CEFET/RJ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

UMA DISCUSSÃO SOBRE A PADRONIZAÇÃO BRASILEIRA PARA A AVALIAÇÃO DE RISCO EM AMBIENTES COMPUTACIONAIS

Carlos Roberto Gonçalves Viana Filho

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ, como parte dos requisitos necessários à obtenção do título de mestre.

Orientador(a): Felipe da Rocha Henriques
Coorientador(a): Raphael Carlos Santos Machado

Rio de Janeiro,
Dezembro 2019

UMA DISCUSSÃO SOBRE A PADRONIZAÇÃO BRASILEIRA PARA A AVALIAÇÃO DE RISCO EM AMBIENTES COMPUTACIONAIS

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ, como parte dos requisitos necessários à obtenção do título de mestre.

Carlos Roberto Gonçalves Viana Filho

Banca Examinadora:

Presidente, Professor D.Sc. Felipe da Rocha Henriques (CEFET/RJ) (Orientador(a))

Professor D.Sc. Raphael Carlos Santos Machado (UFF) (Coorientador(a))

Professor D.Sc. Diego Nunes Brandão (CEFET/RJ)

Professor D.Sc. Michel Pompeu Tcheou (UERJ)

Rio de Janeiro,

Dezembro 2019

Ficha catalográfica elaborada pela Biblioteca Central do CEFET/RJ

V614 Viana Filho, Carlos Roberto Gonçalves.
Uma discussão sobre a padronização brasileira para a avaliação de risco em ambientes computacionais / Carlos Roberto Gonçalves Viana Filho. – 2019.
82f. : il.color. , grafs. ; enc.

Dissertação (Mestrado). Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, 2019.
Bibliografia : f. 77-82.
Orientador : Felipe da Rocha Henriques.
Co-orientador: Raphael Carlos Santos Machado.

1. Redes de computadores – Medidas de segurança. 2. Proteção de dados. 3. Banco de dados. I. Henriques, Felipe da Rocha (Orient.). II. Machado Raphael Carlos Santos (Co-orient). III. Título.

CDD 005.8

Elaborada pelo bibliotecário Leandro Mota de Menezes CRB-7/5281

DEDICATÓRIA

Dedico este trabalho a minha esposa Izabella, a minha filha Roberta, sempre compreensivas, amáveis e pacientes. A Leonardo e Fabiane pelas sugestões e estímulo para iniciarmos esta jornada.

A minha mãe e meus irmãos Frederico e Vanilda pelo incentivo sempre constante.

Aos amigos Carlos Teles, Gabriel e Alexandre pelo apoio frequente.

A Sheila da secretaria do curso pela paciência para com todo os alunos.

Aos companheiros de curso, e a todos os professores do programa, agradeço as dicas, a cooperação e pelos conhecimentos passados.

O presente trabalho foi desenvolvido com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

Uma Discussão Sobre a Padronização Brasileira para a Avaliação de Risco em Ambientes Computacionais

As sociedades modernas encontram-se cada vez mais dependentes de sistemas computacionais, serviços e de toda sua infraestrutura. Portanto, erros, instabilidades e indisponibilidades destes, podem trazer grandes prejuízos materiais e financeiros para empresas, indústrias e governos em seus diversos níveis. Com o objetivo de garantir a segurança para os seus sistemas computacionais e minimizar os riscos inerentes a sua crescente utilização, as organizações têm trabalhado e investido na implantação de programas de avaliação da conformidade para ativos computacionais.

No Brasil, atualmente não existe uma legislação própria (ou padronização) que exija que os sistemas tenham um mínimo de requisitos de segurança e consequentemente que sua avaliação seja realizada e devidamente comprovada. Em muitos casos, padrões internacionais são usados por empresas Brasileiras para avaliação de conformidade. Porém, nem sempre esses padrões estão adequados ao cenário nacional.

Nota-se, seja pela falta de padronização e pela sua pouca maturidade em relação aos quesitos de segurança, que o país sofre com vários desafios para assegurar que seus ativos computacionais estejam devidamente protegidos contra os mais diversos tipos de ataques existentes.

Entretanto embora o estabelecimento de Programas de Avaliação de Conformidade para Tecnologia da Informação e Ativos de Comunicação seja considerado um grande desafio, podemos afirmar que a avaliação de alguns programas por meio de uma abordagem orientada para o risco, tem contribuído concretamente para a solução do problema supracitado.

A adoção de tal abordagem pressupõe a definição de um conjunto de requisitos que devem ser atendidos por um determinado produto e de uma série de ensaios que deverão ser executados sobre o mesmo, de modo a atestar o atendimento àqueles requisitos.

Neste trabalho, propomos uma discussão sobre a padronização para o cenário brasileiro para avaliação de riscos em ambientes computacionais. Uma metanálise é considerada para avaliar a proposta e, com base nos resultados obtidos, verificamos que a adaptação de padrões internacionais para o cenário brasileiro é uma boa alternativa para implantação em larga escala, o que pode levar à redução de custo e tempo para empresas.

Palavras-chave: Riscos; Avaliação da Conformidade; Segurança, Ativos Computacionais

ABSTRACT

A Discussion About Brazilian Standardization for Risk Assessment in Computional Environments

Modern societies are increasingly dependent on computer systems, services and all their infrastructure. Therefore, errors, instabilities and unavailability of these can cause major material and financial damage to companies, industries and governments at their various levels. In order to ensure security for their computing systems and minimize the risks inherent in their increasing use, organizations have worked and invested in implementing compliance assessment programs for computing assets.

In Brazil, there is currently no legislation of its own (or standardization) that requires systems to have a minimum of security requirements and consequently that their evaluation be performed and duly proven. In many cases, international standards are used by Brazilian companies for conformity assessment. However, these standards are not always appropriate to the national scenario.

It is noteworthy, due to the lack of standardization and its lack of security maturity, that the country faces several challenges to ensure that its computational assets are adequately protected against the most diverse types of attacks.

However, although the establishment of Information Technology and Communication Asset Compliance Assessment Programs is considered a major challenge, we can state that the evaluation of some programs through a risk-oriented approach has contributed concretely to solving the problem. above.

The adoption of such an approach presupposes the definition of a set of requirements that must be met by a given product and a series of tests that must be performed on it, in order to attest the fulfillment of those requirements.

In this paper, we propose a discussion about the standardization for the Brazilian scenario for risk assessment in computational environments. A meta-analysis is considered to evaluate the proposal and, based on the results obtained, we find that adapting international standards to the Brazilian scenario is a good alternative for large scale implementation, which can lead to cost and time reduction for companies.

Keywords: Risks; Conformity Assessment; Security, Computational Assets

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira De Normas Técnicas
AC	Autoridades Certificadoras
ATEX	*Atmospheres Explosibles*
CC	*Common Criteria*
CCEVS	*Common Criteria Evaluation and Validation Scheme*
CCRA	*Common Criteria Recognition Arrangement*
CMVP	*Cryptographic Module Validation Program*
CONMETRO	Conselho Nacional De Metrologia, Normalização E Qualidade Industrial
CPL	*Certified Products List*
CSE	*Communications Security Establishment*
CTCPEC	*Canadian Trusted Computer Product Evaluation Criteria*
DNS	*Domain Name System*
EAL	*Evaluation Assurance Level*
EMC	*Electromagnetic Compatibility*
FC	*Federal Criteria*
FIPS	*Federal Information Processing Standards*
IBGC	Instituto Brasileiro De Governança Corporativa
ICP-BRASIL	Infraestrutura De Chaves Públicas Brasileira
IEC	*International Electrotechnical Commission*
INMETRO	Instituto Nacional De Metrologia, Qualidade E Tecnologia
IOT	*Internet of Things*
ISO	*International Organization for Standardization*
ITI	Instituto Nacional De Tecnologia Da Informação
ITSEC	*Information Technology Security Evaluation Criteria*
NBR	Norma Brasileira
NIAP	*National Information Assurance Partnership*
NIST	*National Institute of Standards and Technology*
OMC	Organização Mundial Do Comércio
OTAN	Organização Do Tratado Do Atlântico Norte

PAC	Programas De Avaliação Da Conformidade
PBAC	Programa Brasileiro De Avaliação Da Conformidade
PNCH-TIC	Programa Nacional De Homologação De Equipamentos E Serviços De Tecnologia Da Informação E Comunicação
PP	*Protection Profile*
SBAC	Sistema Brasileiro De Avaliação Da Conformidade
SBC	Sistema Brasileiro De Certificação
SCADA	*Supervisory Control and Data Acquisition*
SHCDCIBER	Sistema De Homologação E Certificação De Produtos De Defesa Cibernética
SINMETRO	Sistema Nacional De Metrologia, Normalização E Qualidade Industrial
ST	*Security Target*
TCSEC	*Trusted Computer Systems Evaluation Criteria*
TDI	*Turbocharged Direct Injection*
TI	Tecnologia Da Informação
TIC	Tecnologia Da Informação E Comunicação
TOE	*Target of Evaluation*
ZVEI	*Zentralverband Elektrotechnik- und Elektronikindustrie*

SUMÁRIO

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.

Notadamente, podemos verificar que a Tecnologia da Informação (TI) está presente no dia a dia das empresas, dos negócios, nas interconexões, na computação na nuvem, na Internet das Coisas e nos mais diversos tipos de dispositivos interconectados [Barafort et al., 2017]. Em tempos de globalização, uma grande quantidade de informações é gerada diariamente, e as empresas, para terem um maior êxito na disputa de seus mercados, dependem cada vez mais dessas informações, e por esta razão, essas precisam ser corretamente administradas e protegidas [Zanon, 2016]. Essa realidade nos mostra um dos grandes problemas existentes em diversos tipos de empresas, pois ativos vulneráveis podem produzir danos lógicos, físicos e financeiros, sendo estes, por vezes, irreparáveis a governos e empresas. Falhas nos sistemas computacionais que controlam as infraestruturas críticas podem levá-las a verdadeiros colapsos de segurança, podendo causar danos operacionais, financeiros ou ainda perda de informações, sejam estas sigilosas ou não.

Portanto, vulnerabilidades de sistemas, hardwares ou ainda de infraestruturas críticas, podem trazer à tona a exposição de diversos problemas, e suas graves consequências, por suas interdependências [Wang et al., 2016], conforme podemos verificar na Figura 1, referente ao levantamento de interconexão da infraestrutura, avaliada no evento do furacão Katrina.

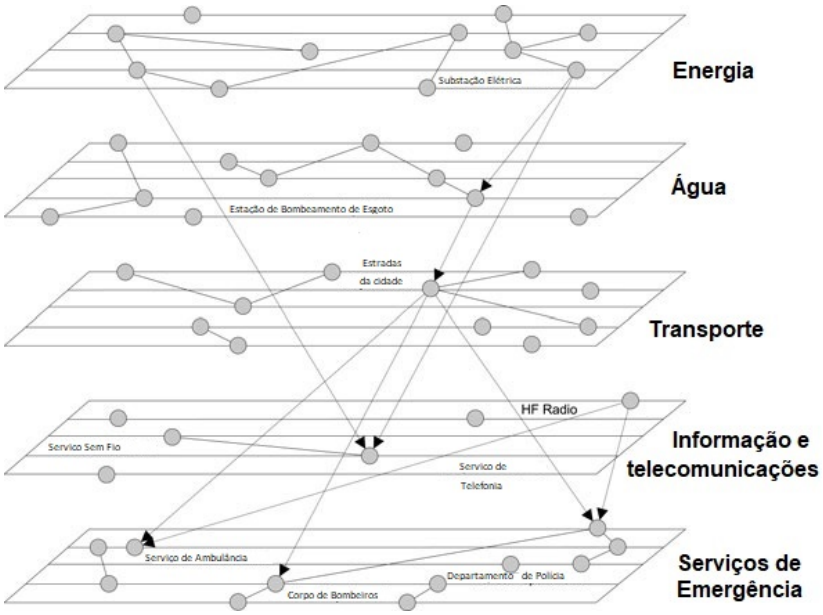


Figura 1 – Interdependências de infraestrutura, ilustradas para o evento do furacão Katrina. Fonte: Kröger, Wolfgang and Zio, Enrico [2011]

Conforme descrito em [Kröger, Wolfgang and Zio, Enrico, 2011], vulnerabilidade pode ser definida como falha ou fraqueza na concepção, implementação, operação e/ou gestão de um sistema, ou ainda de elementos que possam tornar passível a inoperância total ou parcial quando este é apresentado a um perigo ou ameaça.

Por este motivo, governos, universidades, setores privados e institutos de pesquisa vêm trabalhando no sentido de estabelecer mecanismos que permitam garantir níveis mínimos de segurança aos sistemas computacionais dos quais tanto dependem [Gabinete de Segurança Institucional, Presidência da República, 2015].

1.1- Motivação

Conforme podemos constatar em [Machado et al., 2018]; ”A avaliação de ativos de Tecnologia da Informação e Comunicação (TIC) é uma tarefa desafiadora. De fato, o comportamento de tais produtos é potencialmente complexo, uma vez que é determinado pelo software nele embarcado, ou ainda por funções existentes em seu hardware. 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 realista quando se considera a possibilidade de o próprio fabricante do produto intencionalmente ocultar uma funcionalidade espúria ou um comportamento impróprio. ”

Especialmente, sistemas críticos tornam-se cada vez mais expostos a problemas de segurança, sejam estes realizados de modo proposital ou não. Dessa forma, é vital que o desenvolvimento de sistemas críticos tenha fortes requisitos de qualidade de segurança [Mellado et al., 2007]. Assim sendo, ter um sistema de homologação e certificação de produtos e serviços de defesa cibernética, considerando o atual nível de desenvolvimento científico e tecnológico de nossa sociedade, torna-se extremamente necessário [César et al., 2014].

Na história da avaliação da conformidade, encontramos uma série de exemplos de manobras para ocultar funcionalidade espúrias, sendo talvez o mais emblemático o caso dos carros da Volkswagen com motor a diesel *Turbocharged Direct Injection* (TDI). O caso do motor TDI da Volkswagen tornou-se notório pois um sofisticado mecanismo conhecido na literatura como “defeat device" [Hatton and Genuchten, 2016] foi inserido pelo próprio fabricante no software embarcado nos automóveis, sendo capaz de identificar cenários de ensaio e mudar parâmetros de operação do motor, aparentando menores índices de emissão de gases NO_x (Óxido de nitrogênio) [Barrett et al., 2017]. Outras violações, relacionadas a emissões excessivas de gases foram encontradas em carros da Hyundai e da Kia, além dos dispositivos de controle de emissão defeituosos encontrados nos veículos da Mercedes Benz [Barrett et al., 2015].

Quando tratamos de infraestruturas críticas, podemos encontrar relatos de diversos tipos de ataques, principalmente a sistema do tipo *Supervisory Control and Data Acquisition* (SCADA), pois cada vez mais essas redes estão conectadas à Internet e às redes corporativas. A exposição de tais infraestruturas torna os sistemas compostos por elas mais suscetíveis a ataques externos daqueles que desejam interromper os seus serviços [Miller and Rowe, 2012]. A Tabela 1 apresenta uma análise cronológica das falhas das infraestruturas críticas, de acordo com [Miller and Rowe, 2012].

Tabela 1 – Sumário de incidentes. Fonte: Adaptado de Miller and Rowe [2012]

Ano	Descrição	Método
1982	Explosão do Oleoduto Siberiano	Trojan
1992	Sistema de Alerta de Emergência Chevron	Uso indevido de recursos, Comprometimento da conta do usuário
1994	Projeto de Salt River	Senha root comprometida, Trojan
1997	Aeroporto de Worcester	Senha de root comprometida, Negação de serviço
1999	Gazprom	Comprometimento da conta do usuário, Trojan
1999	Gasoduto de Bellingham	Uso indevido de recursos
2000	Sistema de Água Maroochy	Uso indevido de recursos, Comprometimento da conta do usuário,
2001	Operador de sistemas da Califórnia	Senha de root comprometida,
2003	Usina Nuclear de Davis-Besse	Worm
2003	empresa de transportes CSX	Vírus
2007	Autoridade do Canal Tehama Colusa	Uso indevido de recursos
2010	Programa nuclear Iraniano	Worm, Senha de root comprometida, Trojan
2011	Empresas e energia e petróleo	Engenharia social, Comprometimento da conta do usuário, Senha de root comprometida
2011	Sistemas de Controle Industrial	Vírus

Também podemos verificar no relatório da [Symantec Corporation, 2018] que temos um aumento de 13% das vulnerabilidades reportadas; e ainda um incremento de

29% das vulnerabilidades relacionadas aos sistemas de controle industrial. Já na esfera da *Internet of Things* (IoT), temos um aumento de 600% de ataques em 2017, sendo estes partindo principalmente dos Estados Unidos e da China conforme a Figura 2.

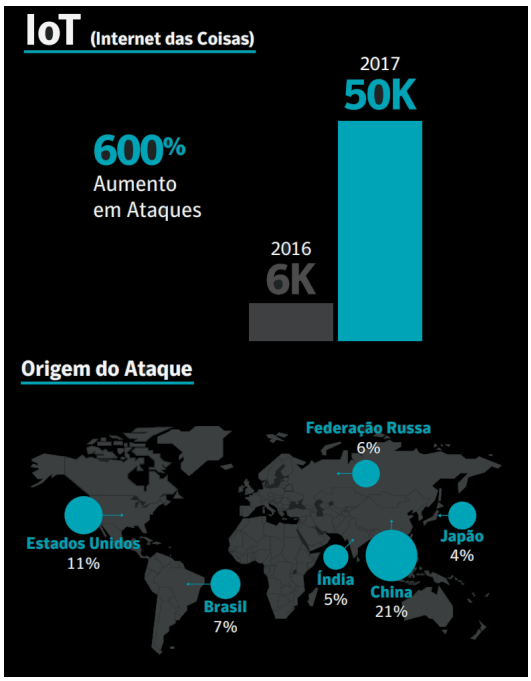


Figura 2 – Origem de ataques Fonte: Symantec Corporation [2018]

Na Tabela 2, são apresentados os 10 países de onde se originaram os maiores ataques a dispositivos IoT. Esta Tabela apresenta casos como os dos ataques ao provedor de *Domain Name System* (DNS) *Dyn* em 2016, foi desencadeado contra este provedor por vários tipos de dispositivos como câmeras de segurança IP, câmeras e impressora dentre tantos dispositivos da IoT [Trend Micro, 2019; Symantec Corporation, 2018].

