



# Introdução à Segurança de Sistemas

Prof. Dr. Lauro Cássio Martins de Paula

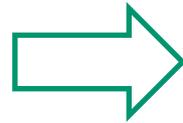
INF 018 – AUDITORIA E SEGURANÇA DE SISTEMAS

lauro.martins@ifba.edu.br

# **Dados e Informações**

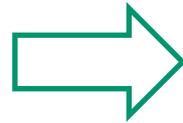
**Dado**

**Dado**

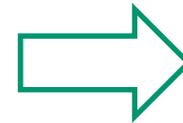


**Informação**

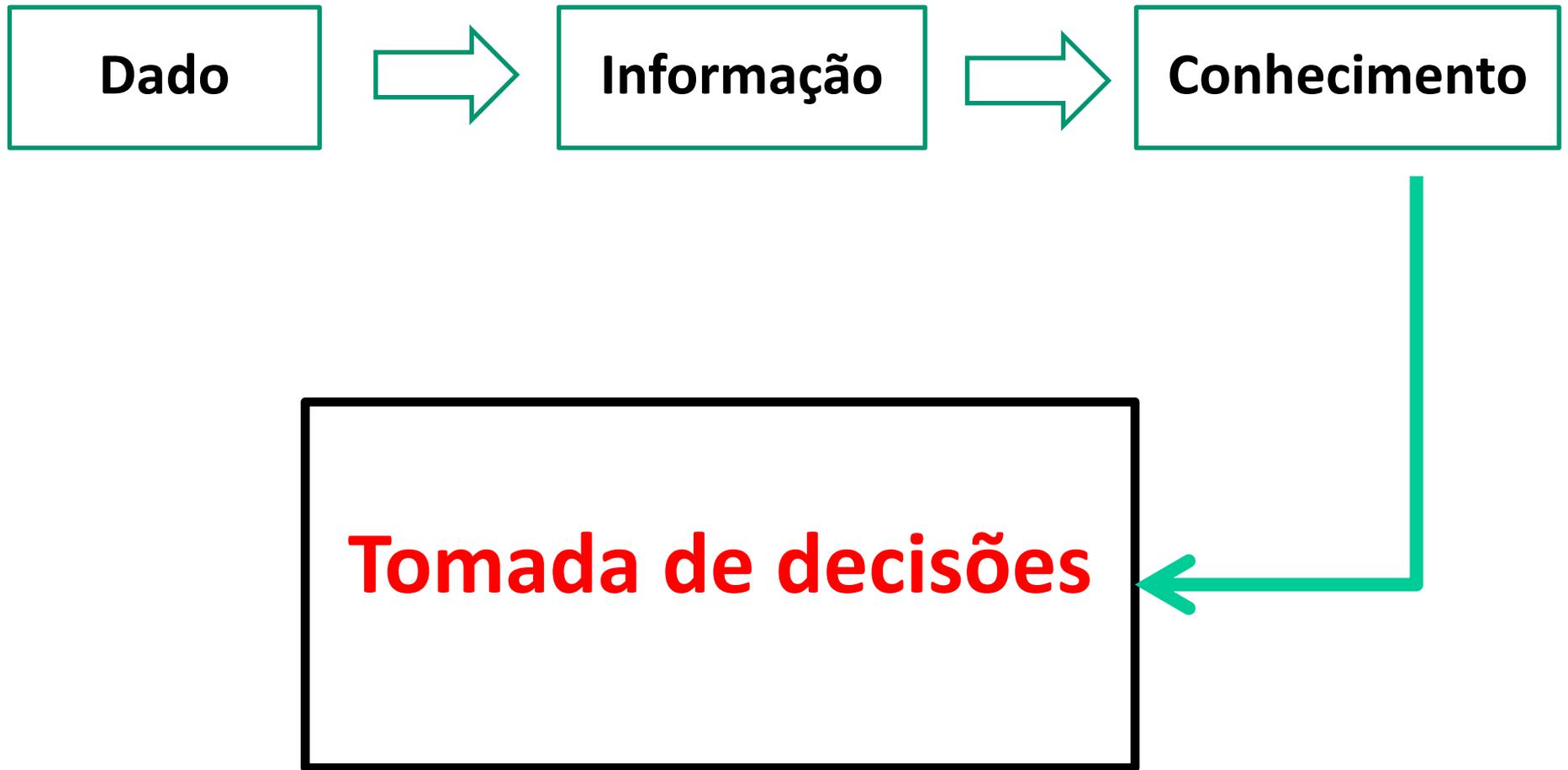
**Dado**



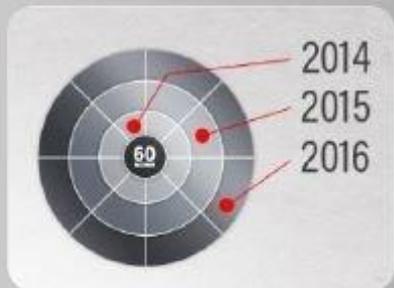
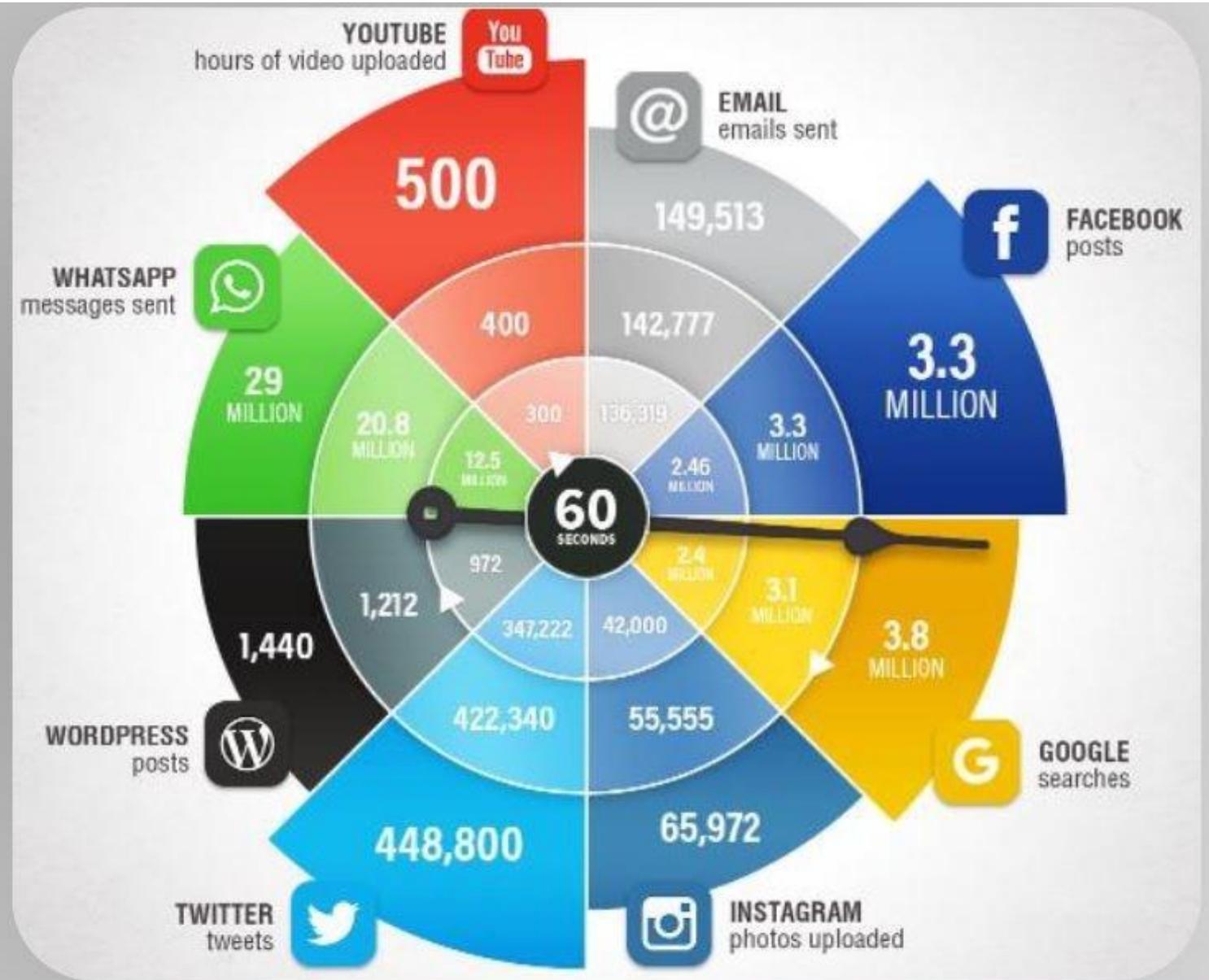
**Informação**



