



Instituto Federal de Educação, Ciência e Tecnologia da Bahia - IFBA
Departamento de Ciência da Computação
Tecnólogo em Análise e Desenvolvimento de Sistemas

Especificação de confiança e segurança

André L. R. Madureira <andre.madureira@ifba.edu.br>
Doutorando em Ciência da Computação (UFBA)
Mestre em Ciência da Computação (UFBA)
Engenheiro da Computação (UFBA)

Requisitos de Confiança e Proteção

- **Requisitos funcionais:**

- Estabelecem os recursos de verificação e recuperação do sistema
- Estabelecem os recursos de proteção contra falhas de sistema e ataques externos

- **Requisitos não funcionais**

- Definem a confiabilidade e a disponibilidade requeridas do sistema

Especificação de requisitos dirigida a riscos

- Estuda eventos que possam causar danos maiores em sistemas ou que sejam suscetíveis de ocorrer frequentemente
 - Eventos pouco relevantes (dano baixo ou que ocorrem raramente) são ignorados



Processo de especificação dirigida a riscos



Potenciais riscos para o sistema são identificados. Dependem do ambiente onde o sistema será usado.

Cada risco é considerado individualmente.

Cada risco é analisado para descobrir suas **causas-raízes** (razões pelas quais um sistema pode falhar).

Propostas para reduzir ou eliminar os riscos identificados.

Identificação de riscos (ou perigos)

- Os principais riscos provêm de perigos que podem levar a um acidente
- Precisamos identificar os potenciais perigos de um sistema
 - **Ex:** perigos de um sistema de bomba de insulina
 - overdose/subdose de insulina (falha de serviço)
 - falha de energia devido a bateria esgotada (elétrico)
 - mau contato de sensor e atuador (físico)
 - infecção causada pela introdução da máquina (biológico)

Avaliação de riscos (ou perigos)

- Busca entender a probabilidade de ocorrer um perigo e as consequências dele (acidente ou incidente associado à ocorrência desse perigo)
 - Entender se um perigo é uma séria ameaça ao sistema ou ambiente
 - Como gerenciar o risco associado ao perigo
- **Resultado:** declaração de aceitabilidade

Classificação de riscos

- Os riscos podem ser classificados de acordo com sua severidade e frequência de ocorrência:
 - **Riscos intoleráveis**
 - **Riscos tão baixos quanto razoavelmente práticos** (*ALARP – As Low As Reasonably Practical*)
 - **Riscos aceitáveis**

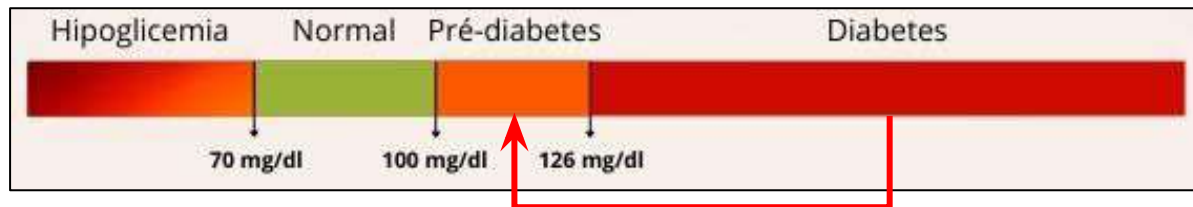
Riscos intoleráveis

- São aqueles que ameaçam a vida humana
 - **Ex:** overdose de insulina, falha no piloto automático de aeronave
- O sistema não deve permitir que esses riscos surjam
- Se eles surgirem, o sistema deve detecta-los antes que provoquem um acidente



Riscos tão baixos quanto razoavelmente práticos

- Também chamados de **Riscos ALARP** (*As Low As Reasonably Practical*)
- São aqueles cujas conseqüências são menos graves, ou que a probabilidade de ocorrência é muito baixa
 - **Ex:** falha no monitoramento de hardware da bomba de insulina
 - **Consequência:** subdosagem de insulina (não é fatal para o paciente)



Riscos aceitáveis

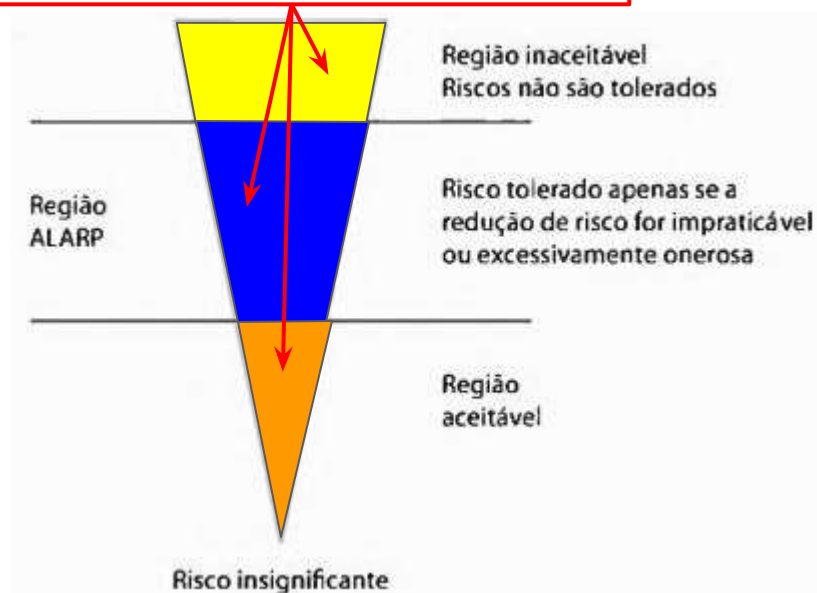
- São aqueles em que os acidentes associados resultam em danos menores
 - **Ex:** reação alérgica do usuário de uma bomba de insulina
 - **Consequência:** irritação de pele
 - Pode não valer a pena usar materiais hipoalergênicos, mais caros, nesse caso



Triângulo de Classificação de Riscos

Área de cada região do triângulo:

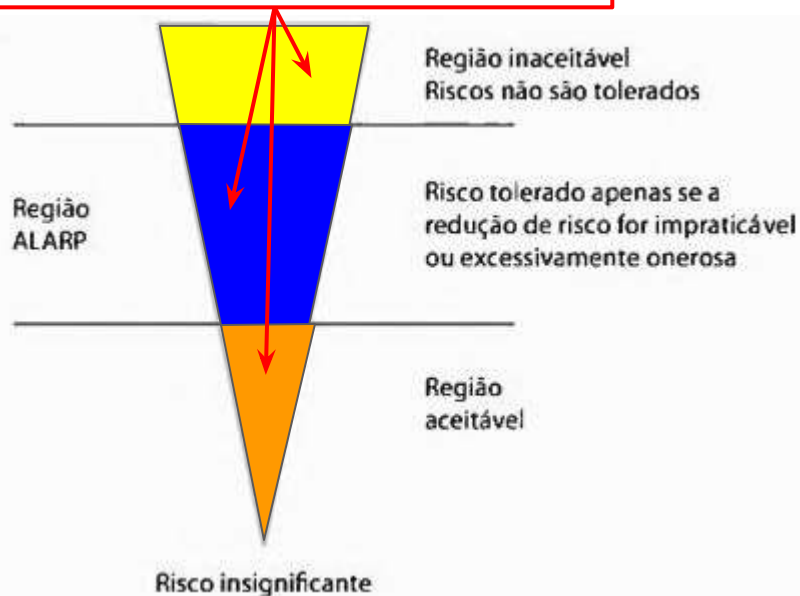
Custo para prevenir incidentes ou acidentes causados por cada categoria de risco



Triângulo de Classificação de Riscos

Área de cada região do triângulo:

Custo para prevenir incidentes ou acidentes causados por cada categoria de risco



A escolha da classificação de um risco nem sempre é feita de maneira técnica

Ex: Pode ser mais barato (e pouco danoso ao ambiente) corrigir a poluição gerada por uma usina depois dos resíduos serem liberados na atmosfera, do que investir no tratamento deles antes da liberação.

