Segurança como diferencial competitivo da Qualidade do Produto de Software Nacional

Segurança e Qualidade de Software, Campinas, 25/10/2010, PBQP-SW

Roteiro

- Vulnerabilidades de Software (CVE)
- Motivação para o tema Segurança
- No mundo: PITAC 05
- Preocupações dos Consumidores
- Segurança de Software
- No Brasil: PCI, OWASP RFP
- Alguns exemplos
- Normas
- Conclusões
- Ações recomendadas

Vulnerabilidades de Software

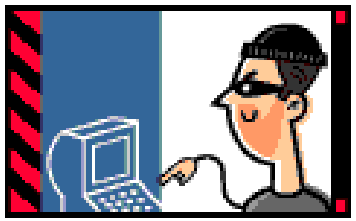
- Em software é uma conjunto de condições que podem levar à violação da política de segurança explícita ou implícita da empresa.
- É o estado de um sistema computacional (ou conjunto de sistemas) que permite que um atacante:

✓ Execute comandos se fazendo passar por outro usuário;

✓ Acesse dados burlando restrições de acesso aos mesmos;

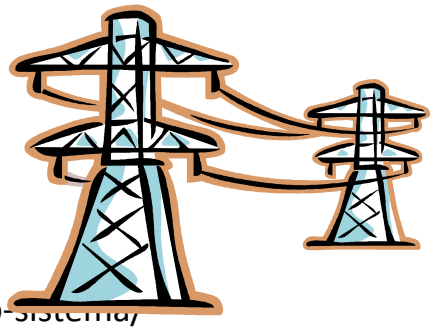
✓ Aja como outra entidade;

✓ Negue a execução do serviço.