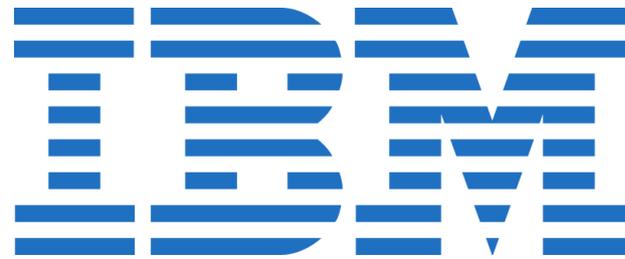
**Conhecimento**



# Os Dados São o Novo Petróleo?



# Sim, os Dados São o Novo Petróleo!!!



Google Cloud

amazon

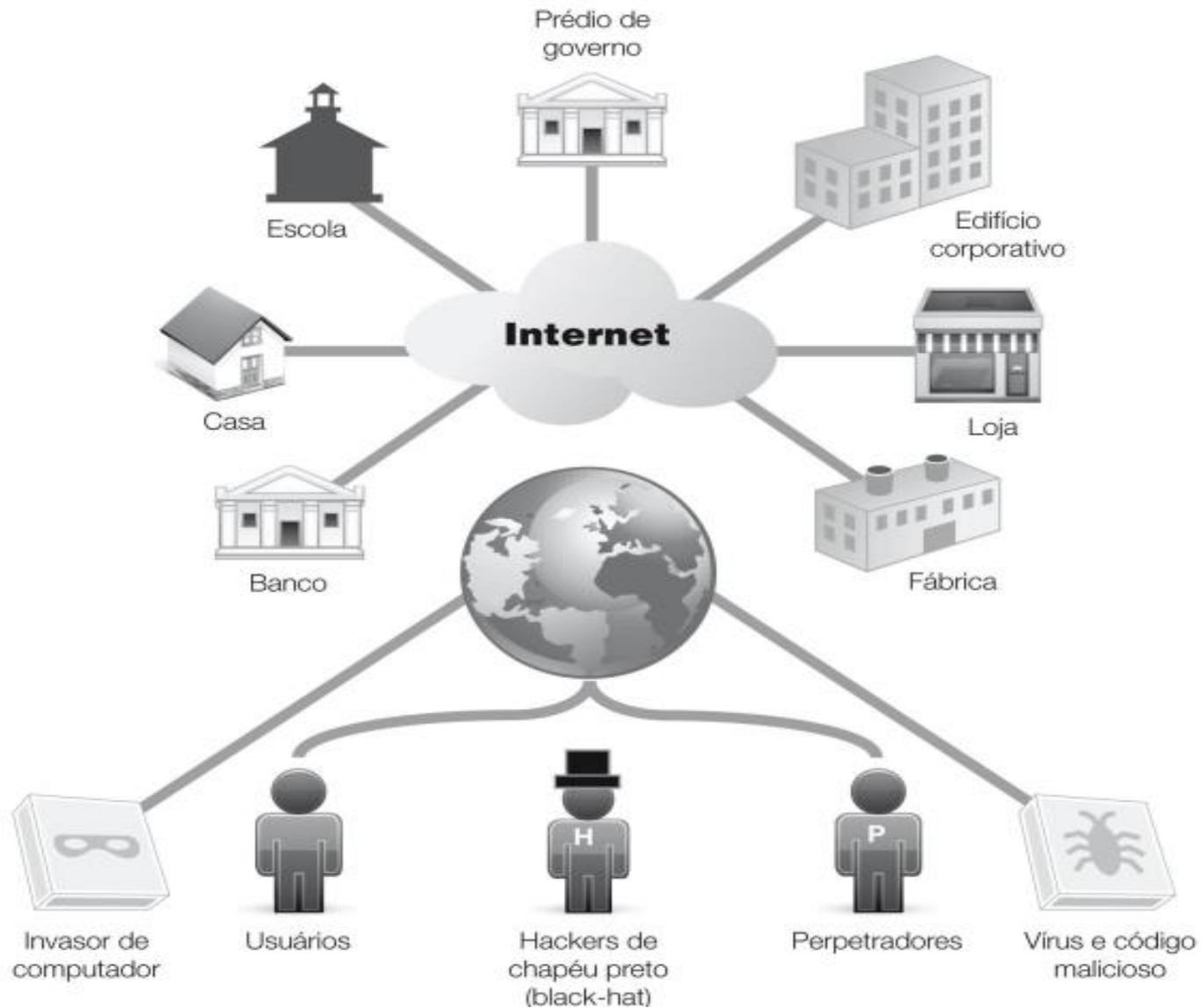


Tesla, Inc.  
Energy innovation company.

