# Avaliação da Conformidade de Ativos de Tecnologias
# Uma Análise Orientada a Riscos

Carlos Roberto Viana

E-mail: carlos.filho@eic.cefet-rj.br

# Sumário

- Objetivo
- Padrões
- Riscos
- Estudo de Caso
- Análise

**Objetivo**

- O estabelecimento de Programas de Avaliação de Conformidade para Tecnologia da Informação

- Uma abordagem orientada à risco, verificando padrões , normas e estudo de casos de alguns países

**Padrões**

## Avaliação da Conformidade

- É a demonstração de que os requisitos especificados relativos a um produto, processo, sistema, pessoa ou organismo são atendidos
- Processo sistematizado, acompanhado e avaliado de forma a proporcionar adequado grau de confiança de que um produto, processo ou serviço
- Atende a requisitos pré-estabelecidos em normas e regulamentos técnicos
- Transmite ao consumidor a confiança de que o produto, processo ou serviço está em conformidade com os requisitos especificados

# Avaliação da Conformidade

## Common Criteria

- Estabelece um nível de confiabilidade de que uma determinada funcionalidade de segurança dos produtos, e que as medidas de garantia aplicadas aos produtos atendem a esses requisitos

- Auxilia na definição de produtos de TI, verificando se os mesmos atendem as suas necessidades de segurança

## FIPS 140-2

- Coordenar os requisitos e padrões para módulos de criptografia que incluem componentes de hardware e software

- Específica os requisitos de segurança atendidos por um módulo criptográfico

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

## Riscos

- Tem o propósito de identificar oportunidades e ameaças

- De eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos

## Identificação do Riscos

Foram identificados 55 riscos divididos entre 9 categorias

- ME - Definição clara dos métodos de ensaio
  - Riscos referentes a importância dos requisitos, quanto a sua falta de clareza e má elucidação

- IM - Quanto ao impacto no mercado
  - Riscos referentes a regulamentação causadas por barreiras técnicas, dificuldades de adequação e desconhecimento destas

- CA - Quanto a custos aceitáveis
  - Riscos referentes aos custos envolvidos  e seu impacto para o processo de regulamentação, falta de laboratórios nacionais  ou concentração geográfica destes

## Identificação do Riscos

- DCT - Quanto à disponibilidade de competência técnica
  - Riscos referentes a disponibilidade de competência técnica, possibilitando a geração de monopólios ou a inviabilização de avaliações por laboratórios

- QTI - Quanto a transparência e imparcialidade
  - Riscos referentes a falta de transparência, imparcialidade, perda de confidencialidade, ausência de controles e comprometimento da propriedade intelectual

- IPC - Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente
  - Riscos referentes ao consumidor e sua proteção , seja pela não conformidade com o mercado, não compreensão, ausência ou rejeição de regulamentação

## Identificação do Riscos

- PCJ - Propiciar concorrência justa entre laboratórios
  - Riscos referentes aos laboratórios , pela inexistência, desequilíbrio ou monopólios

- FCI - Facilitar o comércio internacional
  - Riscos  referentes ao comércio internacional, seja pelo custo, obsolescência ou não alinhamento de requisitos ou para o mercado externo

- FMI - Fortalecer o mercado Interno
  - Risco referente a ineficiência da regulamentação existente  na melhoria necessária para o setor

## Estudo de Caso - China

- Se adequa a padronização com a necessidade da modernização e a melhora de relações econômicas com outros países
- Como forma de integração ao padrão, a China enviou delegações a vários ICCCs (International Common Criteria Conferences)
- Promoveu a visita à diversas agências de avaliação de segurança
- Convidou a diversos especialistas de outros países para a realização de treinamentos

## Estudo de Caso - Rússia

- Rússia adota desde 1995 uma certificação semelhante ao Orange Boook do Department of Defense (DoD) dos Estados Unidos
- Em 2002 adota o Common Criteria como metodologia de avaliação, traduzindo integralmente a norma
- Inicialmente suas certificações utilizavam os TOEs já definidos pelos outros países que já adotavam o Common Criteria
- Em 2012 cria e aprova seus próprios TOEs
- Aumenta sua capacidade de avaliação de vulnerabilidades, melhora de 50%
- Os novos procedimentos adotados, trazem embutidos uma alta nos custos dos laboratórios

