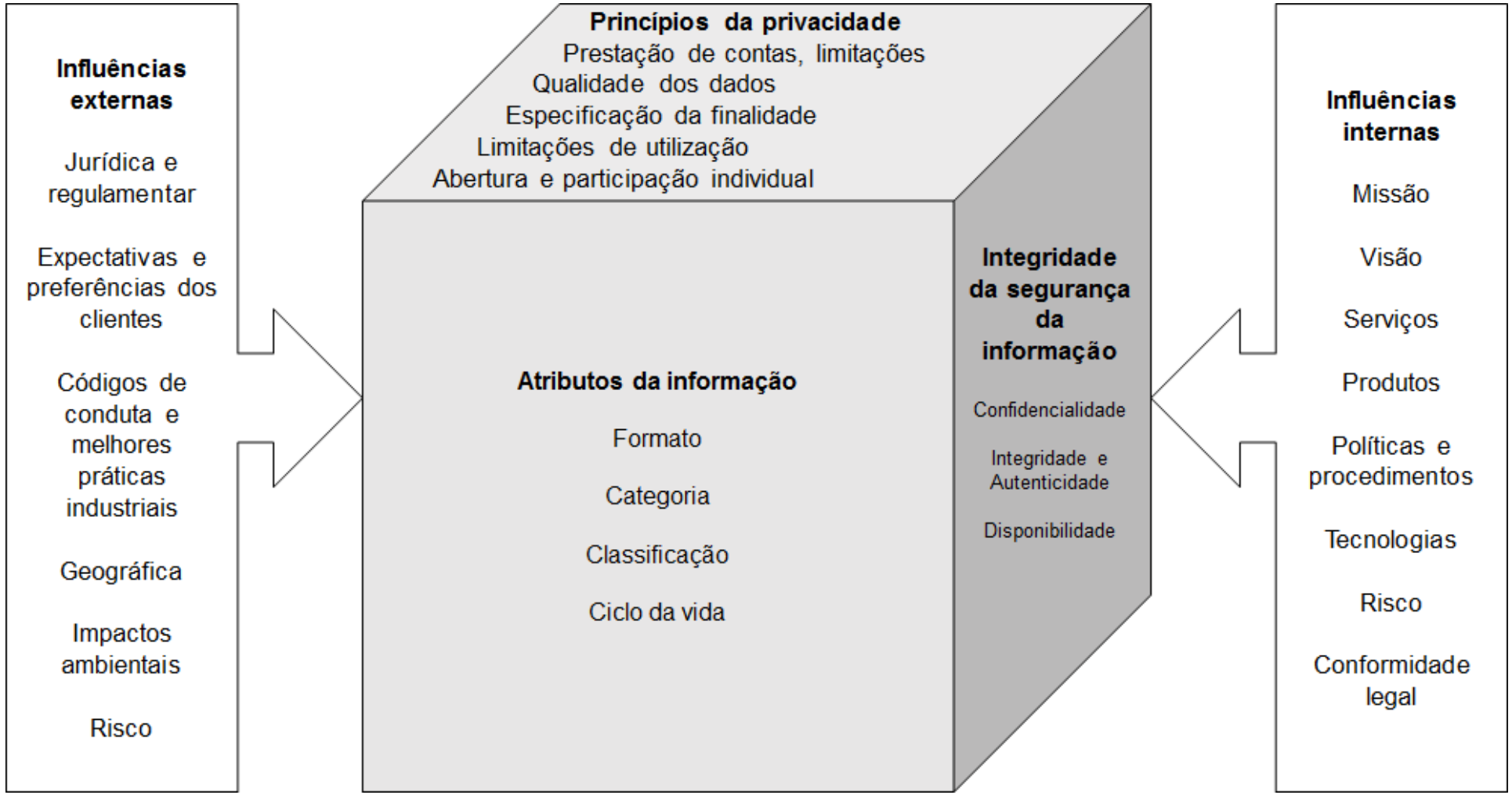
- **C**onfidencialidade: acessível somente por pessoas autorizadas; sigilo;
- **I**ntegridade: completude da informação; não modificação durante o envio; exatidão
- **D**isponibilidade: acessível sempre que necessário a pessoas autorizadas; backup
- **A**utenticidade: reconhecimento dos comunicantes; identidade

Segurança da Informação



HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

Atributos da informação pela perspectiva da privacidade e segurança da informação



Segurança da informação

Governo do Brasil: Secretaria de Segurança da Informação e Cibernética: https://www.gov.br/gsi/pt-br/ssic

Google: como descobrir e apagar as informações que a plataforma tem de você

https://www.bbc.com/portuguese/geral-42332959

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Dúvidas?