Metrologia
Fortaleza - CE 2017

Estratégia para a internalização de padrões internacionais de segurança

Strategy for the internalization of international cyber-security standards

Carlos Roberto Viana [1], **Raphael Machado** [1,2]

[1]PPCIC-CEFET/RJ, [2] PPGMQ-INMETRO

E-mail: carlos.filho@eic.cefet-rj.br; rcmachado@inmetro.gov.br

Resumo: A adoção de regras e padrões internacionais permite a elevação dos níveis de qualidade e segurança de sistemas e produtos. Ao mesmo tempo, a aplicação completa das recomendações contidas em tais normas e padrões, traz desafios quanto à viabilidade técnica e financeira, particularmente na área de segurança da informação. Neste artigo realizamos um estudo da estratégia para a adoção de padrões de segurança no Brasil e no mundo, mostrando que a adoção parcial ou adaptada destas normas pode ser uma boa opção, viabilizando ganhos rápidos e preparando a infraestrutura para uma adoção plena de normas e padrões em médio prazo.

Palavras-chave: Normas, Normatização, Segurança, Padronização.

Abstract: *The adoption of international rules and standards allows the elevation of the levels of quality and safety of systems and products. At the same time, full implementation of the recommendations contained in such standards and standards poses challenges in terms of technical and financial feasibility, particularly in the area of information security. In this article, we study the strategy for the adoption of safety standards in Brazil and in the world, showing that the partial or adapted adoption of these standards can be a good option, making possible rapid gains and preparing the infrastructure for a full adoption of norms and standards in the medium term.*

Keywords: Standards, Normalization, Security, Standardization.

1. INTRODUÇÃO

Nos dias de hoje, em que se observa a proliferação de sistemas de informação, dispositivos inteligentes e equipamentos dotados de software embarcado, garantir a segurança de informação e de sistemas computacionais tornou-se tão importante quanto garantir a proteção de ativos físicos. Um importante caminho para garantir níveis adequados de segurança é a adoção de padrões, normas e recomendações consolidadas junto à comunidade técnica internacional. Ao mesmo tempo, por se tratar de uma área nova e de alta complexidade

tecnológica, a adoção de padrões internacionais na área de segurança da informação tende a ser um processo complexo e custoso, demandando um cuidadoso estudo de viabilidade antes de sua concretização.

No presente trabalho, realizamos uma análise das estratégias para a adoção de padrões de segurança da informação. Estudamos modelos de avaliação da conformidade na área de segurança da informação adotados no Brasil e no mundo, identificando as principais normas de segurança e estudando a forma como tais padrões têm sido implementados para diversos produtos e sistemas. O levantamento realizado evidencia que a adoção de uma norma internacional na área de segurança, pode elevar os custos, comprometendo a própria sustentabilidade de um mercado ou setor, especialmente, quando se trata de uma padronização compulsória, tipicamente associada a um programa de avaliação da conformidade concebido pelo Governo. Argumentamos, no entanto, que mesmo que estes mercados e setores não possam adotar integralmente normas internacionais de segurança, é possível seguir estratégias baseadas na adoção parcial ou adaptada de tais normas, sempre buscando garantir a harmonia conceitual e a compatibilidade técnica em relação ao padrão original. Finalmente, validamos essa ideia por meio da análise do Programa de Avaliação da Conformidade aplicado aos equipamentos ‘da Infraestrutura de Chaves Públicas brasileiro, mostrando que, embora baseado em regulamentação técnica nacional, ele está tecnicamente alinhado ao padrão FIPS (Federal Information Processing Standard) 140-2 que, por sua vez, é reconhecido como padrão internacional ISO (International Organization of Standardization) /IEC (International Electrotechnical Commission) 19790.

