Proposta de um Programa de Certificação Básica de Segurança da Informação*

Raphael C. S. Machado[1,2], Flávia Paiva Agostini[1], Wladmir Araujo Chapetta[1]

[1]Instituto Nacional de Metrologia, Qualidade e Tecnologia
Rio de Janeiro – RJ – Brasil

[2]Programa de Pós-Graduação em Ciência da Computação –
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
Rio de Janeiro – RJ – Brasil
[rcmachado,fpagostini,wachapetta]@inmetro.gov.br

Abstract. *Information Security is a critical issue these days. It is crucial to assess whether a technology asset meets security requirements compatible with the application in which it will be employed and the risks associated with it. We call "certification" the verification of a set of requirements performed by a third party, typically involving a laboratory responsible for conducting rigorous and systematic testing by laboratories. While the conformance assessment programs offers options for the certification of technology assets with respect to information security requirements, most existing approaches have high cost and duration, often avoiding its use by some specific industries. In the present work, we propose a simplified approach to security certification that allows us to attest that an asset meets basic information security requirements, within a process with a reduced cost and duration when compared to the main security certification programs of information.*

Resumo. *Segurança da Informação é uma questão crítica nos dias de hoje. É fundamental avaliar se um ativo de tecnologia atende a requisitos de segurança compatíveis com a aplicação em que ele será empregado e os riscos a ele associado. Denominamos "certificação" à verificação de um conjunto de requisitos realizada por uma terceira parte, tipicamente envolvendo um laboratório responsável pela realização de ensaios rigorosos e sistemáticos por laboratórios. Embora o setor de avaliação da conformidade ofereça opções para a certificação de ativos de tecnologia com relação a requisitos de segurança da informação, a maioria das abordagens existentes possui parâmetros de custo e duração elevados, muitas vezes impeditivos para determinados setores. No presente trabalho, apresentamos uma abordagem simplificada para a certificação de segurança que permite atestar que um ativo atende a requisitos básicos de segurança da informação, dentro de um processo com custo e duração reduzidos, quando comparado com os principais programas de certificação na área de segurança da informação.*

1. Introdução

O termo *certificação* refere-se ao processo de avaliação da conformidade em relação a um conjunto de requisitos realizado por uma terceira parte comprovadamente idônea, independente e tecnicamente habilitada. Na área de segurança da informação, nas

* *Trabalho parcialmente apoiado pelo projeto SHCDCiber.*

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

últimas décadas, a certificação passou a ganhar força como ferramenta para atestar que um produto atende a um conjunto de requisitos [ISO2018]; uma das principais referências, neste sentido, é a certificação baseada *Common Criteria* [MELLADO2007, COMMONCRITERIA2017], padrão internacional consolidado na forma da norma ISO/IEC 15408. Apesar de sua importância para a consolidação do setor de certificações de segurança da informação, o *Common Criteria* possui limitações de aplicação devido à sua complexidade, aos custos e à duração do processo de realização de ensaios e certificação [VIANA2017]. No presente trabalho, propomos um modelo de avaliação da conformidade simplificado para a área de segurança da informação. O modelo concretiza-se na forma do que chamamos de "Certificação Básica de Segurança da Informação" – CBSI. A CBSI visa atender segmentos de mercado que um programa de certificação baseado no *Common Criteria* não teria condições de atender no curto prazo, por conta de seu custo, complexidade e tempo de avaliação. Ainda assim, argumentamos que a existência de um programa nos moldes do CBSI pode ter enorme impacto nos parâmetros de segurança dos ativos envolvidos com tais segmentos.

2. Conceitos básicos

2.1. Avaliação da Conformidade

O conteúdo desta seção baseia-se nos conceitos apresentados em [ISO2018]. *Avaliação de conformidade* é o termo dado a técnicas e atividades que asseguram que um produto, processo, serviço, sistema de gestão, pessoa ou organização atenda a um conjunto de requisitos especificados. A avaliação da conformidade pode ser usada em caráter voluntário ou pode constituir parte de um conjunto de regras obrigatório, geralmente, como parte de um processo regulatório. Neste sentido, a avaliação da conformidade pode ser usada por reguladores para ajudar a implementar políticas públicas. A International Organization for Standardization (ISO) e a International Electrotechnical Commission (IEC) publicam [ISO2018] Normas e Guias Internacionais sobre avaliação de conformidade. Esses Padrões e Guias Internacionais são a base internacionalmente aceita para avaliação de conformidade e são usados por muitos reguladores em todo o mundo.

As principais técnicas de avaliação de conformidade e suas aplicações mais comuns podem ser descritas a seguir:

- *Avaliação* da competência técnica de uma organização;
- *Auditoria* de um sistema de gestão dentro de uma organização;
- *Avaliação* de um produto, processo ou serviço de cumprimento de requisitos especificados que são definidos em um esquema de avaliação de conformidade definido;
- *Exame* da competência de uma pessoa;
- *Inspeção* de uma instalação ou de um produto ou serviço em uso;
- *Teste* de uma característica do produto.

