



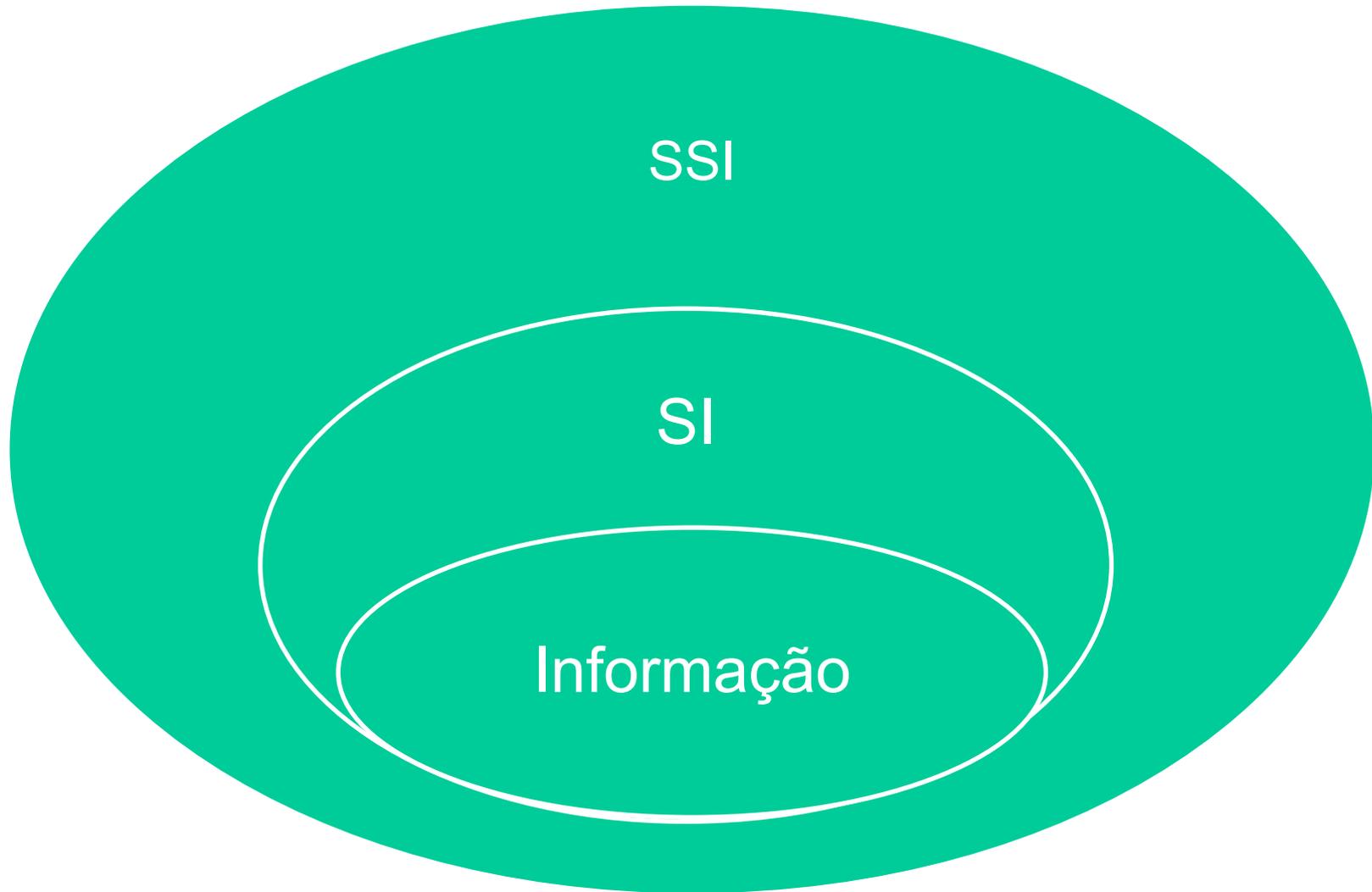
# Introdução à Segurança de Sistemas

Prof. Dr. Mauricio Pitangueira

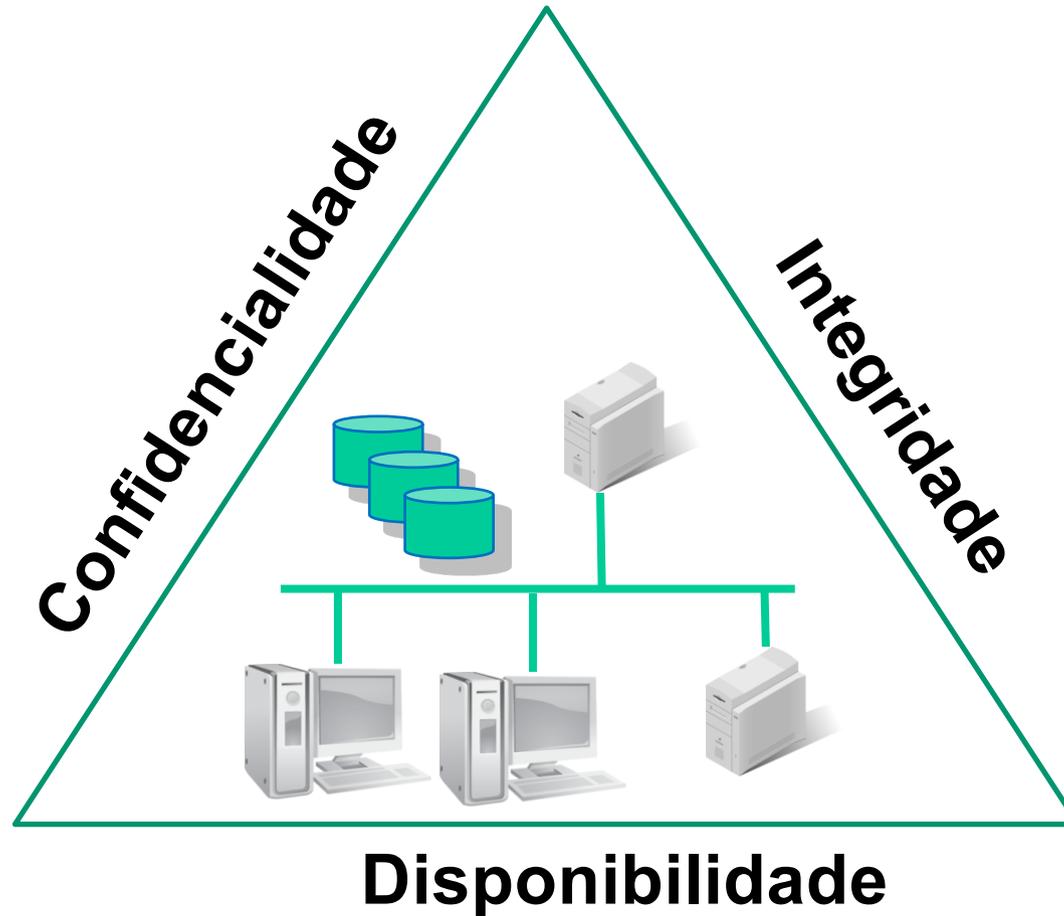
INF 018 – AUDITORIA E SEGURANÇA DE SISTEMAS

[antoniomauricio@ifba.edu.br](mailto:antoniomauricio@ifba.edu.br)