Tabela 2 – Ataques a IoT 2017. Fonte: Symantec Corporation [2018]

Ordem	País	Percentual
1	China	21,00%
2	Estados Unidos	10,60%
3	Brasil	6,90%
4	Federação Russa	6,40%
5	Índia	5,40%
6	Japão	4,10%
7	Turquia	4,10%
8	Argentina	3,70%
9	Coreia do Sul	3,60%
10	México	3,50%

A partir destas ameaças, nota-se que vários países passaram a buscar e tentar

determinar requisitos de segurança cibernética para a realização de contratos públicos em TIC. Um exemplo pode ser encontrado na Hungria onde fabricantes de equipamentos e provedores são encorajados a criar um alto nível de segurança cibernética, tendo como destaque a sua conformidade com padrões internacionais de certificação [Government of Hungary, 2013].

Nos Estados Unidos, podemos notar que estão sendo desenvolvidos padrões para que a indústria possa aumentar a segurança em infraestrutura crítica, além do compartilhamento de informações sobre ocorrências de incidentes, para a melhoria nas respostas dos mesmos. Isto, além da criação de padrões para o setor público e em legislações para setores específicos [Häger and Dackö, 2017].

Na União Europeia, com o estabelecimento de cooperações entre seus membros, pretende-se alcançar um elevado nível de segurança de redes e sistemas, entre todos os setores considerados essenciais para os países membros. Os requisitos de segurança empregados também estão presentes em diversas outras leis que fazem parte de setores específicos, como telecomunicações [Häger and Dackö, 2017].

Na Alemanha, os requisitos de segurança vão além dos exigidos pela comunidade Europeia, tendo as mesmas leis nacionais que reforçam a segurança da infraestrutura crítica de TIC, e vão além com a proteção dos usuários da Internet [Häger and Dackö, 2017].

A França também tem sua legislação além da solicitada pela comunidade Europeia, sendo seus operadores de infraestruturas críticas obrigados, através da lei, a proteger seus sistemas de informação. Além disso, ainda é proibido o fornecimento de alguns tipos de equipamentos para a interceptação de comunicação, a exportação de software e hardware de segurança da informação, incluindo encriptação, salvo se as mesmas forem expressamente autorizadas [Häger and Dackö, 2017].

Já a Austrália, com iniciativas bem próximas dos Estados Unidos e da União Europeia, reforça a segurança em infraestrutura crítica, na área financeira e na privacidade de dados. Esta diferencia-se das demais por não conter iniciativas através da criação de leis específicas, mas sim através de normas, diretrizes e recomendações [Häger and Dackö, 2017].

No Brasil, o Governo passou também a adotar medidas nesta esfera, com o estudo de viabilidade da implantação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDciber), que tem como principal justificativa a

redução da dependência tecnológica do país, principalmente de sistemas militares e de ativos considerados críticos para a nação. Este fato deve-se a verificação de que o Brasil pode vir a perder sua soberania caso não consiga nacionalizar seus sistemas de comando, controle e comunicação da informação para a defesa nacional [Barbalho et al., 2018].

Ligado diretamente ao Ministério da Defesa, e ainda que indiretamente ao Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (SINMETRO), o SHCDciber tem por objetivo trazer uma maior garantia para o setor de defesa cibernética do país. Assim, produtos e serviços desenvolvidos, fornecidos, adquiridos, integrados, implantados e ofertados passam a ter uma segurança cibernética adequada às suas necessidades estratégicas, táticas e operacionais da defesa cibernética do país [Ministério da Defesa do Exército, 2015].

Assim, podemos verificar que o SHCDciber é um sistema integrado que visa o provimento de serviços de homologação e certificação de produtos e serviços a serem utilizados em defesa cibernética. Outrossim, pode-se definir o SHCDciber como um sistema que tem uma arquitetura que garante uma junção entre diversos atores do Governo Federal, incluindo ministérios civil e militares [César et al., 2014]. Segundo Ministério da Defesa do Exército [2015], ele pode ser definido como um ”Sistema de Metrologia, Normalização e Qualidade Industrial em Segurança Cibernética, para fins de Defesa Cibernética do Brasil”.

1.2- Objetivos e Contribuições

No Brasil, com a homologação da nova lei brasileira de proteção de dados (LGPD) [Presidência da República - Casa Civil, 2018], a segurança passa a ser item crucial no desenvolvimento e sustentação de sistemas, devendo fazer parte dos requisitos iniciais dos mesmos. Assim, a validação desses requisitos para atestar a sua conformidade com o solicitado, passa a ter grande importância em todo o ciclo de vida dos sistemas. Entretanto, atualmente não existe uma legislação própria no Brasil (ou padronização) que exija que os sistemas tenham um mínimo de requisitos de segurança e consequentemente que sua avaliação seja realizada e devidamente comprovada. Em

muitos casos, padrões internacionais são usados por empresas Brasileiras para avaliação de conformidade. No entanto, nem sempre esses padrões estão adequados ao cenário nacional.

Deste modo, neste trabalho propomos uma discussão sobre a padronização brasileira para a avaliação de conformidade em ambientes computacionais fundamentado na análise de risco. Um questionário foi proposto, baseado nos principais riscos encontrados na literatura, e aplicado em empesas de tecnologia, públicas e privadas. Uma meta–análise foi realizada, e os resultados obtidos indicam que a adaptação de padrões interacionais para o cenário brasileiro é uma alternativa factível, levando a redução de custos e tempo por parte das empresas no processo de implantação de um padrão nacional.

1.3- Estrutura da Dissertação

Este trabalho está organizado da seguinte maneira: além da introdução que encontramos no primeiro capítulo, pode-se verificar toda a fundamentação teórica para avaliação da segurança e de conformidade no segundo capítulo.

No terceiro capítulo, verificamos padrões de avaliação da conformidade, como o *Common Criteria* e seus elementos, verificamos os perfis de proteção colaborativos e os produtos avaliados pela norma. Verificamos, além disso, o padrão *FIPS 140-2* e sua aplicação em outros países e no Brasil. Após isso passamos a verificar o cenário brasileiro e os mecanismos de avaliação da conformidade.

No quarto capítulo passamos a verificar a avaliação de conformidade baseada no risco, pesquisando a gestão de riscos e a seleção e identificação dos riscos.

Já a metodologia utilizada para a proposta encontra-se no quinto capítulo, com a relação entre controle e riscos, além do questionário formulado, baseado na análise de risco.

No sexto capítulo, encontramos os resultados obtidos pela pesquisa, em relação ao questionário definido, quanto: a definição clara dos métodos; ao impacto no mercado; ao fortalecimento do mercado interno; a informações de proteção ao consumidor; a disponibilidade de competência técnica; aos custos adicionais; a facilitação do comércio

internacional; a propiciação de concorrência justa, além de proposição de uma proposta do padrão brasileiro.

Já no sétimo capítulo, encontramos as considerações finais deste trabalho.

2- Fundamentação Teórica para a Avaliação de Segurança e de Conformidade

2.1- Avaliação de Segurança

Uma das ferramentas que vem ganhando força, nos últimos anos, como abordagem para avaliação de segurança, é a da certificação. Ela consiste na atestação do atendimento a um conjunto de requisitos, tipicamente, a partir da realização de um conjunto de ensaios por uma terceira parte confiável [Reis Da Costa and De Barros, 2012]. Na prática, tal estratégia pressupõe a definição de um conjunto de requisitos que devem ser atendidos por um produto e de uma série de ensaios que deverão ser executados sobre tal produto de modo a atestar o atendimento àqueles requisitos. Idealmente, os documentos que descrevem tais requisitos e ensaios são normas expedidas por organismos internacionais de padronização tais como *International Organization for Standardization* (ISO) e *International Electrotechnical Commission* (IEC), levando a práticas harmonizadas e reconhecidas no mundo todo.

Atualmente podemos encontrar diversos tipos de legislações sobre cibersegurança, e estas podem impor: requisitos as autoridades públicas e operadores privados através do direito interno, com o intuito de proteger infraestruturas críticas ou ainda serviços considerados essenciais; requisitos que abrangem a segurança nacional tentando evitar espionagem, podendo restringir investidores estrangeiros a adquirirem empresas nacionais, sua participação em licitações que envolvam infraestrutura críticas ou ainda a restrição de exportações/fornecimento de tecnologias que envolvam segurança críticas; ou ainda leis que criminalizem cibercrimes, ações como roubo ou furto, pirataria ou ainda interceptação de dados [Häger and Dackö, 2017].

Podemos notar então que segurança não é um desafio apenas das empresas privadas, é um desafio dos governos. Mediante tamanho desafio, a TIC precisa fornecer a proteção necessária para garantir a segurança de seus produtos e serviços. Sabemos que a proteção não é inviolável, um exemplo atual é o caso Edward Snowden [Pilati and

Vieira Cancelier de Olivo, 2014], que gerou crise no governo Obama por ter sido acusado de espionagem, deixando vazar informações sigilosas de segurança dos Estados Unidos, inclusive monitorando conversas da presidente brasileira Dilma Rousseff, na ocasião. Isso comprova que os sistemas não são estáticos, mas sim dinâmicos, necessitando da intervenção humana.

No Brasil, com o intuito de aumentar a segurança necessária para o país, 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 [Presidência da República, 2013].

Segundo o documento do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDciber), a não implementação de um programa de avaliação da conformidade direcionada na área de TIC pode ter consequências diversas, tais como:

1. Perda da soberania do país sobre as informações críticas para a segurança nacional;
2. Fragilidade nas relações diplomáticas, pois outros países podem acessar informações sigilosas do governo brasileiro;
3. Fragilidade das informações sensíveis quanto às riquezas e potencial de exploração de áreas estratégicas, assim como relacionadas à infraestruturas críticas;
4. Incapacidade de manter um esforço de defesa nacional, caso o país esteja em estado de guerra;
5. Dependência tecnológica em áreas prioritárias para a segurança.

Dessa forma, não há dúvida sobre a importância estratégica para qualquer país da atividade regulatória na área da tecnologia da informação e comunicação. Para tal, a utilização de padrões internacionalmente reconhecidos como o *Common Criteria* (CC) também reconhecido como (ISO/ IEC 15408), traz grandes avanços na área de segurança para diversos produtos computacionais no âmbito nacional. Neste trabalho, de modo a melhorar o desempenho de segurança em nível nacional, além de reduzir o custo da implantação de sistemas de avaliação de conformidade, propomos um padrão brasileiro de avaliação de conformidade de sistemas e ambientes computacionais.

2.2- Avaliação de Conformidade

Conceitualmente, a Avaliação da Conformidade é um processo sistematizado, acompanhado e avaliado de forma a proporcionar adequado grau de confiança de que um produto, processo, serviço, ou um profissional, atende a requisitos pré-estabelecidos em normas e regulamentos técnicos [ISO/CASCO, 2019]. Dessa forma, ela torna-se imprescindível para as relações de comércio internacionais, visto que os países têm que procurar cada vez mais sua autossuficiência tecnológica e industrial, além de terem que desenvolver níveis de qualidade e competitividade como um instrumento estratégico para seu desenvolvimento [ISO/CASCO, 2019].

Nos Programas de Avaliação da Conformidade (PAC), encontramos ferramentas que permitem a execução dos regulamentos estabelecidos, facilitando a fiscalização. No caso do Brasil, o Sistema Brasileiro de Avaliação da Conformidade orienta o esforço na formulação do Programa Brasileiro de Avaliação da Conformidade (PBAC), que tem como propósito a promoção à longo prazo para a gestão estratégica da atividade de Avaliação da Conformidade pelas Autoridades Certificadoras (AC) [Inmetro, 2018f].

Essa avaliação tem como objetivo principal, e também fundamental, atender às preocupações sociais, transmitindo ao consumidor a confiança de que o produto, processo ou serviço está em conformidade com os requisitos especificados, ao mesmo tempo em que não se torne um ônus para o fabricante [ISO/CASCO, 2019]. Isso se dá já que, notadamente consumidores, empresas e autoridades públicas têm determinadas expectativas quanto à qualidade, segurança, confiabilidade, interoperabilidade, eficiência, eficácia e ainda quanto a sustentabilidade ambiental de produtos e serviços oferecidos pelos fornecedores [Locke, 2001].

Notamos portanto, que a avaliação da conformidade, baseia sua sustentação em uma abordagem funcional, consistindo em quatro funções principais: seleção, avaliação, revisão e inspeção, como podemos notar na Figura 3.

Figura 3 – Abordagem funcional da avaliação de conformidade. Fonte: ISO/CASCO [2019]

A avaliação da conformidade (AC) fornece os meios que podem assegurar que todas essas características prometidas foram cumpridas, podendo com isso afirmar que atendem a normas, especificações e regulamentos, ou que quaisquer outras especificações relevantes para o produto foram utilizados para o seu ensaio [Locke, 2001].

Existem diversos aspectos que justificam a implantação de programas de avaliação da conformidade, sendo estes: propiciar a concorrência justa; estímulo a melhoria contínua da qualidade; informação e proteção ao consumidor; facilitação do comércio exterior (incremento das exportações); proteção ao mercado interno e agregação de valor às marcas [Associação Brasileira de Avaliação da Conformidade, 2018].

No Sistema Brasileiro de Avaliação da conformidade (SBAC), notamos diversas ferramentas para a verificação da conformidade de um produto, processo ou serviço em relação a critérios, normas e regulamentos técnicos estabelecidos no Brasil [ISO/CASCO, 2019]. Segundo Inmetro [2018e] os mecanismos que são efetuados no SBAC são: a certificação, a declaração da conformidade do fornecedor e a inspeção, a serem explicitados a seguir.

- Certificação de Produtos

  Por definição a certificação de produtos, processos, serviços e sistemas de gestão e pessoal é realizada por uma terceira parte, ou seja, uma entidade independente que seja acreditada pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) para que possa efetuar a avaliação da conformidade. Uma entidade que seja acreditada pelo INMETRO é reconhecida por este instituto como competente

para a realização da avaliação de um objeto [Inmetro, 2018a].

- Declaração da Conformidade do Fornecedor
  É um processo de avaliação da conformidade de primeira parte, ou seja, é o processo ao qual o fornecedor do produto, sob circunstâncias previamente estabelecidas dá a garantia de que o produto, processo ou serviço está em conformidade com os requisitos estabelecidos [Inmetro, 2018b].

- Inspeção
  Conforme apresentado em [Inmetro, 2018d], a inspeção pode ser definida como "Avaliação da Conformidade pela observação e julgamento, acompanhada, conforme apropriado, por medições, ensaios ou uso de calibres." Este é um mecanismo bastante utilizado para a avaliação de serviços após a sua execução.

Um dos mecanismos que vem ganhando força, nos últimos anos, como abordagem para avaliação de segurança, é o da certificação. A certificação consiste na atestação do atendimento a um conjunto de requisitos, tipicamente, a partir da realização de um conjunto de ensaios por uma terceira parte [César et al., 2014]. Na prática, tal estratégia pressupõe a definição de um conjunto de requisitos que devem ser atendidos por um produto e de uma série de ensaios que deverão ser executados sobre tal produto de modo a atestar o atendimento àqueles requisitos. Idealmente, os documentos que descrevem tais requisitos e ensaios são normas expedidas por organismos internacionais de padronização, levando a práticas harmonizadas e reconhecidas no mundo todo [Locke, 2001].

Além disso, uma área que vem ganhando cada vez mais importância nos últimos tempos, e para a qual vem se mostrando importante definir requisitos mínimos que sejam avaliados por meio de Programas de Avaliação da Conformidade (PAC), é a da segurança Cibernética, pois as falhas nos sistemas computacionais que controlam as infraestruturas críticas podem levar a verdadeiros colapsos [Barbalho et al., 2018]. Este fato tem levado governos, indústrias, e sociedades a trabalhar no sentido de estabelecerem mecanismos que permitam garantir níveis mínimos de segurança aos sistemas computacionais dos quais tanto dependem.

Técnicas de avaliação da conformidade geram evidências que devem comprovar o cumprimento de requisitos, e estes requisitos podem ser solicitados sobre produtos, processos, serviço, sistemas de gestão, pessoa ou organização. Considera-se que

existem três partes da reivindicação de qualidade, conforme a [ISO/CASCO, 2019]:

1. Primeira Parte (Declaração de conformidade do fornecedor) - Vários produtos têm declarações de conformidade, sejam estes advindos de fornecedores ou dos próprios fabricantes. Estas podem ser simplesmente baseadas em evidências, que são associadas ao produto ou em avaliações de conformidade, de acordo com as normas ISO/IEC 17050-1:2004 e ISO/IEC 17050-2:2004.

   Encontramos as normas dos requisitos de conformidade de um fornecedor nas ISO/IEC 17050-1:2004 e ISO/IEC 17050-2:2004, sendo que o objeto desta declaração pode ser um produto, sistema de gestão, pessoa ou organização de acordo com os seguintes requisitos:

   - baseados em resultados de avaliação da qualidade;
   - informações da declaração, tendo estas: identificação única, nome e localização do emissor, identificação do produto/serviço/processo, declaração de conformidade, dados do local da emissão, assinatura abalizada, limitações existentes e lista dos requisitos e normas;
   - garantia da conformidade com normativas atuais;
   - arquivos técnicos para as declarações realizadas, contendo: descrição do produto/processo/serviço, documentação, resultados da avaliação (métodos de auditoria, procedimentos, testes, tipos de testes, métodos de testes, avaliação e identificação).