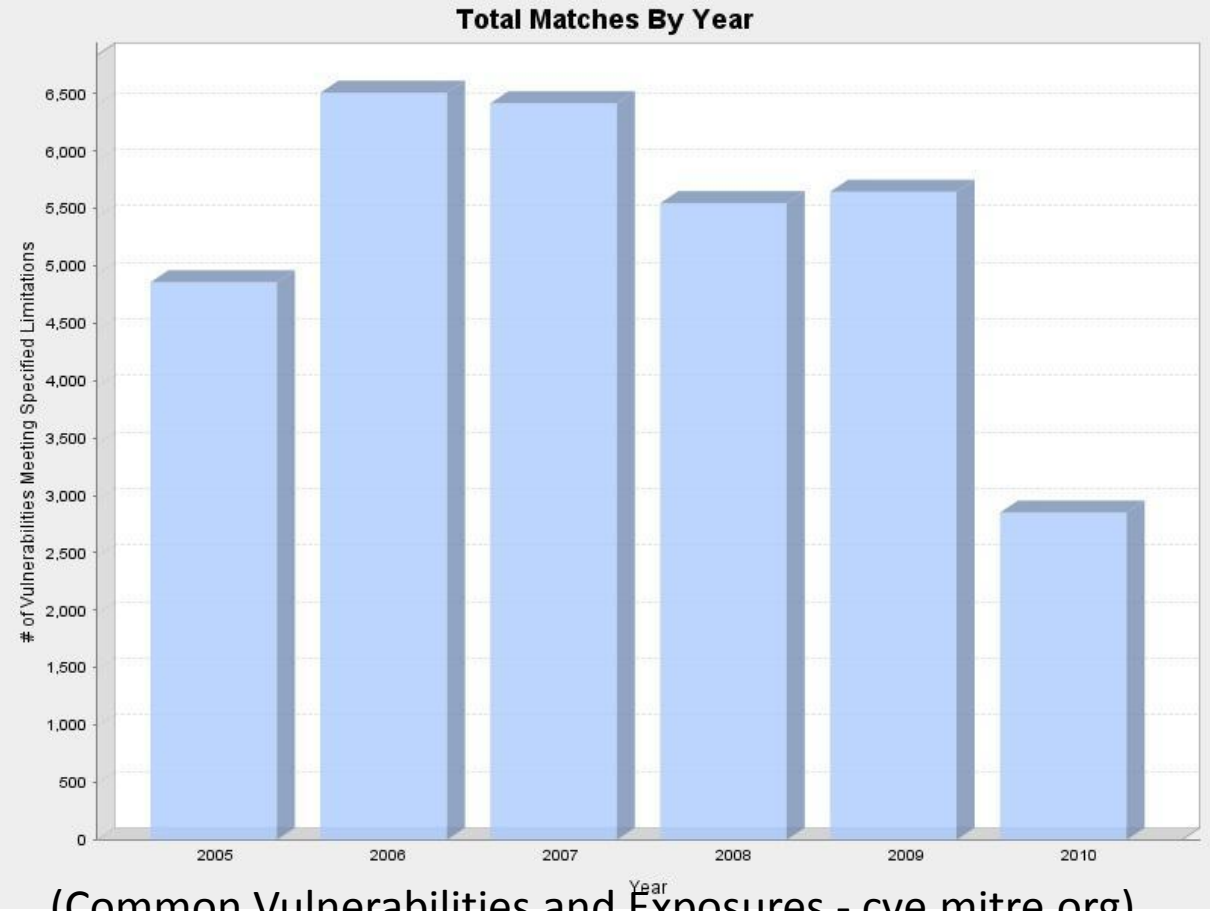
Falha em sistemas corporativos

- Sistemas SCADA – de automação industrial projetados para gerenciar sistemas automatizados;
- Extremamente frágil do ponto de vista de Segurança da Informação;
- O Governo tem consciência deste problema e lançou um Programa para proteger os sistemas de informação de estruturas críticas cujo funcionamento não pode ser interrompido sem prejuízos.



http://www.nfedobrasil.com.br/BlogNfe/index.php/2009/11/12/apagao-vulnerabilidade-no-sistema/

Vulnerabilidades 2005-2010



(Common Vulnerabilities and Exposures - cve.mitre.org)

Common Vulnerabilities and Exposures (CVE)

- CVE-2010-2882/2863
  19 vulnerabilidades do Adobe Shockwave Player que permitem a execução de código arbitrário na máquina do usuário.
  Publicadas em 26/08/2010.

http://www.adobe.com/support/security/advisories/apsa10-01.html

Cyber Security: A Crisis of Prioritization

- No relatório ao presidente dos EUA, intitulado *Cyber Security: A Crisis of Prioritization* [PITAC 05], o seu Comitê Assessor em Tecnologia da Informação dramatizou o problema de vulnerabilidades de software da seguinte maneira:

Citações sobre segurança de software

1. O desenvolvimento de software ainda não é uma ciência ou uma disciplina rigorosa;
2. O processo de desenvolvimento não é controlado de forma a minimizar as vulnerabilidades que atacantes exploram;
3. Os processos danosos podem ser invisíveis para leigos no assunto, enquanto especialistas reconhecem que essas ameaças estão crescendo;
4. Ações preventivas para minimizar os danos a curto prazo.
5. Pesquisas, para estabelecer a base de conhecimentos e competências que poderão embasar a redução de riscos e minimizar os prejuízos no longo prazo.

Preocupações dos Consumidores

- A integridade de recursos críticos depende da confiabilidade e segurança de software que são usados para gerar e controlar estes recursos.

- Existe uma grande escassez de recursos humanos com as competências necessárias para desenvolver software seguro.

Preocupações dos Consumidores

- Questionam a capacidade dos fornecedores de desenvolver e entregar software seguro, com níveis de integridade adequados, e demonstrar a adoção de um mínimo de práticas responsáveis.

