Engenharia de Proteção

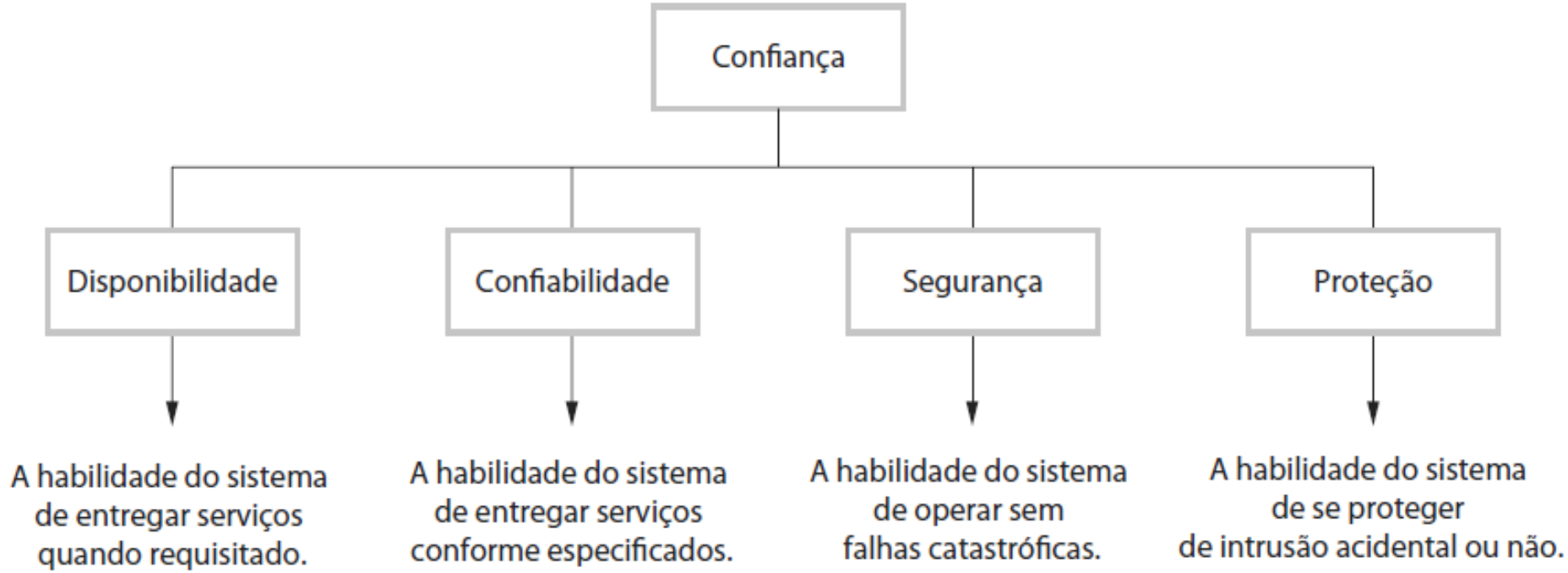
UNIP - Araraquara

Curso: Ciências da Computação

Disciplina: Qualidade de Software

Profº: João Paulo Moreira dos Santos

ENGENHARIA DE PROTEÇÃO



PROTEÇÃO

- A segurança é um atributo do sistema que reflete sua capacidade de se proteger de ataques externos, sejam acidentais ou deliberados.

- Ataques são possíveis porque a maioria dos computadores de uso geral está em rede, portanto está acessível a estranhos.

PROTEÇÃO

- Uso generalizado da internet na década de 90 introduziu um novo desafio:
  - Implementar sistemas protegidos.
- Cada vez mais sistemas foram conectados à internet.
  - Criou-se uma variedade de ataques externos.
- Problemas de proteção de sistemas confiáveis foram aumentando com o tempo.

PROTEÇÃO

- É essencial projetar sistemas para resistir a ataques externos e para recuperar-se desses ataques.

- Sem precauções de proteção é quase inevitável que invasores comprometerão os sistemas em rede.
  - Abusar do hardware do sistema.
  - Roubar dados confidenciais.
  - Interromper serviços dos sistemas.

ENGENHARIA DE PROTEÇÃO

- Com o que a engenharia de proteção está preocupada?