No entanto, a legislação considera esse risco como inaceitável!

A avaliação de riscos envolve estimar a probabilidade de perigo e gravidade de risco, o que difícil

Exercício - Classificar os Riscos de um Sistema de Bomba de Insulina

Perigo identificado	Probabilidade de perigo	Severidade de acidente	Risco estimado	Aceitabilidade
1. Cálculo de overdose de insulina	Média	Alta	Alto	Intolerável
2. Cálculo de dose insuficiente de insulina	Média	Baixa	Baixo	Aceitável
3. Falha de sistema de monitoramento de hardware	Média	Média	Baixo	ALARP
4. Falha de energia	Alta	Baixa	Baixo	Aceitável
5. Máquina ajustada incorretamente	Alta	Alta	Alto	Intolerável
6. Quebra de máquina no paciente	Baixa	Alta	Médio	ALARP
7. Máquina causa infecção	Média	Média	Médio	ALARP
8. Interferência elétrica	Baixa	Alta	Médio	ALARP
9. Reação alérgica	Baixa	Baixa	Baixo	Aceitável

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A escolha de como classificar os riscos é feita considerando a probabilidade de perigo e gravidade do risco, de forma técnica.

II - Riscos ALARP são aqueles cujas consequências são menos graves do que os riscos intoleráveis, ou que a probabilidade de ocorrência é muito baixa.

III - Riscos aceitáveis são aqueles em que os acidentes associados resultam em danos menores do que aqueles associados aos riscos ALARP.

IV - Riscos intoleráveis são aqueles que ameaçam o sistema de forma severa.

☐ Somente I, II e III.

☐ Somente I, III e IV.

☐ Somente II, III e IV.

☐ Somente II e III.

☐ Nenhuma das alternativas anteriores.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A escolha de como classificar os riscos é feita considerando a probabilidade de perigo e gravidade do risco, de forma técnica. **F**

II - Riscos ALARP são aqueles cujas consequências são menos graves do que os riscos intoleráveis, ou que a probabilidade de ocorrência é muito baixa.

III - Riscos aceitáveis são aqueles em que os acidentes associados resultam em danos menores do que aqueles associados aos riscos ALARP.

IV - Riscos intoleráveis são aqueles que ameaçam o sistema de forma severa.

- ☐ Somente I, II e III.
- ☐ Somente I, III e IV.
- ☐ Somente II, III e IV.
- ☐ Somente II e III.
- ☐ Nenhuma das alternativas anteriores.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A escolha de como classificar os riscos é feita considerando a probabilidade de perigo e gravidade do risco, de forma técnica. **F**

II - Riscos ALARP são aqueles cujas consequências são menos graves do que os riscos intoleráveis, ou que a probabilidade de ocorrência é muito baixa. **V**

III - Riscos aceitáveis são aqueles em que os acidentes associados resultam em danos menores do que aqueles associados aos riscos ALARP.

IV - Riscos intoleráveis são aqueles que ameaçam o sistema de forma severa.

- ☐ Somente I, II e III.
- ☐ Somente I, III e IV.
- ☐ Somente II, III e IV.
- ☐ Somente II e III.
- ☐ Nenhuma das alternativas anteriores.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A escolha de como classificar os riscos é feita considerando a probabilidade de perigo e gravidade do risco, de forma técnica. **F**

II - Riscos ALARP são aqueles cujas consequências são menos graves do que os riscos intoleráveis, ou que a probabilidade de ocorrência é muito baixa. **V**

III - Riscos aceitáveis são aqueles em que os acidentes associados resultam em danos menores do que aqueles associados aos riscos ALARP. **V**

IV - Riscos intoleráveis são aqueles que ameaçam o sistema de forma severa.

- ☐ Somente I, II e III.
- ☐ Somente I, III e IV.
- ☐ Somente II, III e IV.
- ☐ Somente II e III.
- ☐ Nenhuma das alternativas anteriores.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A escolha de como classificar os riscos é feita considerando a probabilidade de perigo e gravidade do risco, de forma técnica. **F**

II - Riscos ALARP são aqueles cujas consequências são menos graves do que os riscos intoleráveis, ou que a probabilidade de ocorrência é muito baixa. **V**

III - Riscos aceitáveis são aqueles em que os acidentes associados resultam em danos menores do que aqueles associados aos riscos ALARP. **V**

IV - Riscos intoleráveis são aqueles que ameaçam o sistema de forma severa. **F**

☐ Somente I, II e III.

☐ Somente I, III e IV.

☐ Somente II, III e IV.

☒ Somente II e III.

☐ Nenhuma das alternativas anteriores.

Decomposição de riscos (ou perigos)

- É o processo de descobrir as causas-raízes dos perigos do sistema
 - **Objetivo:** descobrir quais eventos ou combinações de eventos causam uma falha no sistema que resulte em um perigo



Árvore de Defeitos

- Técnica top-down que descobre as possíveis causas de cada perigo identificado no sistema
 1. Coloque o **perigo na raiz da árvore**
 2. Identifique os estados do sistema que podem levar a esse perigo
 3. Continue decompondo os estados do sistema até chegar às causas-raíz do risco (*“folhas da árvore de defeitos”*)

Perigo

Dose incorreta
de insulina
administrada

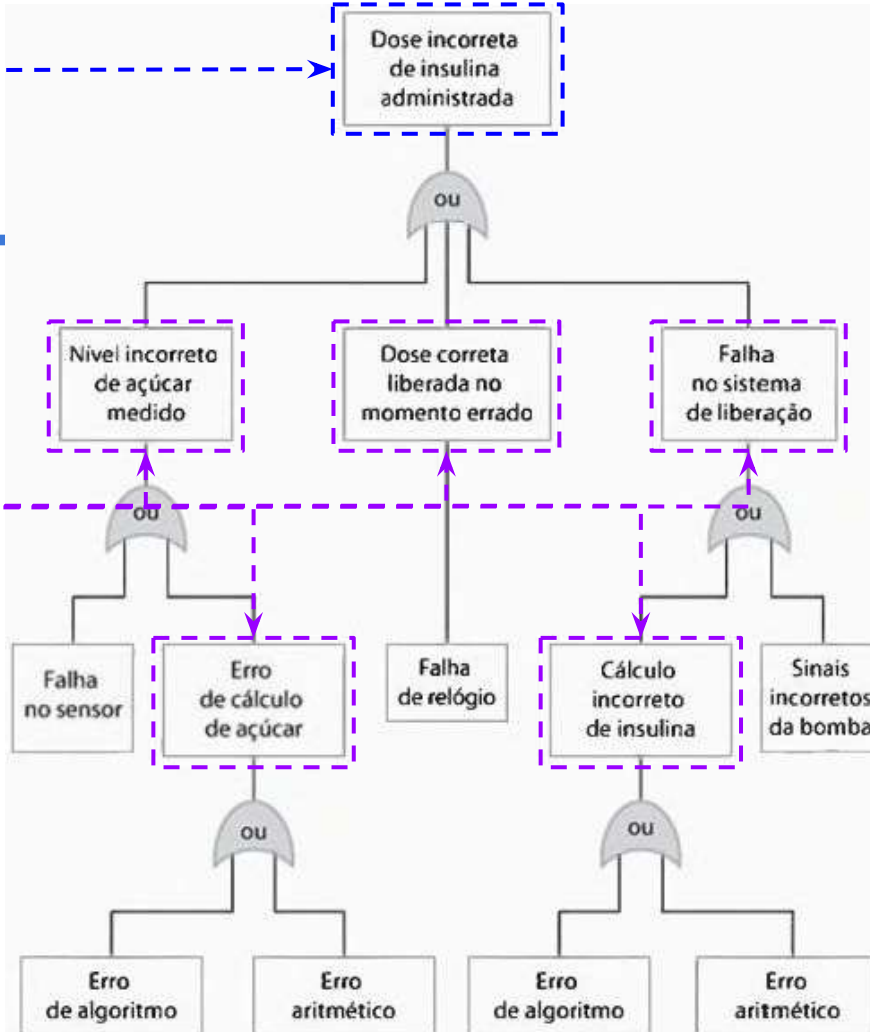
```
graph LR; A[Perigo] -.-> B[Dose incorreta de insulina administrada];
```

The diagram consists of a light gray rectangular background. On the left side of this background, there is a white rectangular box with a solid blue border containing the word 'Perigo'. A dashed blue arrow points from the right side of this box to the left side of another white rectangular box on the right. This second box has a dashed blue border and contains the text 'Dose incorreta de insulina administrada'. A thin vertical line extends downwards from the bottom center of this second box.