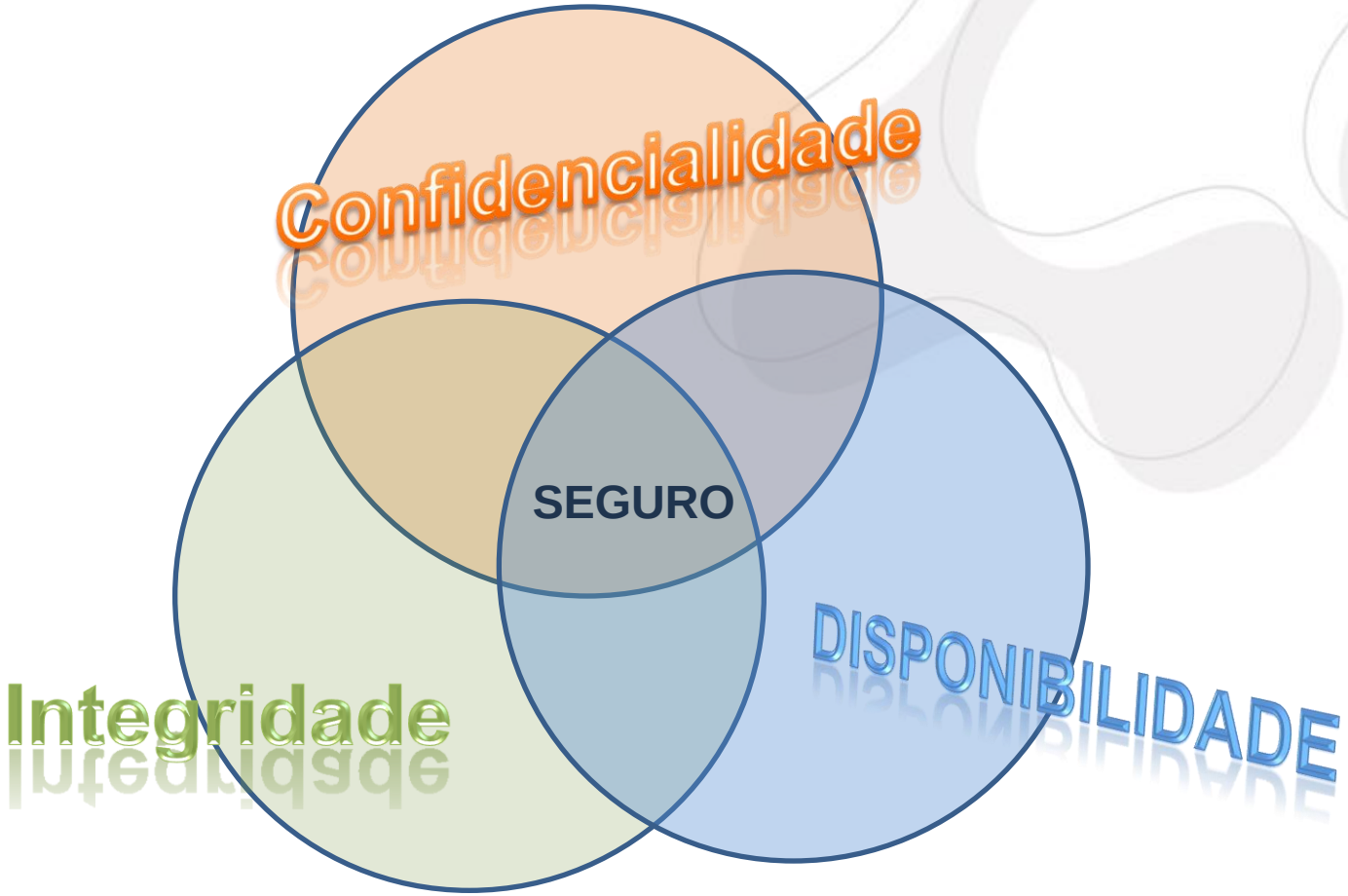
Segurança de computador : TRÊS características básicas, segundo padrões internacionais, são definidas como:

