Conjunto de Boas Práticas Baseadas na Avaliação de Risco para a Padronização Nacional em Ambientes Computacionais

Carlos R. G. Viana Filho[1,2], Marcelo Lintomen[1], Carlos A. M. S. Teles[3,2], Laura Silva de Assis[2], Felipe da Rocha Henriques[2]

[1]PRODERJ/RJ
[2]CEFET/RJ
[3]CLARO

carlos.filho@eic.cefet-rj.br,lintomen@proderj.rj.gov.br,
carlos.teles@eic.cefet-rj.br,{laura.assis,felipe.henriques}@cefet-rj.br

[1]

Abstract. *Nowadays, men, private and public companies, along with sereval devices have been more and more connected. This scenario, however, requires bigger responsibilities related to security, since vulnerabilities in personal computers, servers, softwares and devices can expose personal data, provide financial deviations, stop productions, endangering the security of critical infrastructure of contries. In Brazil, the approval of the new Brazilizan data protection law makes security crucial and part of the initial requirements for the development or maintenance of a system. Thus, the validation of these requisites to certify their compliance with the request becomes of great importance. In this work, we propose a set of good practices for the Brazilian scenario for risk evaluation in computational environments. A meta-analysis is considered to evaluate the proposal and, based on obtained results, we verified that the adaptation of international standards for the Brazilian scenario is a good alternative for large scale deployment, which can lead to the reduction in cost and time for companies.*

Resumo. *Atualmente, homens, empresas privadas e públicas, junto com vários dispositivos, têm estado cada vez mais conectados. Esse cenário, no entanto, exige maiores responsabilidades relacionadas à segurança, uma vez que vulnerabilidades em computadores pessoais, servidores, softwares e dispositivos podem expor dados pessoais, fornecer desvios financeiros, interromper a produção, colocando em risco a segurança da infraestrutura crítica de países. No Brasil, a aprovação da nova lei brasileira de proteção de dados torna a segurança crucial e parte dos requisitos iniciais para o desenvolvimento ou manutenção de um sistema. Assim, a validação desses requisitos para certificar seu cumprimento da solicitação se torna de grande importância. Neste trabalho, propomos um conjunto de boas práticas para o cenário brasileiro para avaliação de riscos em ambientes computacionais. Considera-se uma metanálise para avaliar a proposta e, com base nos resultados obtidos, verificamos que a*

[1]Cadernos do IME - Série Informática
e-ISSN: 2317-2193 (online)
DOI: 10.12957/cadinf.2021.56888

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.

1. Introdução

Nossa atual sociedade está totalmente dependente de sistemas e dispositivos. Essa dependência traz um ganho de qualidade e eficiência para os serviços prestados por empresas públicas e privadas, melhorando, assim, a vida das pessoas.

Segundo [Barafort et al. 2017], a Tecnologia da Informação (TI) se tornou fundamental para qualquer tipo de negócio. Podemos notar uma conexão cada vez maior entre pessoas, e entre os mais diversos tipos de dispositivos, sensores e máquinas à Internet, especialmente por meio da Internet das Coisas [Governo Federal Brasileiro 2018]. Com isso, nota-se que qualquer conteúdo armazenado ou transferido por organizações necessita de sistemas de informação para gerenciá-lo, podendo ser considerado como o seu principal ativo [Zanon 2016].

Esta dependência de sistemas computacionais conectados é ainda mais preocupante, quando voltada para as vulnerabilidades de infraestruturas críticas, por exemplo como as de usinas nucleares, e os diversos riscos os quais ela está exposta, sejam esses intencionais, aleatórios ou naturais. Isso passa a fundamentar a necessidade de análises para identificar possíveis fontes de vulnerabilidades desses sistemas, sua avaliação qualitativa e quantitativa, além da definição das intervenções necessárias para mitigar possíveis danos [Wang et al. 2016].

Assim, diversos países vêm caminhando para a implantação de programas de avaliação da conformidade na área de TI. Estes programas trazem as dificuldades inerentes a sua implantação, tais como: complexidade de especificação de requisitos e de ensaios de verificação; necessidade de uma mão de obra com alta qualificação para a execução de ensaios; execução apropriada dos ensaios pelos laboratórios; e custos de implementação dos fabricantes e da garantia da propriedade intelectual [Machado et al. 2018].

A associação alemã de fabricantes elétricos e eletrônicos afirma que o fortalecimento da segurança cibernética é importante e visa a utilização segura de aplicativos por parte dos clientes, haja vista que a ocorrência de incidentes de segurança pode impactar negativamente na confiança do consumidor em relação a sua marca [Zentralverband Elektrotechnik- und Elektronikindustrie e. V. 2017].

Nos Estados Unidos, o governo e as empresas são compelidos a utilizar regulações para garantir que seus sistemas cumpram os requisitos mínimos para os padrões federais para controle e segurança de sistemas de informação, como o *Common Criteria* (CC) e o NIST (*National Institute of Standards and Technology*) *Special Publication* (SP) 800-53 [Ministério da Defesa et al. 2015]. Para tal, é exigido que as empresas e seus sistemas possam de alguma forma mitigar os riscos de confidencialidade, integridade e disponibilidade que tenham a possibilidade de ser explorados. Deste modo, os operadores de sistemas devem ser capazes de: refletir as considerações técnicas dos documentos regulatórios; demostrar que cumprem determinados requisitos após um processo de acreditação; e assegurar que se advindos de terceiros, estejam em conformidade com as medidas de segurança adotadas pela organização, sejam tais sistemas compostos por serviços *web* ou

ainda em nuvem [Hale and Gamble 2019].

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 um item crucial no desenvolvimento e na 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 uma padronização nacional) 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.

Historicamente, verifica-se que as avaliações de risco possuem registro de mais de 2.400 anos, quando os atenienses verificavam os riscos antes de tomar decisões. Contudo, há menos de 50 anos que se enxerga a avaliação de riscos e a própria gestão de riscos como campo científico, quando surgem as primeiras publicações, assim como a criação de conferências com os fundamentos das ideias e princípios para essa área do conhecimento [Aven 2016].

De modo geral, o conceito de risco é trabalhado constantemente em diversas áreas, desde finanças, engenharia de segurança, saúde, transporte, segurança, gestão da cadeia de suprimentos e engenharia nuclear. A avaliação de risco precisa trabalhar com o tratamento, prevenção, redução, transferência e retenção dos riscos encontrados na mais diversas áreas - como as supracitadas. Assim sendo, a capacidade de se entender de maneira adequada os sinais graves para possíveis eventos de risco é essencial para uma precisa avaliação [Aven 2016]. Outrossim, todos os regulamentos de riscos estão fundamentados em princípios a serem usados no atendimento à determinada incertezas, riscos e possíveis imprevistos.

1.1. Objetivo e contribuições

Desse modo, este trabalho propõe um estudo sobre a padronização brasileira para avaliação de conformidade em ambientes computacionais fundamentado na análise de risco. De modo a analisar como se daria o padrão nacional proposto, um questionário estruturado foi proposto, baseado nos principais riscos encontrados na literatura, e aplicado em empresas de tecnologia, públicas e privadas. Uma meta-análise é realizada, e os resultados obtidos indicam que a adaptação de padrões internacionais para o cenário brasileiro é uma alternativa factível, o que poderia gerar a redução de custos e tempo por parte das empresas no processo de implantação de um padrão nacional. A partir da análise realizada, uma lista de boas práticas é apresentada como proposta de padronização. Por fim, dois estudos de caso são feitos, a partir da aplicação da metodologia proposta em uma empresa pública do RJ.