2. NORMALIZAÇÃO E PADRONIZAÇÃO

Padronizações são referências necessárias para assegurar o cumprimento de requisitos. Já a normalização é a tecnologia consolidada, que permite confiar e reproduzir algo por várias vezes [1]. Normas são documentos que estabelecem uma conformidade aprovada por uma instituição reconhecida, que passa a fornecer regras, orientações ou características para a obtenção de resultados esperados através da utilização de determinados procedimentos [2]. Economicamente a padronização está relacionada à produtividade, pois padrões protegem a segurança, facilitam o comércio, a interoperabilidade e ajudam no desenvolvimento. Por outro lado, a sua utilização de maneira incorreta, reduz opções, competitividade, podendo criar barreiras técnicas [2]. A sua adoção pode elevar os custos devido aos ensaios necessários, levar a criação de novos procedimentos e diminuir o número de laboratório que tenham capacidade para a sua realização [3].

Segundo a ABNT (Associação Brasileira de Normas técnicas), a normalização é uma atividade que estabelece em prescrições destinadas à utilização comum e repetitiva em relação a problemas existentes e potenciais Em particular, a atividade consiste nos processos de elaboração, difusão e implementação de normas [1].

3. BENEFÍCIOS DOS PADRÕES

A ampliação do comércio e o avanço da ciência formam condições para a elaboração de normas técnicas, mas estas por si só, não são condições necessárias para a adoção. Com a maior relação econômica entre os países e o envolvimento de produtos de maior complexidade técnica, surge a necessidade de compatibilização de inúmeras estruturas técnicas e sociais [1]. Os padrões são apontados como um bem público, que estão disponíveis a um custo baixo para todos os produtores e consumidores. Esta informação é o

modelo para o aperfeiçoamento, segurança, interoperabilidade e comércio e são criadas por comitês de especialistas, objetivando o melhoramento de práticas nacionais e internacionais. Sendo assim, os padrões são uma ferramenta fundamental para a divulgação do conhecimento [4].

4. MODELOS DE ADOÇÃO DE PADRÕES

Vimos que a adoção integral de padrões pode trazer desafios do ponto de vista da viabilidade técnica e econômica. Nesta seção, estudamos tais desafios e discutimos a possibilidade da adoção parcial ou adaptada de um padrão, analisando um caso concreto de tal estratégia, que são os padrões para equipamentos da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileiras).

4.1. Adoção integral de normas internacionais

Um documento que preveja a utilização comum, que estabeleça regras e diretrizes de um modo repetitivo, que contenha características para atividades ou seus resultados é um padrão. A adoção de padrões internacionais pode ser tida como empregada, quando normas regionais ou nacionais são idênticas ou modificadas em sua relação. Adotar normas internacionais no âmbito nacional é muito intricado, se regras ou tradições, nacionais relacionadas a estas não convergirem. Toda energia deve ser direcionada para a redução de desvios para um fator mínimo. Se a versão internacional for simplesmente uma reedição será bastante fácil discernir os desvios técnicos do padrão original [5].

4.2. Rússia

A Rússia desde 2002 adota o Common Criteria como metodologia, e desde 2012 avança nesta certificação, além de criar e aprovar novos perfis de proteção, aumentando a eficiência na detecção de vulnerabilidades em 50%, conforme indica o site do Serviço federal de Técnica e Controle de Exportação da Rússia. Entretanto, estes procedimentos elevam o custo dos laboratórios devido ao aumento de ensaios necessários, reduzindo assim, o número de laboratórios capazes de realizar os testes [3].

4.3. Adoção parcial de normas internacionais

Destacamos que a adoção "parcial" de uma norma internacional pode ser uma estratégia que viabilize as melhores práticas de mercado.

Estudo de Caso: ICP-Brasil. Através da medida provisória Nº 2.200, foi criada a ICP-Brasil, com a finalidade de garantir a autenticidade, integridade e a validade jurídica de documentos e sua aplicação, sendo ainda responsável por adotar medidas necessárias e coordenar a implantação e o funcionamento desta, através do estabelecimento de políticas, critério e normas técnicas para o credenciamento de Autoridades Certificadoras (AC) e de Autoridades Registro (AR), além do estabelecimento de diretrizes e normas técnicas para as políticas e regras gerais, sendo o Instituto de Tecnologia da Informação a AC Raiz da ICP-Brasil [6].