Após a aplicação de uma ou mais técnicas de avaliação de conformidade para gerar evidência de cumprimento de requisitos, uma *declaração de conformidade* pode ser feita. Declarações de conformidade podem ser feitas sobre o produto, processo, serviço, sistema de gestão, pessoa ou órgão organizacional – ou seja, sobre o objeto da avaliação de conformidade.

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

As declarações de conformidade podem ser feitas por:

- primeira parte (1ª parte) – a pessoa ou organização que fornece o objeto e que é responsável pelo cumprimento desse objeto dos requisitos especificados (por exemplo, um fabricante);
- segunda parte (2ª parte) – uma pessoa ou organização que tem interesse de usuário no objeto (por exemplo, uma cadeia de varejo que está comprando o produto para venda subsequente);
- terceira parte (3ª parte) – uma pessoa ou organismo que é independente da pessoa ou organização que fornece o objeto e dos interesses do usuário no objeto (por exemplo, um laboratório de testes independente ou imparcial ou um organismo de certificação).

As declarações de conformidade de terceira parte são feitas por organizações que sejam consideradas independentes da pessoa ou organização que fornece o objeto, e também, independentes dos interesses do usuário no objeto. Exemplos de terceiras partes incluem laboratórios de testes independentes e imparciais, organismos de inspeção e organismos de certificação. Declarações de conformidade de terceira parte são o que chamamos de *certificação*.

2.2. Segurança da Informação

Segurança da informação, entendida em sua forma mais ampla, refere-se à proteção da informação e de sistemas computacionais – aos quais, conjuntamente, nos referimos como ativos de tecnologia – em seus aspectos de confidencialidade, integridade, autenticidade e disponibilidade. Na medida em que a informação se torna um ativo cada vez mais valioso, e que os sistemas computacionais passam a reger aspectos cada vez mais críticos do funcionamento das sociedades, a segurança da informação passa a constituir um aspecto crítico a ser avaliado, estimado e mensurado. Em outras palavras, passa a ser cada vez mais importante ser capaz de estimar os riscos à segurança de ativos de tecnologia envolvidos em atividades críticas.

Uma abordagem que vem ganhando cada vez mais importância na avaliação de segurança de ativos de tecnologia é a certificação. Ao recorrer às ferramentas da certificação, promove-se o uso de práticas sistemáticas e a aplicação de procedimentos técnicos rigorosos. Com isso, é possível alcançar elevados patamares de confiança nas avaliações realizadas, além de se obter o reconhecimento de terceiros – inclusive em relações internacionais, quando regidas por um arcabouço normativo internacional,.

Atualmente, entende-se que uma avaliação de conformidade na área de segurança da informação também deva se basear no mesmo arcabouço que aqueles das áreas "clássicas" do Ensaio e da Calibração [LEAMAN2013, LEAMAN2014]. Em outras palavras, para ser internacionalmente reconhecida, uma avaliação de segurança de um ativo de tecnologia deve ser realizada por um laboratório de ensaios que atue conforme a ISO 17025 e que tenha sido acreditado por um organismo de acreditação conforme a ISO 17011 e reconhecido internacionalmente por acordos de reconhecimento mútuo. Além disso, é importante que tal laboratório tenha seus métodos alinhados a padrões técnicos internacionais e que sua proficiência verificada em procedimentos alinhados à ISO 17043. Todo esse arcabouço garante a validade dos resultados de avaliações e o seu consequente reconhecimento internacional.

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

Atualmente, dois padrões técnicos se destacam no cenário internacional de avaliação de segurança: o *Criptographic Module Validation Program* [NIST_FIPS140-2, LEAMAN2013] (NIST FIPS 140-2, associado ao padrão internacional ISO/IEC 19790:2012) e o *Common Criteria for Information Technology Security Evaluation* [LEAMAN2014, COMMONCRITERIA2017] (associado ao padrão internacional ISO/IEC 15408). Ambos os padrões se destacam pela qualidade técnica e pelo reconhecimento internacional que alcançaram. No entanto, a alta complexidade de uma avaliação conduzida no escopo desses padrões – com o consequente custo e duração de avaliação – levou muitos países a definir abordagens próprias para a avaliação de segurança de ativos de tecnologia [ZHUOHUI2008, AISEP, BARABANOV2014, BARABANOV2015]. Na França, por exemplo, o mesmo organismo que promove avaliações *Common Criteria* no país (ANSSI - Agence nationale de la sécurité des systèmes d'information), desenvolveu e mantém um programa de certificação "simplificado" ao qual denominam Certification de Sécurité de Premier Niveau (CSPN) [ANSSI-CSPN]. A Austrália reconhece avaliações realizadas no âmbito do FIPS 140-2 e do *Common Criteria*, mas possui critérios próprios para a avaliação de segurança de ativos de tecnologia definidos no *Australasian Information Security Evaluation Program* [AISEP] mantido pelo *Australian Signals Directorate* (ASD). Outros países como a China [ZHUOHUI2008] e a Russia [BARABANOV2014, BARABANOV2015] possuem abordagens próprias para realizar avaliação de segurança de ativos de tecnologia.