- *Confidencialidade* - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

- *Integridade* - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

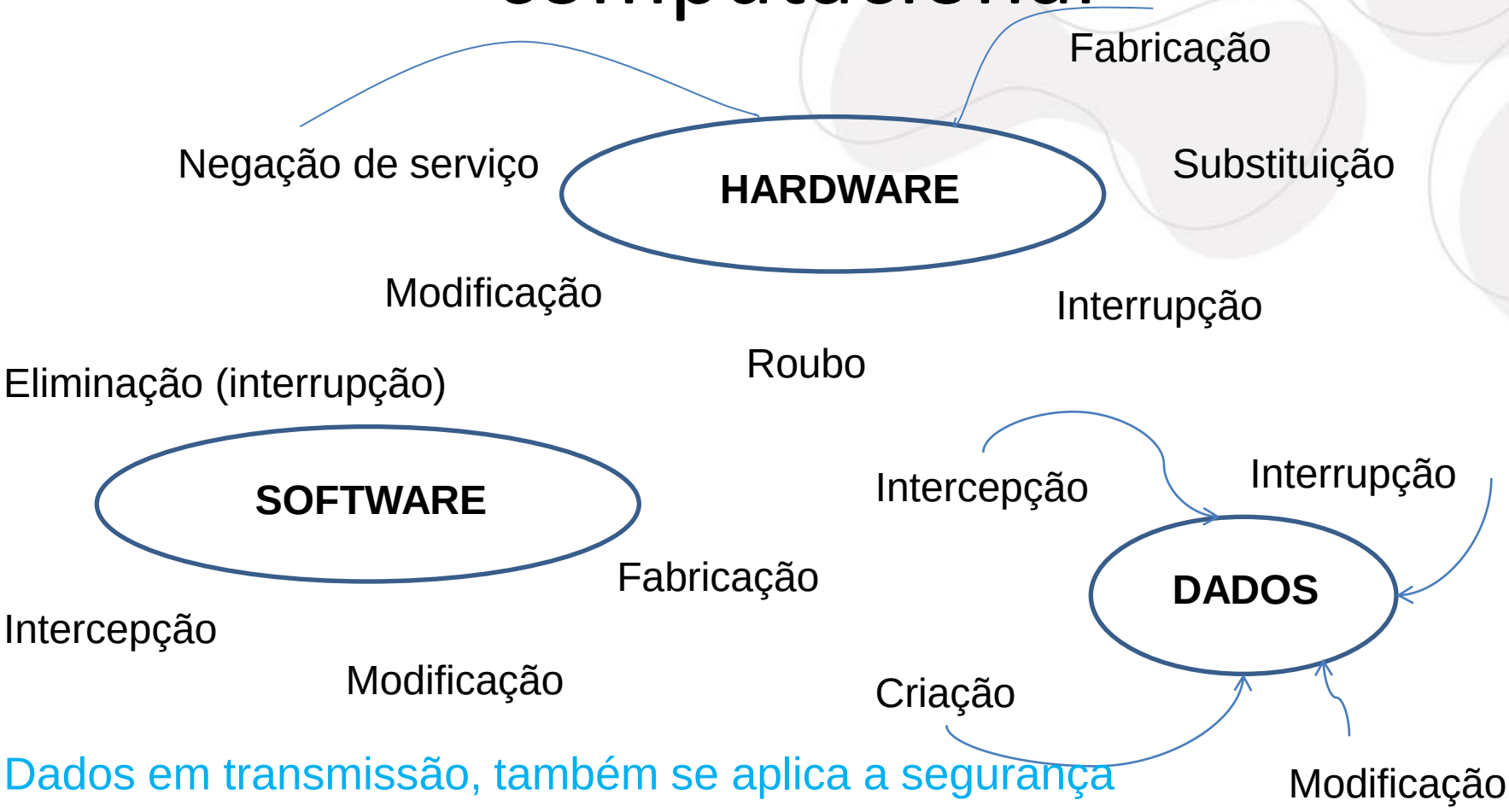
- *Disponibilidade* - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