## Estudo de Caso - Austrália

- Desde 1942 quando a marinha, o exército e aeronáutica se uniram para tentarem decodificar sinais Japoneses na segunda guerra

- A ASD (Australian Signals Directorate) é o órgão responsável pelo fornecimento de informações, assessoria de segurança de TIC para as agências governamentais federais e estaduais

    - Responsável pela orientação política, treinamento em segurança da informação e fóruns, que apoiam a segurança da informação. Prestam ainda assistência à Força de Defesa Australiana e apoio a operações militares

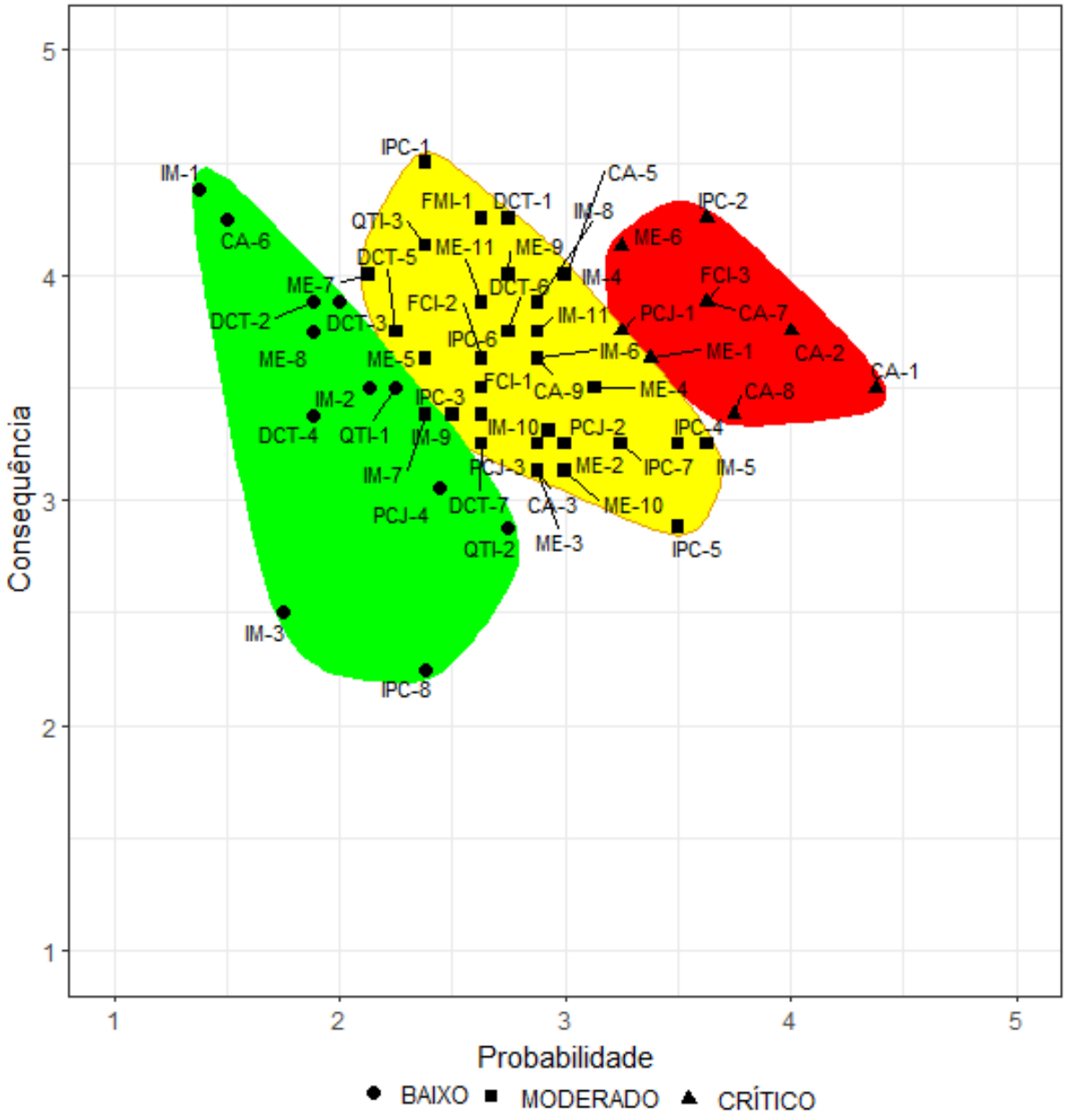
- O FIPS 140-2 é aceito como um dos critérios das avaliações