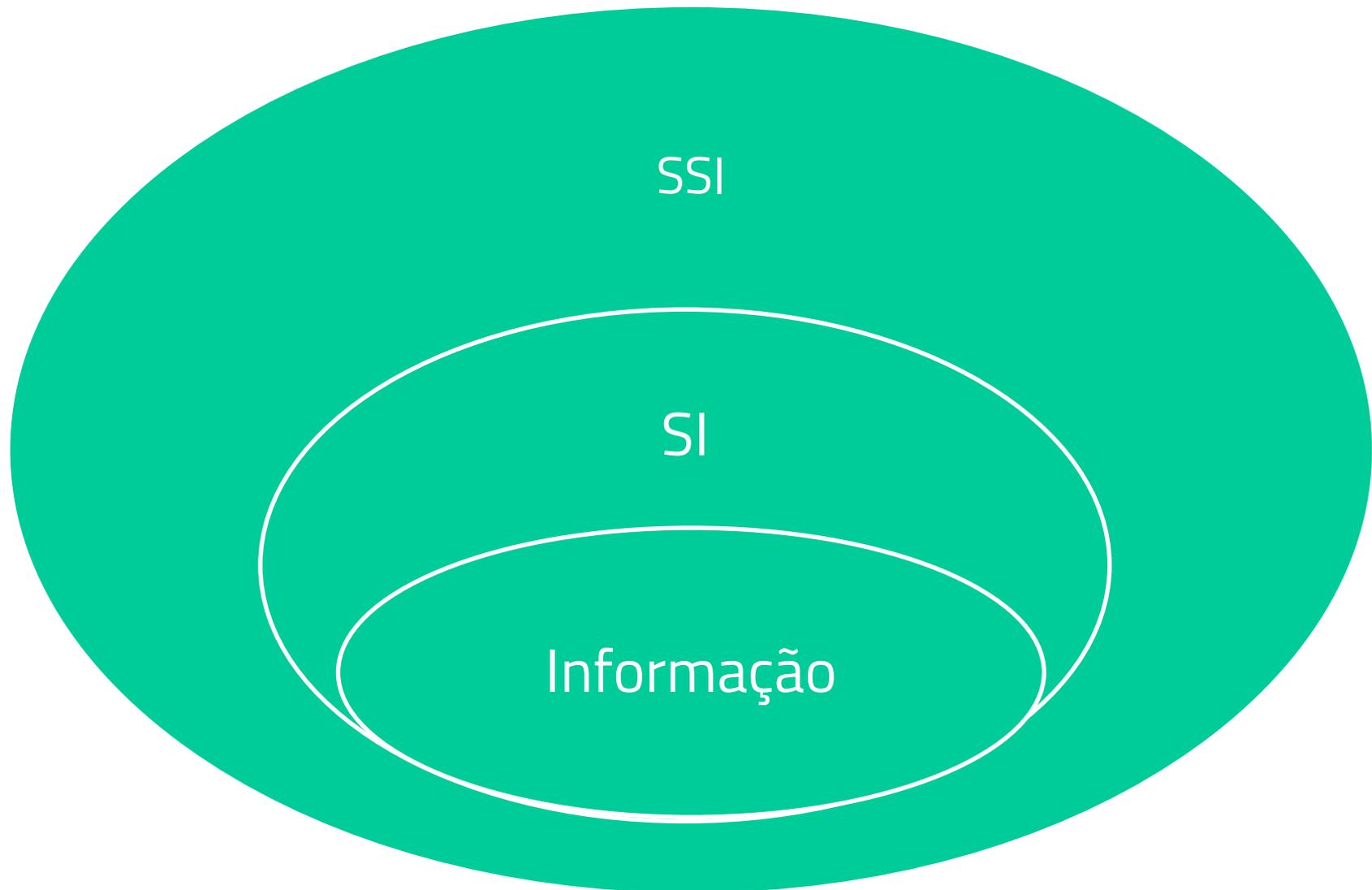


**Como proteger todos esses  
dados?**

# Cenário

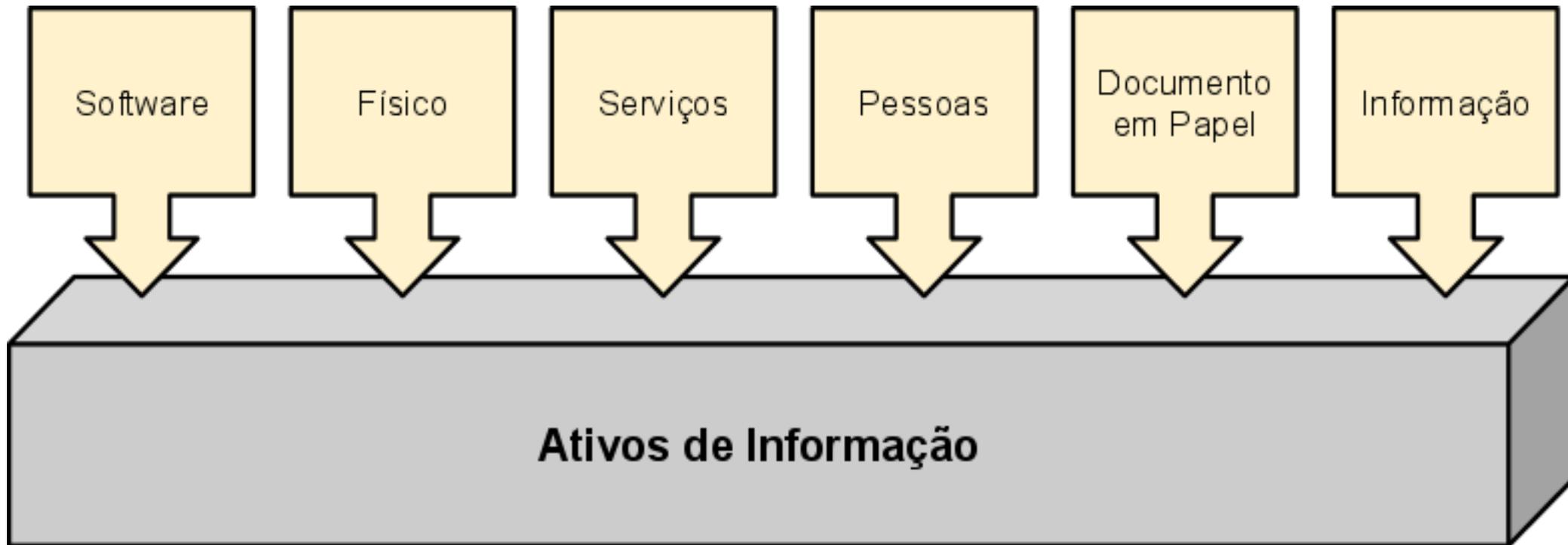


# Cenário



# Classificação e Controle de Ativos de Informação

- **Ativos de Informação**
  - O ativo de informação é composto pela informação e tudo aquilo que a suporta ou se utiliza dela.



# 4 Aspectos essenciais relacionados com a segurança dos ativos de informação

## 1. Probabilidade

- É a chance de uma falha de segurança ocorrer levando-se em conta as vulnerabilidades do ativo e as ameaças que venham a explorar esta vulnerabilidade.

## 2. Vulnerabilidade

- A vulnerabilidade de um ativo é o seu ponto fraco podendo ser explorado ou não.



# Aspectos essenciais relacionados com a segurança dos ativos de informação

## 3. Impacto

- É medido pelas consequências que possam causar aos processos de negócio suportados pelo ativo em questão.
- Quanto maior o valor do ativo, maior será o impacto de um eventual incidente que possa ocorrer.

## 4. Controle

- O controle é todo e qualquer mecanismo para diminuir as fraquezas (ou vulnerabilidades) de um ativo da informação, seja um equipamento, tecnologia, pessoa ou processo.

# Segurança da Informação



Envolve:

## Riscos

Probabilidade de que algo ruim aconteça a um bem da empresa.