# Cenário



# A Tríade da Segurança de Sistemas de Informação



# Aspectos da Informação

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

# Aprofundando a 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*

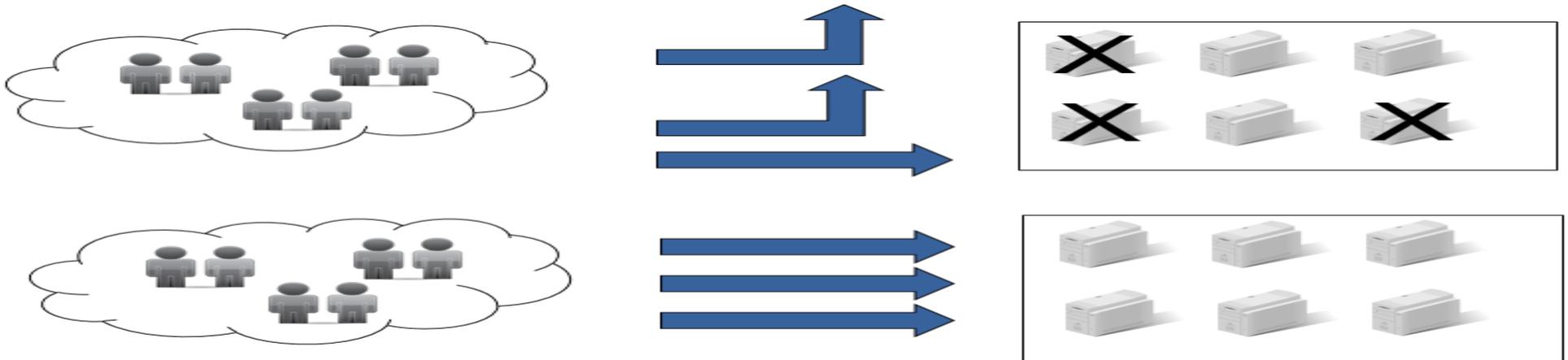
*Tempo de utilização total + Tempo de paralisação*