Perigo

Dose incorreta
de insulina
administrada

Estados do
sistema que
causam o perigo



Perigo

Dose incorreta
de insulina
administrada

**Estados do
sistema que
causam o perigo**

Nível incorreto
de açúcar
medido

Dose correta
liberada no
momento errado

Falha
no sistema
de liberação

**Causas-raiz do risco
(folhas da árvore)**

Falha
no sensor

Erro
de cálculo
de açúcar

Falha
de relógio

Cálculo
incorreto
de insulina

Sinais
incorretos
da bomba

Erro
de algoritmo

Erro
aritmético

Erro
de algoritmo

Erro
aritmético

Redução de riscos

- Agora que identificamos os riscos potenciais do sistema, podemos evita-los ou mitiga-los através dos **requisitos de segurança**
 - **Requisitos de segurança:** Gerenciam os riscos, de modo a garantir que incidentes ou acidentes não ocorram

Redução de riscos

- Agora que identificamos os riscos potenciais do sistema, podemos evita-los ou mitiga-los através dos **requisitos de segurança**
 - **Requisitos de segurança:** Gerenciam os riscos, de modo a garantir que incidentes ou acidentes não ocorram
- Com os requisitos de segurança, podemos utilizar as seguintes estratégias para lidar com os riscos do sistema:
 - **Prevenção de perigos**
 - **Detecção e remoção de perigos**
 - **Limitação de danos**

Exemplo de requisitos de segurança

RS1: O sistema não deve liberar doses de insulina maiores do que a dose máxima.

RS2: O sistema deve ter uma dose diária máxima de insulina, definida pelo usuário do sistema.

RS3: O sistema deve ter um módulo de diagnostico de hardware, que será executado 4x por hora.

RS4: O sistema deve ter um tratador de exceções, para todas as condições de exceção identificadas.

RS5: O alarme deve ser soado quando anomalias forem detectadas.

RS6: Em caso de alarme, uma mensagem de diagnóstico deve ser armazenada.

Confiabilidade x Segurança x Proteção

- Confiabilidade é diferente de segurança e de proteção
 - Confiabilidade é um **atributo mensurável** do sistema
 - Segurança e proteção não são mensuráveis, pois estão associados à **evitar eventos indesejados** no sistema

Confiabilidade como atributo mensurável

- É possível avaliar a confiabilidade de um sistema especificando uma métrica (**nível de confiabilidade**)
 - Acompanhamos a operação do sistema ao longo do tempo e verificamos se o nível de confiabilidade foi alcançado

Confiabilidade como atributo mensurável

- É possível avaliar a confiabilidade de um sistema especificando uma métrica (**nível de confiabilidade**)
 - Acompanhamos a operação do sistema ao longo do tempo e verificamos se o nível de confiabilidade foi alcançado
- **Ex:** um sistema A não deve ser reiniciado mais de 1x por semana em decorrência de falhas
 - Nesse caso, o nível de confiabilidade do sistema A está atrelado a quantidade de vezes que o sistema é reiniciado

Segurança e Proteção para evitar eventos indesejados

- Não faz sentido medir o número de falhas de segurança ou proteção de um sistema, pois, quando elas ocorrem, elas devem ser prontamente corrigidas
 - **Ex:** uma única falha de segurança em um reator nuclear pode ser inaceitável, e causar graves problemas ambientais



Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A decomposição de riscos pode ser feita utilizando duas técnicas: top-down ou bottom-up.

II - A árvore de defeitos é uma técnica de decomposição de riscos na qual o perigo é posicionado na raiz da árvore. Em seguida, os estados do sistema são identificados e decompostos até se alcançar as causas-raiz do perigo (folhas da árvore).

III - Na etapa de redução de riscos, os requisitos de segurança são definidos de modo a garantir que incidentes ou acidentes não ocorram.

IV - Existem várias estratégias que podem ser utilizadas para evitar acidentes, tais como limitação de danos, prevenção, detecção e remoção de perigos.

☐ Todas as assertivas são verdadeiras.

☐ Somente I, II e IV.

☐ Somente I e II.

☐ Somente I, II e III.

☐ Somente II, III e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A decomposição de riscos pode ser feita utilizando duas técnicas: top-down ou bottom-up.

II - A árvore de defeitos é uma técnica de decomposição de riscos na qual o perigo é posicionado na raiz da árvore. Em seguida, os estados do sistema são identificados e decompostos até se alcançar as causas-raiz do perigo (folhas da árvore).

III - Na etapa de redução de riscos, os requisitos de segurança são definidos de modo a garantir que incidentes ou acidentes não ocorram.

IV - Existem várias estratégias que podem ser utilizadas para evitar acidentes, tais como limitação de danos, prevenção, detecção e remoção de perigos.

V

☐ Todas as assertivas são verdadeiras.

☐ Somente I, II e IV.

☐ Somente I e II.

☐ Somente I, II e III.

☐ Somente II, III e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A decomposição de riscos pode ser feita utilizando duas técnicas: top-down ou bottom-up. **V**

II - A árvore de defeitos é uma técnica de decomposição de riscos na qual o perigo é posicionado na raiz da árvore. Em seguida, os estados do sistema são identificados e decompostos até se alcançar as causas-raiz do perigo (folhas da árvore). **V**

III - Na etapa de redução de riscos, os requisitos de segurança são definidos de modo a garantir que incidentes ou acidentes não ocorram.

IV - Existem várias estratégias que podem ser utilizadas para evitar acidentes, tais como limitação de danos, prevenção, detecção e remoção de perigos.

☐ Todas as assertivas são verdadeiras.

☐ Somente I, II e IV.

☐ Somente I e II.

☐ Somente I, II e III.

☐ Somente II, III e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A decomposição de riscos pode ser feita utilizando duas técnicas: top-down ou bottom-up. **V**

II - A árvore de defeitos é uma técnica de decomposição de riscos na qual o perigo é posicionado na raiz da árvore. Em seguida, os estados do sistema são identificados e decompostos até se alcançar as causas-raiz do perigo (folhas da árvore). **V**

III - Na etapa de redução de riscos, os requisitos de segurança são definidos de modo a garantir que incidentes ou acidentes não ocorram. **V**

IV - Existem várias estratégias que podem ser utilizadas para evitar acidentes, tais como limitação de danos, prevenção, detecção e remoção de perigos.

☐ Todas as assertivas são verdadeiras.

☐ Somente I, II e IV.

☐ Somente I e II.

☐ Somente I, II e III.

☐ Somente II, III e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - A decomposição de riscos pode ser feita utilizando duas técnicas: top-down ou bottom-up. **V**

II - A árvore de defeitos é uma técnica de decomposição de riscos na qual o perigo é posicionado na raiz da árvore. Em seguida, os estados do sistema são identificados e decompostos até se alcançar as causas-raiz do perigo (folhas da árvore). **V**

III - Na etapa de redução de riscos, os requisitos de segurança são definidos de modo a garantir que incidentes ou acidentes não ocorram. **V**

IV - Existem várias estratégias que podem ser utilizadas para evitar acidentes, tais como limitação de danos, prevenção, detecção e remoção de perigos. **V**



☒ Todas as assertivas são verdadeiras.