- Com o desenvolvimento e a evolução de sistemas que possam resistir a ataques mal-intencionados para danificar o sistema ou seus dados.

ENGENHARIA DE PROTEÇÃO

- O que considerar sobre questões de proteção?
  - Software de aplicação.
  - Infraestrutura sobre a qual esse sistema é construído.

ENGENHARIA DE PROTEÇÃO

- Infraestrutura para aplicações complexas devem incluir:

Aplicação
Componentes reusáveis e bibliotecas
Middleware
Gerenciamento de banco de dados
Aplicações genéricas compartilhadas (*browsers*, e-mail etc.)
Sistema operacional

ENGENHARIA DE PROTEÇÃO

- A maioria dos ataques externos foca as infraestruturas de sistemas.
  - Os componentes são bem conhecidos e amplamente disponíveis.
  - Invasores investigam pontos fracos e compartilham informações sobre as vulnerabilidades.
  - Vulnerabilidades levam invasores a obterem acesso não autorizado e aos dados dos sistemas.

ENGENHARIA DE PROTEÇÃO

- Proteção de aplicação x Proteção de infraestrutura
- Aplicação: é um problema de engenharia de software em que os engenheiros devem assegurar que o sistema seja projetado para resistir a ataques.
- Infraestrutura: é um problema de gerenciamento em que os gerentes de sistema configuram a infraestrutura para resistir a ataques.
  - Uso mais eficaz de quaisquer recurso de proteção da infraestrutura.
  - Corrigir vulnerabilidades de proteção de infraestrutura.

ENGENHARIA DE PROTEÇÃO

- Gerenciamento de proteção de sistemas não é uma tarefa única, onde inclui uma gama de atividades.
  - Gerenciamento de usuários e permissões;
  - Implantação e manutenção de sistema de software; e
  - Monitoração, detecção e recuperação de ataques.