1.2. Estrutura

Este trabalho está organizado da seguinte maneira: uma revisão da literatura é apresentada na Seção 2. Na Seção 3 são apresentadas as definições para a avaliação da conformidade, padrões internacionais para a avaliação de sistemas, e o sistema de homologação e

certificação de produtos de defesa cibernética. Na Seção 4, a metodologia de pesquisa é apresentada, compondo os riscos considerados na proposta, e o questionário desenvolvido para a coleta de dados. A Seção 5 apresenta os resultados obtidos a partir das respostas dos questionários, que gerou uma lista de boas práticas para uma padronização nacional apresentada na Seção 6. Um estudo de casos da aplicação da proposta de padrão é apresentado na Seção 7. Por fim, as conclusões são discutidas na Seção 8.

2. Trabalhos Relacionados

Nesta seção, traremos uma revisão da literatura sobre a importância da segurança da informação e de gerenciamento de riscos em sistemas computacionais.

Os autores de [Soares et al. 2021] discutem a importância da implementação de uma política de segurança da informação dentro das organizações, de sorte a poderem proteger as suas informações. Os autores desenvolveram uma proposta de política de segurança de informação aplicada em uma instituição de ensino através de um estudo de caso.

Já o trabalho de [Lyu et al. 2019] realiza uma revisão da literatura sobre técnicas de gerenciamento de risco e segurança para Sistemas Ciber-físicos (do inglês, *Cyber Physical Systems* - CPS) [Zanero 2017], [Alguliyev et al. 2018]. Os autores destacam a importância desse tipo de sistema, atualmente considerado como o núcleo da Indústria 4.0 [Pivoto et al. 2021]. Os autores concluem constatando que ainda há várias lacunas a serem preenchidas na integração entre a segurança e os sistemas ciber-físicos. A falta de algoritmos para resolver conflitos de segurança, e a necessidade de técnicas de gerenciamento de risco que atuem *online* (em tempo real) são dois desses exemplos, ainda a serem explorados por novas pesquisas.

Em [Cho et al. 2019], os autores fazem uma revisão da literatura acerca de métricas, medidas, atributos de métricas e ontologias associadas à sistemas de segurança. Nesse contexto, eles propõem um arcabouço de métricas de acreditação chamado de STRAM (*Security, Trust, Resilience, and Agility Metrics*). Os autores aplicam o sistema proposto para avaliar a qualidade de sistemas computacionais, e discutem os principais desafios e limitações observados por eles.

O gerenciamento de riscos é discutido em [Zio 2018], onde o autor investiga possibilidades de uso de simulações para análise de risco, e o uso de dados para realizar um monitoramento contínuo para o que se chama de "gerenciamento dinâmico de risco" [Villa et al. 2016]. Além disso, propostas são elaboradas levando-se em consideração a aplicação do gerenciamento de risco de segurança em sistemas ciber-físicos. Já um estudo mais recente investiga a segurança de sistemas ciber-físicos de energia (do inglês, *cyber-physical energy systems*) [Zografopoulos et al. 2021]. Neste artigo, os autores propõem um modelo de ameça, onde se consegue identificar quais são os principais pontos de vulnerabilidade do sistema. Além disso, um processo de gerenciamento de riscos é proposto, de sorte a avaliar o nível de criticidade do sistema. A proposta dos autores é analisada através de estudos de caso.

Em [Murashbekov 2019], podemos notar algumas das grandes dificuldades da segurança da informação, utilizando um método de moderação, com a criação de um sistema de auditoria de sistemas da informação, além de um sistema de informação e analítico para

formar indicadores nacionais. Com isso o monitoramento constante torna-se necessário, tendo em conta a dinâmica das mudanças socioeconômicas, e a escalada de ameaças cibernéticas. O trabalho ainda indica que a identificação, a categorização e o registro são são problemas difíceis não apenas no Cazaquistão (local onde se aplicou a referida pesquisa), mas também em diversos outros locais e com soluções diversas de acordo com suas respectivas particularidades.

Através dos trabalhos supracitados, podemos perceber que a aplicação de métodos de gerenciamento de riscos em sistemas de segurança da informação é uma proposta que tem sido discutida atualmente. Além disso, a formação de indicadores nacionais é importante. Nesse contexto, destacamos como contribuição deste trabalho a proposta de um conjunto de boas práticas para a avaliação de risco em sistemas computacionais, em um cenário brasileiro.

3. Fundamentação Teórica para Avaliação da Conformidade

De acordo com a definição do Inmetro, a avaliação da conformidade é um "procedimento que objetiva prover adequado grau de confiança em um determinado produto, mediante o atendimento de requisitos definidos em normas ou regulamentos técnicos" [INMETRO 2018].

Com a adoção da avaliação da conformidade, pode-se demonstrar que requisitos especificados de determinados sistemas ou produtos estão sendo devidamente atendidos pelos fabricantes. Logo, pode-se melhorar sua competitividade no mercado, pois passa-se a obter determinados níveis de qualidade para as suas mercadorias, comprovando, desse modo, que os requisitos para os sistemas e produtos foram efetivamente seguidos e aplicados [ABNT 2005, Furtado and Laperrière 2011].

A avaliação da conformidade é dividida em três partes, sendo a primeira parte aquela em que o produto tem declarações de conformidade, sejam elas dos fornecedores ou dos fabricantes; na segunda parte, o adquirente do produto passa a realizar a avaliação da conformidade; na terceira, as avaliações são realizadas por entidades independentes [ISO/CASCO 2019].

Dentre os órgãos internacionais capazes de definir padrões de avaliação de conformidade, destacam-se: a *International Organization for Standardization* (ISO) / *International Electrotechnical Commission* (IEC) 15.408, derivada da norma *Common Criteria*, que estabelece critérios de avaliação de segurança [Sun et al. 2012], e que será mais detalhada na Subseção 3.1. Além do *Common Criteria*, ainda traremos como fundamentação teórica para este trabalho: o NIST SP 800-53; uma abordagem de perfis de proteção colaborativa; uma abordagem horizontal utilizada na Alemanha; e o sistema de homologação e certificação de produtos para a defesa cibernética, nas subseções seguintes.

3.1. *Common Criteria*

O *Common Criteria* é um padrão internacional para a certificação de TI que tem por objetivo fornecer ao usuário uma estrutura que possa assegurar que os requisitos de garantia e segurança funcional foram devidamente implantados [Barbalho et al. 2018].

Segundo [César et al. 2014], o *Common Criteria* pode ser aplicado em diversos aspectos de segurança, mesmo aqueles que são gerados a partir de atividades humanas.

Para assegurar a segurança, ele define sete níveis de garantia de avaliação, ou *Evaluation Assurance Level* (EAL), sendo que a cada nível é adicionado um componente de requisito de segurança para os produtos de TI, e que as definições desses requisitos, a partir de um objetivo de avaliação - *Target of evaluation* (TOE) - estão expressas em um *Protection Profile* (PP), para ater a necessidades específicas dos clientes.

3.2. NIST SP 800-53: Controles de segurança recomendados para sistemas de informações federais

O trabalho de [National Institute of Standards and Technology 2014] foi desenvolvido pelo NIST, dentro de uma força tarefa, na qual destaca-se como participante o Departamento de Defesa dos Estados Unidos, através da comunidade de inteligência, em conjunto com o departamento de Defesa e o Comitê de Sistemas de Segurança Nacional. Em sua quarta revisão, este documento oferece uma visão mais abrangente no que se refere à segurança da informação e ao gerenciamento de risco, entregando às organizações a amplitude necessária dos controles de segurança, sendo estes indispensáveis aos sistemas de informações, permitindo que eles se fortaleçam dos contra-ataques cibernéticos [National Institute of Standards and Technology 2014].