2. Segunda Parte (Reivindicações de conformidade) - Compradores, fornecedores ou qualquer um que tenha interesse no objeto pode reivindicar a sua conformidade. Neste caso, o comprador realiza a avaliação de conformidade, verificando se o objeto atende aos requisitos. Não existe nenhuma norma ISO ou IEC específicas para a avaliação da conformidade de segunda parte, e várias técnicas podem ser combinadas para a reivindicação;

3. Terceira Parte (Reivindicações de conformidade de terceiros) - Realizadas por instituições independentes (laboratórios, órgãos de inspeção ou organismos de certificação) das empresas ou pessoas que estão fornecendo o objeto da avaliação, presentes nas seguintes normas:

- ISO/IEC 17067:2013 - Avaliação da conformidade - Fundamentos para certificação de produtos e diretrizes de esquemas para certificação de produtos;
- ISO/IEC 28:2004 - Avaliação da conformidade - Diretrizes sobre o sistema de certificação de produtos por terceira parte;
- ISO/IEC 53:2005 - Avaliação da conformidade - Orientação sobre o uso de sistema de gestão da qualidade de uma organização na certificação de produto;
- ISO/IEC 17021:2016 - Avaliação da conformidade - Requisitos para organismos que fornecem auditoria e certificação de sistemas de gestão - Parte 1: Requisitos;
- ISO/IEC 17024:2012 - Avaliação de Conformidade - Requisitos Gerais para Organismos de Certificação que Executam Certificação de Pessoas;
- ISO/IEC 17065:2012 - Avaliação da conformidade — Requisitos para organismos de certificação de produtos, processos e serviços.

Para a avaliação de conformidade da terceira parte, temos:

(a) esquemas de certificação de produtos:

- ISO/IEC 17067:2013, onde encontramos os fundamentos, além das diretrizes para a certificação de produtos, processos e serviços;
- ISO/IEC 28:2004, um guia que contém orientações para a terceira parte, com as condições necessárias para a conformidade de um produto, por meio de ensaios, amostras e supervisão dos ensaios de amostras de produtos.
- ISO/IEC 53:2005, um guia em que os organismos de certificação podem utilizar esquemas de certificação, com a utilização de sistemas de gestão da qualidade de uma empresa, não substituindo os requisitos da ISO/IEC 65 [ISO/CASCO, 2019].

(b) Requisitos de certificação:

- ISO/IEC 17021:2016, que envolve os princípios de imparcialidade dos organismos que oferecem certificações e auditorias, requisitos para a competência, além da coerência e imparcialidade na auditoria;
- ISO/IEC 17024:2012, que contém os requisitos e princípios para organismos que certificam pessoas em suas determinadas especificidades e o

seu esquema de certificação;

- ISO/IEC 17065:2012, que compreende os organismos de certificação e seus requisitos para competência necessária, sua operação e além de sua imparcialidade, isto para a certificação de produtos, processos e serviços [ISO/CASCO, 2019].

Os conceitos descritos acima consideram basicamente os mesmos aspectos: confiança, atendimento a requisitos e custos, que embora sejam escritos de forma diferente, compõem um conjunto de macroprocessos interligados para atender a sociedade, que necessita de acesso a serviços confiáveis de avaliação da conformidade.

3- Padrões de Avaliação de Conformidade

3.1- Common Criteria

O desenvolvimento de produtos de TIC que possam atender a requisitos de segurança, atualmente é uma das maiores preocupações para seus desenvolvedores e consumidores. Assim, para que estes produtos possam garantir o nível de segurança desejado, é necessário que se sigam alguns padrões no seu desenvolvimento. O *Common Criteria* (CC) é formado para atingir este objetivo. Dessa forma, a segurança passa a ser uma preocupação do projeto do produto a ser seguida desde o início e sendo uma prioridade [Razzazi et al., 2006].

Ainda segundo Razzazi et al. [2006], o CC é resultado de diversos padrões de diferentes países. De forma cronológica, podemos ver sua formação da seguinte forma:

- 1985 - Surgimento nos Estados Unidos dos primeiros critérios de avaliação, sendo estes chamados de *Trusted Computer Systems Evaluation Criteria* (TCSEC);
- 1991 - Reino Unido, a Alemanha, a França e a Holanda formam um padrão chamado *Information Technology Security Evaluation Criteria* (ITSEC);
- 1993 - É criado o padrão Canadense, o *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC);
- 1993 - Os Estados Unidos, conjuntamente com o Canadá, estabelecem o *Federal Criteria* (FC);
- 1993 - A Comissão Europeia funde o ITSEC com o FC, introduzindo o CC pela primeira vez.

O manual do *Common Criteria* (CC), em sua primeira parte, fornece um conjunto de requisitos para funcionalidades de segurança de produto de TI e de medidas aplicadas a esses produtos durante a avaliação de segurança, podendo ser referentes a hardware, *firmware* ou *software*. Este processo de avaliação estabelece que os requisitos atendam à

um nível de confiabilidade para determinadas funcionalidades de segurança dos produtos, e que as medidas de garantia aplicadas aos produtos atendam a esses requisitos [Mellado et al., 2007].

O CC tem um comportamento em níveis na avaliação de produtos de segurança de TIC. Esta avaliação é formada por níveis de segurança, *Evaluation Assurance Level* (EAL), atestados pelo desenvolvedor. Esses níveis (EAL) são escalas predefinidas para a garantia de um alvo de avaliação, chamado de *Target of Evaluation* (TOE) [Razzazi et al., 2006].

No CC existem sete níveis na escala de garantia de segurança EAL, sendo o mais baixo o nível um (EAL1) e o mais elevado o nível sete (EAL7), sendo adicionado novos componentes a cada nível, ajudando com isso aos consumidores na definição de seus requisitos de segurança para produtos de TI [Mellado et al., 2007].

Proporcionando aos consumidores, a verificação, e atendimento de suas necessidades de segurança, servindo assim, como um balizador para o desenvolvimento, avaliação e/ou aquisição de produto de TI em relação as suas funcionalidades de segurança. Desta forma os usuários podem especificar seus requisitos de segurança, para que os responsáveis pelo desenvolvimento possam especificá-los igualmente e, principalmente, permitir assim que laboratórios avaliadores consigam determinar se os produtos efetivamente atendem às exigências requeridas [Mellado et al., 2007]. Dentre os elementos que compõem o CC temos o *Protection Profile* (PP), o *Security Target* (ST) e o TOE. O primeiro consiste em um documento formal com um conjunto de requisitos. Já o segundo é a forma de monitoramento do PP e traz ainda os mecanismos de reivindicação dos fornecedores. Finalmente o último é o sistema ou o produto que deve ser avaliado.

Atualmente temos doze países participando do desenvolvimento do CC, adotando-o para especificação e avaliação de segurança de produtos de TIC. Estes países participantes também concederam a licença de sua utilização para que ela fosse empregada como uma norma de padrão internacional, conhecida como ISO/IEC 15408.

O *Common Criteria* (CC) é utilizado para podermos avaliar características específicas de ativos de Tecnologia de Informação e Comunicação (TI), e é definido também como um catálogo de requisitos de segurança e suas dependências [Vintimilla et al., 2017].

Segundo Herrmann [2002] o CC é o ápice do desenvolvimento e união de várias organizações pelo mundo, vide as Tabelas 3 e 4, onde são listados os países autorizadores

e consumidores do *Common Criteria Recognition Arrangement* (CCRA), sendo que os primeiros mantêm o direito de utilizar, copiar, distribuir, traduzir ou ainda de modificar a versão do CC, e os segundos são países que consomem os certificados de avaliação [Common Criteria, 2018].

Tabela 3 – Órgãos dos Países Autorizadores. Fonte: Common Criteria [2017]

País	Órgão Responsável
Alemanha	BSI (Bundesamt für Sicherheit in der Informationstechnik)
Austrália	ASD (Australian Signals Directorate)
Canadá	CSE (Communications Security Establishment)
Coreia do Sul	NSRI (National Security Research Institute)
Espanha	Ministerio de Administraciones Públicas CCN (Centro Criptológico Nacional)
Estados Unidos	NSA (National Security Agency) NIST (National Institute of Standards and Technology)
França	ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
Japão	IPA (Information Technology Promotion Agency)
Nova Zelândia	GCSB (Government Communications Security Bureau)
Países Baixos	AIVD (Netherlands National Communications Security Agency)
Reino Unido	NCSC (National Cyber Security Centre)
Suécia	FMV (Swedish Defence Materiel Administration)

Tabela 4 – Órgãos do Países Consumidores. Fonte: Common Criteria [2018]

País	Órgão Responsável
Áustria	Federal Chancellery of Austria
Catar	Ministry of Transport and Communications
Cingapura	Cyber Security Agency of Singapore
Dinamarca	Center for Cyber Security
Etiópia	INSA (Information Network Security Agency)
Finlândia	FICORA (Finnish Communications Regulatory Authority)
Grécia	National Intelligence Service
Hungria	Ministry of National Development
Israel	The Standards Institution of Israel
Paquistão	Ministry of Defence
República Checa	National Security Authority of the Czech Republic

As dificuldades referentes a segurança estão presentes há muito tempo e não só a partir da Internet. Estes requisitos de segurança começam a se apresentar em sistemas de defesa há algum tempo, tendo primeiramente a intenção de evitar acessos indevidos, comprometimento ou manipulação de dados classificados de forma não autorizada. Para tal, estes requisitos de segurança são aplicados em várias fases de um sistema, como: projeto; desenvolvimento; implementação; avaliação e até na sua operação [Herrmann, 2002]. Desse modo, é necessário que possamos entender os elementos que constituem o CC, a serem descritos a seguir.

3.1.1 Elementos do Common Criteria

O CC é formado por alguns elementos básicos, que destacamos abaixo:

- PP - Protection Profile

  O PP é um documento que contém os requisitos de segurança funcionais e de

garantia visando o atendimento as especificidades dos consumidores. Com a criação dos PP os consumidores passam a ter um maior esclarecimento, definição de seus requisitos de segurança. Este documento fornece elementos básicos para os desenvolvedores, além do fornecimento de insumos para que a avaliação de segurança possa ser executada [Herrmann, 2002].

- ST - Security Targets

  O ST fornece os recursos e funções de segurança que atendem aos requisitos especificados no PP [Herrmann, 2002]. Desse modo, o ST fornece os meios fundamentais para que as especificações solicitadas pelos clientes possam ser avaliadas por laboratórios independentes [Vintimilla et al., 2017].

- TOE -Target of Evaluation

  Um TOE é um produto ou sistema gerado a partir da efetivação concreta do que foi solicitado em ST. Junto dele ainda encontramos uma documentação relacionada à orientação a administradores e usuários [Herrmann, 2002].

Ainda segundo Common Criteria [2012], os resultados das avaliações, seguem a sequência listada abaixo, conforme verificado na Figura 4.

- avaliações de PP conduzem a um registro de PP avaliado;
- o registro do PP leva a vários ST avaliados;
- cada ST avaliado leva a uma avaliação de TOE, conduzindo a um registro de TOE.

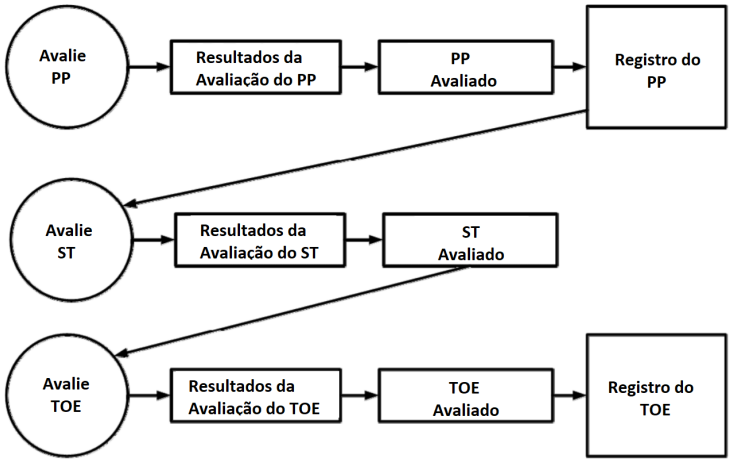


Figura 4 – Sequência de avaliação. Fonte: Common Criteria [2012]

Definida na terceira parte da ISO/IEC 15408, o EAL define sete níveis de avaliação hierárquica, ou seja é um pacote de garantias. A cada nível acrescentado, o EAL inclui novos e mais rigorosos componentes de garantia. Segundo Herrmann [2002], há os seguintes níveis:

- EAL 1 - Fornece um nível mínimo de confiança, adequado para locais sem ameaças de segurança;
- EAL 2 - Proporciona um nível de confiança de baixo a moderado, na maioria da vezes utilizado para sistemas legados;
- EAL 3 - Proporciona um nível moderado de confiança, apresenta uma completa investigação do Target of Evaluation (TOE), iniciando na fase de projeto;
- EAL 4 - Fornece um nível de confiança de moderado a elevado, contém rigorosas práticas de desenvolvimento e com exame da política de segurança;
- EAL 5 - Proporciona um elevado nível de confiança, utiliza desenvolvimento e práticas e técnicas de engenharia de segurança especializadas, sendo apropriado para locais que tenham potencial para ter resistência a ataques moderados;
- EAL 6 - Fornece um alto nível de confiança, utilizado em locais com alto risco, devem proteger ativos com alto potencial de ataque;
- EAL 7 - Proporciona um nível muito elevado de confiança, representa um nível completo, e destina-se a ser utilizado em ambientes de alto risco que devem proteger ativos de alto valor.

Cumpre destacar que os laboratórios avaliadores [Common Criteria, 2018] devem ser licenciados pelo CCRA, além de terem competência e independência, para que possam verificar se as propriedades de segurança estão sendo cumpridas nos sistemas avaliados. Com isto, a certificação das propriedades de segurança de um produto avaliado, passa a ser reconhecida por todos os países que participam do *Common Criteria Recognition Arrangement* (CCRA) e estes produtos podem, a partir de então, ser adquiridos pelos países participantes sem a necessidade de uma nova avaliação.

A avaliação deve ter resultados objetivos, que possam ser reproduzidos e com a citação de evidências. Existir um conjunto de critérios de avaliação é uma condição necessária para que a avaliação leve a um resultado, e assim possa fornecer uma base

técnica, para que o os resultados da avaliação possam ser reconhecidos mutuamente [Common Criteria, 2012].

Atualmente, alguns países estão adotando uma nova estratégia para o CC, através de uma visão mais colaborativa, como podemos notar em [Common Criteria Recognition Arrangement, 2012], que é o documento de declaração de visão para a futura direção do CC e do CCRA. Neste documento, verifica-se um grande interesse no desenvolvimento de *Protection Profile* (PP) que sejam colaborações entre agências governamentais de participantes da CCRA, fornecedores de produtos e laboratórios.

3.1.2 Perfis de Proteção Colaborativos

Estados Unidos

O *National Information Assurance Partnership* (NIAP) dentro do Estados Unidos é o órgão responsável pela implantação do CC, incluindo o gerenciamento dos *Common Criteria Evaluation and Validation Scheme* (CCEVS), do programa nacional para o desenvolvimento de PP, metodologias de avaliação, e de políticas que garantam que os requisitos solicitados possam ser reproduzíveis e testáveis. O *National Institute of Standards and Technology* (NIST) em parceria com o NIAP também aprova Laboratórios de Testes para conduzir essas avaliações de segurança nas operações do setor privado em todo os Estados Unidos para o CC. Já em conjunto com a Organização do Tratado do Atlântico Norte (OTAN) e com organismos de normalização como a ISO, trabalha para evitar a duplicação de esforços na avaliação do CC [National Information Assurance Partnership].

Segundo National Information Assurance Partnership [2012] os PPs da metodologia de avaliação estão sendo alterados, tratando o desenvolvimento dos perfis de proteção e metodologias de avaliação como abordagens colaborativas, não mais especificando os níveis dos *Evaluation Assurance Level* (EAL). Assim, passa-se a apoiar a criação de comunidades técnicas internacionais de representantes de governos, indústrias, academia e usuários, criando assim avaliações mais consistentes e com maior possibilidade de

reprodução. Com isso, pode-se obter metodologias de avaliação mais bem aceitas em todos os laboratórios que utilizam o CC.

As mudanças na política fazem parte da percepção de que a garantia pode ser alcançada com diversos tipos de tecnologias e de que suas limitações podem ser obtidas mediante à avaliação de produtos do fornecedor. Isto deve-se aos requisitos do EAL 4 que se tornaram padrões genéricos, mas não relevantes, realizáveis e repetitivos [National Information Assurance Partnership, 2012].

Assim, o NIAP não aceita mais avaliações baseadas no EAL, migrando para avaliações de conformidade com os PP próprios da tecnologia com o intuito de fornecer resultados viáveis, reproduzíveis e testáveis [National Information Assurance Partnership, 2019].

Verificamos ainda em [National Information Assurance Partnership, 2012] que os resultados de avaliação exigem um modelo em que o conjunto de requisitos funcionais de segurança sejam relacionados em um PP; que os resultados da avaliação sejam comparáveis e consistentes, exigindo documentação das atividades para cada requisito; e que haja divulgação de mais informações através de esquemas *Common Criteria Recognition Arrangement* (CCRA), garantindo a confiança da execução no mesmo nível de competência.

Alemanha

Na Alemanha, a *Zentralverband Elektrotechnik- und Elektronikindustrie* (ZVEI), também preocupada com a segurança e com a efetiva regulação dos produtos, enfatiza alguns princípios, conforme podemos verificar na Tabela 5. Ela considera que seu quadro legislativo consiste em uma base ideal para a efetivação regulatória desses princípios. Estes princípios devem ter o objetivo de realizar a seleção de requisitos de segurança, garantindo a sua praticidade [Zentralverband Elektrotechnik- und Elektronikindustrie e. V., 2018, 2017].