No Brasil, não existe um programa "amplo" para tratar a questão da avaliação de segurança de ativos de tecnologia. O que se observa é o surgimento de variadas iniciativas pelos reguladores de diversos setores no sentido de definir requisitos de segurança da informação e mecanismos de avaliação da conformidade para aplicações específicas. Por exemplo, na área de Metrologia Legal, diversos tipos de medidores devem passar por ensaios que avaliam a segurança da informação e a proteção do software embarcado, tais como medidores de energia [INMETRO2012]. Na área de relações de trabalho, também o Registrador Eletrônico de Ponto [INMETRO2011] (REP) deve atender a requisitos de segurança da informação e proteção do software embarcado. Outro setor onde requisitos de segurança são avaliados é o de Certificados Digitais padrão ICP Brasil [INMETRO2013], que inclui equipamentos tais como *tokens* criptográficos, *smart cards* para assinatura digital e módulos de segurança criptográfica. Nos três casos anteriormente citados – Metrologia Legal, REP e equipamentos ICP Brasil –, os ensaios são realizados por laboratórios acreditados conforme a ISO 17025; no entanto, o arcabouço normativo técnico compõe-se de regulamentos e normas nacionais e voltadas para os objetos específicos em questão. Outros setores do Governo vêm demonstrando interesse em desenvolver programas de avaliação da conformidade nestes moldes, com destaque para áreas de Defesa Cibernética [BARBALHO2018] e da Administração Pública Federal [EPING].

O surgimento de diversos programas de avaliação da conformidade com foco em aspectos de segurança da informação e avaliação de software apontam para a oportunidade de concepção de um programa unificado. O *Common Criteria* fornece um possível arcabouço para a unificação de tais programas – e essa é uma direção que deve ser buscada. Por outro lado, os custos envolvidos na criação e implantação de um programa de certificação baseado no *Common Criteria* levam a crer que a disponibilização de programas "básicos" de avaliação da conformidade – por exemplo, nos moldes do modelo francês do CSPN – oferece uma oportunidade de curto prazo

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

para uma efetiva harmonização entre os programas atualmente existentes. O termo "básico" não deve ser visto como depreciativo; ao contrário, ele reflete uma abordagem de ensaios simples e objetiva, com foco nos aspectos fundamentais de segurança da informação, mas que permitem alcançar um primeiro nível de maturidade em segurança e de visibilidade de riscos, especialmente, em cenários onde existem limitações quanto ao tempo de execução de ensaios e aos custos envolvidos.

3. Proposta da Certificação Básica de Segurança da Informação

3.1. Abordagem Proposta pelo Programa CBSI

O Programa de Certificação Básica de Segurança da Informação segue uma abordagem pragmática que busca caracterizar dois aspectos práticos relacionados à segurança de ativos: a *caracterização da solução de segurança* do ativo avaliado e a avaliação da explorabilidade de vulnerabilidades eventualmente identificadas por atacantes reais. Tais aspectos são discutidos a seguir.

O primeiro aspecto avalia a capacidade das partes interessadas (por exemplo, fabricantes, reguladores, adquirentes, etc.) em endereçar as questões de segurança, seja identificando riscos, especificando requisitos, implementando ou testando a segurança do ativo. Neste sentido, em linhas gerais, o processo de avaliação deve permitir a resposta às seguintes perguntas:

- Quais riscos foram mapeados?
- Quais requisitos foram especificados para tratar os riscos?
- Quais soluções foram especificadas e implementadas para atender tais requisitos?
- Como as soluções implementadas deveriam ser testadas e como foram testadas?

O segundo aspecto avalia o grau de dificuldade que um atacante típico teria para explorar vulnerabilidades e falhas de segurança eventualmente presentes e identificadas no ativo. Neste sentido, em linhas gerais, o processo de avaliação deve permitir responder às seguintes perguntas:

- Quão realístico é o modelo de ataques apresentado por uma parte interessada?
- Qual o esforço realizado por cada tipo de atacante para explorar as vulnerabilidades eventualmente identificadas?
- Qual o impacto da exploração de cada tipo vulnerabilidade identificada?