☐ Somente I, II e IV.

☐ Somente I e II.

☐ Somente I, II e III.

☐ Somente II, III e IV.

Especificação de confiabilidade

- A especificação de confiabilidade pode ser descrita através de dois tipos de requisitos:
 - **Requisitos não-funcionais:** descrevem métricas para avaliar confiabilidade
 - **Ex:** Disponibilidade, Tempo entre falhas, Probabilidade de falhas
 - **Requisitos funcionais:** definem características de confiabilidade, de forma qualitativa.

Métricas de confiabilidade (requisitos nao-funcionais)

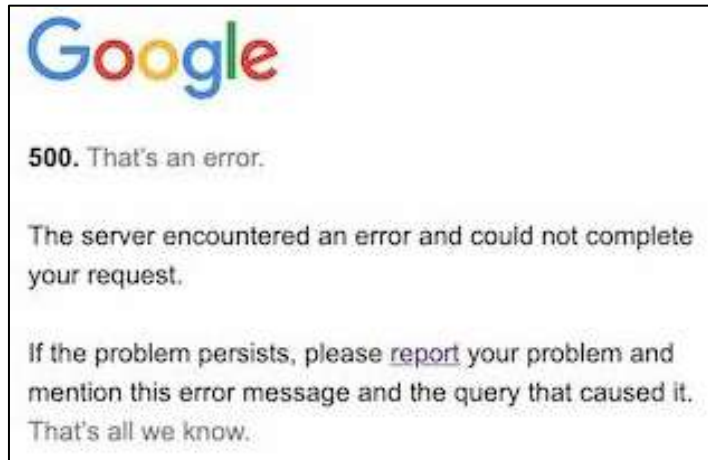
- Podemos avaliar o nível de confiabilidade de um sistema usando as seguintes métricas:
 - **Probabilidade de falha sob demanda** (*POFOD*)
 - **Taxa de ocorrência de falhas** (*ROCOF*)
 - **Tempo médio para falhas** (*MTTF*)
 - **Disponibilidade** (*AVAIL*)

Probabilidade de falha sob demanda (*POFOD*)

- Probabilidade de uma demanda por serviços de um sistema resultar em uma falha de sistema

$$POFOD = \frac{falhas}{tentativas} \cdot 100$$

- **Ex:** Seja um sistema do Google, no qual a cada 200 tentativas de acesso há 2 falhas
- $POFOD = 2/200 \times 100 = 1\%$



Taxa de ocorrência de falhas (ROCOF)

- Número de falhas ocorridas ao longo de um determinado período

$$ROCOF(tempo) = \frac{falhas}{tempo}$$

- **Ex:** Seja um sistema A que falha 1 vez por ano
 - $ROCOF(\text{ano}) = 1 / (1 \text{ ano}) = 1 \text{ falha ao ano}$
 - $ROCOF(\text{mês}) = 1 / (1 \text{ ano} \times 12 \text{ meses}) = 0,083 \text{ falhas ao mes}$
 - $ROCOF(\text{dia}) = 1 \text{ falha} / (1 \text{ ano} \times 12 \text{ meses} \times 30 \text{ dias}) = 0,0027 \text{ falhas ao dia}$

Tempo médio para falhas (*MTTF*)

- Tempo transcorrido entre falhas de um sistema

$$MTTF(tempo) = \frac{tempo}{falhas}$$

- **Ex:** Seja um sistema A que falha 3 vez por ano. Calcule o MTTF.
 - **MTTF (mês) = 1 ano x 12 meses / (3 falhas) = 4 meses**

Tempo médio para falhas (*MTTF*)

- Tempo transcorrido entre falhas de um sistema

$$MTTF(T) = \frac{|T_2 - T_1| \cdot |T_3 - T_2| \cdots |T_n - T_{n-1}|}{n}$$

- **Ex:** Seja um sistema A que falhou nos instantes de tempo 1s, 5s e 15s. Calcule o MTTF dele em segundos.

$$MTTF(seg) = \frac{(1 - 0) + (5 - 1) + (15 - 5)}{3} = 5 \text{ seg}$$

Disponibilidade (*AVAIL*)

- Reflete a capacidade do sistema de prestar serviços quando solicitado
- Probabilidade de um sistema estar em operação quando surgir uma demanda por um serviço

$$AVAIL = 100 - \frac{tempoIndisponivel}{tempoTotal}$$

$$tempoIndisponivel = ROCOF \cdot tempoReparacao$$

Exemplo de Cálculo de Disponibilidade (*AVAIL*)

- **Ex:** Seja um sistema **X**, que falha 1 vez a cada 10 min. Sabendo que o reparo de cada falha de **X** demora 5 min, calcule a disponibilidade do sistema.

ROCOF (hora):
 $\text{Tempo_total} / \text{MTTF} =$
 $60 \text{ min} / 10 \text{ min} =$
6 falhas / hora

X

**Tempo para reparo
de cada falha:**
5 min

=

Tempo do sistema offline:
30 min offline a cada hora

Disponibilidade:
 $100 - 100 \times \text{tempo_offline} / \text{tempo_total} =$
 $100 - 100 \times 30 \text{ min offline} / 60 \text{ min} =$
 $100 - 100 \times 0,5 = \mathbf{50\%}$

Quando usar cada uma dessas métricas?

- **POFOD** é muito utilizado em sistemas críticos de segurança
 - **Ex:** POFOD = 0,01% em um freio ABS indica que haverá uma falha no sistema de freio a cada 10.000 tentativas de frear o carro
- **ROCOF** é mais adequado para quando o sistema possui demandas periódicas (não intermitentes), realizadas regularmente
 - **Ex:** Em um sistema bancário, há um número X de transações que ocorre a cada hora. Nesse caso, podemos definir ROCOF de 10 falhas por dia, por exemplo

Quando usar cada uma dessas métricas?

- **MTTF** é utilizado quando o tempo absoluto entre falhas é importante
 - **Ex:** Em um sistema de bomba de insulina, pode ser necessário administrar insulina no paciente a cada 3 horas. Então, temos que $MTTF > 3h$ para garantir a segurança do paciente.
- **AVAIL** é utilizado quando o sistema possui uma exigência de disponibilidade (isto é, não deve ficar muito tempo indisponível)
 - **Ex:** Sistema bancário deve ter um AVAIL alto ($\geq 99.9\%$), para que transferências financeiras possam ser realizadas

Exercício - Métricas de confiabilidade

- Calcule o ROCOF, MTTF e o AVAIL do sistema abaixo:
 - **Sistema X:** falha 1 vez a cada 20 min e o reparo de cada falha demora 8 min

ROCOF(hora):

$$1 \text{ falha} / (20 \text{ min}) \times 60 \text{ min/h} = 3 \text{ falhas} / \text{h}$$

Tempo para reparo de cada falha:

8 min

Tempo do sistema offline:

$$3 \text{ falhas} / \text{h} \times 8 \text{ min} = 24 \text{ min offline a cada hora}$$

MTTF:

20 min entre falhas

Disponibilidade (AVAIL):

$$100 - 100 \times 24 \text{ min offline} / 60 \text{ min} = 100 - 40 = 60\%$$

Dificuldade na medição da confiabilidade

- O cálculo das métricas de confiabilidade requer estatísticas de uso do sistema, coletadas através de sucessivos testes com o sistema
 - Isso muitas vezes é um processo muito custoso e impraticável no mundo real
 - **Ex:** Assegurar uma POFOD de 0,0001% requer a execução de ao menos 10.000 testes para se constatar uma falha no sistema
 - Na prática, precisaríamos de algo em torno de 50 a 60 mil testes para assegurar o POFOD de 0,0001%

Dificuldade na medição da confiabilidade

- O sistema deve ter a confiabilidade estritamente necessária para atender aos requisitos estabelecidos em sua especificação
 - **Nem todo sistema requer altos níveis de confiabilidade**
 - As partes do sistema suscetíveis a falhas menos graves podem ter níveis de confiabilidade menores
 - **Ex:** um banco pode tolerar algumas falhas, desde que ele consiga desfazer essas transações incorretas (transferencia, empréstimo, etc) sem grandes prejuízos

Exercício

$$AVAIL = 100 - \frac{tempoIndisponivel}{tempoTotal}$$

$$tempoIndisponivel = ROCOF \cdot tempoReparacao$$

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Seja um sistema A que falha 6 vezes ao longo de 1 ano. A taxa de ocorrência de falhas (ROCOF) de A, considerando um intervalo de tempo de um mês, será de 0,50 falhas por mês.