Tabela 5 – Quadro legislativo ZVEI. Fonte: Zentralverband Elektrotechnik- und Elektronikindustrie e. V. [2018]

Princípio da melhor regulamentação	**Princípio ”SMERC”**
Regulamento estabelece os objetivos de proteção geral, detalhes e requisitos são definidos através de normas e padrões	*Specific* - específico os requisitos devem ser considerados em relação à aplicação específica
Classificados e baseados em risco	*Measurability* - mensurabilidade, os requisitos devem ser claramente mensuráveis/-verificáveis
A manutenção da flexibilidade dos fabricantes na aplicação das disposições	*Enforceability* - exigibilidade, a conformidade com os requisitos deve ser executória pelas autoridades de fiscalização do mercado
Incorporação de normas internacionais	*Relevance* - relevância, os requisitos devem ser relevantes para a segurança e os usuários
Aceitação da Organização Mundial do Comércio (OMC) e compatibilização internacional	*Competition-friendly* - competição amigável significativa, impactos nocivos para a competitividade da indústria não devem surgir
Condições de concorrência igualitária para fabricantes e importadores	
Neutro em relação à tecnologia e soluções	

É esperado que os princípios da “melhor regulamentação” e o Princípio “SMERC”, sejam essenciais para a regulamentação de segurança cibernética, fortalecendo assim as necessidades de inovação da indústria, pois a segurança é um acontecimento transversal, e nenhuma área, seja da sociedade em geral ou da indústria, ficará isolada [Zentralverband Elektrotechnik- und Elektronikindustrie e. V., 2018].

Existem modelos que não são considerados novos, como as diretivas *Electromagnetic Compatibility* (EMC) que tratam de compatibilidade eletromagnética e a diretiva *Atmospheres Explosibles* (ATEX) para trabalhos em ambientes explosivos, em que fabricantes definem a utilização e suas categorias, produzindo com isso requisitos especificados, além de procedimentos de avaliação da conformidade [Zentralverband Elektrotechnik- und Elektronikindustrie e. V., 2018].

Ainda em [Zentralverband Elektrotechnik- und Elektronikindustrie e. V., 2018],

entende-se que atualmente o foco está na definição dos requisitos funcionais e nas formas de avaliação da conformidade, não sendo suficiente o enfoque em apenas a um dos dois aspectos.

Podemos notar na Figura 5 a apresentação de uma avaliação conhecida como horizontal, que existe quando as avaliações de risco antecedem a definição dos requisitos de segurança, além de um adequado sistema de avaliação da conformidade e de fiscalização do mercado.

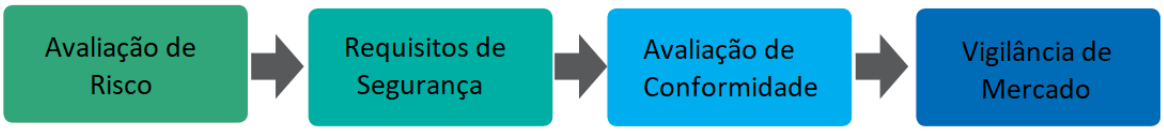


Figura 5 – Avaliação horizontal. Fonte: Zentralverband Elektrotechnik- und Elektronikindustrie e. V. [2018]

3.1.3 Produtos Avaliados

Os produtos avaliados pelo CC, disponíveis na lista do seu endereço eletrônico, têm validade de cinco anos. Após este período, eles são retirados da lista de produtos certificados e transferidos para uma outra área do portal. Os certificados permanecem na *Certified Products List* (CPL) por cinco anos. A partir de 1º de junho de 2019, os certificados com um período de validade expirado (ou seja, 5 anos ou mais a partir da data de emissão do certificado) são movidos para uma lista de arquivos no portal da *Common Criteria Recognition Arrangement* (CCRA). Podemos notar no gráfico da Figura 6, a evolução da certificação e seus níveis, de 1999 até o ano de 2018.

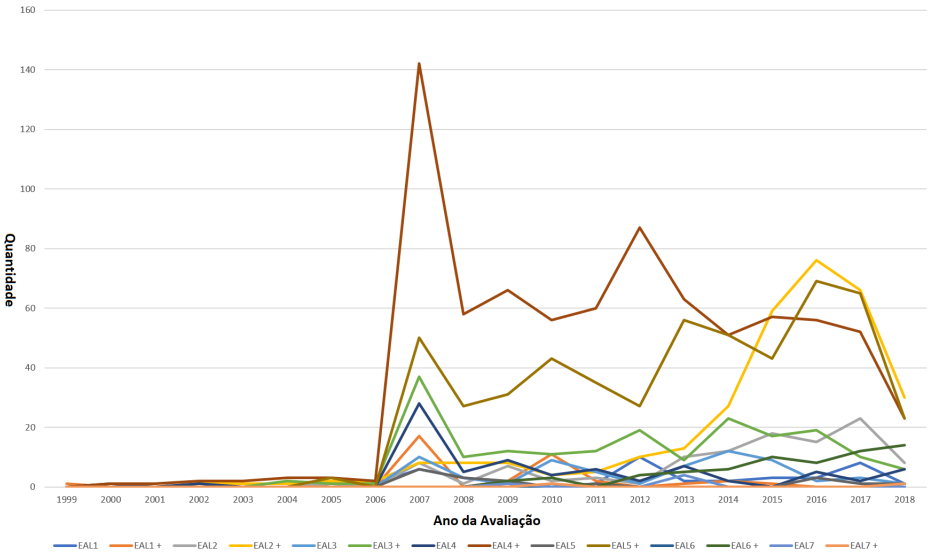


Figura 6 – Quantidade de Produtos certificados por níveis e ano. Fonte: Common Criteria [2018]

Na lista de produtos avaliados em [Common Criteria, 2018], pode-se encontrar um total de 2.430 produtos divididos em 15 categorias, conforme podemos verificar na Tabela 6.

Tabela 6 – Quantidade de produtos por categoria. Fonte: Common Criteria [2018]

Categoria de Produto	Qtd.Produto
Sistemas biométricos e dispositivos	3
Dispositivos e sistemas de detecção	11
Sistemas de gerenciamento de chaves	22
Mobilidade	31
Bancos de dados	33
Computação Confiável	33
Dispositivos e sistemas de controle de acesso	69
Proteção de dados	69
Dispositivos e sistemas de proteção de limite	80
Produtos para assinaturas digitais	101
Sistemas operacionais	102
Dispositivos multifuncionais	192
Dispositivos e sistemas relacionados à rede e à rede	244
Outros dispositivos e sistemas	286
ICs, cartões inteligentes e dispositivos e sistemas relacionados a cartões inteligentes	1154

Pode-se notar na Tabela 6 e na Figura 7 que a maior parte dos produtos está na categoria de cartões inteligentes, tendo 1.154 produtos certificados, correspondendo à 48% do total encontrado [Common Criteria, 2018].

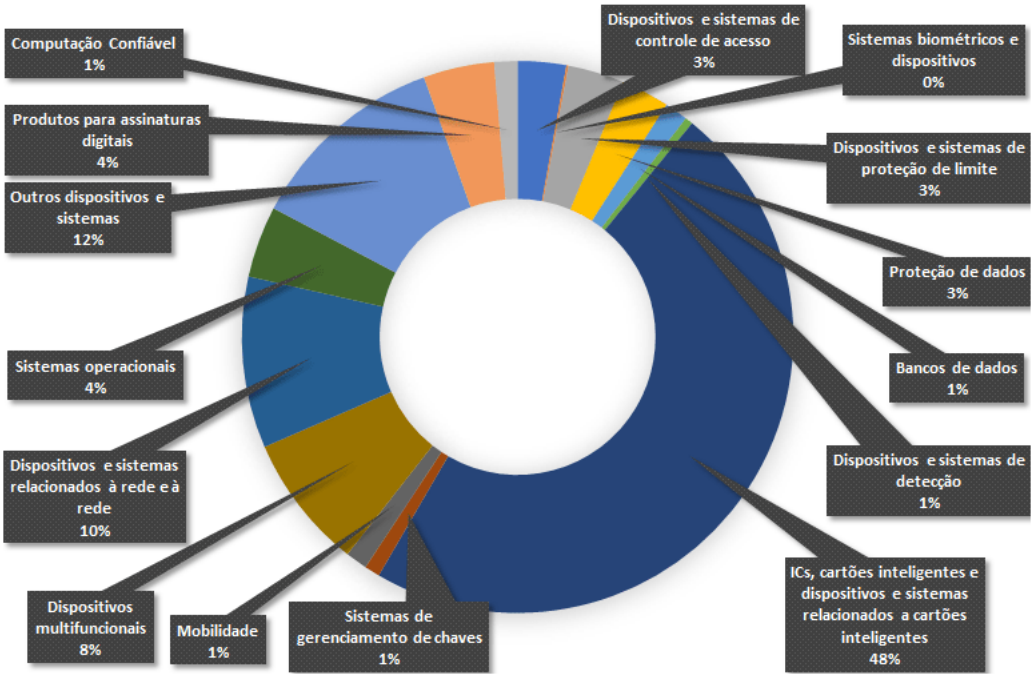


Figura 7 – Quantidade de Produtos por Categoria.
Fonte: Common Criteria [2018]

3.2- Federal Information Processing Standard: FIPS 140-2

O *Federal Information Processing Standard* é um conjunto de padrões para módulos criptográficos. É amplamente utilizado para a proteção de informações de sistemas, computadores e envio de dados. O FIPS 140-2 veio a suceder ao FIPS 140-1 devido a alterações na tecnologia [Vintimilla et al., 2017].

Os requisitos de segurança do FIPS 140-2 compreendem o âmbito do projeto e implementação segura de um módulo criptográfico. O padrão proporciona quatro níveis incrementais de segurança. Esses níveis pretendem englobar uma abrangente gama de aplicativos, além de possíveis locais onde estes módulos possam ser utilizados [National Institute of Standards and Technology, 2001]. A segurança de módulos criptográficos é encontrada também na norma ISO/IEC 19790:2012 com o título de Tecnologia da informação - Técnicas de segurança - Requisitos de segurança para módulos criptográficos.

O FIPS é um conjunto de normas publicadas pelo NIST órgão do Departamento de Comércio dos Estados Unidos. No primeiro nível, os requisitos básicos de segurança para um módulo criptográfico são caracterizados. No segundo nível encontramos uma melhora do mecanismo de segurança física do nível anterior, sendo que encontramos

uma autenticação baseada em função, e autenticação à autorização do operador para acesso a um conjunto de serviços. No terceiro nível temos a incorporação de mecanismos de detecção de intrusão, o que evita acessos não autorizados a parâmetros de segurança localizados nos módulos criptográficos. No quarto e último nível encontramos os mais altos requisitos de segurança, sendo encontrada uma completa proteção ao redor do módulo criptográfico, sendo este indicado para ambientes fisicamente desprotegidos.

Segundo ITI [2016], o FIPS 140-2 engloba diversas áreas de atuação, relativas à implementação de um módulo criptográfico. As áreas de atuação no FIPS 140-2 são apresentadas conforme a Tabela 7.

Tabela 7 – Áreas de atuação contidas no FIPS 140-2. Fonte: ITI [2016]

Seção	Áreas de atuação do padrão FIPS 140-2
1	Documentação do módulo criptográfico
2	Identificação de portas e interfaces do módulo criptográfico
3	Nível de identificação de papéis, serviços e autenticação do operador
4	Descrição do modelo de estado finito
5	Nível de segurança física
6	Ambiente operacional
7	Gerenciamento de chaves criptográficas
8	Interferência e compatibilidade eletromagnética
9	Autotestes
10	Garantia do projeto
11	Mitigação de outros ataques Tabela

O FIPS 140-2 é aplicado no setor público nos Estados Unidos para a proteção dos sistemas de informação do governo, além de ser utilizado e referenciado em diversos outros documentos técnicos em diversos países [Vintimilla et al., 2017].

Podemos verificar a utilização do FIPS 140-2 no caso da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Os seus Manuais de condutas Técnicas são divulgados pelo Instituto Nacional de Tecnologia da Informação (ITI). No Canadá existe o *Cryptographic Module Validation Program* (CMVP), que é um programa gerenciado em conjunto pelo *Communications Security Establishment* (CSE) e NIST. O FIPS 140-2 também é amplamente utilizado nos Países da América do Sul como: Venezuela, Peru, Paraguai, Equador, Colômbia, Chile, Bolívia, Argentina e Brasil [Vintimilla et al., 2017].

3.3- O Cenário Brasileiro

No Brasil, o Programa Brasileiro de Avaliação da Conformidade (PBAC) tem como objetivo principal o desenvolvimento de uma visão de longo prazo, além de fazer a gestão da atividade de Avaliação da Conformidade no Brasil. Sua contribuição é crucial para o desenvolvimento econômico brasileiro e melhoria contínua da qualidade, através da produção e comercialização de bens e serviços que atendam às necessidades dos consumidores, em um ambiente de justa competição [Inmetro, 2018f]

A busca pelo aperfeiçoamento torna-se crítica à medida que a concorrência é cada vez maior na busca pela qualidade e produtividade, levando com isso a empresas brasileiras a buscarem melhores condições para a disputa do mercado [Fernandes, 2011]. Neste contexto, a avaliação da conformidade auxilia asseguradamente para que as empresas tenham maior competitividade e acesso aos mercados internacionais, acarretando com isso uma melhora para as exportações brasileiras [INMETRO, 2012].

Desde sua criação em 1973, o INMETRO tem a incumbência do fortalecimento das empresas brasileiras, de modo a ampliar sua eficiência pela melhoria da qualidade de produtos e serviços [Inmetro, 2018c]. Já o SINMETRO (SBAC) passou por várias fases. Seu modelo inicial foi instituído em 1978 pela resolução Conmetro (Conselho Nacional de Metrologia, Normalização e Qualidade Industrial) de nº 05/78 e nº 06/78, tendo como centro de certificação o INMETRO, segundo [Reis Da Costa and De Barros, 2012].

O trabalho de Fernandes [2011] nos indica que já nos anos 80, seguindo uma tendência internacional, e a uma crescente procura de avaliação da conformidade, o INMETRO inicia a acreditação de organismos de certificação. O modelo estabelecido em 1978, como um subsistema de certificação, foi alterado 1992 pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro), originando com isso o Sistema Brasileiro de Certificação (SBC), que é estruturado para atender aos esforços de consolidação no que diz respeito a avaliação da conformidade, e novamente reformulado em 1997 com as matérias relativas à defesa do consumidor, à acreditação, à avaliação e reconhecimento internacional.

Em 2002, o Conmetro aprova a transformação do SBC para SBAC, estabelecendo diretrizes e políticas para o gerenciamento do sistema e atribuindo ao INMETRO a incumbência da implantação dessas políticas [Fernandes, 2011].

3.3.1 Mecanismos de avaliação da Conformidade no Brasil

Existem diferentes formas para avaliação da conformidade no Brasil: Certificação, inspeção, declaração do fornecedor, ensaios [ISO/CASCO, 2019]. Cada uma dessas formas de avaliação serão brevemente descritas a seguir.

1. Certificação: é um conjunto de atividades desenvolvidas por um organismo independente da relação comercial, com o objetivo de atestar publicamente, por escrito, que o produto, processo ou serviço está em conformidade com os requisitos especificados;

2. Inspeção: é definida pela observação e julgamento acompanhados, conforme apropriado, por medições, ensaios e etc.;

3. Declaração do fornecedor: é o mecanismo utilizado pelo fornecedor de um produto, processo ou serviço, baseado em um conjunto de procedimentos estabelecidos e reconhecidos que ele utiliza e declara, de sua própria responsabilidade, que o seu produto, processo ou serviço, está de acordo com os requisitos especificados;

4. Ensaios: é uma operação técnica que consiste na determinação de uma ou mais características de um produto, de acordo com o procedimento especificado.

A definição do mecanismo mais adequado que deva ser empregado no programa leva em consideração algumas questões referentes e presentes em [Inmetro, 2018e]: características do produto; processo ou serviço avaliado; risco de eventual acidente de consumo; efeito e constância da falha; volume de produção; velocidade do aperfeiçoamento tecnológico no setor; tamanho de fabricantes envolvidos; dispersão geográfica; influência sobre a competitividade do produto; e nível de dificuldade de seu acompanhamento no mercado.

4- Avaliação de Conformidade Baseada no Risco

O entendimento acerca da gestão de riscos nos permite identificar ameaças envolvidas, além do correto cumprimento dos objetivos estabelecidos em um programa de avaliação de conformidade. Segundo a norma Associação Brasileira de Normas Técnicas (ABNT) Norma Brasileira (NBR) ISO 31000:2009, o processo de gestão de riscos é definido como a aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos [Associação Brasileira de Normas Técnicas, 2009a].

Todas as atividades de uma organização, seja ela pública ou privada, com ou sem fins lucrativos, envolvem sobremaneira o risco. As influências internas ou fatores externos podem tornar incerto o atingimento dos objetivos, e, é exatamente o efeito dessa incerteza que denominamos risco. A ABNT NBR ISO 31000:2009 descreve a gestão de riscos com o propósito de possibilitar, dentre outros fatores, um significativo aumento no atingimento dos objetivos e uma melhora na identificação de oportunidades e ameaças. Esta norma define o processo de gestão de riscos como sendo a aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

O conceito de risco, segundo a referida norma, é entendido como “o efeito da incerteza nos objetivos”, podendo ser expresso na combinação de consequências de um evento e a probabilidade de ocorrência. O guia de orientação para o gerenciamento de riscos corporativos, criado pelo Instituto Brasileiro de Governança Corporativa (IBGC), define o risco como evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência. Da mesma forma, sua definição de incerteza está relacionada ao evento futuro identificado, ao qual não é possível associar uma probabilidade de ocorrência [Instituto Brasileiro de Governança Corporativa, 2007].