NBR ISO/IEC 17799:2005



Relação entre Confidencialidade , Integridade, Disponibilidade

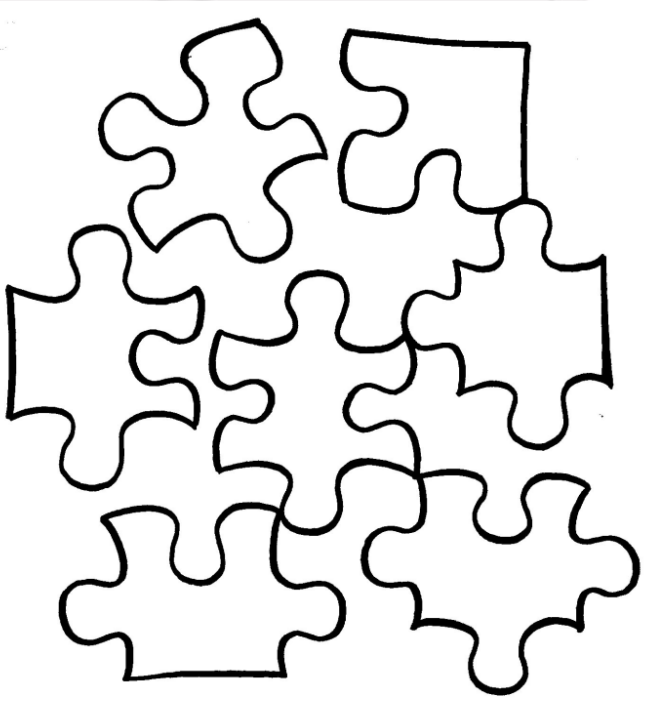
O significado da segurança computacional



Dados em transmissão, também se aplica a segurança

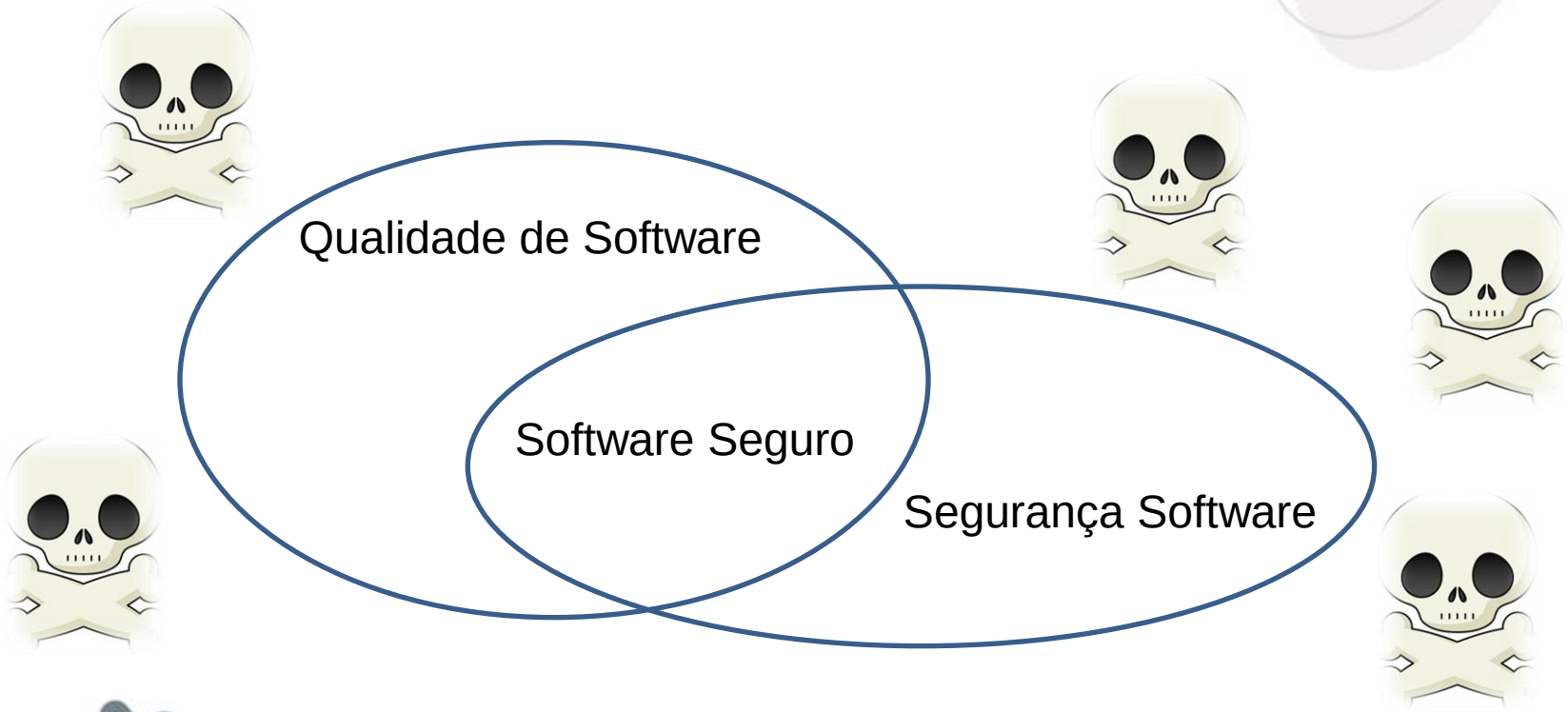
Qualidade de Produto de Software
Característica Segurança