Esta revisão se deu pelo grande aumento do número de ataques cibernéticos, além de sua crescente sofisticação e profissionalização. Para tanto, o documento mencionado aborda áreas como: computação móvel e em nuvem; segurança de aplicativos; fidedignidade, garantia e resiliência dos sistemas de informação; ameaça interna; segurança da cadeia de suprimentos; e a ameaça persistente avançada.

Para proporcionar um melhor controle e uma estrutura metodológica com os requisitos mínimos de segurança exigidos, este padrão divide-se em 18 grupos, ou famílias, que incluem: controle de acesso, conscientização e treinamento, auditoria e responsabilização, avaliação de segurança e autorização, gerenciamento de configurações, planejamento de contingência, identificação e autenticação, resposta a incidentes, manutenção, proteção de mídia, proteção física e ambiental, planejamento, segurança pessoal, avaliação de risco, aquisição de sistemas e serviços, sistema e proteção de comunicações, integridade do sistema e da informação e gestão de programas.

Em seu apêndice H, o [National Institute of Standards and Technology 2014] demonstra, ainda, sua compatibilização (a partir do mapeamento com padrões internacionais de segurança da informação) com a ISO 15408 (*Common Criteria*) e com a ISO 27001 (sistema de gestão da segurança da informação). Desse modo, gera-se uma maior segurança na implantação do NIST SP 800-53, pois consegue-se especificar e atestar um determinado conjunto de funcionalidades de segurança, a partir das compatibilizações supracitadas [National Institute of Standards and Technology 2014].

3.3. Perfis de proteção colaborativos

O perfil colaborativo é uma iniciativa de comunidades técnicas internacionais, governos, indústrias, academia e usuários para a criação de uma abordagem conjunta do PP (*Protection Profile*). Desse modo, não se faz necessária a especificação do *Evaluation Assurance Level*, criando assim perfis de avaliação mais consistentes e repetíveis [National Information Assurance Partnership].

Em [CCRA 2014], verifica-se que perfis de proteção colaborativos e seus anexos relacionados definem um conjunto mínimo de requisitos funcionais de segurança e suas garantias, incluindo as análises de vulnerabilidades para a garantia de que os produtos certificados possam atingir o nível desejado de segurança.

O perfil de proteção colaborativo não pode depender exclusivamente de esquemas nacionais de avaliação da conformidade. Por outro lado, esse perfil deve se referir claramente a padrões internacionais para criptografia, e ainda permitindo a utilização dos demais protocolos nacionais, bem como possibilitando a inclusão de componentes do EAL entre os níveis 2 e 4 quando requisitado [CCRA 2014].

Os resultados destes níveis devem exigir que os requisitos funcionais de segurança estejam elencados no *Protection Profile*, permitindo que eles possam ser comparados coerentemente com a documentação de cada requisito. Por fim, espera-se ainda que eles possam ser comunicados através dos esquemas do *Common Criteria Recognition Arrangement* (CCRA) garantido desta forma seu reconhecimento mútuo por todos os países participantes, e que uma diversidade de tecnologias possa ser acreditada através da avaliação dos fornecedores [CCRA 2014].

Nos Estados Unidos, o *National Information Assurance Partnership* está envolvido com diversos atores do sistema de segurança nacional para garantir que os *Protection Profiles* tenham uma certificação simplificada para seus produtos, em conjunto com a documentação do Departamento de Defesa dos Estados Unidos [National Information Assurance Partnership 2012].

3.4. Abordagem horizontal

Na Alemanha, pode-se encontrar uma proposta de regulação horizontal do produto para a cibersegurança, que utiliza a responsabilidade compartilhada entre as partes interessadas, sejam fabricantes, usuários ou indústrias. Para alcançar o objetivo da proteção desejada, ações devem ser implementadas, para que os produtos finais tenham a robustez necessária para a cibersegurança [Zentralverband Elektrotechnik- und Elektronikindustrie e. V. 2018]. Além disso, define-se que, para haver uma regulamentação mais eficaz, alguns princípios devem ser considerados, tais como:

- **Princípio da Melhor Regulamentação:** regulamento com os objetivos de proteção geral, classificação de risco, flexibilidade dos fabricantes na aplicação de disposições, inserção de normas internacionais, compatibilidade internacional e aceitação pela Organização Mundial do Comércio, além da neutralidade em relação a tecnologia e soluções.
- **Princípio SMERC para requisitos:** *Specific* - os requisitos são considerados conforme a aplicação; *Measurability* - os requisitos devem ser mensuráveis e passíveis de verificação; *Enforceability* - a autoridade responsável pela fiscalização deve ter capacidade de verificação dos requisitos; *Relevance* - os requisitos devem ser relevantes para a segurança; *Competition-friendly* - não deve haver impactos prejudiciais à competitividade.

Segundo [Zentralverband Elektrotechnik- und Elektronikindustrie e. V. 2018], o princípio SMERC garante que os requisitos correspondam aos recursos do produto, garantindo que ajustes possam ser executados a qualquer momento, e tenha aplicação para a

Internet das Coisas. Assim, a disponibilidade, a integridade e a confidencialidade podem ser utilizadas de maneira horizontal à todas as áreas de aplicação, podendo existir uma priorização conforme sua avaliação de risco e análise de ameaças.

A abordagem horizontal traz a vantagem de formular requisitos uniformes para a cibersegurança através de regulamentos editados entre organismos de normatização ou outras plataformas, criando uma base de produtos que têm medidas uniformes, abrangentes e confiáveis. Essa abordagem permite que empresas, indústrias, governos e diversos setores, quando exijam requisitos mais rigorosos de segurança, mantenham as especificidades mesmo quando elas vão além das condições básicas de cibersegurança [Zentralverband Elektrotechnik- und Elektronikindustrie e. V. 2018].

3.5. Sistema de homologação e certificação de produtos de defesa Cibernética

Quando se considera o tema de "defesa cibernética", destaca-se, dentre outros casos, o escândalo de espionagem *Snowden*, em que os e-mails e o telefone da ex-presidente Dilma Rousseff foram alvos de espionagem. Desde então, o Governo passou a adotar ações nesse campo da segurança, como a criação de uma Escola Nacional de Defesa Cibernética, e um Sistema Nacional de Homologação e Certificação de Produtos de Defesa Cibernética [Barbalho et al. 2018].

A certificação de produtos e serviços de defesa cibernética atualmente é uma necessidade imediata. O benefício que atualmente temos com a utilização e conectividade de computadores, celulares, relógios inteligentes e Internet das Coisas, trazem também embutidos os aspectos da privacidade do indivíduo [César et al. 2014]. Nesse sentido, a administração pública federal criou a Política Nacional de Segurança da Informação, com o intuito de garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em nível nacional [Presidência da República 2019].

A Política Nacional de Segurança da Informação tem como objetivos: proporcionar a segurança do indivíduo, da sociedade e do Estado; impulsionar pesquisas científicas e inovação; aprimorar as normatizações referentes a segurança da informação; estimular a qualificação de mão de obra necessária; estimular o conhecimento da segurança da informação na sociedade; orientar ações sobre a custódia dos dados por entes públicos, segurança da informação em infraestruturas críticas; gerar a proteção dos dados de pessoas que possam ter sua segurança ou de suas atividades afetadas; realizar o tratamento das informações; e contribuir para a memória cultural do Brasil.