4.1- Gestão de Riscos

A Associação Brasileira de Normas Técnicas [2009a] estabelece algumas etapas para o processo de gerir os riscos, sendo todos os aspectos que norteiam os inúmeros conceitos, descritos a seguir:

1. Comunicação e consulta, que prevê a criação de um canal de relacionamento com todas as partes interessadas, internas e externas, devendo a comunicação e a consulta se estender, ao longo de todo o processo de gestão de risco, desde o estabelecimento do contexto até o tratamento dos riscos. Como a própria norma destaca, ambas são ”processos contínuos e interativos que uma organização conduz para fornecer e compartilhar ou obter informações e se envolver o diálogo com as partes interessadas e outros, com relação a gerenciar riscos”;

2. Estabelecer o contexto que define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecer o escopo e os critérios de risco para o restante do processo. O contexto externo, afirma a norma ABNT NBR ISO 31000:2009, é o “ambiente externo no qual a organização busca atingir seus objetivos” e deve conter, dentre alguns fatores, os diferentes ambientes e as percepções das partes interessadas externas. O contexto interno, por sua vez, deve compreender e estar alinhado com a cultura, estrutura e estratégia da organização e deve considerar todos os fatores internos que possam de alguma forma impactar na gestão de riscos;

3. Processo de gestão de riscos prevê que sejam estabelecidos os objetivos, as estratégias, o escopo e os parâmetros das atividades da organização, ou daquelas partes da organização em que o processo de gestão de riscos está sendo aplicado; ou seja, nesta contextualização devem ser definidas metodologias, responsabilidades e escopos, dentre outros fatores, com o intuito de facilitar a aplicação da gestão de riscos;

4. Definição dos critérios de risco, que devem ser compatíveis com a política de gestão de riscos da organização, definidos no início de qualquer processo de gestão de riscos e analisados criticamente de forma contínua. Nestes critérios é necessário dar atenção à definição do nível em que o risco é considerado aceitável ou tolerável.

A Figura 8 mostra as atividades que compõem um processo de gerenciamento de risco (seções 4 e 5 da ISO 31000), sendo este um processo interativo que consiste em uma aplicação metódica de políticas de gestão, procedimentos, reconhecimentos, exames, tratamentos, acompanhamentos e revisões dos riscos [Proenca et al., 2017].

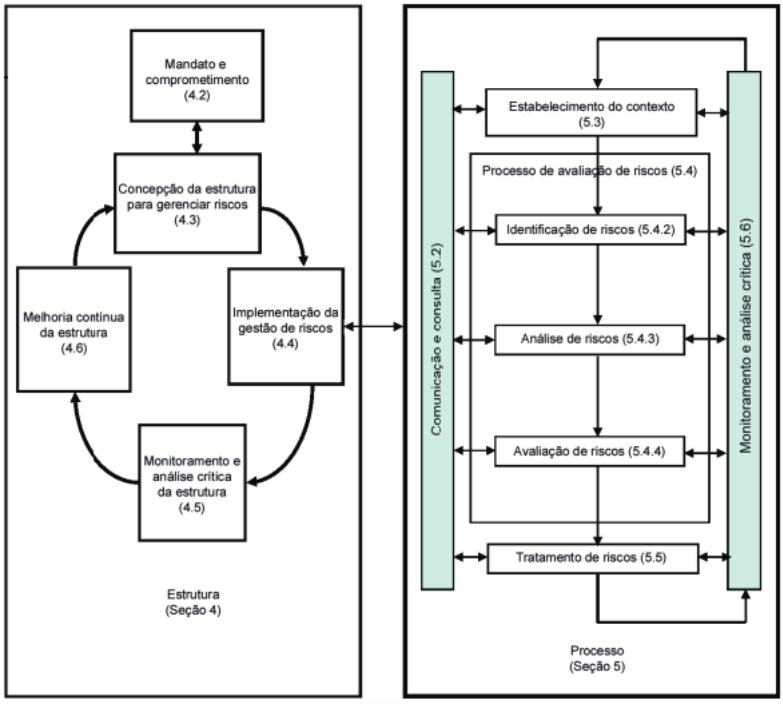


Figura 8 – Atividades que compõem o processo de gerenciamento de risco.
Fonte: Associação Brasileira de Normas Técnicas [2009a]

Passada a etapa de estabelecimento do contexto, tem-se início o processo de avaliação de riscos propriamente dito, que inclui a identificação, análise e avaliação de riscos. A identificação de riscos tem por objetivo “gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos” [Associação Brasileira de Normas Técnicas, 2009a].

A partir da lista com os riscos identificados, dá-se início à análise que servirá de base para a avaliação e tratamento de riscos. A análise de riscos deve envolver a apreciação das causas e as fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer [Associação Brasileira de Normas Técnicas, 2009a].

Por último, inicia-se a avaliação dos riscos, quando é decidido quais riscos serão tratados a partir da comparação do nível de risco encontrado durante o processo de análise. O tratamento proposto deve ser objeto de um plano com diversas informações que

incluem a justificativa para a escolha das opções, os responsáveis, as ações propostas, os recursos necessários, as medidas de desempenho, os requisitos de monitoramento e um cronograma [Associação Brasileira de Normas Técnicas, 2009a].

O monitoramento e análise crítica de riscos devem ser periódicos. Sua importância está, não apenas no acompanhamento do processo para fins de melhoria, mas, sobretudo na detecção de mudanças nos contextos que possam ensejar novos tratamentos de risco ou na emergência de novos riscos [Associação Brasileira de Normas Técnicas, 2009a].

Todas essas etapas contidas na norma, podem ser aplicadas a qualquer tipo de organização, tanto etapas em conjunto, quanto separadas ou isoladas em qualquer momento, em qualquer nível e em qualquer aérea, bem como a qualquer projeto. Devido a essa amplitude, foram criadas metodologias mundialmente reconhecidas para auxílio e aplicação dos conceitos a serem seguidos para tornar uma gestão de riscos eficaz.

Apresentamos ainda os principais conceitos contidos nas normas e guias sobre a gestão de riscos, conforme a ABNT ISO GUIA 73:2009 [Associação Brasileira de Normas Técnicas, 2009b].

1. Risco

   (a) Efeito da incerteza no objetivo é um desvio em relação ao esperado, podendo ser positivo ou negativo;

   (b) Possibilidade de um evento que terá impacto no cumprimento dos objetivos. É expresso em termos de probabilidades e consequências;

   (c) O risco em sua tendência mais comum é avaliado como uma ameaça, neste sentido, os esforços institucionais visam reduzi-lo, evitando-o, transferindo-o ou mitigando-o.

2. Identificação de riscos é o processo de busca, reconhecimento e descrição de riscos (identificando fontes de risco, eventos, causas e consequências).

3. Análise de riscos é o processo de compreender a natureza do risco e determinar o nível do risco.

4. Avaliação de riscos é processo de comparar os resultados da análise do risco com os critérios de riscos, determinando se sua magnitude é aceitável ou tolerável.

5. Tratamento de riscos - Processo para modificar o risco.

Após a assimilação dos conceitos necessários para o conhecimento de Riscos, podemos trabalhar na sua correta identificação, análise e avaliação.

4.2- Seleção e Identificação de Riscos

O trabalho de Machado et al. [2018] indica que para o estabelecimento do contexto, devem-se considerar os parâmetros externo e interno para se gerenciar riscos, estabelecendo-se uma finalidade e os critérios a serem utilizados. Assim, a consideração de diferentes fatores, e seus diversos cenários, como cenário nacional, fornecedores, desenvolvedores de tecnologias, laboratórios de ensaios, órgãos de controle devam ser verificados. Outrossim, uma averiguação nos contextos políticos, financeiro, regulatório e jurídico também deva ser levado em consideração na avaliação.

Identificar os riscos é um processo de busca, análise e descrição dos mesmos. É a definição de um grupo de ocorrências, sejam estas externas ou internas, tendo como origem as possibilidades de um contexto, que podem impactar nos objetivos previamente traçados. Inclui também a identificação das causas e fontes de risco, situações ou circunstâncias que poderiam ter um impacto material sobre os objetivos.

Dentre os métodos utilizados para a identificação de riscos na norma ABNT NBR ISO / IEC 31010:2012, Machado et al. [2018] utiliza da técnica de *Brainstorming* para o levantamento destas.

Conforme visto ainda em Machado et al. [2018], para a mensuração da probabilidade e a avaliação do impacto dos riscos, foi utilizada uma abordagem qualitativa, em que profissionais de Regulação e de Tecnologia da Informação foram entrevistados e imputaram uma nota, entre 1 e 5, para a probabilidade de ocorrência de cada risco e para o impacto, caso o risco se concretize, sendo calculada a média de probabilidade e de impacto sobre todas as respostas.

Foram realizadas entrevistas com cinco especialistas em regulação e avaliação da conformidade, e outras três com profissionais com experiência em TIC. O “valor do 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 foi menor que 8, Risco Médio se o valor foi de 8 a 12, e Risco Crítico se o valor de risco foi superior a 12.

Nessa perspectiva, a gestão de risco e sua avaliação sistemática, podem garantir que os governos e seus órgãos possam ter uma referência segura para o atendimento aos seus objetivos na implantação de PAC para a área de TIC [Machado et al., 2018].

Conforme podemos verificar em Machado et al. [2018], foram apresentados 55 riscos divididos em nove categorias, conforme descritos abaixo.

- ME- Definição clara dos métodos de ensaio
  - 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.
  - ME-2- Diferença nos resultados entre laboratórios: Risco pela diferença de Precisão dos requisitos entre os laboratórios e pela impossibilidade de comparação dos resultados entre laboratórios.
  - ME-3- Excesso de requisitos desnecessários: Risco devido a revisão periódica dos requisitos para readequação das necessidades.
  - ME-4- Custo dos ensaios: Risco referente a falta de padronização dos ensaios, por conta de requisitos gerais, aumentando o número de ensaios necessários.
  - ME-5- Requisito rigoroso demais: Risco referente ao rigor excessivo do escopo.
  - ME-6- Requisito prescritivo demais: Risco referente ao teor de norma, regra, preceito, determinação; normativo: regulamento prescritivo.
  - ME-7- Interpretação errônea dos dados internos (incerteza de medição): Risco referente a interpretação dados – nas habilidades técnicas da pessoa que está executando o ensaio ou avaliando.
  - ME-8- Controle de qualidade dos processos e equipamentos: Riscos devido a falha de infraestrutura, processos e procedimentos bem definidos.
  - ME-9- Resultados não comparáveis: Risco devido a precisão dos requisitos para a realização de auditorias, habilidades técnicas ou ainda pela infraestrutura disponível.
  - ME-10- Ausência de material de referência: Risco referente a falta de material de referência para habilidades técnicas ou para infraestrutura disponível.

  - ME-11- Requisito mal definido: Risco devido à falta de clareza do problema que se quer resolver, falta de conhecimento.

- IM- Quanto ao impacto no mercado

  - IM-1- Prejuízo total do mercado nacional: Risco devido a necessidade de um melhor levantamento junto as partes interessadas.
  - IM-2- Prejuízo parcial do mercado nacional: Risco devido a necessidade de um melhor levantamento junto as partes interessadas.
  - IM-3- Barreira técnica à importação: Risco devido à restrição e de barreiras técnicas do setor.
  - IM-4- Dificuldade de adequação à regulamentação. Risco devido a adequação à regulamentação (maturidade do processo de produção), gerando baixa qualidade do produto (quanto pior a qualidade, maior é a fonte de risco).
  - IM-5- Dificuldade de compreensão sobre a regulamentação: Risco devido à pouca compreensão da regulamentação (maturidade do processo de produção), gerando baixa qualidade do produto (quanto pior a qualidade maior é a fonte de risco).
  - IM-6- Desconhecimento do setor quanto à regulamentação: Risco referente a ignorar e não conhecer sobre normas vigentes. Falta de mobilização do setor produtivo em torno da regulamentação.
  - IM-7- Formação de monopólios/oligopólios: Risco devido ao controle da maior parcela do mercado por uma ou poucas empresas ou lobby.
  - IM-8- Aumento da informalidade: Risco referente ao aumento da informalidade devido a normatização.
  - IM-9- Aumento do desemprego: Risco referente ao aumento do desemprego devido a normatização.
  - IM-10- Dificuldade de interação com o regulamentador/participação em Comissões: Risco devido a dispersão geográfica do setor produtivo com o setor normativo.
  - IM-11- Atendimento de interesses de uma empresa/setor: Riso devido a possibilidade de criação de monopólios, oligopólios ou lobby.

- CA- Quanto a Custos aceitáveis
  - 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.
  - CA-2 - Onerar o processo de produção: Risco referentes a recursos financeiros insuficientes devido ao aumento do custo da produção.
  - CA-3- Desequilíbrio entre organismos de Avaliação da Conformidade: Risco devido a escassez de recursos financeiros e pela inexistência de infraestrutura tecnológica necessária.
  - CA-5- Ausência de laboratórios: Riscos devido à falta de laboratórios (infraestrutura acreditada).
  - CA-6- Ausência de organismos: Riscos devido à falta de organismos de regulamentação (infraestrutura acreditada).
  - CA-7- Laboratórios apenas nas regiões S/SE: Riscos devido a maioria dos laboratórios estar presentes nas regiões Sul e Sudeste.
  - CA-8- Organismos apenas nas regiões S/SE: Riscos devido a maioria dos organismos de controle estar presentes nas regiões Sul e Sudeste.
  - CA-9- Desinteresse de laboratório e organismos pelo escopo: Risco referente a falta de interesse de laboratórios e organismos devido aos Custos e tempo da acreditação e do retorno do investimento.
- DCT- Quanto a disponibilidade de competência técnica
  - DCT-1- Inadequação do regulamento: Risco devido à falta de competência técnica específica do regulamentador.
  - DCT-2- Inviabilizar o processo produtivo: Riscos devido ao impedimento do processo produtivo devido à falta de competência técnica, indisponibilidade de recursos humanos com expertise no setor.
  - DCT-3- Inviabilizar as avaliações por parte dos laboratórios: Risco devido ao impedimento de avaliações por parte dos laboratórios por falta de competência técnica, treinamento insuficiente.

  - DCT-4- Inviabilizar as avaliações por parte dos OAC: Risco pela falta de competência técnica nos Organismos de Avaliação da Conformidade, treinamento insuficiente.
  - DCT-5- Perda da confidencialidade: Risco que pode ser inferido por trabalho não supervisionado de pessoal ou ainda pela má conduta de recursos humanos envolvidos.
  - DCT-6- Perda de dados: Risco devidos à perda de dados de vido a processamento ilegal dos dados ou ainda devido a erros realizados por funcionários.

- QTI- Quanto a transparência e imparcialidade
  - QTI-1- Comprometimento da propriedade intelectual: Risco devido a direitos intelectuais, como a utilização de cópias ilegais ou falsificação, inexistência de procedimento de direitos de propriedade intelectual ou ainda indisponibilidade de recursos humanos com expertise no setor.
  - QTI-2- Falta de controle interno de acesso adequado: Risco na utilização de cópias não controladas (inexistência de controles internos, indisponibilidade de recursos humanos com expertise no setor).
  - QTI-3- Confidencialidade no processo de avaliação: Risco devido a atribuições inadequada das responsabilidades ou indisponibilidade de recursos humanos com expertise no setor.

- IPC- Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente
  - IPC-1- Ineficácia do regulamento: Risco do não atendimento ao consumidor no que foi proposto, PAC inadequado ou dificuldade em acompanhar inovação.
  - 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.
  - IPC-3- Regulamento não compreendido pela sociedade: Risco devido a falta de elaboração de campanhas voltadas ao consumidor, complexidade técnica do objeto regulado dificultando a divulgação de massa.

  - IPC-4- Ausência de comunicação sobre a regulamentação: Risco devido a produtos regulados com público específico mas sem mídia especializada no tema.
  - IPC-5- Crítica ao regulamento: Risco referente a regulamentação de objeto regulado e amplamente comercializado e consumido pelo “consumidor final”.
  - IPC-6- Índice de rejeição à regulamentação pela sociedade: Risco referente a regulamentação de objeto regulado e amplamente comercializado e consumido pelo “consumidor final”.
  - IPC-7- Comunicação ineficiente sobre a regulamentação: Risco pelo pouco envolvimento das entidades representativas dos consumidores na regulamentação.
  - IPC-8- Não acesso a um público especializado: Risco referente a inexistência de veículos de mídia especializada sobre o produto regulado.

- PCJ- Propiciar concorrência justa entre fabricantes e laboratórios
  - PCJ-1- Inexistência de laboratório acreditado: Risco pela falta de laboratórios especializados e baixa expectativa de lucro.
  - PCJ2- Desequilíbrio entre laboratórios: Risco devido a diferença de especialização entre laboratórios.
  - PCJ-3- Gerar monopólio/oligopólio entre laboratórios: Risco devido ao controle da maior parcela do mercado por uma ou poucas empresas, capacitação de pessoal ou pela infraestrutura disponível.
  - PCJ-4- Gerar monopólio/oligopólio entre organismos: Risco devido ao controle da maior parcela do mercado por poucos órgãos, capacitação de pessoal ou pela infraestrutura disponível.

- FCI- Facilitar o comércio internacional
  - FCI-1- Requisitos desalinhados com requisitos internacionais: Risco referente ao acesso ao mercado externo, os produtos certificados não atendem ao mercado externo.
  - FCI-2- Requisitos obsoletos em relação a requisitos internacionais: Risco devido a não existência de revisão de normas nacionais com os padrões solici-

tados internacionalmente, os produtos certificados não atendem ao mercado externo.

  - 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.

- FMI- Fortalecer o mercado Interno

  - FMI-1- Ineficácia do regulamento em promover melhoria no setor: Risco pela falta de eficiência na melhoria nas regulamentações.

Os desafios e os tipos de risco relacionados à implantação de Programas de Avaliação da Conformidade (PAC)s na área de Tecnologia da Informação e Comunicação (TIC) são essencialmente os mesmos em qualquer país, indústria ou mercado. O que varia é a relevância que cada risco terá em cada ambiente. Por exemplo, a disponibilidade de recursos humanos qualificados é um desafio para a implantação de PACs na área de TIC em qualquer local do mundo, mas certamente será um risco mais relevante em países menos desenvolvidos, onde a formação de profissionais de ponta em áreas como Eletrônica, Computação e Criptografia pode não ser suficiente para atender às necessidades de laboratórios, fabricantes e reguladores.

