Avaliação da Conformidade de Ativos de Tecnologias: uma Análise Orientada a Riscos

Raphael Machado^{1,2}, Carlos Roberto Viana¹, Letícia de Sousa², Carlos A M de S Teles¹

¹CEFET-RJ - PPCIC

²Inmetro - DIPPG

rcmachado@inmetro.gov.br, carlos.filho@eic.cefet-rj.br

leticia_mrs@hotmail.com, carlos.teles@eic.cefet-rj.br

Abstract. *In the present work, we consider the challenge of establishing Conformity Assessment Programs for Information Technology and Communications Assets. We propose an evaluation of such Programs through a risk-oriented approach. The work was carried out in three stages, each of which represents a concrete contribution to the problem in question. In the first stage, identifying a set of 58 risks from the interview to specialists in the areas of conformity assessment and information technology. In the second stage, the identified risks were analyzed through the application of a questionnaire to this same set of specialists, allowing to assign, at each risk, an estimate of probability and impact, and making it possible to determine priority risks that need treatment. In the third and last step, we identified possible strategies for the treatment of risks from the survey and analysis of more Programs of Evaluation of the Conformity of Assets of Information Technologies and Communications throughout the world.*

Resumo. *No presente trabalho, consideramos o desafio de se estabelecer Programas de Avaliação da Conformidade (PAC) para Ativos de Tecnologias da Informação e de Comunicações. Propomos uma avaliação de tais Programas por meio de uma abordagem orientada a riscos. O trabalho foi realizado em três etapas, cada uma das quais representa uma contribuição concreta para o problema em questão. Na primeira etapa, identificamos um conjunto de 58 riscos a partir da entrevista de especialistas das áreas de avaliação da conformidade e de tecnologia da informação. Na segunda etapa, os riscos identificados foram analisados por meio da aplicação de questionário a este mesmo conjunto de especialistas, permitindo atribuir, a cada risco, uma estimativa de probabilidade e de impacto, e possibilitando determinar riscos prioritários que necessitam de tratamento. Na terceira e última etapa, identificamos possíveis estratégias para o tratamento dos riscos a partir do levantamento e análise de mais de Programas de Avaliação da Conformidade de Ativos de Tecnologias da Informação e de Comunicações ao longo do mundo.*

1. Introdução

As sociedades modernas encontram-se cada vez mais dependentes de sistemas computacionais. Se, por um lado, o uso de computadores levou a um aumento da eficiência e da qualidade dos serviços oferecidos aos cidadãos, por outro lado, os impactos potenciais de eventuais falhas em tais computadores são cada vez maiores. Falhas nos sistemas

computacionais que controlam as infraestruturas críticas podem levar a verdadeiros colapsos. Por este motivo, governos, indústrias, e sociedades vêm trabalhando no sentido de estabelecer mecanismos que permitam garantir níveis mínimos de segurança a estes.

Dentre os mecanismos adotados, a acreditação de organismos e laboratórios é possivelmente a de maior relevância, pois reconhece a capacidade destes para a certificação de produtos, processos, serviços, sistemas de gestão e pessoal [Furtado and Laperri 2011].

A avaliação de ativos de TIC (Tecnologia da informação e comunicação) é uma tarefa desafiadora. De fato, o comportamento destes ativos é, potencialmente, complexo, uma vez que é determinado pelos softwares, componentes e hardwares que nele estão embarcados. Dessa forma, a realização de ensaios "ingênuos", que não considerem os detalhes de implementação do produto, pode inviabilizar a identificação de não-conformidades. Tal risco é particularmente realístico quando se considera a possibilidade de o próprio fabricante do produto intencionalmente ocultar uma funcionalidade espúria ou um comportamento impróprio. Como podemos verificar em [Hatton and Genuchten 2016] e [Barrett et al. 2017] sobre o caso do "defeat device" dos motores TDI da Volkswagen.

Além da Introdução, este trabalho está organizado da seguinte forma. Na seção 2, apresentamos a forma e a identificação dos riscos apurados. Na seção 3, realizamos a avaliação de controles dos estudos de casos em outros países. Na seção 4, são apresentadas nossas considerações finais.