- Confidencialidade
- Integridade
- Não-repúdio
- Responsabilidade
- Autenticidade



DISPONIBILIDADE

Existe uma sobreposição entre a qualidade de software e a segurança do software porque ambos tratam as falhas subjacentes que fazem com que o software se porte mal de uma certa maneira.



Riscos

- Sistemas de informação dependem de seus componentes de software, apesar destes serem os elos mais frágeis desses sistemas.
- Tamanho e complexidade de software, obscurecendo suas intenções e dificultando o processo de testes de segurança.
- Terceirização do desenvolvimento de software e dependência de cadeias de suprimento não credenciadas

Riscos

- Disponibilidade de software de ataque sofisticados que facilitam a exploração de fragilidades e vulnerabilidades de software e usuários (ataques pret-a-porte).
- Reuso e interfaceamento de software legado com novas aplicações, em ambientes e redes díspares e crescentemente complexos, resultando em conseqüências inesperadas e no crescente número de alvos vulneráveis.

Segurança de Software

- Segurança de Software surgiu, então, como uma resposta ao dramático aumento de riscos às missões e negócios, que são sabidamente atribuíveis à exploração de software vulneráveis.

Segurança de Software

- **Previsibilidade:** pode-se estar justificadamente confiante de que o software, quando executado, irá funcionar como se espera;
- **Confiabilidade:** não há nenhuma vulnerabilidade explorável ou lógica maliciosa no software, que tenha sido inserida por descuido ou intencionalmente;
- **Resiliência:** se comprometido, os danos ao software serão minimizados, e ele vai recuperar rapidamente um nível aceitável de capacidade operacional;
- **Conformidade:** garantir, de forma sistemática e planejada, que processos e produtos de software estejam conformes com os requisitos, e procedimentos e normas aplicáveis.