II - Considere um sistema B que falha 1 vez a cada 15 min e demora 3,75 min para ser reparado (sistema retornar ao estado online). Nesse caso, a disponibilidade de B ao longo de uma hora é de aproximadamente 75,00%.

III - O cálculo das métricas de confiabilidade requer estatísticas de uso do sistema, coletadas através de sucessivos testes.

IV - As partes de um sistema suscetíveis a falhas menos graves podem ter níveis de confiabilidade menores, desde que o sistema atenda aos requisitos de confiabilidade estabelecidos em sua especificação.

$$POFOD = \frac{falhas}{tentativas} \cdot 100$$

$$ROCOF(tempo) = \frac{falhas}{tempo}$$

$$MTTF(tempo) = \frac{tempo}{falhas}$$

Exercício


Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Seja um sistema A que falha 6 vezes ao longo de 1 ano. A taxa de ocorrência de falhas (ROCOF) de A, considerando um intervalo de tempo de um mês, será de 0,50 falhas por mês. **V**

II - Considere um sistema B que falha 1 vez a cada 15 min e demora 3,75 min para ser reparado (sistema retornar ao estado online). Nesse caso, a disponibilidade de B ao longo de uma hora é de aproximadamente 75,00%. **V**

III - O cálculo das métricas de confiabilidade requer estatísticas de uso do sistema, coletadas através de sucessivos testes. **V**

IV - As partes de um sistema suscetíveis a falhas menos graves podem ter níveis de confiabilidade menores, desde que o sistema atenda aos requisitos de confiabilidade estabelecidos em sua especificação. **V**

-  ☐ Todas as assertivas são verdadeiras.
- ☐ Somente I, II e III.
- ☐ Somente III e IV.
- ☐ Somente I e III.
- ☐ Somente II, III e IV.

Seguem as assertivas com os ajustes necessários para torná-las VERDADEIRAS:

$$\begin{aligned}\text{ROCOF(A, meses)} &= \text{\#falhas(A)} / \text{intervalo_tempo(meses)} \\ &= 6 \text{ falhas} / 12 \text{ meses} \\ &= 0,50\end{aligned}$$

$$\begin{aligned}\text{MTTF(B, min)} &= 15 \text{ min} \\ t_{\text{reparo}}(\text{B, min}) &= 3,75 \text{ min}\end{aligned}$$

$$\begin{aligned}\text{AVAIL(B, h)} &= 100 - 100 \times t_{\text{ocioso}}(\text{B, h}) / t_{\text{total}}(\text{B, h}) \\ t_{\text{ocioso}}(\text{B, h}) &= t_{\text{reparo}}(\text{B, h}) \times \text{\#falhas(B, h)} \\ t_{\text{reparo}}(\text{B, h}) &= 3,75 \text{ min} / 60 \text{ min por hora}\end{aligned}$$

$$\begin{aligned}\text{\#falhas(B, h)} &= 1 / \text{MTTF (B, h)} \\ &= 1 / (15 \text{ min} / 60 \text{ min por hora}) \\ &= 60 / 15 \text{ falhas em uma hora}\end{aligned}$$

$$\begin{aligned}t_{\text{ocioso}}(\text{B, h}) &= (3,75 / 60) \times (60 / 15) = 3,75 / 15 \text{ horas ocioso} \\ t_{\text{total}}(\text{B, h}) &= 1 \text{ hora} \\ \text{AVAIL(B, h)} &= 100 - 100 \times (3,75 / 15) / 1 \\ &= 75\end{aligned}$$

Requisitos funcionais de confiabilidade

- Existem três tipos de requisitos funcionais de confiabilidade para um sistema
 - Requisitos de **verificação**
 - Requisitos de **recuperação**
 - Requisitos de **redundância**

Requisitos de verificação

- Garantem que entradas incorretas ou fora dos limites sejam detectadas antes de serem processadas pelo sistema
 - **Ex:** validação de formulários HTTP antes do POST / SUBMIT

JÁ POSSUI UMA CONTA?

Se você já possui uma conta, informe os dados de acesso.

Email *

*Campos Obrigatórios

Campo obrigatório.

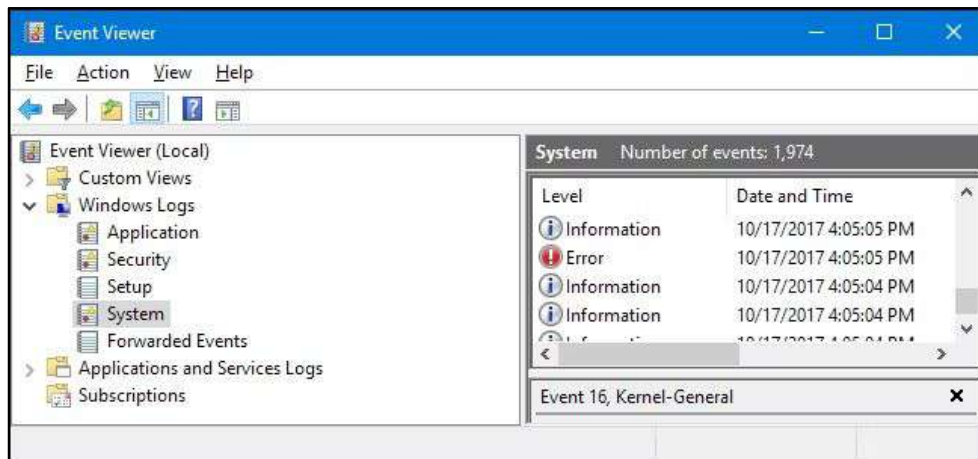
Senha *

Campo obrigatório.

Requisitos de recuperação

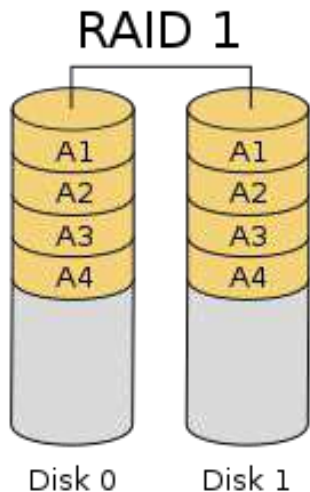
- Ajudam o sistema a se recuperar de falhas
 - **Ex:** backup e restauração de dados, imagem de sistema operacional, logs em bancos de dados

Failure configuring Windows updates
Reverting changes
Do not Turn off your computer.



Requisitos de redundância

- Definem características redundantes do sistema que garantem que a falha de um único componente não causa a perda do serviço completo
 - **Ex:** RAID de HDDs



RAID 1:
Armazenar uma cópia de
um HDD em outro

Objetivo:
Se qualquer um dos
HDDs falhar, não
perdemos dados

Exercício - Mapeie os requisitos funcionais de confiabilidade de acordo com sua classificação

RC1:

Um intervalo predefinido deve ser estabelecido para as entradas do operador. O sistema verificará se as entradas do operador estão dentro desse intervalo.

Recuperação

RC2:

Cópias da base de dados de pacientes devem ser mantidas em dois servidores separados, não alojados no mesmo edifício.