A indústria de Tecnologia da Informação e Comunicação (TIC) precisa fornecer a proteção necessária para garantir a segurança de seus produtos e serviços, seja para empresas privadas ou órgãos governamentais. Um exemplo atual é o caso Edward Snowden, que gerou crise no governo Obama por ter sido acusado de espionagem, deixando vazadas informações sigilosas de segurança dos Estados Unidos, inclusive monitorando conversas da presidente Dilma Rousseff, na ocasião, o que comprova que os sistemas não são estáticos e sim dinâmicos [Pilati and Vieira Cancelier de Olivo 2014].

No Brasil, foi criado o Programa Nacional de Homologação de Equipamentos e Serviços de Tecnologia da Informação e Comunicação (PNCH-TIC), em atendimento ao disposto no decreto no 8.135, de 4 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autarquia, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional [Brasil 2013].

Segundo [da Defesa et al. 2015] a não-implementação de um programa de avaliação da conformidade direcionada na área de TIC podem ter consequências diversas: a) perda da soberania do país sobre as informações críticas para a segurança nacional; b) fragilidade nas relações diplomáticas, pois outros países podem acessar informações sigilosas do governo brasileiro; c) fragilidade das informações sensíveis quanto às riquezas e potencial de exploração de áreas estratégicas assim como relacionado ao planejamento de infraestruturas críticas; d) incapacidade de manter um esforço de defesa nacional caso o país esteja em estado de guerra; e) dependência tecnológica em áreas prioritárias para a segurança.

2. Identificação dos Riscos

Para essa etapa foi escolhido a técnica de Brainstorming, em sessões de trabalho que envolveram a participação de 9 profissionais de instituições públicas atuando nas áreas de

Avaliação da Conformidade ou de Tecnologia da Informação. A metodologia escolhida foi aplicada e dividida em categorias com base nos objetivos principais da Avaliação da Conformidade, que foram descritos como categorias de risco. Foram identificados 58 riscos divididos entre as nove categorias.

Para estimar a probabilidade e o impacto associado a cada um dos riscos identificados, seguimos uma abordagem qualitativa, na qual especialistas em Regulação e especialistas em Tecnologia da Informação foram entrevistados e atribuíram uma nota, numa escala de 1 a 5, para a probabilidade de ocorrência de cada risco e para o impacto, caso o risco se concretize. Cada entrevistado foi orientado a atribuir tais notas de acordo com sua percepção e experiências pessoais e, para cada risco, foi calculada a média de probabilidade e de impacto sobre todas as respostas. Neste primeiro estudo, foram realizadas 8 entrevistas, sendo que 5 dos entrevistados possuem ampla experiência em atividades de regulação e avaliação da conformidade – não-necessariamente envolvendo produtos de tecnologia da informação, enquanto outros 3 são profissionais com formação ou experiência em tecnologia da informação (aos quais foram apresentados conceitos básicos de regulação e avaliação da conformidade). O “valor de risco” foi calculado como o produto entre a probabilidade média e o impacto médio, e cada risco foi classificado como Risco Baixo se o valor de risco foi menor que 8, Risco Médio se o valor de risco foi de 8 a 12, e Risco Crítico se o valor de risco foi superior a 12, conforme a tabela 1.