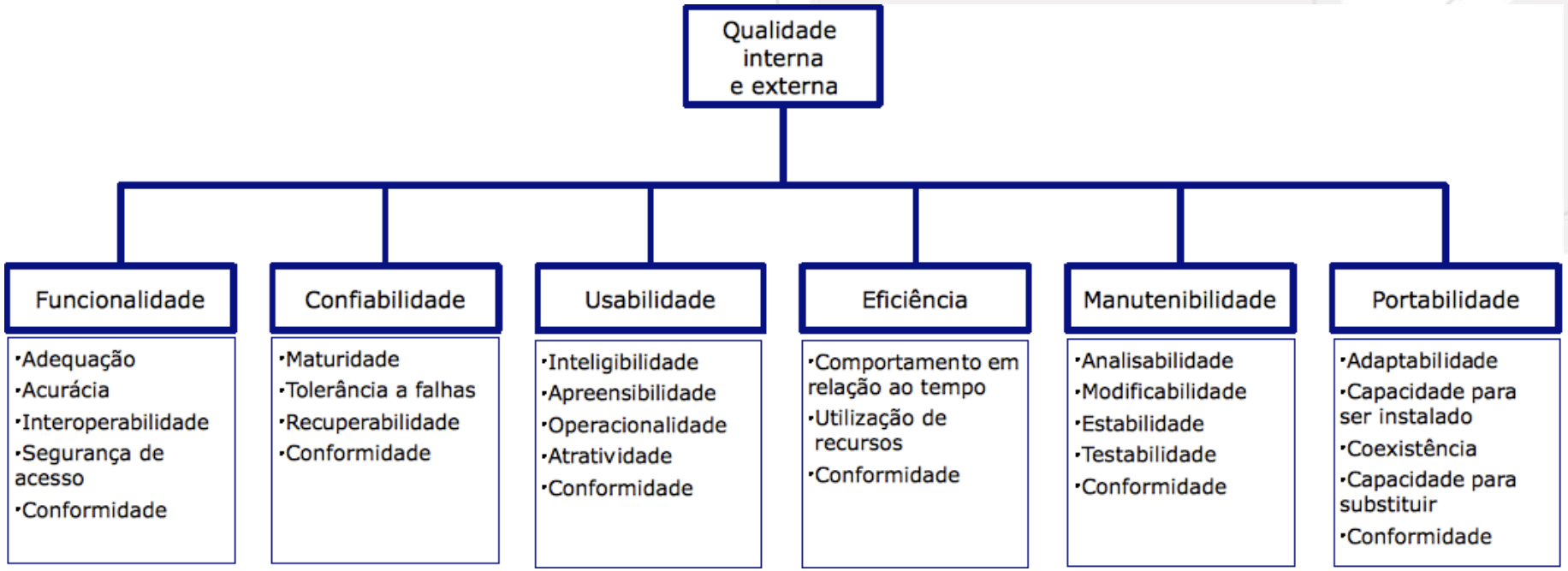
No Brasil

- O único esforço sistemático (caveat) em andamento está associado à indústria de cartões de crédito, que aplica o padrão PCI-DSS, o qual exige que aplicações de comércio eletrônico que façam uso de cartões de crédito, submetam suas aplicações Web a auditorias periódicas de segurança.

No Brasil

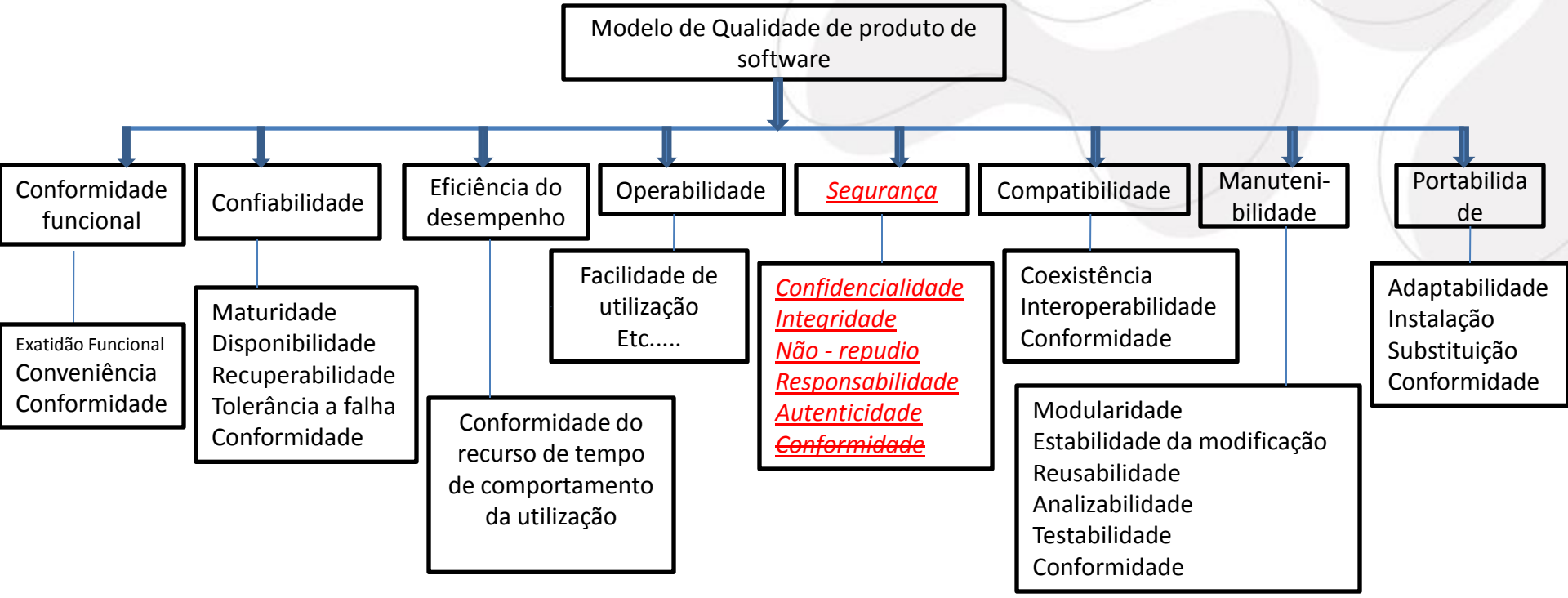
- Algumas organizações, principalmente na área governamental, estão adotando as recomendações do *Open Web Application Security Project* (OWASP), mas ainda de forma incipiente.
- Discussões sobre a norma ISO/IEC 25010 que irá substituir a norma NBR ISO/IEC 9126, que estabelece os padrões de qualidade de produtos de software.