5- Metodologia Utilizada para a Proposta

5.1- Relação entre Controles e Riscos

Uma característica interessante em relação ao cenário avaliado em [Machado et al., 2018] é que diversos controles identificados, envolvem decisões que podem mitigar um conjunto de riscos ou intensificar outro conjunto. Por exemplo, o uso de padrões internacionais é uma forma de mitigar o risco de criação de barreiras técnicas ao comércio internacional e consequentes questionamentos pela Organização Mundial do Comércio. Por outro lado, tais padrões nem sempre são perfeitamente alinhados às necessidades nacionais, podendo levar a requisitos demasiadamente exigentes e de difícil atendimento pela indústria local.

Uma vez identificados os possíveis controles para mitigar os riscos, passamos à etapa de seleção dos controles mais indicados aos riscos críticos, identificados na área vermelha da Figura 9.

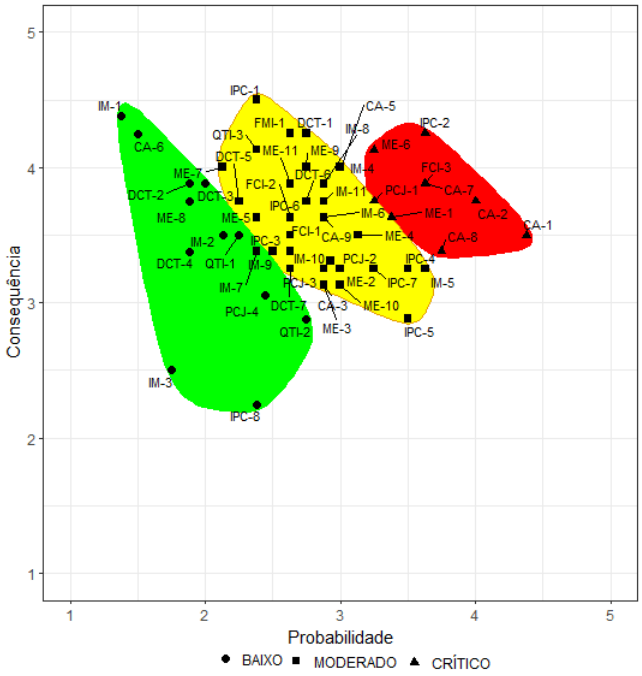


Figura 9 – Riscos identificados a partir de Machado et al. [2018].

Observa-se que os riscos ME-1, ME-6 e IPC-2, estão 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, o que sinaliza fortemente para uso de padrões internacionais.

Quanto aos riscos CA-1, CA-2, CA-7, CA-8, PCJ-1 e FCI-3, eles estão relacionados aos custos do processo regulatório. O controle aplicável para mitigar tais riscos é o uso de padrões personalizados ao cenário de cada mercado, o que, no entanto, entra em conflito com o uso de padrões internacionais definido no parágrafo anterior. Dessa forma, entendemos que uma estratégia apropriada é a referência a padrões internacionais, com a eliminação de requisitos e ensaios de altos custos.

Ainda podemos verificar que existem riscos que não atingiram um alto grau de criticidade, mas que devem ser considerados relevantes (IPC-2, IPC-6, IPC-7 e FMI-1). Recomenda-se para tais riscos, a utilização de boas práticas no processo regulatório, especialmente no que diz respeito a um estudo prévio do mercado, participação dos envolvidos e realização de consulta pública.

Controles relacionados ao tratamento de riscos de PACs na área de TIC podem ser complexos, tanto na sua identificação quanto à sua aplicação. Após a etapa de análise dos riscos, destacamos aqueles riscos que foram classificados como críticos, observados na Tabela 8, e que estão associados à qualidade técnica dos requisitos.

Desta pesquisa, foram extraídos os riscos classificados como críticos, observados na Tabela 8. Pode-se verificar que a maioria dos requisitos listados na Tabela estão associados à qualidade técnica dos requisitos.

Tabela 8 – Riscos Críticos. Fonte: Machado et al. [2018]

Cod.	Risco identificado	Média
CA-2	Onerar o processo de produção	15,00
CA-1	Onerar o processo de regulamentação	15,31
CA-7	Laboratórios apenas nas regiões S/SE	14,04
ME-6	Requisito prescritivo demais	13,40
CA-8	Organismos apenas nas regiões S/SE	15,65
FCI-3	Custo da certificação	14,04
IPC-2	Produto não conforme no mercado	15,40
ME-1	Falta de clareza no requisito/Interpretação equivocada	12,23
PCJ-1	Inexistência de laboratório acreditado	12,18

Após a detecção dos risos críticos, listamos na Tabela 9, os riscos moderados que

estavam no limiar para crítico.

Tabela 9 – Riscos com criticidade média. Fonte: Machado et al. [2018]

Cod.	Risco identificado	Média
CA-5	Ausência de laboratórios	12.00
IM-5	Dificuldade de compreensão sobre a regulamentação	11.78
DCT-1	Inadequação do regulamento	11.68
IPC-4	Ausência de comunicação sobre a regulamentação	11.37
FMI-1	Ineficácia do Regulamento em promover a melhoria no setor	11.15
IM-8	Aumento da informalidade	11.14
ME-9	Resultados não comparáveis	11.00

Os riscos listados foram utilizados nesta dissertação para a realização de uma pesquisa entre profissionais de segurança da informação, como forma de identificar a sua correta mitigação.

5.2- Questionário Baseado na Análise de Risco

A partir dos riscos considerados na Subseção 5.1, um questionário foi construído de modo a identificar quais práticas devem estar inseridas em um padrão nacional para avaliação de segurança em ambientes computacionais.

1. ME - Definição clara dos métodos de ensaio

   - ME-9 -Resultados não comparáveis(11,00)
     Para a efetividade de comparação dos resultados obtidos, devemos:
     (a) Definir uma norma ampla e abrangente
     (b) Definir uma norma concisa e restrita
     (c) Apenas seguir um padrão internacional
     (d) Adaptar um padrão existente
     (e) Ignorar normas ou padrões
   - ME-1 - Falta de clareza no requisito/Interpretação equivocada(12,23)
     Para evitar a falta de clareza ou interpretações errôneas nos requisitos para a segurança, devemos:
     (a) Utilizar padrão de documentação que detalhe ao máximo o requisito

(b) Utilizar padrão de documentação que seja apenas o suficiente para o entendimento dos requisitos

(c) Utilizar documentação padrão, com treinamento para o técnico responsável pelo levantamento

(d) Não utilizar documentação padrão, apenas realizar treinamento para o técnico responsável pelo levantamento

(e) Ignorar qualquer tipo de documentação

- ME-6 - Requisito prescritivo demais(13,40)

  Para evitar que uma norma venha a atrapalhar a regulação ou não seja adotada efetivamente, devemos:

  (a) Criar normas nacionais

  (b) Adotar simplesmente normas internacionais

  (c) Adaptar normas internacionais a realidade nacional

  (d) Melhorar primeiramente os requisitos

  (e) Não adotar normatização

2. IM - Quanto ao impacto no mercado

- IM-8 - Aumento da informalidade(11,14)

  Qual a melhor forma de se impedir a informalidade?

  (a) Adotar normas internacionais

  (b) Criar normas nacionais

  (c) Adaptar normas internacionais já existentes a realidade nacional

  (d) Melhorar a fiscalização

  (e) Não adotar normas

- IM-5 - Dificuldade de compreensão sobre a regulamentação(11,78)

  Como melhorar e divulgar uma regulamentação?

  (a) A regulamentação deve ser compreensível a todos, bastando sua publicação

  (b) Criar grupos de trabalho para o treinamento e divulgação das normas

  (c) Não devem existir normas para segurança

  (d) Criar publicações para a divulgação das normas

(e) Adaptar uma norma conhecida para não existir a necessidade de divulgação

3. FMI - Fortalecer o mercado Interno

- FMI-1 - Ineficácia do Regulamento em promover a melhoria no setor(11,15)
  Como a regulação pode promover uma melhora no mercado interno?
  (a) A regulação proverá a melhora da qualidade dos produtos
  (b) A regulação garantirá que os produtos podem ser auditados
  (c) A regulação incentiva uma melhoria técnica dos fornecedores
  (d) Para a regulação realmente ser eficiente, deve haver um órgão que possa garantir o controle sobre os laboratórios
  (e) Todas as questões acima

4. IPC - Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente

- IPC-4 - Ausência de comunicação sobre a regulamentação(11,37)
  A ausência de comunicação sobre a regulamentação pode causar grandes danos para uma implantação eficiente?
  (a) Sim, pois fornecedores podem continuar a produzir sem qualidade
  (b) Sim, pois os laboratórios não terão as informações necessárias para a avaliação
  (c) Não é necessário ter uma comunicação da regulamentação, somente a sua publicação é suficiente
  (d) A comunicação não é necessária para o consumidor final
  (e) Sim, pois fornecedores, laboratórios e consumidores não terão conhecimento da regulamentação
- IPC-2 - Produto não conforme no mercado(15,40)
  Um produto que não seja produzido conforme a regulamentação de mercado, pode prejudicar um país?
  (a) Não há necessidade de se criar uma regulamentação
  (b) Produtos que seguem regulamentações internacionais têm uma probabilidade de entrar em novos mercados

(c) Regulamentações nacionais podem ajudar a melhorar o mercado interno

(d) Produtos que seguem uma regulamentação têm uma maior qualidade

(e) Produtos que não sigam uma regulamentação podem prejudicar uma país em seu comércio

5. DCT - Quanto a disponibilidade de competência técnica

- DCT-1 -Inadequação do regulamento(11,68)
  A adoção de regulamentos para os quais não existam técnicos habilitados pode não ser efetivo?

  (a) Sim, deve-se apenas adotar regulações que possuam viabilidade técnica disponível

  (b) Sim, deve-se investir em cursos técnicos com os regulamentos adotados

  (c) Sim, a sua adoção deve ser precedida de um estudo de viabilidade técnica

  (d) Sim a existência de técnicos habilitados é essencial para a correta adoção de regulamentos

  (e) Todas as opções acima

6. CA - Quanto a custos aceitáveis

- CA-5 - Ausência de laboratórios(12,00)
  A ausência de laboratórios pode onerar o produto?

  (a) Sim, pois a utilização de laboratórios estrangeiros pode ser necessária

  (b) Sim, a ausência de laboratórios com competência técnica deve ser prevista antes da adoção de regulamentos

  (c) Sim, a ausência de laboratório sem competência técnica pode requerer que o poder público o faça

  (d) Sim, a utilização de laboratórios públicos pode não ser efetiva

  (e) Todas acima

  (f) Não onera

- CA-1- Onerar o processo de regulamentação(15,31)
  Como evitar que a adoção de uma regulamentação onere todo o processo de regulamentação?

  (a) Adotando normas internacionais

(b) Criando normas nacionais

(c) Adaptando normas internacionais a realidade nacional

(d) Adotando laboratórios públicos para regular a concorrência com os laboratórios particulares

(e) Criando todo um processo de divulgação, treinamento e cursos das normas envolvidas

- CA-2- Onerar o processo de produção(15,00)
  Como evitar que a adoção de uma regulamentação onere o processo de produção?

  (a) Adotando normas internacionais

  (b) Criando normas nacionais

  (c) Adaptando normas internacionais a realidade nacional

  (d) Adotando laboratórios públicos para regular a concorrência com os laboratórios particulares

  (e) Criando todo um processo de divulgação, treinamento e cursos das normas envolvidas

- CA-7- Laboratórios apenas nas regiões S/SE(14,04)
  CA-8- Organismos apenas nas regiões S/SE(12,65)
  Como levar laboratórios e organismos para todas as regiões?

  (a) Adotando laboratórios públicos

  (b) Criando todo um processo de divulgação, treinamento e cursos das normas envolvidas nas regiões com carências técnicas

  (c) Criando incentivos para a criação de novos laboratórios

  (d) Criando incentivos para que os laboratórios existentes criem filiais nas regiões carentes

  (e) Todas acima

7. FCI - Facilitar o comércio internacional

- FCI-3- Custo da certificação(14,04)
  Os custos envolvidos na certificação podem onerar os produtos, como realizá-la?

  (a) Adotando normas internacionais

(b) Criando normas nacionais

(c) Adaptando normas internacionais a realidade nacional

(d) Adotando laboratórios públicos para regular a concorrência com os laboratórios particulares

(e) Criando todo um processo de divulgação, treinamento e cursos das normas envolvidas

8. PCJ - Propiciar concorrência justa entre laboratórios

- PCJ-1- Inexistência de laboratório acreditado(12,18)
  Como proporcionar uma justa concorrência técnica entre os laboratórios?

  (a) Adotando normas internacionais

  (b) Criando normas nacionais

  (c) Adaptando normas internacionais a realidade nacional

  (d) Adotando laboratórios públicos para regular a concorrência com os laboratórios particulares

  (e) Criando todo um processo de divulgação, treinamento e cursos das normas envolvidas

6- Resultados e Discussões

Esta seção traz os resultados de uma meta–análise, a partir das respostas obtidas da aplicação do questionário apresentado na Subseção 5.2. O questionário foi respondido por diversos profissionais da área tecnológica, pública e privada, tais como segurança da informação e desenvolvimento de sistemas em diversos estados Brasileiros. A Figura 10 apresenta a área de atuação das empresas que participaram deste estudo, entre pública e privada.

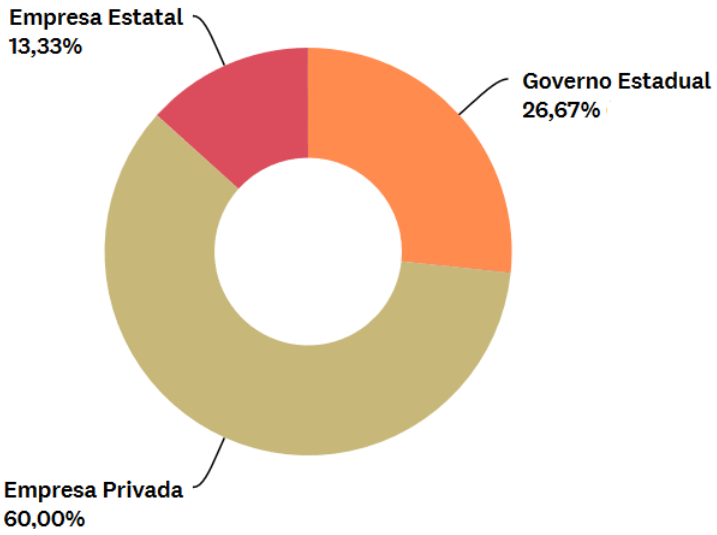


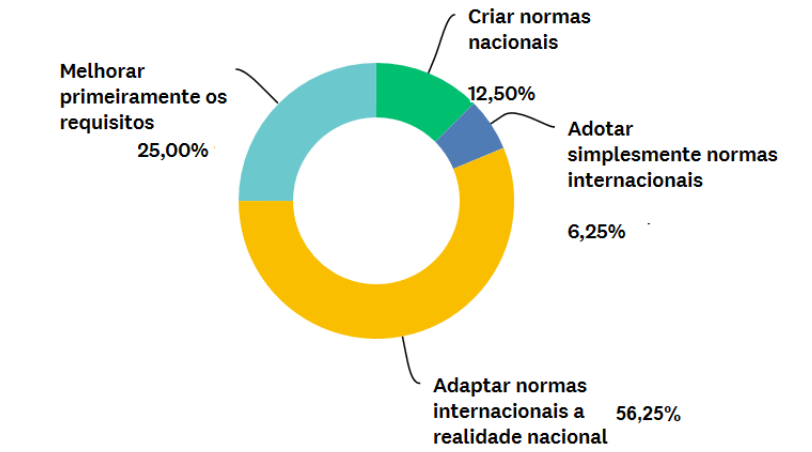
Figura 10 – Área de atuação da organização participante deste estudo, entre pública e privada.

Os resultados apresentados a seguir são relativos a um quantitativo de 16 respostas por parte de empresas, tendo obtido um balanceamento entre as empresas públicas e privadas quase que igualitário, conforme visto na Figura 10.

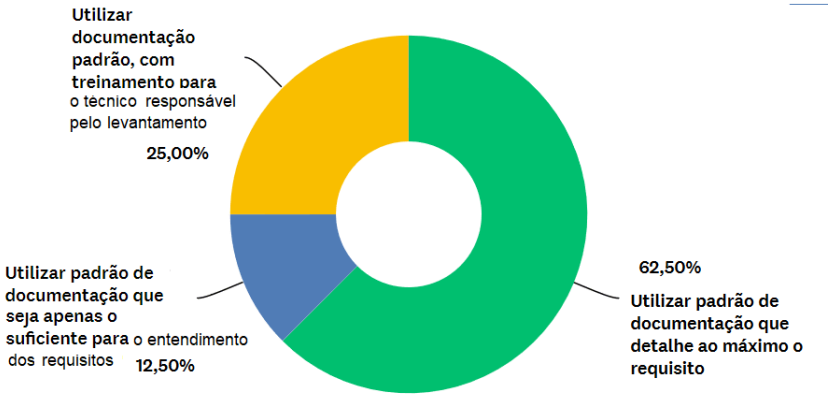
6.1- ME – Quanto a definição clara dos métodos:

Verifica-se na Figura 11, que a utilização de uma padronização ampla e abrangente, que detalhe ao máximo os requisitos, e que a adaptação de normas internacionais

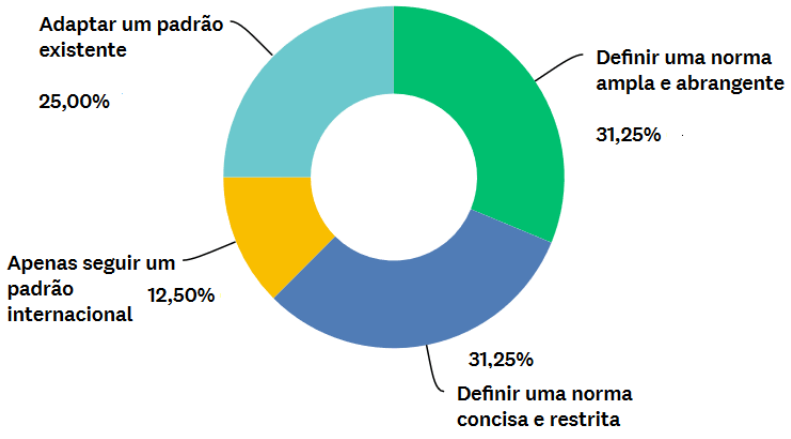
ao cenário Brasileiro é um caminho para implementar um padrão de segurança.