Tabela 1: Riscos Identificados e sua classificação Fonte: Os autores

Código	Risco	Consequência Média	Probabilidade Média	Média
Definição clara dos métodos de ensaio – ME				
ME-1	Falta de clareza no requisito/Interpretação equivocada	3.625	3.375	12.23438
ME-2	Diferença nos resultados entre laboratórios	3.25	3	9.75
ME-3	Excesso de requisitos desnecessários	3.125	2.875	8.984375
ME-4	Custo dos ensaios	3.5	3.125	10.9375
ME-5	Requisito rigoroso demais	3.625	2.375	8.609375
ME-6	Requisito prescritivo demais	4.125	3.25	3.40625
ME-7	Interpretação errônea dos dados internos	4	2.125	8.5
ME-8	Controle de qualidade dos processos e equipamentos	3.75	1.875	7.03125
ME-9	Resultados não comparáveis	4	2.75	11
ME-10	Ausência de material de referência	3.125	3	9.375
ME-11	Requisito mal definido	3.875	2.625	10.17188
Quanto ao impacto no mercado – IM				
IM-1	Prejuízo total do mercado nacional	4.375	1.375	6.015625
IM-2	Prejuízo parcial do mercado nacional	3.5	2.125	7.4375
IM-3	Barreira técnica à importação	2.5	1.75	4.375
IM-4	Dificuldade de adequação à regulamentação	4	3	12
IM-5	Dificuldade de compreensão sobre a regulamentação	3.25	3.625	11.78125
IM-6	Desconhecimento do setor quanto à regulamentação	3.625	2.875	10.42188
IM-7	Formação de monopólios/oligopólios	3.375	2.375	8.015625
IM-8	Aumento da informalidade	3.875	2.875	11.14063
IM-9	Aumento do desemprego	3.375	2.5	8.4375
IM-10	Dificuldade de interação com o regulador/participação em Comissões	3.25	2.875	9.34375
IM-11	Atendimento de interesses de uma empresa/setor	3.75	2.875	10.78125
Quanto a custos aceitáveis – CA				
CA-1	Onerar o processo de regulamentação	3.5	4.375	15.3125
CA-2	Onerar o processo de produção	3.75	4	15
CA-3	Desequilíbrio entre organismos de Avaliação da Conformidade	3.125	2.875	8.984375
CA-4	Ausência de laboratórios	4	3	12
CA-5	Ausência de organismos	4.25	1.5	6.375
CA-6	Laboratórios apenas nas regiões S/SE	3.875	3.625	14.04688
CA-7	Organismos apenas nas regiões S/SE	3.375	3.75	12.65625
CA-8	Desinteresse de laboratório e organismos pelo escopo	3.625	2.875	10.42188
Quanto à disponibilidade de competência técnica – DCT				
DCT-1	Inadequação do regulamento	4.25	2.75	11.6875
DCT-2	Inviabilizar o processo produtivo	3.875	1.875	7.265625
DCT-3	Inviabilizar as avaliações por parte dos laboratórios	3.875	2	7.75
DCT-4	Inviabilizar as avaliações por parte dos OAC	3.375	1.875	6.328125
DCT-5	Perda da confidencialidade	3.75	2.25	8.4375
DCT-6	Perda de dados	3.75	2.75	10.3125
DCT-7	Gerar monopólio/oligopólio entre laboratórios	3.25	2.625	8.53125
Quanto a transparência e imparcialidade – QTI				
QTI-1	Comprometimento da propriedade intelectual	3.5	2.25	7.875
QTI-2	Falta de controle interno de acesso adequado	2.875	2.75	7.90625
QTI-3	Confidencialidade no processo de avaliação	4.125	2.375	9.796875
Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente – IPC				
IPC-1	Ineficácia do regulamento	4.5	2.375	10.6875
IPC-2	Produto não conforme no mercado	4.25	3.625	15.40625
IPC-3	Regulamento não compreendido pela sociedade	3.375	2.625	8.859375

IPC-4	Ausência de comunicação sobre a regulamentação	3.25	3.5	11.375
IPC-5	Crítica ao regulamento	2.875	3.5	10.0625
IPC-6	Índice de rejeição à regulamentação pela sociedade	3.75	2.75	10.3125
IPC-7	Comunicação ineficiente sobre a regulamentação	3.25	3.25	10.5625
IPC-8	Não acesso a um público especializado	2.25	2.375	5.34375
Propiciar concorrência justa entre laboratórios – PCJ				
PCJ-1	Inexistência de laboratório acreditado	3.75	3.25	12.1875
PCJ-2	Desequilíbrio entre laboratórios	3.31	2.937	9.73
PCJ-3	Gerar monopólio/oligopólio entre laboratórios	3.125	2.875	8.984375
PCJ-4	Gerar monopólio/oligopólio entre organismos	3.062	2.437	7.4648
Facilitar o comércio internacional – FCI				
FCI-1	Requisitos desalinhados com requisitos internacionais	3.5	2.625	9.1875
FCI-2	Requisitos obsoletos em relação a requisitos internacionais	3.625	2.625	9.515625
FCI-3	Custo da certificação	3.875	3.625	14.04688
Fortalecer o mercado interno – FMI				
FMI-1	Ineficácia do Regulamento em promover a melhoria no setor	4.25	2.625	11.15625

Da tabela 1 foram listados os riscos e valores identificados como críticos, sendo: I) ME-1 - Falta de clareza no requisito/Interpretação equivocada (12,4), II) ME-6 - Requisito prescritivo demais (15,2), III) CA-1 - Onerar o processo de regulamentação (15,4), IV) CA-2 - Onerar o processo de produção (15,8), V) CA-7 - Laboratórios apenas nas regiões S/SE (15,2), VI) CA-8 - Organismos apenas nas regiões S/SE (15,2), VII) IPC-2 - Produto não conforme no mercado (14,2), VIII) PCJ-1 - Inexistência de laboratório acreditado (12,4) e IX) FCI-3 - Custo da certificação (14,4).