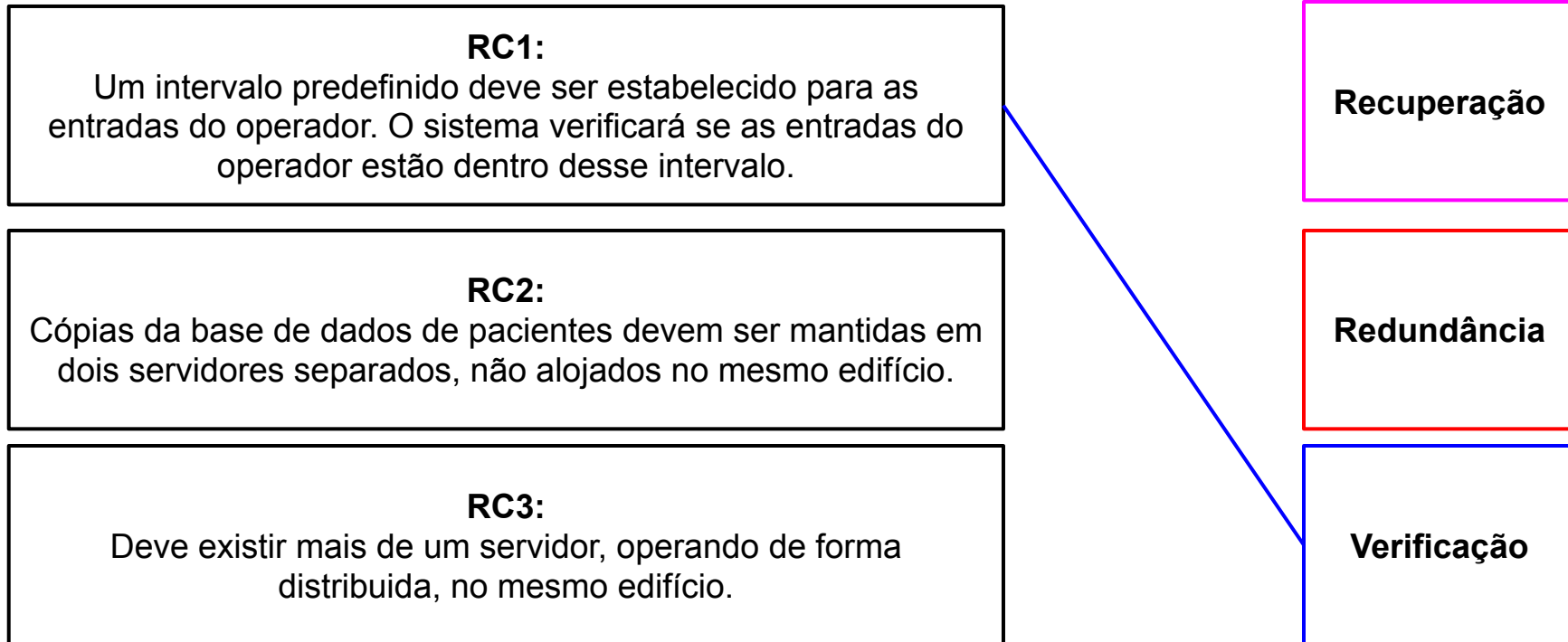
Redundância

RC3:

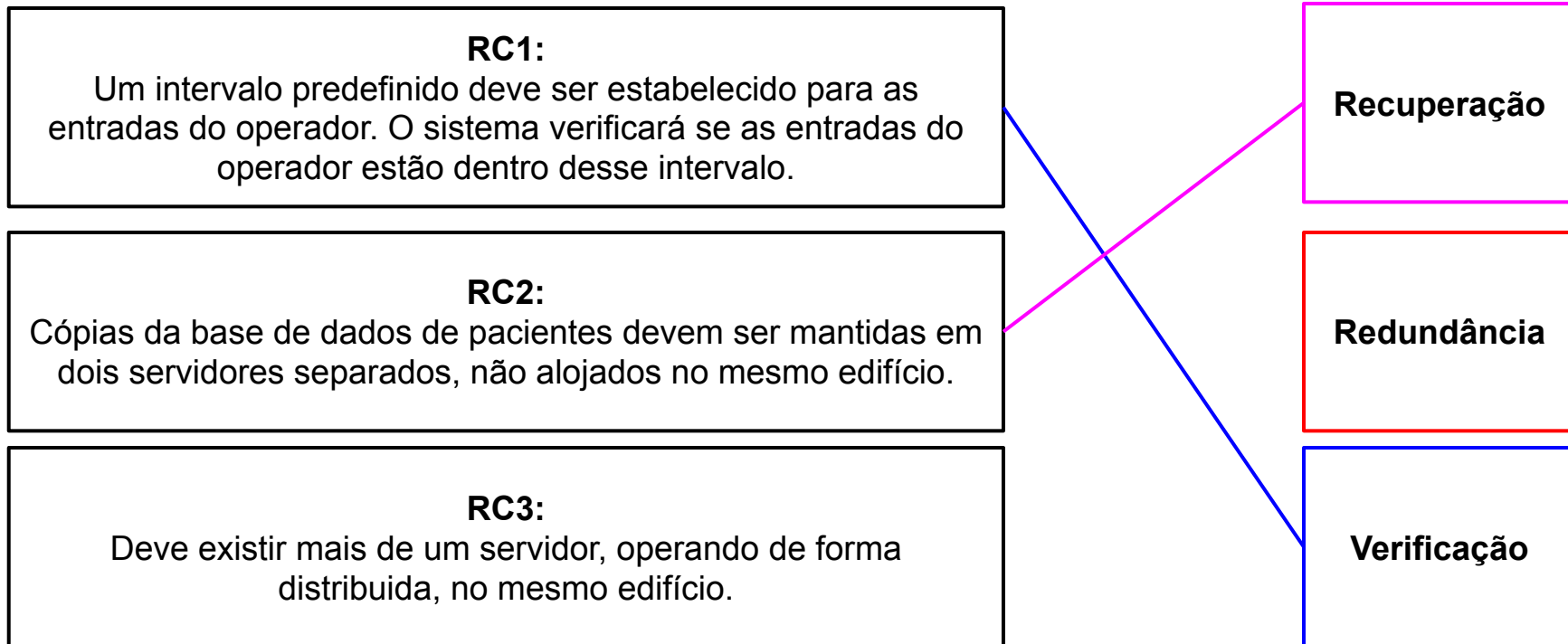
Deve existir mais de um servidor, operando de forma distribuída, no mesmo edifício.