(a) ME-6



(b) ME-1

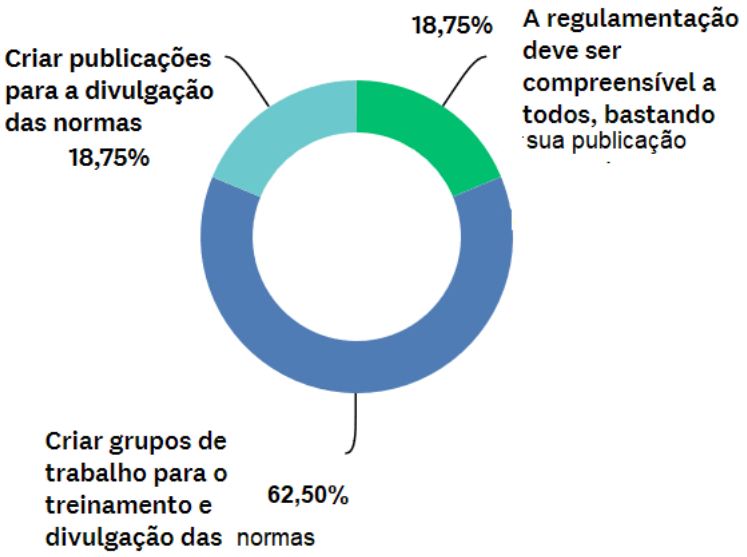


(c) ME-9

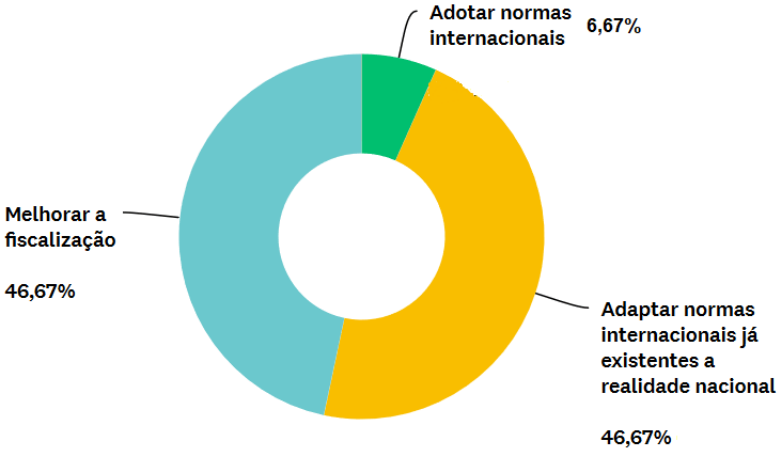
Figura 11 – Questões que tratam da definição clara dos métodos de ensaio.

6.2- IM – Quanto ao impacto no mercado:

Pode-se notar, a partir da Figura 12, que a criação de grupos de trabalho e a devida divulgação das normas aparece como a melhor forma de melhorar e divulgar um novo padrão. Além disso, quanto ao impedimento da informalidade, a pesquisa aponta a adaptação de normas internacionais à realidade nacional com a melhoria da fiscalização como o melhor caminho a ser seguido.



(a) IM-5



(b) IM-8

Figura 12 – Questões relativas ao impacto da criação de um padrão no mercado.

6.3- FMI – Quanto ao fortalecimento do mercado interno:

No que se refere ao fortalecimento do mercado interno, verifica-se nos resultados apresentados na Figura 13 que os respondentes entendem que o mercado se fortalecerá com a regulação, trazendo uma melhora na qualidade técnica dos fornecedores e dos produtos, possibilitando a auditoria dos mesmos. E ainda, para sua efetividade, há a necessidade de um órgão de controle sobre os laboratórios existentes.

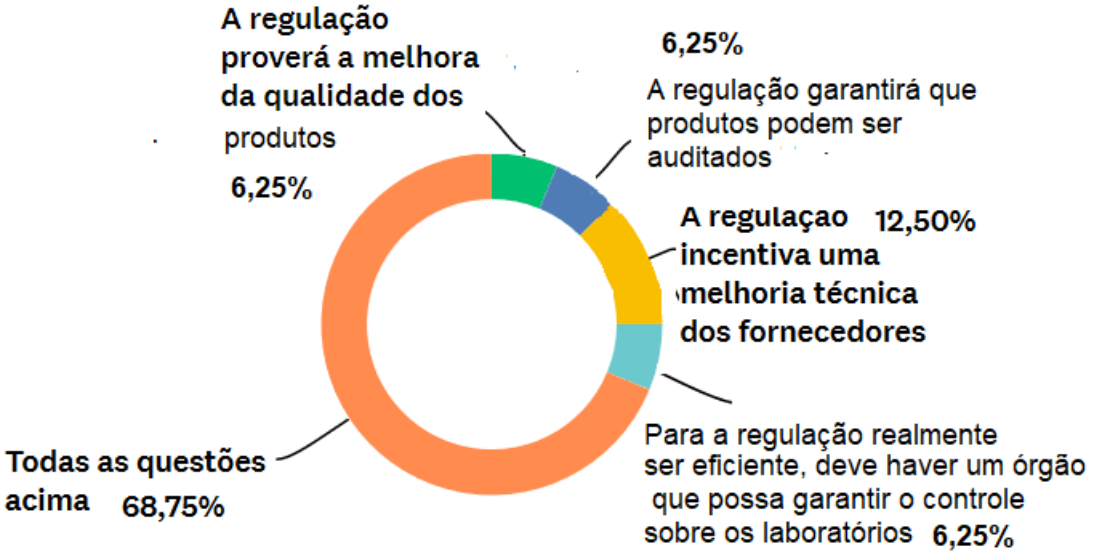
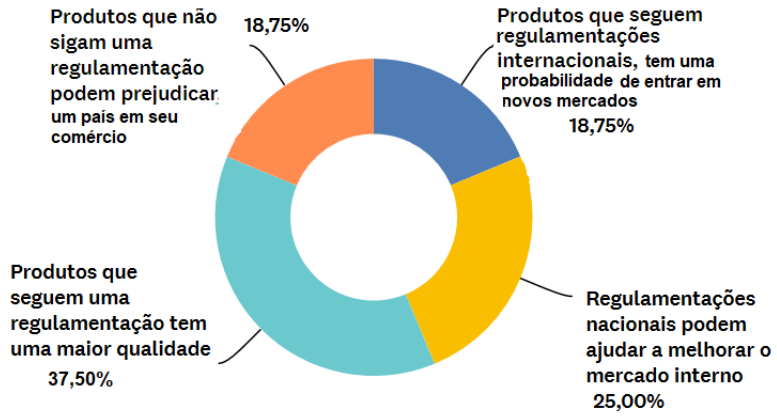


Figura 13 – Questão que diz respeito ao fortalecimento do mercado interno a partir da criação de um padrão.

6.4- IPC – Quanto às informações de proteção ao consumidor:

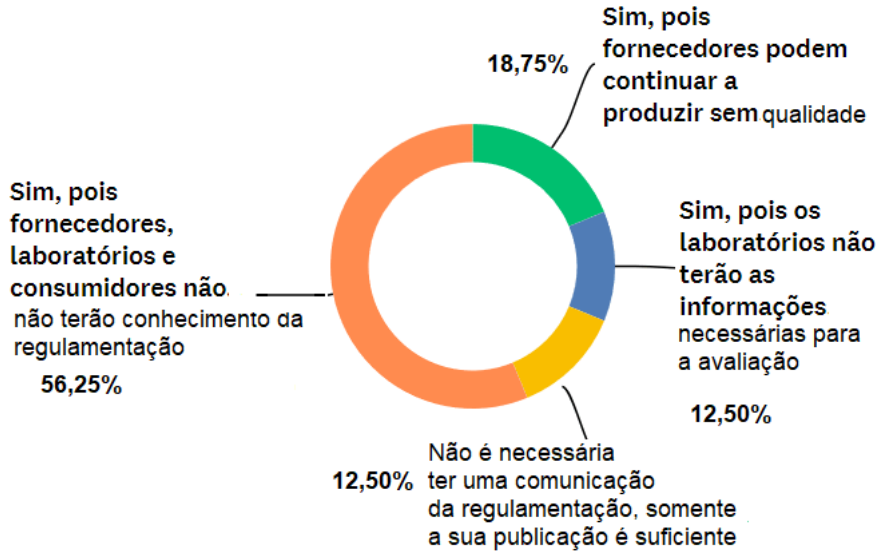
Com relação as informações de proteção ao consumidor quanto a saúde, segurança e meio ambiente podemos verificar, de acordo com as respostas apresentadas nas Figuras 14 e 15 , que os respondentes em sua maioria reconhecem que a regulamentação trará uma maior qualidade ao produto.

Contudo, pode-se notar que os respondentes verificam a necessidade da melhoria da informação à fornecedores, laboratórios e consumidores sobre essas regulamentações.



(a) IPC-2

Figura 14 – Questões sobre a informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente.



(a) IPC-4

Figura 15 – Questões sobre a informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente.

6.5- DCT – Quanto a disponibilidade de competência técnica:

No tocante a disponibilidade de competência técnica, podemos verificar a necessidade da adoção de regulações com viabilidade técnica, de acordo com a Figura 16. Para

tal, faz-se necessária a existência de cursos capazes de formar técnicos devidamente habilitados e informados a respeito dos regulamentos existentes.

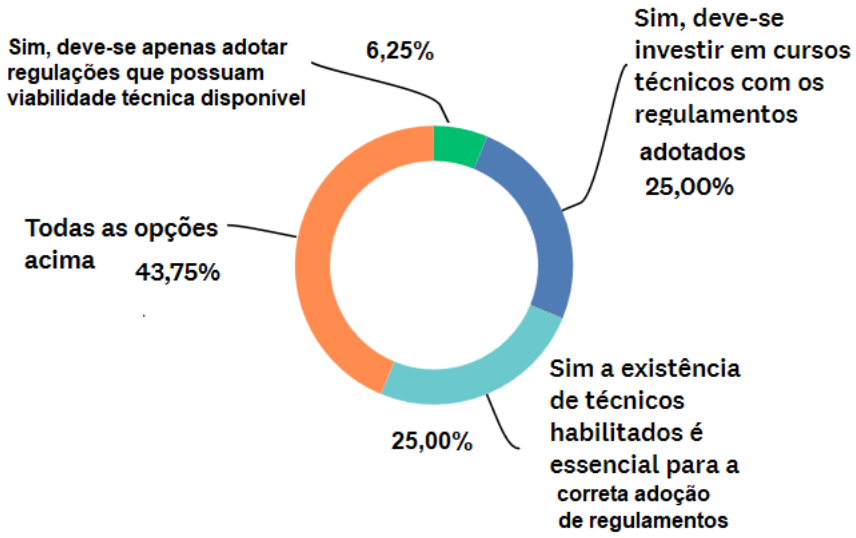
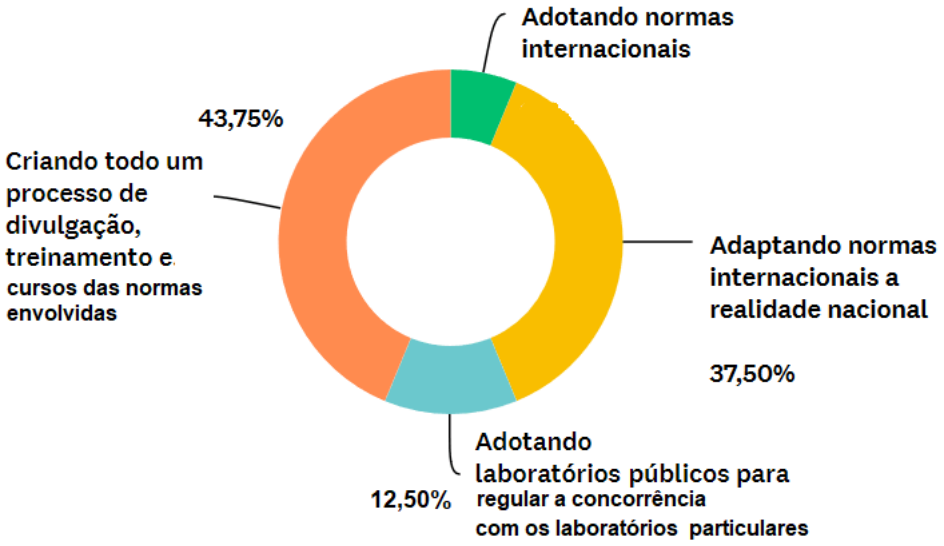


Figura 16 – Questão relativa à disponibilidade de competência técnica.

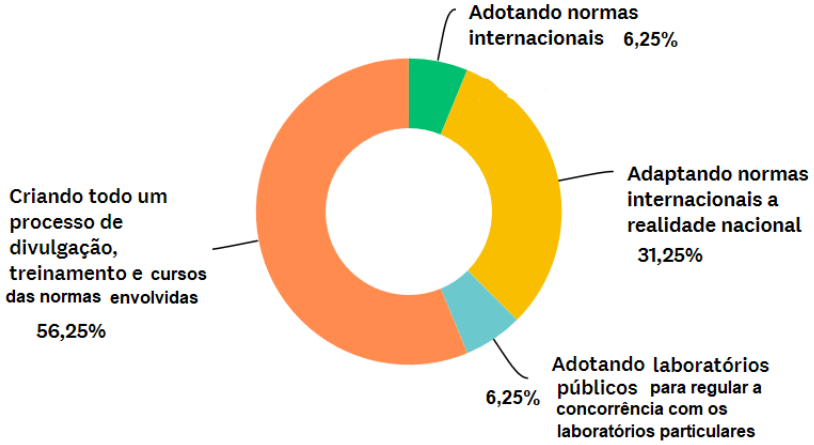
6.6- CA – Quanto aos custos adicionais:

No que diz respeito aos custos aceitáveis para a implementação de um padrão, podemos verificar nas Figuras 17 e 18, que a criação de um processo e divulgação, treinamento e custos da normas envolvidas é essencial. Porém, a adaptação de normas internacionais a realidade nacional é necessária, devendo ainda existir um processo de incentivos para a criação de novos laboratórios ou de abertura de filiais dos mesmos.

Pode-se verificar ainda que a não existência de laboratórios com competência técnica deve ser prevista antes da implantação de um padrão, podendo haver a necessidade da utilização de laboratórios estrangeiros, e ainda a necessidade de incentivos para a divulgação e treinamento para a implementação das normas em regiões onde existam carências técnicas.

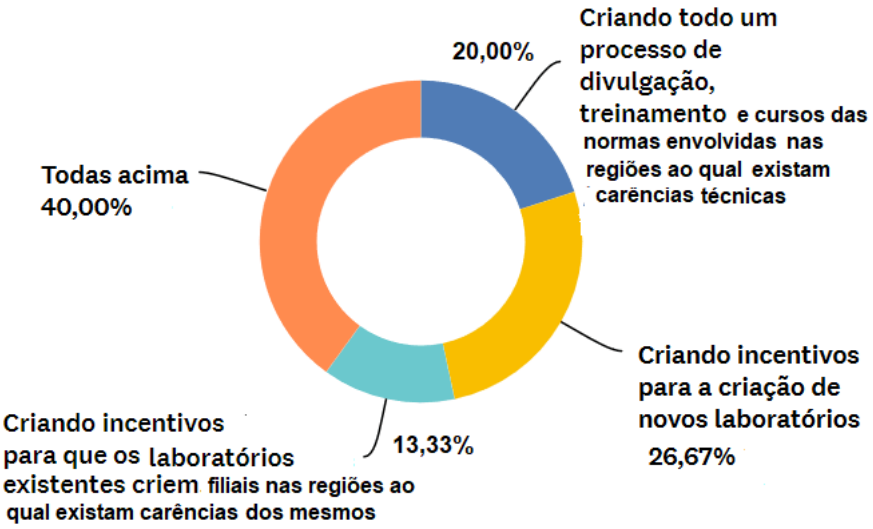


(a) CA-1

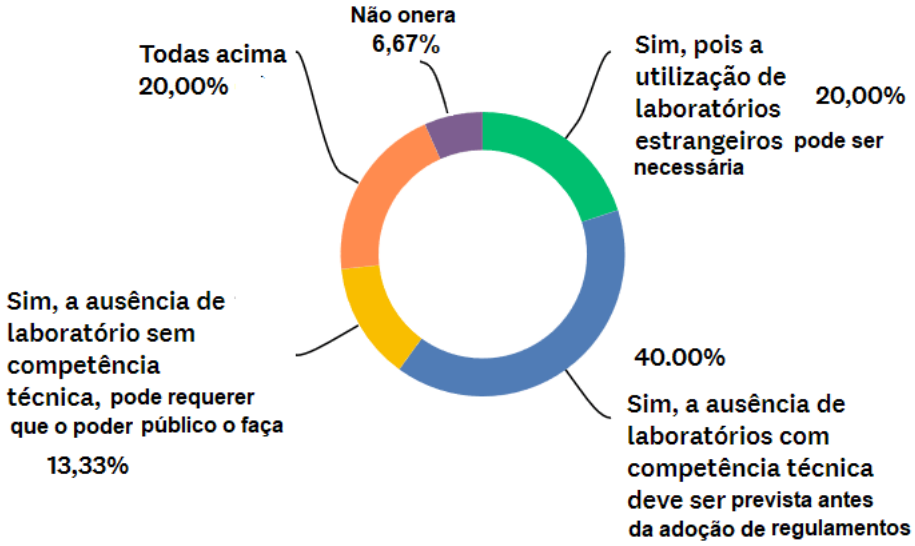


(b) CA-2

Figura 17 – Questões que tratam dos custos aceitáveis para a implementação de um padrão.