3. Avaliação de controles

Uma característica da área em questão é a pouca disponibilidade de material acadêmico a respeito de questões relacionadas à regulação e à avaliação da conformidade. Dessa forma, todo o levantamento apresentado a seguir baseia-se na análise de documentos públicos e legislações encontrados em websites de governos. Dos governos pesquisados, foram escolhidos países como Austrália, China e Rússia, sendo a primeira pela suas características de extensão territorial e as demais pelo status de "emergente", conforme listado a seguir:

- **Austrália**- Na Austrália o órgão responsável pelo fornecimento de informações, assessoria de segurança de TIC para as agências governamentais federais e estaduais é a ASD (Australian Signals Directorate). Ela é 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 [Directorate 5 23].
- **China**- A China vem desde 1997 traduzindo o CC (Common Criteria), para a adoção de um programa de avaliação de conformidade de ativos de TIC. Já no ano de 2001 emite uma tradução da ISO (International Organization for Standardization)/ IEC(International Electrotechnical Commission) 15408:1999 a GB (Guobiao standards)/T 18336 (tecnologia da informação – segurança Parte 1-3), tendo também desenvolvido requisitos de segurança para cartões inteligentes. Como forma de integração ao padrão a China enviou delegações a vários ICCCs (International Common Criteria Conferences), e ainda promoveu a visita à diversas agências de avaliação de segurança, além do convite a diversos especialistas de outros países para a realização de treinamentos [Zhuohui Liu 5 07].
- **Rússia**- Segundo encontramos em [Barabanov and Markov 2015], a Rússia adota desde 1995 uma certificação semelhante ao Orange Book do DoD (Department of Defense) dos Estados Unidos, como metodologia de avaliação, já em 2002 adota o CC como metodologia de avaliação, traduzindo integralmente a norma. Inicialmente suas certificações utilizavam os TOEs (Target of Evaluation) já definidos

pelos outros países que já adotavam o CC. Em 2012 a Rússia cria e aprova seus próprios TOEs, aumentando sua capacidade de avaliação de vulnerabilidades e tendo com isto uma melhora em torno de 50%, isto conforme o FSTEC (Federal Service for Technical and Export Control).

3.1. Análise crítica dos Programas

A partir dos estudos de caso levantados, foi possível identificar uma série de estratégias de implantação de Programas de Avaliação da Conformidade (PAC) na área de TIC. Observou-se que tais programas se caracterizam por um conjunto de escolhas que, de certa forma, permitem tratar os diversos riscos identificados.

Padrões internacionais versus padrões locais- Um dos pontos-chave em relação à definição de um PAC diz respeito ao tipo de padrão que irá definir os requisitos a serem avaliados e os procedimentos de ensaios a serem seguidos. Observou-se desde Programas que referenciam diretamente padrões internacionais consolidados (tipicamente, ISO/IEC), passando por Programas que definem padrões locais baseados em padrões internacionais (mas que não referenciam diretamente tais padrões), até Programas totalmente baseados em padrões locais.

Uso de Organismo de Certificação de Produto conforme à ISO/IEC 17065- Outro aspecto que caracteriza as diversas estratégias para a implantação de PACs – incluindo aqueles na área de TIC – é a opção pelo uso de organismos de certificação aderentes à ISO/IEC 17065. Enquanto alguns Programas fazem uso de tais Organismos, mantendo o processo de avaliação da conformidade totalmente aderente às leis de Mercado, outros Programas fazem uso de organismos de governo como responsáveis pelo processo de “registro”, que caracteriza a aprovação de um ativo para uso em determinada aplicação.