Conforme [Barbalho et al. 2018], a certificação de equipamentos de tecnologia de informação é baseada na existência de laboratórios de certificação, sendo seus resultados inclusos em relatórios técnicos e acreditados por organismos internacionais. Desse modo, deve-se criar um determinado nível de garantia e confiabilidade para os ativos de tecnologia envolvidos. Nesse sentido, a criação de um padrão brasileiro para a avaliação de conformidade de sistemas e ambientes computacionais faz-se importante no combate a possíveis ataques, desde a fabricação de produtos e *softwares*.

4. Metodologia Utilizada para a Proposta

4.1. Avaliação baseada no risco

Em [Machado et al. 2018], uma lista de riscos foi definida, sendo classificados como de baixa, média e alta criticidade, conforme pode-se verificar na Figura 1, e listados a seguir.

Como forma de classificação, segundo [Machado et al. 2018], especialistas em Regulação e especialistas em Tecnologia da Informação foram entrevistados e atribuíram uma nota, numa escala de 1 a 5, para a probabilidade de ocorrência de cada risco, considerando o seu impacto, caso o risco se concretize. Após essa etapa, calculou-se a média da probabilidade de ocorrência desses riscos e o impacto sobre as respostas. Desse modo, os riscos foram classificados como: **Risco Baixo**, se o valor do indicador de risco foi menor que 8; **Risco Médio**, se o valor de risco foi de 8 a 12; e **Risco Crítico**, se o valor de risco foi superior a 12.

Esse riscos foram agrupados pela classificação, quais sejam: ME- Definição clara dos métodos de ensaio; IM- Quanto ao impacto no mercado; FMI- Fortalecer o mercado Interno; IPC- Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente; DCT- Quanto a disponibilidade de competência técnica; CA- Quanto a custos aceitáveis; FCI- Facilitar o comércio internacional; PCJ- Propiciar concorrência justa entre laboratório.

1. **Riscos de baixa criticidade:**
    - **ME-8:** Controle de qualidade dos processos e equipamentos
    - **IM-1:** Prejuízo total do mercado nacional
    - **IM-2:** Prejuízo parcial do mercado nacional
    - **IM-3:** Barreira técnica à importação
    - **CA-6:** Ausência de organismos
    - **DCT-2:** Inviabilizar o processo produtivo
    - **DCT-3:** Inviabilizar as avaliações por parte dos laboratórios
    - **DCT-4:** Inviabilizar as avaliações por parte dos Organismos de Avaliação da Conformidade
    - **QTI-1:** Comprometimento da propriedade intelectual
    - **QTI-2:** Falta de controle interno de acesso adequado
    - **IPC-8:** Não acesso a um público especializado
    - **PCJ-4:** Gerar monopólio/oligopólio entre organismos
2. **Riscos de média criticidade:**
    - **ME-2:** Diferença nos resultados entre laboratórios
    - **ME-3:** Excesso de requisitos desnecessários
    - **ME-4:** Custo dos ensaios
    - **ME-5:** Requisito rigoroso demais
    - **ME-7:** Interpretação errônea dos dados internos
    - **ME-9:** Resultados não comparáveis
    - **ME-10:** Ausência de material de referência
    - **ME-11:** Requisito mal definido
    - **IM-4:** Dificuldade de adequação à regulamentação
    - **IM-5:** Dificuldade de compreensão sobre a regulamentação
    - **IM-6:** Desconhecimento do setor quanto à regulamentação
    - **IM-7:** Formação de monopólios/oligopólios
    - **IM-8:** Aumento da informalidade
    - **IM-9:** Aumento do desemprego
    - **IM-10:** Dificuldade de interação com o regulamentador participação em Comissões
    - **IM-11:** Atendimento de interesses de uma empresa/setor

- **CA-3:** Desequilíbrio entre organismos de avaliação da conformidade
- **CA-4:** Desequilíbrio entre laboratórios
- **CA-5:** Ausência de laboratórios
- **CA-9:** Desinteresse de laboratório e organismos pelo escopo
- **DCT-1:** Inadequação do regulamento
- **DCT-5:** Perda da confidencialidade
- **DCT-6:** Perda de dados
- **DCT-7:** Gerar monopólio/oligopólio entre laboratórios
- **DCT-8:** Gerar monopólio/oligopólio entre organismos
- **QTI-3:** Confidencialidade no processo de avaliação
- **IPC-1:** Ineficácia do regulamento
- **IPC-3:** Regulamento não compreendido pela sociedade
- **IPC-4:** Ausência de comunicação sobre a regulamentação
- **IPC-5:** Crítica ao regulamento
- **IPC-6:** Índice de rejeição à regulamentação pela sociedade
- **IPC-7:** Comunicação ineficiente sobre a regulamentação
- **PCJ-2:** Desequilíbrio entre laboratórios
- **PCJ-3:** Gerar monopólio/oligopólio entre laboratórios
- **FCI-1:** Requisitos desalinhados com requisitos internacionais
- **FCI-2:** Requisitos obsoletos em relação a requisitos internacionais
- **FMI-1:** Ineficácia do regulamento em promover a melhoria no setor

3. **Riscos de alta criticidade:**
    - **ME-1:** Falta de clareza no requisito/Interpretação equivocada
    - **ME-6:** Requisito prescritivo demais
    - **CA-1:** Onerar o processo de regulamentação
    - **CA-2:** Onerar o processo de produção
    - **CA-7:** Laboratórios apenas nas regiões S/SE
    - **CA-8:** Organismos apenas nas regiões S/SE
    - **IPC-2:** Produto não conforme no mercado
    - **PCJ-1:** Inexistência de laboratório acreditado
    - **FCI-3:** Custo da certificação

Como forma de verificação para a correta implantação de programas de avaliação da conformidade, neste trabalho, foram selecionados os Riscos Críticos, e os Riscos Médios que estavam próximos a área crítica, conforme apresentados na Tabela 1.

Tabela 1. Riscos pertencentes à área crítica.

ME- Definição clara dos métodos de ensaio	ME-6 - Requisito prescritivo demais (crítico) ME-1 - Falta de clareza no requisito / Interpretação equivocada (crítico) ME-9 -Resultados não comparáveis (médio)
IM- Quanto ao impacto no mercado	IM-5 - Dificuldade de compreensão sobre a regulamentação (médio) IM-8 - Aumento da informalidade (médio)
FMI- Fortalecer o mercado Interno	FMI-1 - Ineficácia do Regulamento em promover a melhoria no setor (médio)
IPC- Informação e proteção ao consumidor quanto a saúde, segurança e meio ambiente	IPC-2 - Produto não conforme no mercado (crítico) IPC-4 - Ausência de comunicação sobre a regulamentação (médio)
DCT- Quanto a disponibilidade de competência técnica	DCT-1 -Inadequação do regulamento (médio)
CA- Quanto a custos aceitáveis	CA-1- Onerar o processo de regulamentação (crítico) CA-2- Onerar o processo de produção (crítico) CA-7- Laboratórios apenas nas regiões Sul e Sudeste (crítico) CA-5 - Ausência de laboratórios (médio)
FCI- Facilitar o comércio internacional	FCI-3- Custo da certificação (crítico)
PCJ- Propiciar concorrência justa entre laboratórios	PCJ-1- Inexistência de laboratório acreditado (crítico)