## Ameaças

É qualquer ação que possa danificar um bem; um ataque potencial a um ou mais ativos de informação

# Segurança de Sistemas de informação

- A **Segurança da Informação** se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais.
- **Segurança de Sistemas de Informação** é a coleção de atividades que protegem o sistema de informação.

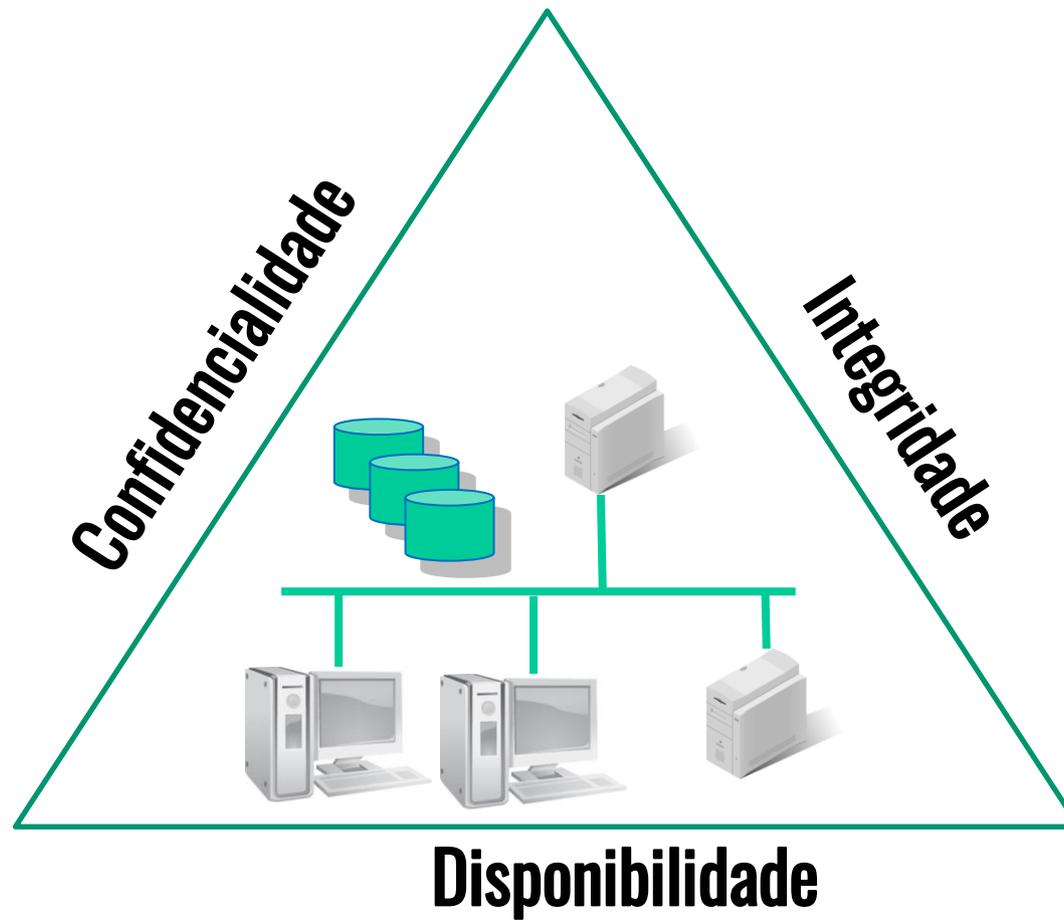
# O que deve ser protegido?



- Dados particulares de indivíduos
  - Nome, endereço, data de nascimento
  - Número de identidade
  - Nome de banco, número de conta
  - Número de cartão de crédito
  - Número de conta de serviços utilitários
  - Número hipoteca
  - Número de apólice de seguro
  - Números de conta de investimento
- Propriedade intelectual corporativa
  - Segredos comerciais
  - Desenvolvimento de produtos
  - Estratégias de vendas e marketing
  - Registros financeiros
  - Direitos autorais, patentes etc.
- Transações on-line B2C e B2B
  - Operações bancárias on-line
  - Reivindicações de plano de saúde e seguro on-line
  - Serviços, comércio eletrônico, governo eletrônico
  - Educação e transcrições on-line
- Propriedade intelectual de governo
  - Segurança nacional
  - Estratégias militares e do Departamento de Defesa

# **Princípios de Segurança de Informação**

# A Tríade da Segurança de Sistemas de Informação



# Aspectos da Informação

- **Requisitos da Informação Segura:**
  - **Disponibilidade** – a informação é acessível por usuários autorizados sempre que a solicitarem.
  - **Confidencialidade** – somente usuários autorizados podem visualizar a informação.
  - **Integridade** – somente usuários autorizados podem alterar informação.