Obrigatoriedade da Conformidade- A opção entre tornar a avaliação voluntária ou compulsória é outro aspecto importante dos diversos programas de avaliação da conformidade. A criação de Programas voluntários, frequentemente, é uma etapa preliminar à consolidação de tais programas. Em outros casos, opta-se pela criação de programas compulsórios desde o primeiro momento.

Processo Regulatório- As características do processo regulatório também são um importante fator de sucesso de PACs. Processos regulatórios com grande envolvimento do Mercado e da Sociedade tendem a ser mais bem-aceitos. No entanto, interesses de grupos e setores restritos podem levar o rumo de tais Programas a divergir, dificultando o atendimento aos objetivos iniciais e a interesses de Estado.

Vigilância do mercado- Uma vez implantado um PAC, é necessário definir o nível de vigilância do mercado. Altos níveis de vigilância tendem, naturalmente, a reduzir os riscos de produtos não-conforme no mercado – com a evidente consequência de custos.

Governança, papéis e responsabilidades- Uma importante característica observada nas diversas estratégias de implantação de PACs na área de TIC diz respeito à definição de papéis e responsabilidades, principalmente, que funções serão exercidas por organizações públicas e que funções serão exercidas por organizações.

4. Considerações finais

Inicialmente, observamos que os riscos ME-1, ME-6 e IPC-2 são riscos relacionados à qualidade técnica dos requisitos. Dessa forma, entendemos que tais riscos podem ser mitigados com a implantação de regulamentos baseados em padrões técnicos consolidados e reconhecidos internacionalmente, como podemos notar nos casos da China e Austrália.

Observe, ainda, que os requisitos CA-1, CA-2, CA-7, CA-8, PCJ-1 e FCI-3 são riscos relacionados aos custos do processo regulatório. O controle aplicável para mitigar tais riscos é o uso de padrões personalizados com encontrado na Rússia e na criptografia utilizada na Austrália, estes no entanto podem entrar conflito com o uso de padrões internacionais ou ainda elevar os custos das certificações.

Concluimos, que a avaliação sistemática dos riscos, associados a projetos de implantação de Programas de Avaliação da Conformidade na área de Tecnologia da Informação e Comunicações compõe uma referência e guia para que órgãos reguladores implantem PACs na área de TIC.

Referências

- Barabanov, A. and Markov, A. (2015). Modern trends in the regulatory framework of the information security compliance assessment in russia based on common criteria. *Proceedings of the 8th International Conference on Security of Information and Networks*, 44(4):30–33.
- Barrett, S. R. H., Speth, R. L., Eastham, S. D., Yim, S. H. L., Lee, G. L., Hwan, I., Jhun, I., Coull, B. A., Schwartz, J., Levy, J. I., Woo, M. K., Penn, S. L., Silva, R. A., West, J. J., Zhang, Y., Chossière, G. P., Malina, R., Ashok, A., Dedoussi, I. C., and Eastham, S. D. (2017). climate change public health impacts of excess no x emissions from volkswagen diesel passenger vehicles in germany. *Environmental Research Letters*.
- Brasil (2013). In *Presidência da República - Decreto nº 8135*.
- da Defesa, M., do Exército, C., (DCT), D. d. C. e. T., and (CDCiber), C. d. D. C. (2015). Estudo de Viabilidade Preliminar do SHCDCiber no Âmbito do Projeto ENaDCiber-SHCDCiber@DCDN.
- Directorate, A. A. S. (Acesso: 2018-05-23). *Australasian Information Security Evaluation Program*. <https://www.asd.gov.au/infosec/aisep/faq.htm#acafunctions>.
- Furtado, J. P. and Laperri, H. (2011). Avaliação da avaliação. desafios da avaliação de programas e serviços em saúde. *arXiv preprint arXiv:1304.3557*, pages 19–39.
- Hatton, L. and Genuchten, M. V. (2016). IEEE Software - When software crosses a line. *IEEE Software*.
- Pilati, J. I. and Vieira Cancelier de Olivo, M. (2014). Sequencia : Estudos jurídicos e políticos. *Universidade Federal de Santa Catarina (UFSC)*, 35(69):281–300.
- Zhuohui Liu, C. X. C. (Acesso: 2018-05-07). *Common Criteria in China*. <https://www.commoncriteriaportal.org/iccc/9iccc/pdf/A2311.pdf>.