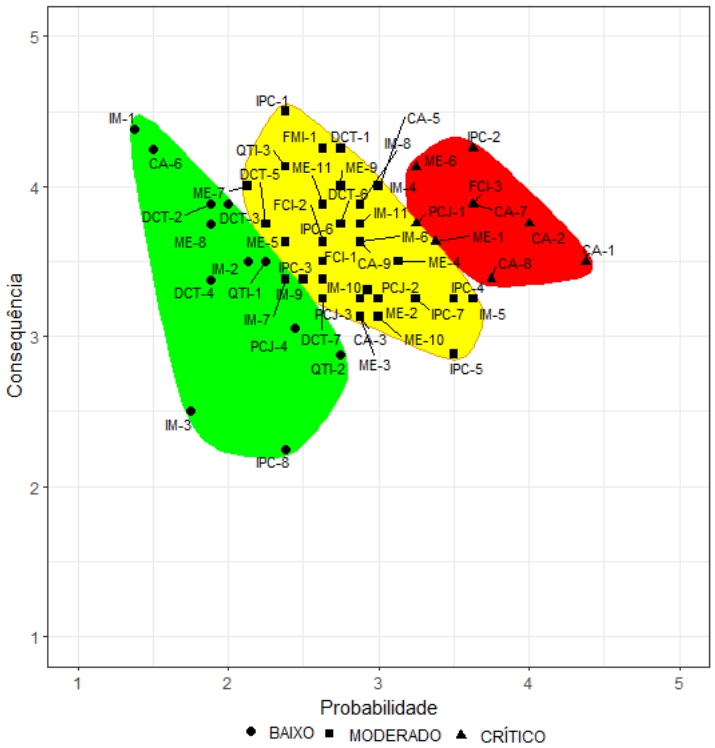

Figura 1. Classificação de riscos segundo [Machado et al. 2018].

4.2. Questionário baseado na análise de risco

A partir dos riscos considerados na Subseção 4.1, um questionário estruturado foi construído de modo a identificar quais práticas devem estar inseridas em um padrão nacional para avaliação de segurança em ambientes computacionais, cujas questões são elencadas a seguir.

1. ME-6: Para evitar que uma norma venha a atrapalhar a regulação e não seja adotada efetivamente, devemos:
2. ME-1: Para evitar a falta de clareza e interpretações errôneas nos requisitos para a segurança, devemos:
3. ME-9: Para a efetividade de comparação dos resultados obtidos nas avaliações, devemos:

4. IM-5: Como melhorar e divulgar uma regulamentação?
5. IM-8: Qual a melhor forma de se impedir a informalidade?
6. FMI-1: Como a regulação pode promover uma melhora no mercado interno?
7. IPC-2: Um produto que não seja produzido conforme a regulamentação de mercado pode prejudicar um país?
8. IPC-4: A ausência de comunicação sobre a regulamentação pode causar grandes danos para uma implantação eficiente?
9. DCT-1: A adoção de regulamentos para os quais não existam técnicos habilitados pode não ser uma prática efetiva?
10. CA-1: Como evitar que a adoção de uma regulamentação onere todo o processo de regulamentação?
11. CA-2: Como evitar que a adoção de uma regulamentação onere o processo de produção?
12. CA-7 e CA-8: Como levar laboratórios e organismos para todas as regiões?
13. CA-5: A ausência de laboratórios pode onerar o produto?
14. FCI-3: Os custos envolvidos na certificação podem ter impacto negativo no valor final dos produtos envolvidos, e como minimizar isso?
15. PCJ-1: Como proporcionar uma justa concorrência técnica entre os laboratórios?

5. Resultados e Discussões

Esta seção traz os resultados de uma meta-análise, a partir das respostas obtidas da aplicação do questionário apresentado na Subseção 4.2. O questionário foi respondido por um total de 25 profissionais da área tecnológica, dos setores público e privado, tais como segurança da informação e desenvolvimento de sistemas, em diversos estados Brasileiros. Dentre as empresas respondentes, citamos: Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo (PRODAM), *Extreme Digital Solutions* (EDS), Controladoria do Estado do Rio de Janeiro (CGE), Claro, Orange, TIM S.A., Eletrobras e Proderj. A técnica de amostragem utilizada para a seleção dos respondentes foi a *snowball*, uma técnica não-probabilística e intencional, em que indivíduos selecionados indicam outros indivíduos pertencentes à população de interesse.

A Figura 2 apresenta a área de atuação das empresas que participaram deste estudo, entre pública e privada. Os resultados apresentados nas subseções a seguir são relativos a um quantitativo de 25 respostas por parte de empresas, tendo obtido um balanceamento bem próximo entre as empresas públicas e privadas, conforme visto na Figura 2.

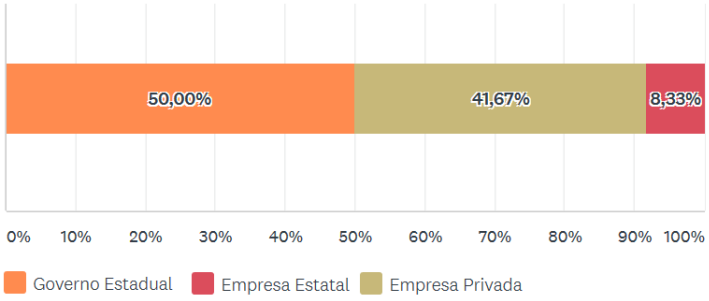

Figura 2. Área de atuação da organização participante deste estudo, entre pública e privada.

5.1. ME – Quanto à definição clara dos métodos:

Verifica-se na Figura 3 que a utilização de uma padronização ampla e abrangente, que detalhe ao máximo os requisitos, e a adaptação de normas internacionais ao cenário brasileiro é um caminho indicado para a implementação de um padrão de segurança.

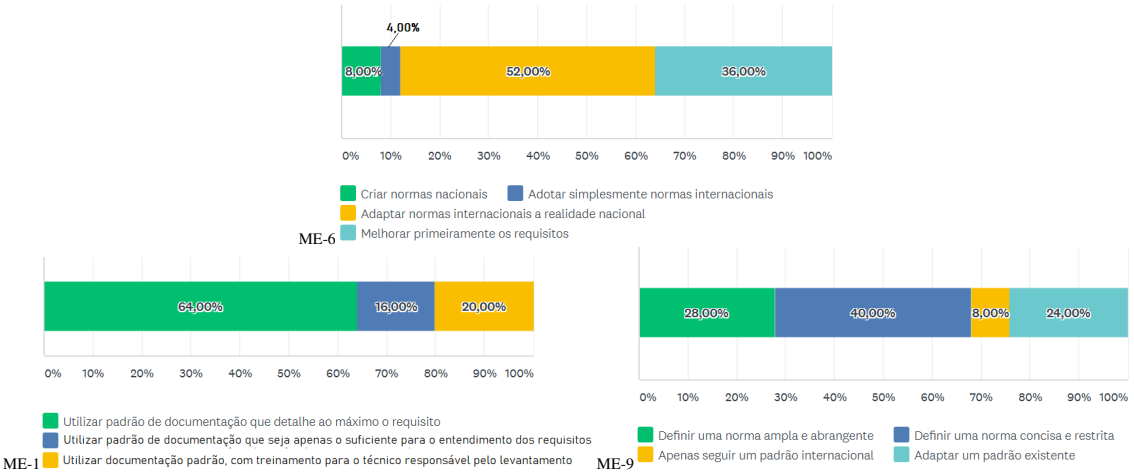

Figura 3. Questões que tratam da definição clara dos métodos de ensaio.