NBR ISO/IEC 9126



Modelo de Qualidade de Produto de Software

Modelo de Qualidade



Em estudo na : Software Engineering - Software Product Quality Requirements and Evaluation (SQuaRE) Quality model - ISO 25010

Conclusões

- O que se conclui do cenário mundial e da situação no Brasil é que os usuários e operadores de sistemas de informação estão paulatinamente se dando conta de que os problemas de segurança estão estreitamente ligados a vulnerabilidades e fragilidades de produtos de software.

Conclusões

- Isso faz com que o consumidor esteja passando a demandar segurança de software com mais um requisito, na contratação de serviços de desenvolvimento ou na compra de produtos de prateleira.
- Os países desenvolvidos estão investindo fortemente no desenvolvimento de tecnologias de segurança de software, tais como

Conclusões

- Metodologias de desenvolvimento seguro;
- Metodologias de contratação ou compra de software seguro (requisitos, aceitação);
- Desenvolvimento de normas de segurança de software;
- Metodologias de testes de segurança de software.

- E na formação de recursos humanos qualificados para realizar todas essas tarefas.

Diferencial Competitivo

- Desta forma, é evidente que a implementação de procedimentos e técnicas para a produção e testes de software que incorporem segurança desde seu projeto até sua manutenção, isto é, no seu ciclo de vida, será, em curto prazo, um diferencial competitivo na venda de serviços e aplicações de prateleira.

Diferencial Competitivo

- Como a incorporação de segurança no ciclo de vida de software é muito mais um modo de pensar, do que a implementação de processos, o Brasil tem a oportunidade de sair na frente nesta corrida pelo mercado de software seguro, por meio do treinamento adequado de recursos humanos qualificados.

Recomendações

- É importante também que a indústria de software brasileira seja conscientizada a respeito dos problemas associados a segurança de software e sobre a existência deste nicho de mercado, talvez através da SOFTEX.

Recomendações

- Uma outra forma de estimular essa mudança consiste em usar o poder de compra do governo para estimular o desenvolvimento de software seguro. Tanto em benefício do governo e seus clientes, quanto para o desenvolvimento das tecnologias e processos necessários para isso.

PERGUNTAS ??

Prof. Dr. Antonio Montes Filho
Pesquisador Titular – Divisão de Segurança de Sistemas de Informação - DSSI/CTI
antonio.montes@cti.gov.br