- O FIPS 140-2 não substitui a avaliação criptográfica da ASD

## Análise - Riscos Críticos

| Risco | Descrição | Média |
|---|---|---|
| ME-1 | Falta de clareza no requisito/Interpretação equivocada : Risco de que o requisito descrito em uma norma esteja impreciso, ambíguo, inconsistente ou com descrição deficiente, dificultando entendimento por fabricantes e laboratórios | 12,23 |
| ME-6 | Requisito prescritivo demais: Risco referente teor de norma, regra, preceito, determinação; normativo: regulamento prescritivo | 13,41 |
| CA-1 | Onerar o processo de regulamentação: Risco devido ao aumento das necessidades de infraestrutura de controle pré e pós mercado, podendo esta, ser insuficiente | 15,31 |
| CA-2 | Onerar o processo de produção: Risco referentes a recursos financeiros insuficientes devido ao aumento do custo da produção | 15,00 |
| CA-7 | Laboratórios apenas nas regiões S/SE: Riscos devido a maioria dos laboratórios estar presentes nas regiões Sul e Sudeste | 14,05 |
| IPC-2 | Produto não conforme no mercado. Risco referente a realização de PAC inadequados, pela dificuldade de acompanhamento da inovação ou ainda causada pela falta de Recursos | 15,41 |
| PCJ-1 | Inexistência de laboratório acreditado: Risco pela falta de laboratórios especializados e baixa expectativa de lucro | 12,19 |
| FCI-3 | Custo da certificação: Risco devido ao alto custo de elaboração e redação dos requisitos de certificação para o mercado internacional e o seu impacto no preço do produto | 14,05 |

## Análise


Consequência
Probabilidade
1
2
3
4
5
IPC-1
IM-1
CA-6
FMI-1
DCT-1
CA-5
IM-8
IPC-2
QTI-3
ME-11
ME-9
ME-6
DCT-5
IM-4
FCI-3
ME-7
DCT-6
FCI-2
PCJ-1
CA-7
DCT-2
DCT-3
IM-11
IPC-6
IM-6
ME-1
CA-2
ME-8
ME-5
FCI-1
CA-9
ME-4
CA-1
CA-8
IM-2
IPC-3
DCT-4
QTI-1
IM-9
IM-10
PCJ-2
IPC-4
IM-7
PCJ-3
ME-2
IPC-7
IM-5
PCJ-4
DCT-7
CA-3
ME-10
QTI-2
ME-3
IPC-5
IM-3
IPC-8
BAIXO
MODERADO
CRÍTICO

**Análise**

| Riscos | Relação | Mitigação | Casos |
|---|---|---|---|
| ME-1, ME-6 e IPC-2 | Qualidade técnicas dos requisitos | Implantação de regulamentos baseados em padrões técnicos baseados em padrões internacionais (utilização de padrões internacionais) | China e Austrália |
| CA-1, CA-2, CA-7, CA-8, PCJ-1 e FCI-3 | Custos do processo regulatório | Utilização de padrões personalizados utilizando os padrões internacionais como referência | Rússia e Austrália |

Avaliação da Conformidade de Ativos de Tecnologias
Uma Análise Orientada a Riscos

Carlos Roberto Viana

E-mail: carlos.filho@eic.cefet-rj.br