5.2. IM – Quanto ao impacto no mercado:

Pode-se notar, a partir da Figura 4, que a criação de grupos de trabalho e a devida divulgação das normas aparecem como as formas mais interessantes de se melhorar e divulgar um novo padrão. Além disso, quanto ao impedimento da informalidade, a pesquisa aponta para a adaptação de normas internacionais à realidade nacional com a melhoria da fiscalização, como o melhor caminho a ser perseguido.

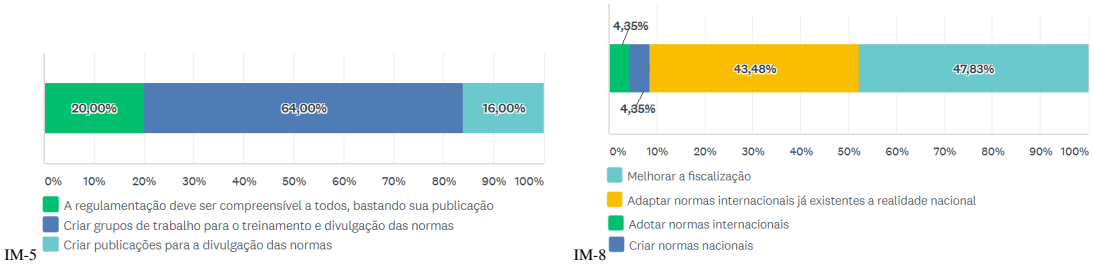

Figura 4. Questões relativas ao impacto da criação de um padrão no mercado.

5.3. FMI – Quanto ao fortalecimento do mercado interno:

No que se refere ao fortalecimento do mercado interno, verifica-se nos resultados apresentados na Figura 5 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.

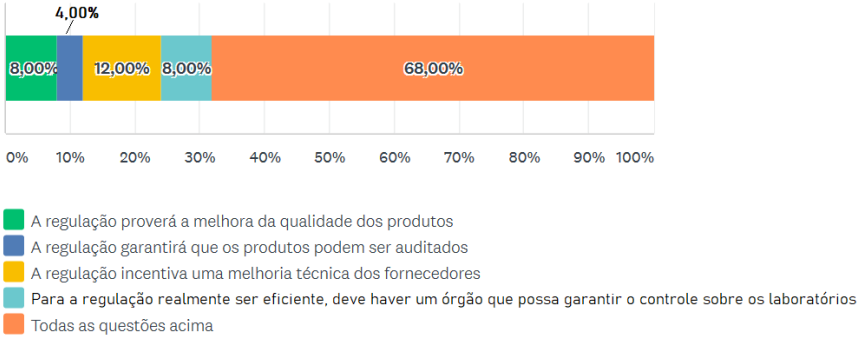

Figura 5. Questão que diz respeito ao fortalecimento do mercado interno a partir da criação de um padrão.

5.4. IPC – Quanto às informações de proteção ao consumidor:

Com relação as informações de proteção ao consumidor sobre a saúde, segurança e meio ambiente, pode-se verificar, de acordo com as respostas apresentadas na Figura 6, 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 as essas regulamentações.

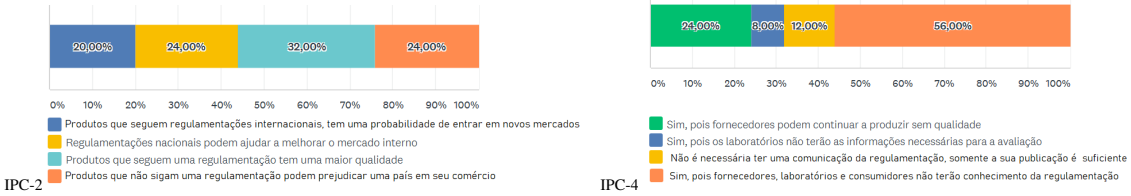

Figura 6. Questões sobre a informação e proteção ao consumidor quanto à saúde, segurança e meio ambiente.

5.5. DCT – Quanto à disponibilidade de competência técnica:

No tocante a disponibilidade de competência técnica, pode-se verificar a necessidade da adoção de regulações com viabilidade técnica, de acordo com a Figura 7. Para tal, faz-se necessária a existência de cursos capazes de formar técnicos devidamente habilitados e informados a respeito dos regulamentos existentes.

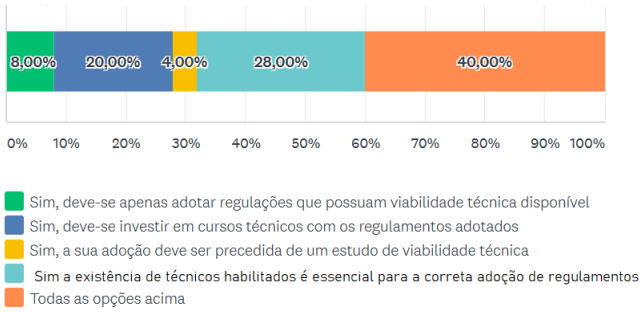

Figura 7. Questão relativa à disponibilidade de competência técnica.

5.6. CA – Quanto aos custos adicionais:

No que diz respeito aos custos aceitáveis para a implementação de um padrão, podemos verificar na Figura 8 que a criação de um processo e divulgação, treinamento e custos da normas envolvidas é essencial. Porém, a adaptação de normas internacionais à realidade nacional é necessária, devendo ainda existir um processo de incentivos para a criação de novos laboratórios ou de abertura de filiais.

Pode-se verificar ainda que a não existência de laboratórios com competência técnica deve ser avaliada 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.

Figura 8. Questões que tratam dos custos aceitáveis para a implementação de um padrão.

5.7. FCI – Quanto à facilitação do comércio internacional:

Quanto a facilitar o comercio internacional, verifica-se na Figura 9 que a maioria dos respondentes indica a necessidade de criação de um processo de divulgação, treinamento e cursos a respeito das normas envolvidas, pois a não existência desses quesitos pode trazer um impacto negativo no valor final dos produtos envolvidos.

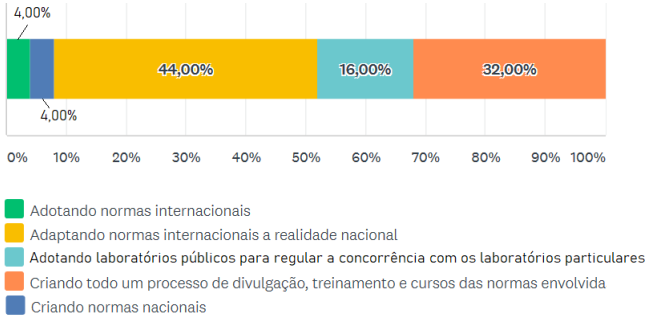

Figura 9. Questão sobre a facilitação do comercio internacional.

5.8. PCJ – Quanto à propiciação de concorrência justa:

Com relação a propiciar concorrência justa entre laboratórios verifica-se na Figura 10 que os respondentes em sua maioria indicam a necessidade do poder público ter laboratórios próprios para ajudar na regulação.