Verificação

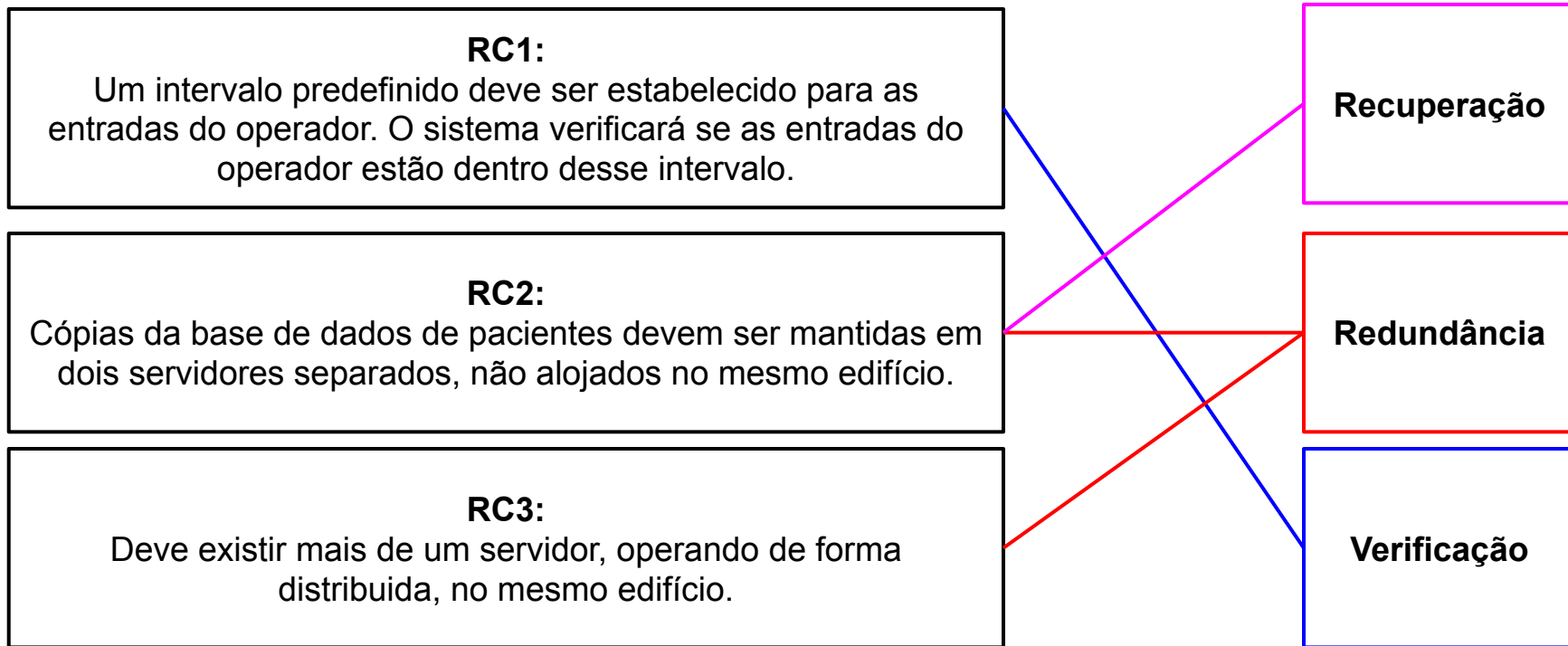
Exercício - Mapeie os requisitos funcionais de confiabilidade de acordo com sua classificação



Exercício - Mapeie os requisitos funcionais de confiabilidade de acordo com sua classificação



Exercício - Mapeie os requisitos funcionais de confiabilidade de acordo com sua classificação



Especificação de proteção

- Não podemos definir métricas quantitativas para avaliar o nível de proteção de um sistema
 - Os requisitos de proteção definem o que não é aceitável, em vez de definir a funcionalidade desejada
 - **Ex:**
 - **RP1:** O sistema não deve permitir acesso a dados sigilosos por usuários não autorizados

Desafios da especificação de proteção

- Definir requisitos de proteção é mais desafiador do que os de segurança, porque:
 - Assumimos que os ataques ao sistema são deliberados
 - O invasor talvez tenha conhecimento de pontos fracos do sistema
 - Encontrar a causa-raiz de pode ser uma tarefa difícil
 - O invasor tentará esconder seus rastros
 - Ataques podem deliberadamente reduzir o desempenho do sistema ou desliga-lo por completo

Desafios da especificação de proteção

#VisãoCNN



VAZAMENTO DE SENHA

16 MILHÕES DE PACIENTES DA COVID TÊM DADOS EXPOSTOS

Funcionário do Hospital Albert Einstein divulgou acesso

VIVO

CNN
BRASIL

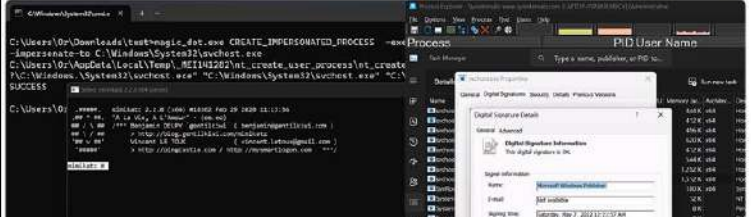
IBOV ▼ 0,21%

@CNNBrasil Siga as nossas redes sociais f i t y t @CNNBrasil

Pesquisadores descobrem falhas no Windows que concedem aos hackers poderes semelhantes aos do rootkit