# Disponibilidade em SSI

- Em SI, normalmente é expressa como a quantidade de tempo que um usuário pode usar um sistema. Exemplos de Medidas:
  1. Tempo de utilização (ou uptime)
  2. Tempo de paralisação (ou downtime)
  3. Tempo médio para falha (Mean time to failure):
    1. quantidade média de tempo entre falhas para determinado sistemas
  4. Tempo médio para reparo (Mean time to repair):
    1. Quantidade média de tempo necessária para reparar um sistema.
  5. Objetivo de tempo de recuperação (Recovery Time objective)
    1. Quantidade de tempo necessária para recuperar e tornar um sistema e seus dados disponíveis após uma parada.

# Como medir a disponibilidade?

*Tempo de utilização total*

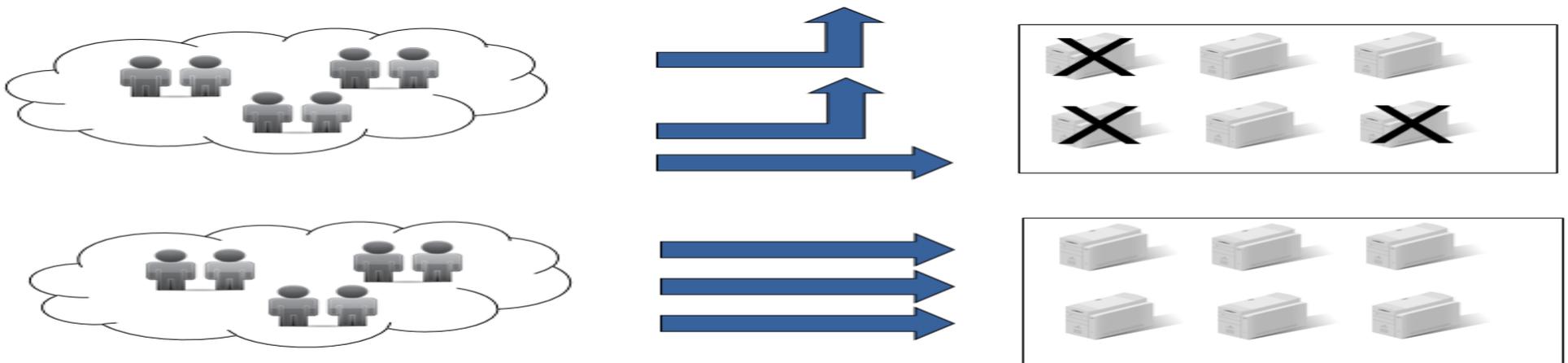
*Tempo de utilização total + Tempo de paralisação*

## EXEMPLO

Para um Mês de 30 dias, em que houve 30 minutos de paralisação

Disponibilidade = (43.200 min) / (43.200 min \* 30 min) = 0,99393 ou 99,93%.

Observação: 30 dias x 24 horas/dia x 60 min/hora = 43.200 minutos



# Confidencialidade em SSI

- Proteger as informações de todo mundo, exceto daqueles que tenham direito a elas.



## Dados e informações Pessoais

- Números de cartões de crédito e cartão de bancos
- CPF e endereços



## Propriedade Intelectual

- Copyrights, banco de dados e especificações técnicas



## Segurança Nacional

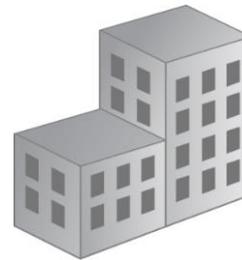
- Inteligência Militar
- Informações relacionadas ao governo

# Integridade em SSI

A integridade lida com a validade e a precisão dos dados



- User names e passwords



- Patentes and copyrights
- Código Fonte



- Informações diplomáticas
- Dados Financeiros

# Referências

- Kim & Solomon, Fundamentos de Segurança de Sistemas de Informação. Ed. LTC, 2014.
- Schimdt et al. Fundamentos de Auditoria de Sistemas. Ed. Atlas, 2006.

**Dúvidas?**