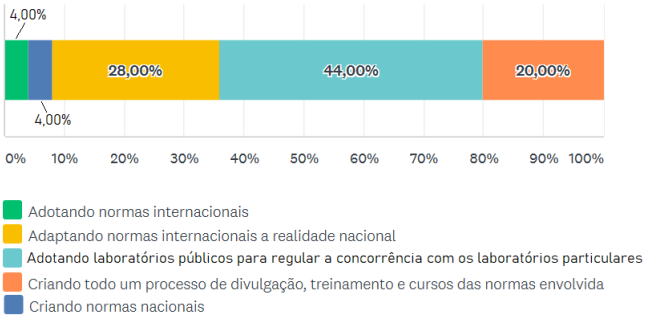

Figura 10. Questão referente a propiciação de concorrência justa entre laboratórios.

6. Proposta de Boas Práticas para o Padrão Brasileiro

Nesta seção, apresentamos uma lista de boas práticas a serem usadas na proposta de um padrão brasileiro para avaliação de conformidade em ambientes computacionais baseada em riscos. Esta lista, apresentada a seguir, utiliza os resultados apresentados na Seção 5 como um indicativo.

- 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 de estudos de casos envolvidos (mitigação), conforme a Figura 11.

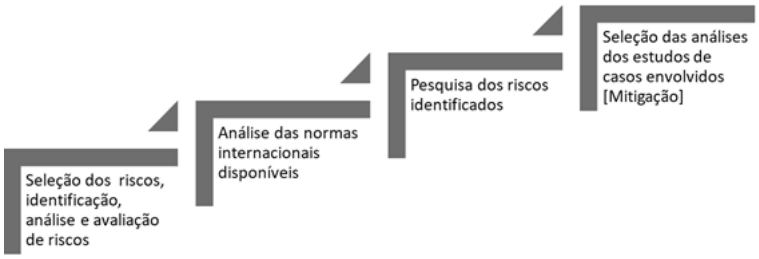

Figura 11. Diagrama da proposta de padronização.

- **Seleção de riscos, identificação, análise e avaliação de risco:**
  Nessa parte, deve-se tentar identificar onde podem ocorrer os riscos, devendo-se levar em conta a organização, contextos dos riscos e sua finalidade. É proposto que se possa utilizar de ferramentas como *brainstormings*, entrevistas ou mesmo a utilização de listas de riscos, sendo que sua utilização deve ser proposta conforme o nível de conhecimento, e como cada equipe envolvida poderá tirar o melhor valor a partir deste estudo inicial.
- **Análise das normas internacionais disponíveis:**
  O contexto internacional nos leva a verificar que existem diversas normas já utilizadas no Brasil, mas que a nível internacional temos muito mais regras à disposição no contexto que se deseja. Sendo assim, a sua utilização vem a trazer credibilidade para os produtos, *softwares*, *hardwares*, instalações e/ou configurações de produtos e equipamentos das mais diversas formas.
- **Pesquisa dos riscos identificados:**
  A pesquisa dos riscos identificados pode ser realizada de várias formas. Em geral, a ideia é fazer que se selecione os diversos risco e suas principais correlações com normas que possam, por sua vez, trazer de alguma maneira o contexto em que está sendo analisado.
- **Seleção das análises dos estudos de casos envolvidos (Mitigação):**
  Após as etapas anteriores, aplica-se a norma como forma de se mitigar os riscos analisados. Cada risco selecionado pode ter sua mitigação através de mais de um tipo de norma existente que tenha correlação com o contexto analisado.

7. Estudos de Caso da Aplicação do Conjunto de Boas Práticas Proposto

Esta seção traz dois casos de estudo práticos da aplicação da análise de riscos em uma empresa pública do RJ.

7.1. Caso de estudo 1

Como aplicação da metodologia proposta, a Diretoria de Infraestrutura Tecnológica do Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro está normatizando uma série de requisitos de seus *Data Centers*, dada a heterogeneidade desses ambientes, que vão desde uma sala cofre, uma sala segura, além de um ambiente de *colocation* em diferentes locais. Em ação conjunta, a diretoria e as equipes responsáveis por esses locais, fizeram um levantamento dos riscos de média e alta criticidade, referentes a seus ambientes para iniciar sua normatização (primeira etapa do diagrama apresentado na Figura 11), conforme a Tabela 2.

Tabela 2. Uso da análise de riscos em um *data center* referente ao estudo de caso 1.

Nº	Descrição do Risco	Consequência	Probabilidade de Ocorrência	Impacto	Severidade
1	Climatização	Perda do equipamento, degradação, parada e instabilidade do serviço	Baixa	Alto	Média
2	Climatização - Corredores	Perda de eficiência	Baixa	Alto	Média
3	Instalação Elétrica (rack)	Indisponibilidade	Alta	Alto	Alta
4	Utilização de Gerador	Falta de Continuidade do fornecimento de energia	Alta	Alto	Alta
5	Utilização de No-break	Falta de Continuidade do fornecimento de energia	Alta	Alto	Alta
6	Controle de acesso eletrônico	Controle de pessoal o ambiente de datacenter	Alta	Alto	Alta
7	Controle de acesso físico	Controle de pessoal o ambiente de datacenter	Alta	Alto	Alta
8	Cabeamento estruturado	Baixa de Taxa de transmissão	Alta	Alto	Alta
10	Detecção e combate a incêndio	Perda dos ativos e vidas	Alta	Alto	Alta
11	Sala de Telecom	Acesso indevido	Alta	Baixo	Média
12	Monitoramento do datacenter	Evitar perda de ativos	Alta	Alto	Alta
13	Redundância	Indisponibilidade	Alta	Alto	Alta

Após esse levantamento, foram analisadas normas internacionais e nacionais disponíveis (segunda e terceira etapas do diagrama da Figura 11), como forma de mitigação aos riscos, conforme me podemos verificar na Tabela 3.

Tabela 3. Mitigação dos riscos em um ambiente de *data center*

Nº	Descrição do Risco	Mitigação do Risco	Norma
1	Climatização	Melhoria da climatização	ABNT NBR 14565:2013
2	Climatização - Corredores	Correta climatização do ambiente	ABNT NBR 14565:2013
3	Instalação Elétrica (rack)	Garantia de uma adequada instalação elétrica	ABNT NBR 5410, TIA 942
4	Utilização de Gerador	Garantir o fornecimento de energia ininterrupto para o data center	ABNT 8528, ABNT NBR 14565:2013, TIA 942
5	Utilização de No-break	Garantir a estabilização do ambiente elétrico	ABNT 8528, ABNT NBR 14565:2013, TIA 942
6	Controle de acesso eletrônico	Garantir o acesso de forma controlada ao ambiente	CONPORTOS (Normas de Controle de Acesso), NBR 60839-11-1:2019, ANSI/BICSI 002-2014
7	Controle de acesso físico	Garantir o acesso de forma controlada ao ambiente	CONPORTOS (Normas de Controle de Acesso), ANSI/BICSI 002-2014
8	Cabeamento estruturado	Melhora da taxa de transmissão	TIA 942, 568 A, ABNT 16665
9	Piso elevado Datacenter	Melhora da distribuição de peso, mobilidade e distribuição de ar e elétrica	NBR 11802:1991, TIA 942
10	Detecção e combate a incêndio	evitar perdas de ativos e vidas	ISO 7240
11	Sala de Telecom	Evitar acesso indevidos	TIA 942
12	Monitoramento do datacenter	Ter um correto monitoramento do ambiente	TIA 942,ABNT 14565
13	Redundância	Aumento da disponibilidade dos sistemas	ABNT 14565

Após a identificação das mitigações necessárias, está em construção um procedimento normativo pela Diretoria responsável, que passará a nortear os ambientes dos *data centers*, tendo como referências os riscos identificados e as normas selecionadas, como parte da solução rápida e eficaz para a manutenção desses locais (última etapa do conjunto de boas práticas apresentado na Figura 11).