22 de abril de 2024 Redação

Rootkit / Segurança de software



Descoberta contínua de superfícies de ataque e testes de penetração

Descubra, priorize e mitigue continuamente

exposições com ASMA, Passwords e Red Teaming

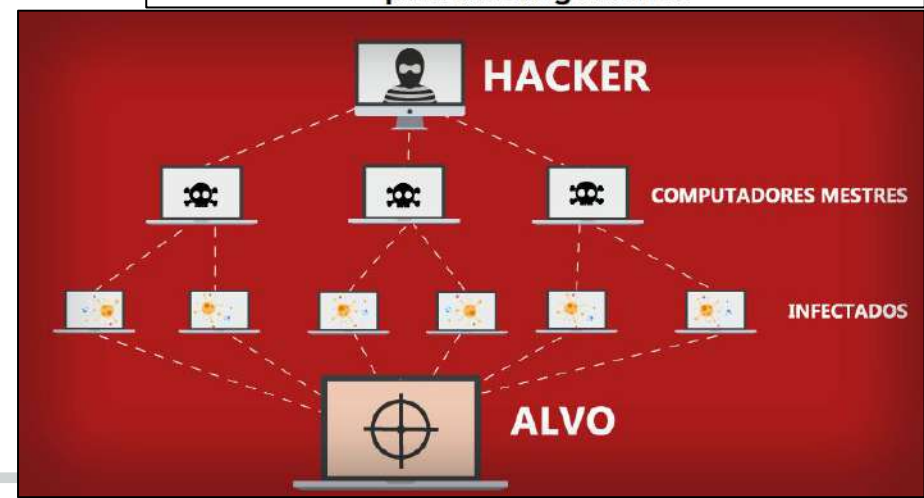
CISO
Advisor

Newsletter Branded Posts Opiniões Categorias Streamings Anunciar

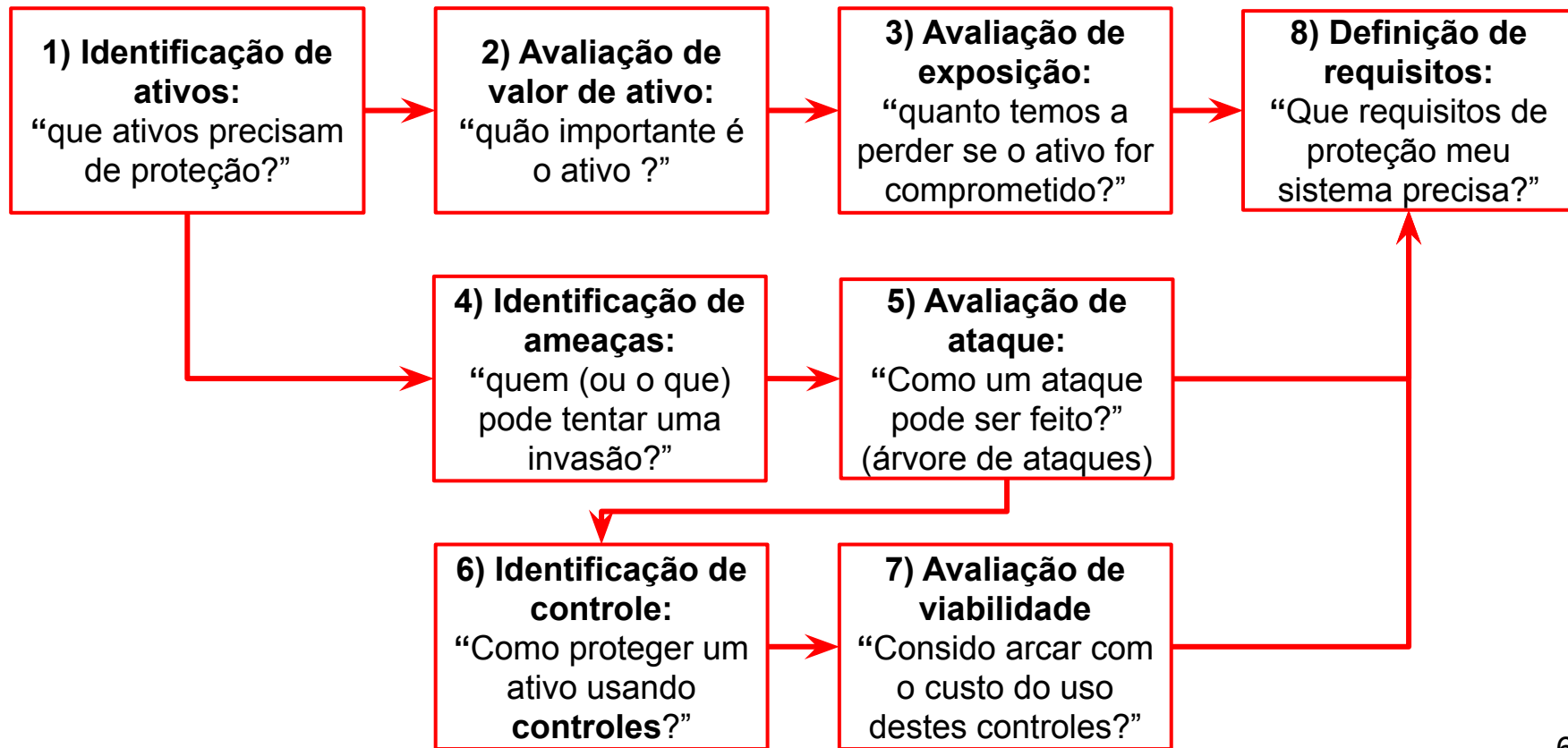
Busca



Hackers ocultam malware no logo do Windows para atacar governos



Processo de especificação de proteção



Exemplo de especificação de proteção (sistema hospitalar)

Ativo	Valor	Exposição
O sistema de informação	Alto. Necessário para suportar todas as consultas clínicas. Potencialmente crítico de segurança.	Alta. Perdas financeiras à medida que consultas podem ter de ser canceladas. Custos de restauração de sistema. Possível dano ao paciente caso o tratamento não possa ser prescrito.
O banco de dados de pacientes	Alto. Necessário para suportar todas as consultas clínicas. Potencialmente crítico de segurança.	Alta. Perdas financeiras à medida que consultas podem ter de ser canceladas. Custos de restauração de sistema. Possível dano ao paciente caso o tratamento não possa ser prescrito.
Um registro individual de paciente	Normalmente baixo, embora possa ser elevado para determinados pacientes, dependendo do perfil.	Perdas diretas baixas, mas uma possível perda de reputação.

Com essas informações, podemos descrever que **ameaças** existem no sistema, sua **probabilidade** de acontecer, **controles** e **viabilidade** das soluções

Exemplo de especificação de proteção (sistema hospitalar)

Ameaça	Probabilidade	Controle	Viabilidade
Usuário não autorizado ganha acesso como administrador de sistema e torna o sistema indisponível	Baixa	Somente permitir a administração de sistema a partir de locais específicos, fisicamente protegidos.	Baixo custo de implementação, mas é preciso ter cuidado com a distribuição de chaves, para garantir que elas estejam disponíveis em caso de emergência.
Usuário não autorizado ganha acesso como usuário de sistema e acessa informações confidenciais	Alta	Exigir autenticação de todos os usuários, por meio de um mecanismo biométrico. Registrar todas as alterações nas informações do paciente para acompanhar o uso do sistema.	Tecnicamente possível, mas o custo seria muito alto. Possível resistência de usuários. Implementação simples e transparente, também suporta a recuperação.

Controle: técnica para evitar a concretização da ameaça

Especificação de proteção

- Organizações (empresas, entidades governamentais, etc) podem definir **políticas de proteção organizacional**
 - **Política de proteção organizacional:** define o que deve e o que não deve ser permitido em todos os sistemas de uma organização
 - **Ex:** Na marinha, documentos são classificados como 'ultra-secretos', 'secretos', 'confidenciais' ou 'abertos'.
 - **Política de proteção:** somente os soldados de alta patente devem ter acesso aos documentos 'ultra-secretos'.
- Políticas de proteção facilitam a definição de requisitos de proteção

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os requisitos de proteção definem a funcionalidade ou técnicas de proteção exigidas ou utilizadas pelo sistema.

II - Os requisitos de segurança são mais desafiadores do que os de proteção, pois se assume que os ataques a um sistema são deliberados.

III - Os requisitos de segurança são mais desafiadores do que os de proteção, pois um invasor pode esconder seus rastros, além de possuir algum conhecimento sobre os pontos fracos do sistema.

IV - Ataques podem deliberadamente reduzir o desempenho do sistema ou desligá-lo por completo.

- ☐ Somente I.
- ☐ Somente I, II e III.
- ☐ Somente II, III e IV.
- ☐ Somente IV.
- ☐ Somente I e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os requisitos de proteção **definem a funcionalidade ou técnicas** de proteção exigidas ou utilizadas pelo sistema. **F**

II - Os requisitos de segurança são mais desafiadores do que os de proteção, pois se assume que os ataques a um sistema são deliberados.

III - Os requisitos de segurança são mais desafiadores do que os de proteção, pois um invasor pode esconder seus rastros, além de possuir algum conhecimento sobre os pontos fracos do sistema.

IV - Ataques podem deliberadamente reduzir o desempenho do sistema ou desligá-lo por completo.

- ☐ Somente I.
- ☐ Somente I, II e III.
- ☐ Somente II, III e IV.
- ☐ Somente IV.
- ☐ Somente I e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os requisitos de proteção **definem a funcionalidade ou técnicas** de proteção exigidas ou utilizadas pelo sistema. **F**

II - Os requisitos de segurança são mais desafiadores do que os de proteção, pois se assume que os ataques a um sistema são deliberados. **F**

III - Os requisitos de segurança são mais desafiadores do que os de proteção, pois um invasor pode esconder seus rastros, além de possuir algum conhecimento sobre os pontos fracos do sistema.

IV - Ataques podem deliberadamente reduzir o desempenho do sistema ou desligá-lo por completo.

- ☐ Somente I.
- ☐ Somente I, II e III.
- ☐ Somente II, III e IV.
- ☐ Somente IV.
- ☐ Somente I e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os requisitos de proteção **definem a funcionalidade ou técnicas** de proteção exigidas ou utilizadas pelo sistema. **F**

II - Os requisitos de segurança são mais desafiadores do que os de proteção, pois se assume que os ataques a um sistema são deliberados. **F**

III - Os requisitos de segurança são mais desafiadores do que os de proteção, pois um invasor pode esconder seus rastros, além de possuir algum conhecimento sobre os pontos fracos do sistema. **F**

IV - Ataques podem deliberadamente reduzir o desempenho do sistema ou desligá-lo por completo.

☐ Somente I.

☐ Somente I, II e III.

☐ Somente II, III e IV.

☐ Somente IV.

☐ Somente I e IV.

Exercício

Marque a alternativa que contém **somente** as assertivas VERDADEIRAS.

I - Os requisitos de proteção **definem a funcionalidade ou técnicas** de proteção exigidas ou utilizadas pelo sistema. **F**

II - Os requisitos de segurança são mais desafiadores do que os de proteção, pois se assume que os ataques a um sistema são deliberados. **F**

III - Os requisitos de segurança são mais desafiadores do que os de proteção, pois um invasor pode esconder seus rastros, além de possuir algum conhecimento sobre os pontos fracos do sistema. **F**

IV - Ataques podem deliberadamente reduzir o desempenho do sistema ou desligá-lo por completo. **V**

☐ Somente I.

☐ Somente I, II e III.

☐ Somente II, III e IV.

 ☒ Somente IV.

☐ Somente I e IV.

Referencial Bibliográfico

- SOMMERVILLE, Ian. **Engenharia de Software**. 6. ed. São Paulo: Addison-Wesley, 2003.
- PRESSMAN, Roger S. **Engenharia de Software**. São Paulo: Makron Books, 1995.
- JUNIOR, H. E. **Engenharia de Software na Prática**. Novatec, 2010.