## EXEMPLO

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

Disponibilidade =  $(43.200 \text{ min}) / (43.200 \text{ min} + 30 \text{ min}) = 0,9993$  ou 99,93%.

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

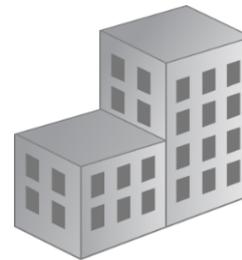


# Aprofundando a integridade

A integridade lida com a validade e a precisão dos dados



- User names e passwords



- Patentes and copyrights
- Código Fonte



- Informações diplomáticas
- Dados Financeiros

# Aprofundando a Confidencialidade

Proteger informações e todos, 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

# Outros aspectos da Informação

- **Além destes últimos aspectos, temos também:**
  1. Autenticação: garantir que um usuário é de fato que alega ser;
  2. Legalidade: garantir que o sistema esteja aderente à legislação pertinente;
  3. *Privacidade*: capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações (por exemplo, o sistema de voto eletrônico);

# Classificação do ativo da informação

## Nível I: informação pública

Ativos públicos ou não classificados. Se forem divulgadas fora da organização não trarão impactos para o negócio.

## Nível II: informação interna

Ativos cujo acesso do público externo deve ser evitado, entretanto, caso venham a se tornar públicos, as consequências não são críticas.

## Nível III: informação confidencial

Os ativos desta categoria devem ter acesso restrito dentro da organização e protegidos do acesso externo. A integridade é vital. O acesso não autorizado destas informações pode trazer comprometimentos às operações da organização e causar perdas financeiras.

## Nível IV: informação secreta

O acesso interno e externo a estas informações é extremamente crítico para a organização.

# Aspectos Humanos da Segurança da Informação

- **Visão Geral**
  - As pessoas são os elementos centrais dos sistemas de segurança;
    - Os incidentes de segurança sempre envolvem pessoas, sendo por:
      - Vulnerabilidades exploradas;
      - Ameaças que explorar essas vulnerabilidades.



# Aspectos Humanos da Segurança da Informação

- **Security Officer - O Profissional de Segurança**
  - A preocupação com a segurança deve ser de todos os colaboradores;
  - Se isto não estiver na mente de todos, não haverá sucesso em nenhuma iniciativa de segurança;
  - Neste contexto, nasce um novo profissional chamado de "**CSO (Chief Security Officer)**";
  - É responsável pela coordenação do planejamento, implementação, monitoramento e melhoria da segurança da informação em uma empresa.

# Aspectos Humanos da Segurança da Informação

- **Security Officer - O Profissional de Segurança**
  - As seguintes responsabilidades são atribuídas à ele:
    - Coordenação da área de segurança e da infraestrutura organizacional;
    - Planejamento dos investimentos de segurança;
    - Definição dos índices e indicadores para a segurança corporativa;
    - Definição, elaboração, divulgação, treinamento, implementação e administração da política de segurança, plano de continuidade de negócios e plano de contingência;
    - Investigação sobre incidentes de segurança;
    - Análise de riscos envolvendo segurança.

# Referências

Kim & Solomon, Fundamentos de Segurança de Sistemas de Informação. Ed. LTC, 2014.

Schimdt et al. Fundamentos de Auditoria de Sistemas. Ed. Atlas, 2006.