(a) CA-7 - CA-8



(b) CA-5

Figura 18 – Questões que tratam dos custos aceitáveis para a implementação de um padrão.

6.7- FCI – Quanto a facilitação do comércio internacional:

Quanto a facilitar o comercio internacional verifica-se na Figura 19 que a maioria dos respondentes indica a necessidade de criação de um processo de divulgação, treinamento e cursos das normas envolvidas.

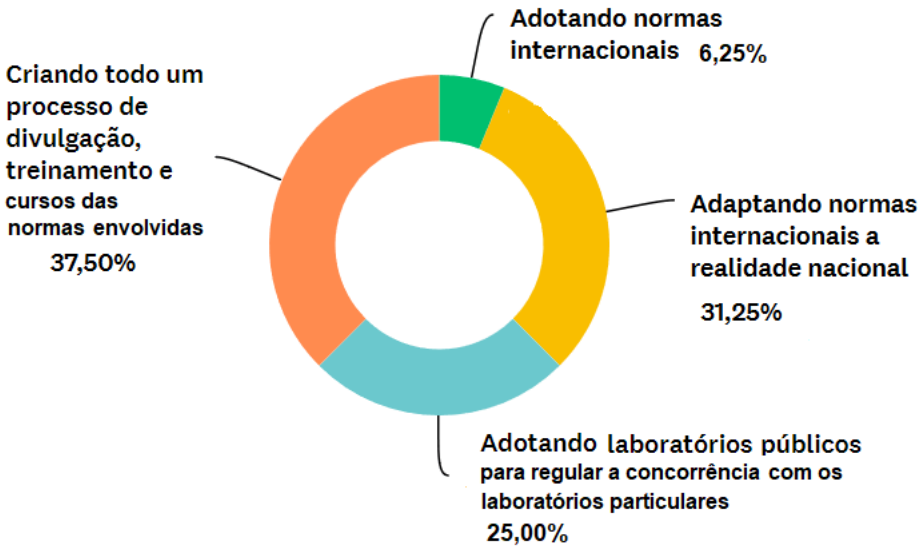


Figura 19 – Questão referente a facilitação do comercio internacional.

6.8- PCJ – Quanto a propiciação de concorrência justa:

Com relação a propiciar concorrência justa entre laboratórios verifica-se na Figura 20 que os respondentes em sua maioria nos indicam a necessidade de o poder público ter laboratórios próprios para ajudar na regulação.

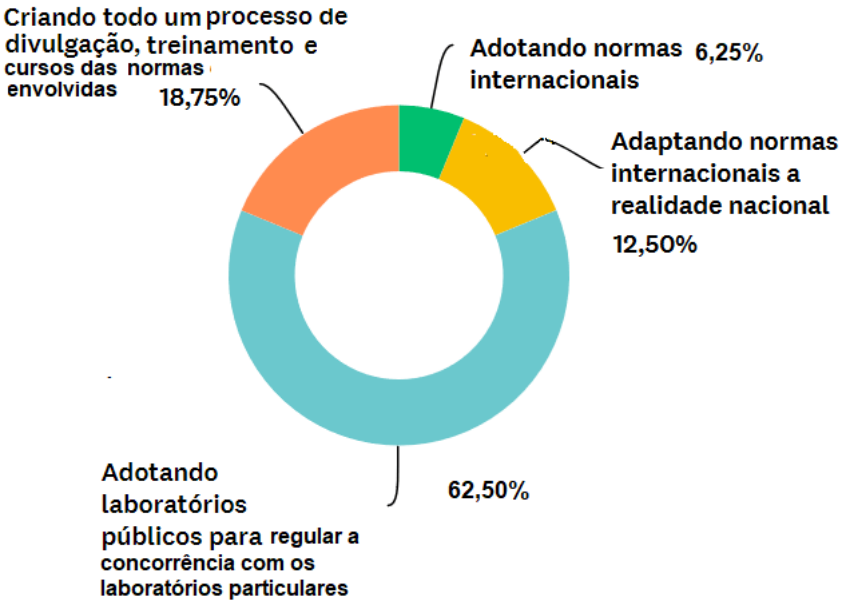


Figura 20 – Questão referente a propiciação de concorrência justa entre laboratórios.

6.9- Proposta do Padrão Brasileiro

Nesta seção, apresentamos uma lista de boas práticas a serem usadas na proposta de um padrão Brasileiro para avaliação de risco em ambientes computacionais. Esta lista baseia-se nos resultados apresentados na Seção 6.

- Adaptação de normas internacionais ao cenário Brasileiro;
- Padronização da documentação necessária para os requisitos de segurança;
- Criação de grupos de trabalho para divulgação e treinamento das normas;
- Incentivo para a criação de novos laboratórios;
- Adoção de laboratórios públicos como forma de regulação.

Sugere-se que toda norma a ser adotada possa seguir a proposta de boas práticas apresentada, incluindo os seguintes itens: seleção dos riscos que incluem a identificação, análise e a avaliação de riscos, análise das normas internacionais disponíveis, pesquisa dos riscos identificados e como resultado a seleção das análises dos estudos de casos envolvidos (mitigação) conforme a Figura 21.

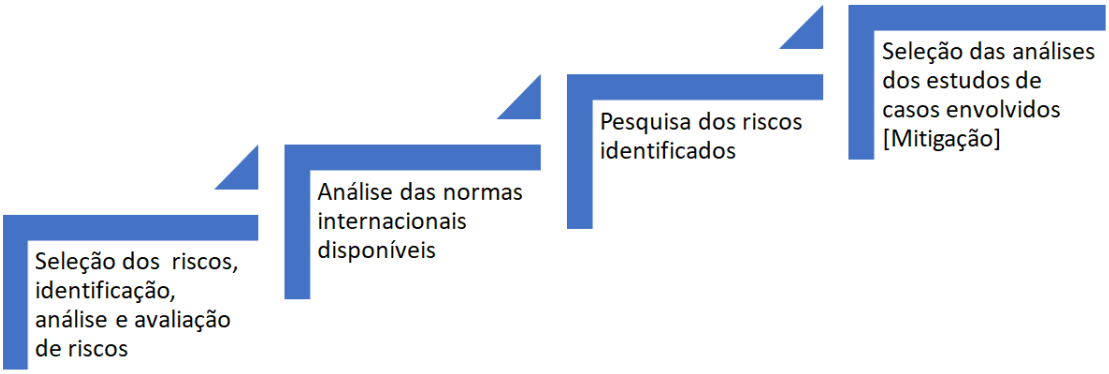


Figura 21 – Diagrama da proposta de padronização.

7- Considerações Finais

A base normativa é um dos elementos essenciais do sistema de homologação, sendo o plano básico para a operacionalização das certificações [National Institute of Standards and Technology, 2014]. Essa base normativa deve servir de alinhamento para uma arquitetura, conforme podemos verificar no *National Institute of Standards and Technology* (NIST), que é uma agência governamental ligada ao Departamento de Comércio dos Estados Unidos, em relação a confidencialidade, integridade e disponibilidade de sistemas federais norte-americanos de informações [Kissel et al., 2008].

A adoção de padrões internacionais é um caminho a ser trilhado. Entretanto, sua adoção pode trazer embutida grandes dificuldades na sua implementação, se regras nacionais e tradições não convergirem para a mesma. Por isso, a adoção parcial ou adaptação destas normas, pode ser a melhor solução para viabilizar as melhores práticas de mercado [Filho and Machado, 2017].

Assim sendo, neste trabalho um questionário foi desenvolvido e aplicado às empresas de tecnologia e segurança da informação, de modo que sirva de base para a proposição de um padrão Brasileiro de gerenciamento de risco para ambientes computacionais, através de uma lista de boas práticas. O questionário baseou-se em estratégias de análise dos risco críticos e médios que estivessem próximos aos riscos críticos; com isso, espera-se que o padrão proposto seja composto por normativas rígidas de segurança.

A partir dos resultados obtidos, pode-se perceber, principalmente, que adaptar normas internacionais ao cenário brasileiro é interessante porque podemos reduzir custo e tempo para implantação das normas, visto ainda o nível de maturidade do Brasil.

Referências Bibliográficas

Associação Brasileira de Normas Técnicas (2009a). *NBR ISO 31000: Gestão de riscos - Princípios e diretrizes*.

Associação Brasileira de Normas Técnicas (2009b). *NBR ISO 73: Gestão de riscos - Princípios e diretrizes*.

Associação Brasileira de Avaliação da Conformidade (2018). Avaliação a conformidade. Disponível em: https://www.abrac-ac.org.br/a-abrac/avaliacao-da-conformidade. Acesso em 10-07-2018.

Barafort, B., Mesquida, A. L., and Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards and Interfaces*, 54:176–185.

Barbalho, S., Miranda, R., Monteiro, S., and Reis, A. C. (2018). Diagnóstico dos processos de homologação e certificação de produtos de natureza cibernética: perspectivas para a construção de um sistema nacional. *Revista Produção Online*, 18.

Barrett, S. R. H., Speth, R. L., Eastham, S. D., Dedoussi, I. C., Ashok, A., Malina, R., and Keith, D. W. (2015). Impact of the volkswagen emissions control defeat device on us public health impact of the volkswagen emissions control defeat device on us public health. *Environmental Research Letters*, 10:114005.

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*.

Common Criteria (2012). Common criteria for information technology security evaluation part 1 : Introduction and general model september 2012 revision 4 foreword. Technical Report September, Common Criteria.

Common Criteria (2017). *Common Criteria for Information Technology Security Evaluation - Part 3 : Security assurance components*, volume 3.1.

Common Criteria (2018). Common criteria. Disponível em: https://www.commoncriteriaportal.org. Acesso em 22-06-2018.

Common Criteria Recognition Arrangement (2012). Common criteria management committee vision statement. Disponível em: https://www.commoncriteriaportal.org/vision.cfm. Acesso em 23-05-2018.

César, S., Barbalho, M., Carla, A., Reis, B., Borges, S., Monteiro, S., Carlos, J., Souza, F. D., and Oliveira, E. C. (2014). Fundamentos do sistema de homologação e certificação de produtos e serviços de defesa cibernética (shcdciber). *Brasília: Universidade de Brasília*.

Fernandes, W. A. (2011). *O Movimento da Qualidade no Brasil*, volume INMETRO. Essencial Idea Publishing.

Filho, C. R. G. V. and Machado, R. C. S. (2017). Estratégia para a internalização de padrões internacionais de segurança. In *Congresso Brasileiro de Metrologia (CBM)*, pages 1–4.

Gabinete de Segurança Institucional, Presidência da República (2015). Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf. Acesso em 19-07-2019.

Government of Hungary (2013). National cyber security strategy nº 1139/2013. Disponível em: https://www.enisa.europa.eu/news/enisa-news/new-cyber-security-strategy-hungary-and-worldwide. Acesso em 08-05-2018.

Häger, E. W. and Dackö, C. (2017). Cybersecurity law overview. Technical Report april, Mannheimer Swartling.

Hatton, L. and Genuchten, M. V. (2016). When software crosses a line. *IEEE Software*, 33(1):29–31.

Herrmann, D. S. (2002). *Using the Common Criteria for IT Security Evaluation*. Auerbach Publishers Inc.

INMETRO (2012). Avaliação da conformidade. a sociedade demanda. o inmetro faz. Technical report, INMETRO.

Inmetro (2018a). Certificação - avaliação da conformidade. Disponível em: http://www.inmetro.gov.br/qualidade/certificacao.asp. Acesso em 01-08-2018.

Inmetro (2018b). Declaração do fornecedor - avaliação da conformidade. Disponível em: http://www.inmetro.gov.br/qualidade/declaFornecedor.asp. Acesso em 01-08-2018.

Inmetro (2018c). Histórico do inmetro. Disponível em: http://www.inmetro.gov.br/inmetro/historico.asp. Acesso em 01-08-2018.

Inmetro (2018d). Inspeção - avaliação da conformidade. Disponível em: http://www.inmetro.gov.br/qualidade/inspecao.asp. Acesso em 01-08-2018.

Inmetro (2018e). Mecanismos de avaliação da conformidade. Disponível em: http://www.inmetro.gov.br/qualidade/mecanismo-de-avaliacao-conformidade.asp. Acesso em 01-08-2018.

Inmetro (2018f). Programa brasileiro de avaliação da conformidade. Disponível em: http://www.inmetro.gov.br/qualidade/pbac.asp. Acesso em 2018-03-17.

Instituto Brasileiro de Governança Corporativa (2007). *Guia de orientação para gerenciamento de Riscos Corporativos*. Number 3.

ISO/CASCO (2019). Using iso/casco standards in regulations. Disponível em: http://www.iso.org/sites/cascoregulators/documents/casco-regulators-fulltext.pdf. Acesso em 01-09-2018.

ITI (2016). Infraestrutura de chaves públicas otimizadora. Disponível em: http://www.iti.gov.br/images/servicos/homologacao/MCT-7__Vol.1_V_2.0_.pdf. Acesso em 10-09-2018.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., and Gulick, J. (2008). Security considerations in the system development life cycle. Disponível em: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf. Acesso em 20-07-2019.

Kröger, Wolfgang and Zio, Enrico (2011). *Vulnerable Systems*. Springer Publishing Company, Incorporated.

Locke, R. M. (2001). Construindo confiança - Avaliação da Conformidade (ISO/UNIDO). *Econômica*, 3(2):253–281.

Machado, R., Viana, C. R., Sousa, L. D., and Teles, C. A. M. D. S. (2018). Avaliação da conformidade de ativos de tecnologias : uma análise orientada a riscos. In *IV Workshop Sobre Regulação, Avaliação da Conformidade, Testes e Padrões de Segurança, 2018, Rio de Janeiro*.

Mellado, D., Fernández-Medina, E., and Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces*, 29(2):244–253.

Miller, B. and Rowe, D. (2012). A survey scada of and critical infrastructure incidents. *Proceedings of the 1st Annual conference on Research in information technology - RIIT '12*, page 51.

Ministério da Defesa do Exército (2015). Estudo de viabilidade preliminar do shcdciber. Departamento de Ciência e Tecnologia (DCT) Centro, Ministério da Defesa Comando do Exército, Partícipes.

National Information Assurance Partnership. About - national information assurance partnership. Disponível em : https://www.niap-ccevs.org/. Acesso em 28-02-2019.

National Information Assurance Partnership (2012). Frequently asked questions for niap / ccevs and the use of common criteria in the us. Disponível em: https://www.niap-ccevs.org/NIAP_Evolution/faqs/niap_evolution/FAQs28Mar_v6.pdf. Acesso em 28-02-2019.

National Information Assurance Partnership (2019). Frequently asked questions (faq). Disponível em: https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm. Acesso em 28-02-2019.

National Institute of Standards and Technology (2001). Fips 140-2. *Change*, 46(2):69. Acesso em 10-09-2018.

National Institute of Standards and Technology (2014). *NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations*.

Pilati, J. I. and Vieira Cancelier de Olivo, M. (2014). Um novo olhar sobre o direito à privacidade: caso snowden e pós-modernidade jurídica. volume 35, pages 281–300. Universidade Federal de Santa Catarina (UFSC).

Presidência da República - Casa Civil (2018). Lei 13.709/2018. Disponível em: http://www.planalto.gov.br/ccivil_03_ato2015-2018/2018/lei/L13709.htm. Acesso em 10-07-2019.

Presidência da República (2013). Decreto nº 8.135/2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm. Acesso em 01-08-2018.

Proenca, D., Estevens, J., Vieira, R., and Borbinha, J. (2017). Risk management: A maturity model based on iso 31000. In *2017 IEEE 19th Conference on Business Informatics (CBI)*, pages 99–108. IEEE.

Razzazi, M., Jafari, M., Moradi, S., Sharifipanah, H., Damanafshan, M., Fayazbakhsh, K., and Nickabadi, A. (2006). In *Proceedings - 2006 International Conference on Information and Communication Technologies: From Theory to Applications, ICTTA 2006*, volume 2, pages 3287–3292.

Reis Da Costa, S. R. and De Barros, M. (2012). Estudo comparativo do sistemas brasileiro de avaliação da conformidade com o sistema da comunidade europeia. VIII Congresso Nacional de Excelência em Gestão.

Symantec Corporation (2018). Symantec - Relatório de Ameaças à Segurança na Internet. Technical report, Symantec Corporation. Disponível em: https://www.symantec.com/pt/br/security-center/threat-report.

Trend Micro (2019). O ecossistema da iot está quebrado. como consertar isso? Disponível em: http://blog.trendmicro.com.br/o-ecossistema-da-iot-esta-quebrado-como-consertar-isso/. Acesso em 11-05-2019.

Vintimilla, A. D. O., Zenteno, J. A. C., and Burgos, F. J. B. (2017). Cryptographic standards applied to the public key infraestructure in south america. pages 14–32. Edição 23, Vol.6 – Nº 3.

Wang, T.-R., Pedroni, N., and Zio, E. (2016). Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent acts: A sensitivity-based decision-making approach. *Reliability Engineering & System Safety*, 147:9–18.

Zanon, S. B. (2016). Gestão e segurança da informação eletrônica: Exigências para uma gestão documental eficaz no Brasil. *Biblios: Revista electrónica de bibliotecología, archivología y museología*, 63(57):3.

Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (2017). Eu framework for certification and labelling limits and possibilities for iot security. Technical Report September 2017, ZVEI - German Electrical and Electronic Manufacturers. Disponível em: https://www.zvei.org/en/subjects/cyber-security/eu-framework-for-certification-and-labelling-limits-and-possibilities-for-iot-security/.

Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (2018). Horizontal Product Regulation for Cybersecurity. Technical Report December 2018. Disponível em: https://www.zvei.org/en/press-media/publications/horizontal-product-regulation-for-cybersecurity-whitepaper/.