7.2. Caso de estudo 2

Assim como no Caso de estudo 1, a Assessoria de Segurança da Informação do Centro de Tecnologia da Informação e Comunicação do Estado do Rio de janeiro também iniciou a normatização dos requisitos de segurança daquele órgão. Utilizou-se, para isso, a metodologia proposta neste artigo para a necessária análise de riscos.

O trabalho foi iniciado a partir do preenchimento de uma planilha de avaliação de maturidade disponibilizada pela Associação Brasileira de Empresas Públicas de TIC - ABEP-TIC, contendo macros, com vistas à identificação da maturidade das várias empresas de TIC dos estados. Após o devido preenchimento, foi apresentada uma nota, utilizada para o comparativo das demais empresas afiliadas à ABEP-TIC. Entretanto, não se pôde evidenciar quais eram os maiores riscos a serem mitigados.

Desta forma, iniciou-se a utilização do modelo aqui proposto com uma fase inicial de *brainstorm* da equipe de segurança, onde foram sendo enumerados os vários riscos identificados (primeira etapa da proposta apresentada no diagrama da Figura 11). Após

essa etapa inicial, começou-se a atribuir valores de risco entre baixo, médio e alto para cada um deles, em conjunto com a probabilidade de ocorrência e o seu possível impacto, assim como feito em [Machado et al. 2018]. Após essa etapa, a equipe responsável prosseguiu com os três itens seguintes descritos no diagrama da Figura 11, ou seja, o estudo de normas existentes, a pesquisa e correlação com os riscos e a etapa de mitigação.

Apesar da assessoria ter conseguido um crescimento surpreendente na maturidade em segurança comparada às demais empresas afiliadas à ABEP-TIC, tendo a equipe trabalhado nas diversas lacunas anteriormente encontradas na planilha de avaliação de maturidade, o gasto de energia foi alto em virtude da falta de uma ferramenta que conseguisse apresentar a criticidade. Desse modo, a equipe acabou desperdiçando energia em melhorias secundárias, não tendo conseguido enxergar os maiores ofensores. Após a adoção do modelo aqui proposto, ilustrado na Figura 11, ficaram claros os alvos que deveriam ser perseguidos, que foram classificados através de sua probabilidade e impacto. Com isso, pôde-se levantar quais os riscos mais críticos para priorizar os esforços.

Diante do ganho obtido por esta diretoria na visibilidade imediata da criticidade dos riscos de segurança, identificou-se a necessidade do desenvolvimento de uma metodologia que conseguisse ainda, após inseridos os parâmetros necessários, gerar a criticidade, probabilidades e impactos dos riscos de maneira automatizada.

8. Conclusões e Trabalhos Futuros

A base normativa é um dos elementos essenciais do sistema de homologação, sendo considerada como o plano básico para a operacionalização das certificações [Kissel et al. 2008]. 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 à confidencialidade, integridade e disponibilidade de sistemas federais norte-americanos de informações [National Institute of Standards and Technology 2014].

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

Assim sendo, neste trabalho, um estudo foi feito acerca da padronização nacional para a avaliação de conformidade de sistemas computacionais, baseada em risco. Como procedimento metodológico, um questionário estruturado foi desenvolvido e aplicado em 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 de risco a partir dos níveis altos e médios. Com isso, espera-se que a metodologia proposta seja composta por normativas rígidas de segurança, que possam avaliar e mitigar tais riscos críticos. Os resultados obtidos indicam, principalmente, que adaptar normas internacionais ao cenário brasileiro é interessante, visto que pode-se reduzir custo e tempo para a sua implantação.

Como trabalhos futuros, pretende-se expandir a pesquisa para mais empresas, in-

cluindo o grupo de segurança da ABEP-TIC (Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação). Com isso, espera-se fortalecer ainda mais os resultados apresentados neste trabalho. Além disso, pretende-se regulamentar uma norma para o setor de segurança da informação do Centro de Tecnologia da Informação e Comunicação do Governo do Estado do RJ, a partir da metodologia proposta neste trabalho. Para tanto, outros casos de estudo devem ser avaliados, de modo a corroborar com os resultados indicados neste estudo.

Referências

ABNT (2005). Nbr iso/iec 17000:2005 -avaliação de conformidade. Technical report.

Alguliyev, R., Imamverdiyev, Y., and Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, 100:212–223.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1):1–13.

Barafort, B., Mesquida, A.-L., and Mas, A. (2017). Integrating risk management in it settings from iso standards and management systems perspectives. *Computer Standards Interfaces*, 54:176 – 185. Standards in Software Process Improvement and Capability Determination.

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.

CCRA (2014). *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*.

Cho, J.-H., Xu, S., Hurley, P. M., Mackay, M., Benjamin, T., and Beaumont, M. (2019). Stram: Measuring the trustworthiness of computer-based systems. *ACM Comput. Surv.*, 51(6).

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*.

Furtado, J. P. and Laperrière, H. (2011). Avaliação da Avaliação. *Desafios da avaliação de programas e serviços em saúde*, pages 19–39.

Governo Federal Brasileiro (2018). Estratégia brasileira para a transformação digital e-digital.

Hale, M. L. and Gamble, R. F. (2019). Hierarquias semânticas para extrair , modelar e conectar requisitos de conformidade em padrões de controle de segurança de informações Palavras-chave. pages 1–56.

INMETRO (2018). Inmetro - Avaliação da Conformidade. Acesso em 16-06-2018.

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.

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 25-10-2022.

Lyu, X., Ding, Y., and Yang, S.-H. (2019). Safety and security risk assessment in cyber-physical systems. *IET Cyber-Physical Systems: Theory & Applications*, 4(3):221–232.

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*.

Ministério da Defesa, and do Exército, C., (DCT), D. d. C. e. T., and (CDCiber), C. d. D. C. (2015). Estudo de Viabilidade Prelimi- nar do SHCDCiber no Âmbito do Projeto ENaDCiber-SHCDCiber@DCDN. 55(61).

Murashbekov, O. (2019). Challenges on introducing information security standards: A case study. *Journal of Security & Sustainability Issues*, 8(4).

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 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*.

Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., and Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: A literature review. *Journal of Manufacturing Systems*, 58:176–192.

Presidência da República (2019). Decreto nº 9.637.

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 25-10-2022.

Soares, S. P. L., da Silva Soares, A. C., and Alves, A. A. (2021). A importância da implementação de uma política de segurança da informação. *Brazilian Journal of Development*, 7(4):37162–37171.

Sun, G., Yajima, K., Miura, J., Shi, K., Goto, Y., and Cheng, J. (2012). A supporting tool for creating and maintaining security targets according to ISO/IEC 15408. *ICSESS 2012 - Proceedings of 2012 IEEE 3rd International Conference on Software Engineering and Service Science*, pages 745–749.

Viana, C. R. and Machado, R. (2017). Estratégia para a internalização de padrões internacionais de segurança. pages 1–4.

Villa, V., Paltrinieri, N., Khan, F., and Cozzani, V. (2016). Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety science*, 89:77–93.

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.

Zanero, S. (2017). Cyber-physical systems. *Computer*, 50(4):14–16.

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/.

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, 177:176–190.

Zografopoulos, I., Ospina, J., Liu, X., and Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. *IEEE Access*, 9:29775–29818.