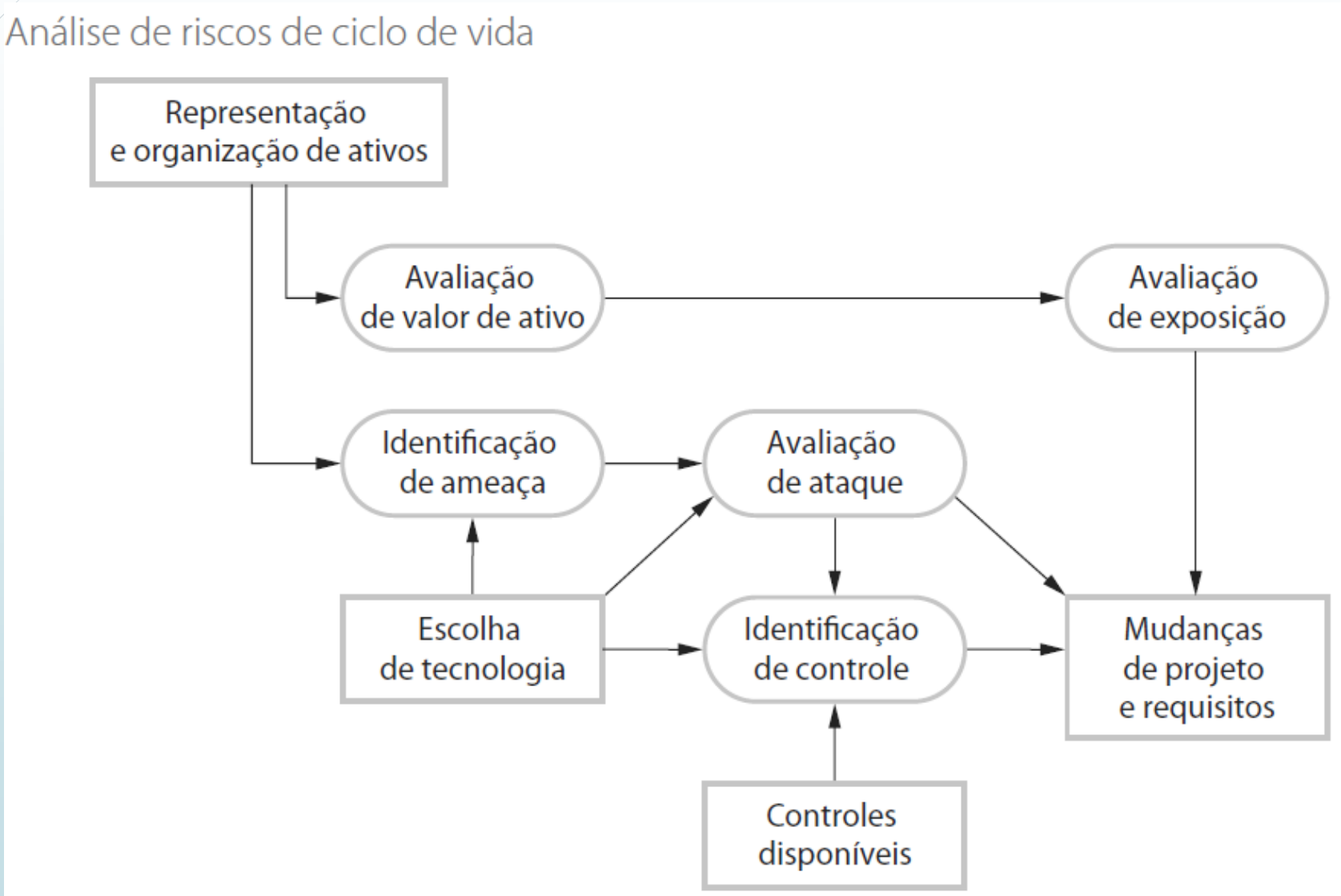
GERENCIAMENTO DE RISCOS DE PROTEÇÃO

- Gerenciamento e avaliação de riscos de proteção são essenciais para a eficácia da engenharia de proteção.
  - Preocupa com possíveis perdas que possam resultar de ataques a ativos do sistema;
  - Preocupa com o balanço dessas perdas em relação aos custos de procedimentos de proteção que possam reduzi-las.
- Exemplo: Empresas de cartão de crédito.

GERENCIAMENTO DE RISCOS DE PROTEÇÃO

- Avaliações de riscos:
  - Avaliação preliminar de riscos.
  - Avaliação de riscos de ciclo de vida.
  - Avaliação de riscos operacionais.

GERENCIAMENTO DE RISCOS DE PROTEÇÃO



PROJETO PARA PROTEÇÃO

- É possível adicionar proteção a um sistema depois que tenha sido implementado?
  - Sim, porém é muito difícil.

- Necessário levar em consideração questões de proteção durante o processo de projeto.

PROJETO PARA PROTEÇÃO

- Como as decisões de projeto de arquitetura afetam a proteção de um sistema?
- Quais são as boas práticas aceitáveis para o projeto de sistemas protegidos?
- Qual suporte deve ser projetado em sistemas para evitar a introdução de vulnerabilidades quando um sistema for implantado para uso?

PROJETO PARA PROTEÇÃO

- O projeto de um sistema de proteção envolve compromissos.
  - Possível projetar várias medidas de proteção que reduzirão as chances de um ataque bem-sucedido.
    - Podem afetar o desempenho.
      - Criptografia.
  - Tensões entre proteção e usabilidade.
    - Exigir que o usuário lembre e forneça informações adicionais, porém podem esquecer.

PROJETO PARA PROTEÇÃO

- Não existem regras simples e rápidas de como alcançar a proteção do sistema.
  - Diferentes tipos de sistemas requerem medidas técnicas diferentes para se atingir um nível de proteção aceitável.

- Existem diretrizes gerais que tem ampla aplicabilidade durante o projeto de soluções de proteção de sistemas.
  - Encapsulam boas práticas de projetos para a engenharia de sistemas de proteção

PROJETO PARA PROTEÇÃO

Diretrizes de proteção

1. Basear as decisões de proteção em uma política explícita de segurança
2. Evitar um ponto único de falência
3. Falhar de maneira protegida
4. Equilibrar a proteção e a usabilidade
5. Registrar ações de usuários
6. Usar redundância e diversidade para reduzir riscos
7. Validar todas as entradas
8. Compartimentar seus ativos
9. Projetar para implantação
10. Projetar para recuperabilidade

SOBREVIVÊNCIA DE SISTEMAS

- A sobrevivência de sistema é a capacidade de um sistema de continuar a entregar serviços essenciais de negócios ou de missão crítica para usuários legítimos, enquanto ele está sob ataque ou após parte do sistema ter sido danificado.