Entre os documentos descritos, podemos verificar nos MCTs (Manuais de conduta técnica) de 1 a 11, referências ou a utilização de várias normas e padrões internacionais.

Os MCTs servem de base para que os LEA (Laboratórios de Ensaios e Auditoria) possam avaliar e emitir laudos correspondentes, e que o ITI (Instituto Nacional de Tecnologia da Informação) homologue o objeto avaliado. Esta avaliação contém vários itens, e dentre eles podemos verificar a identificação de requisitos obrigatórios e opcionais de homologação e as discrepâncias encontradas [7].

Para validar os argumentos defendidos ao longo do texto, apresentamos um estudo em maior nível de detalhes a respeito do MCT 7, que é o manual que contém as orientações para homologação dos HSM (Hardware Security Modules). Uma análise do MCT7 mostra que o Manual é aderente a

diversos padrões internacionais, dentre os quais destacamos os seguintes: ANSI (X9.31, X9.62, X9.80, X9.81-1, X9.82-1), IEC.(CISPR 22, CISPR 24, 60050 - 161), ISO/IEC 8825-1, FIPS (197, 800-38C, 46-3, 140-2, 186-2, 196, 198, 180-2), NIST (SP 800-17, SP 800-20, 800-38B). Destacamos os requisitos do FIPS 140-2 que são utilizados pelo MCT7: de forma integral como na utilização de diagramas de transição de estado, de forma complementar como na documentação da especificação dos métodos do módulo criptográfico e de forma adaptada como na definição de um algoritmo de segurança referente à chave criptográfica [8].

6. CONCLUSÃO

Podemos verificar que a adoção de padrões traz enormes benefícios, sejam estes para empresas privadas ou órgãos públicos, pois melhoram o processo, reduzem o tempo, evitam o desperdício e promovem a melhoria de intercâmbio entre as nações. Padrões são instrumentos de governança, que podem interferir na vida de uma população, pois são ferramentas que fornecem requisitos para vários setores, inclusive aqueles relacionados à segurança.

No Brasil, não há leis específicas que regulamentem as questões de segurança e padronizações. Diversos órgãos utilizam diferentes padrões de segurança, sejam estes oriundos de outras normas internacionais ou próprias.

Com a criação dos MCTs, o ITI passa a adotar diversos padrões internacionais, principalmente o conjunto de normas do FIPS. Com a utilização destas padronizações internacionais, e ainda com a adoção de padrões internos Brasileiros, os MCTs, passam a proporcionar os requisitos, materiais, e os documentos técnicos para a homologação de cartões criptográficos, leitoras de cartões, tokens criptográficos e software para assinatura digital dentre outros. Com isto, há um enorme salto na qualidade do conhecimento, apontando para um processo de normatização e padronização de segurança.

Como estratégia, sugerimos como solução ideal, a adoção de uma padronização internacional para as questões de segurança, e que na impossibilidade da sua aplicação total, que se adote uma padronização parcial, ou ainda na impossibilidade desta última, que seja utilizada uma normatização nacional ou até mesmo parcial ou adaptada para os quesitos de segurança.

REFERÊNCIA

[1] Normas, B. D. E. (2011). Historia da normalização brasileira

[2] Mariani, E. J. (2006). As Normas ISO. Revista Cientifica Eletrônica de administração

[3] Barabanov, A. and Markov, A. (2015). Modern trends in the regulatory framework of the information security compliance assessment in Russia based on common criteria.

[4] Standards Australia (2013). Research Paper: The Economic Benefits of Standardization.

[5] Standards, I. (2005). GUIDE 21-1 Regional or national adoption of International Standards and other International Deliverables.

[6] Presidência da República (2015). Diário da República, - nº 116.

[7] Instituto de Tecnologia da Informação – http://antigo.iti.gov.br/icp-brasil/navegadores/132-servicos/homologacoes/4759-laboratorios-de-ensaios-e-auditoria-leas-credenciados - acessado em 23/07/2017

[8] ICP-Brasil: MCT 7 Vol. I - Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Módulos de Segurança Criptográfica (MSC).