Ao tratar esses dois aspectos, é possível trazer para a certificação uma visão pragmática que contempla os pontos de vista do defensor e do atacante: um ativo será considerado conforme – e, portanto, certificado – se o fabricante construiu e implementou um modelo consistente de segurança (ponto de vista do defensor) e se o avaliador (atacante) não conseguiu realizar ataques bem-sucedidos que comprometessem aquele modelo (ponto de vista do atacante).

A abordagem descrita no parágrafo anterior já aponta para os tipos de ensaios que serão realizados no contexto da CBSI. Por um lado, por meio da análise de documentação, inspeção de código-fonte e/ou testes de funcionalidades de segurança, o avaliador buscará identificar que os aspectos de segurança foram endereçados de maneira consistente pelo fabricante do ativo sob avaliação. Por outro lado, por meio da realização de testes de penetração, o avaliador buscará identificar o grau de dificuldade

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

para que um atacante possa comprometer o modelo de segurança desenvolvido pelo fabricante, por meio da exploração de vulnerabilidades e falhas de segurança.

Observe que a obtenção de uma certificação no escopo do Programa CBSI não está associada a um nível particular de segurança da solução ou do conjunto de requisitos de segurança atendidos, mas evidencia uma postura adequada do fabricante no tratamento de riscos de segurança. Nesse sentido, o "certificado CBSI" não será tratado como uma caracterização única no nível de segurança do ativo, mas deverá vir acompanhada da documentação que foi usada como referência na realização dos ensaios. Essa é uma abordagem análoga àquela empregada pelo *Common Criteria*, onde uma avaliação pode ser feita com base em uma documentação de referência denominada *Protection Profile*, onde estão detalhados os aspectos de segurança que devem ser considerados no processo de avaliação do ativo.

3.2. Organização do Programa CBSI

O Programa CBSI prevê a participação de quatro tipos de participante:

- Gestor do Programa,
- Patrocinador da Certificação,
- Laboratório de Avaliação,
- Demandante de Certificação.

O Gestor do Programa é uma autoridade nacional de avaliação da conformidade na área de segurança da informação. Esse participante é o responsável por definir as regras e funcionamento do Programa. No modelo proposto, o Gestor do Programa também é o responsável por validar avaliações emitidas por laboratórios, emitindo um Relatório Final de Avaliação do produto. Finalmente, o Gestor do Programa assume, naturalmente, a interface com os outros participantes do programa.

O Patrocinador de Certificação de Produto é a entidade que solicita a avaliação de um produto no escopo do Programa CBSI. Na maioria das vezes, o Patrocinador de Certificação de Produto será o próprio fabricante ou fornecedor do produto, embora nada impeça que a solicitação de certificação seja feita por terceiros.

O Laboratório de Avaliação é a "terceira parte" responsável pela realização dos ensaios de avaliação do produto. Ao final dos ensaios, o Laboratório de Avaliação emite um Relatório Técnico de Ensaios.

O Demandante da Certificação é uma entidade que demanda a certificação para alguma aplicação específica na qual está envolvida. Por exemplo, pode ser um órgão de governo que regula determinado setor e define a obrigatoriedade de certificação para determinado equipamento usado naquele setor. Ou pode ser uma organização que, em um processo de aquisição de equipamentos, determina que tais equipamentos devam ser certificados. Mesmo não estando diretamente envolvido no processo de certificação, os Demandantes de Certificação são fundamentais para o sucesso do Programa CBSI, na medida em que são eles que criam um "mercado" para os laboratórios que atuam no Programa.

3.3. Níveis de Avaliação do Programa CBSI

O CBSI prevê diferentes níveis de avaliação de conformidade. Tais níveis não estão associados ao "rigor" dos requisitos de segurança atendidos pelo ativo sob avaliação,

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

mas ao grau de detalhamento da solução avaliada pelo laboratório – e aos ensaios por ele realizados. Nessa linha, o CBSI prevê três níveis de avaliação:

- Nível conceitual,
- Nível operacional,
- Nível formal.

Os níveis de avaliação apresentados refletem patamares crescentes de informação e detalhamento a respeito da solução avaliada. Descrevemos, a seguir, o significado de cada um desses níveis.

A avaliação CBSI em nível conceitual baseia-se na análise de documentação e especificações de alto nível a respeito do ativo sob avaliação para atestar que a "proposta" de solução de segurança é conceitualmente consistente com os princípios e conceitos fundamentais de segurança da informação. Não são realizados testes funcionais ou analisados detalhes de implementação. A avaliação em nível conceitual tem por objetivo tão-somente atestar a inexistência de falhas básicas de projeto, sendo adequada, apenas, para a avaliação de ativos de baixíssimo risco. Também não há realização de testes de penetração no nível básico da CBSI.

A avaliação CBSI em nível operacional reflete um nível adicional de detalhamento a respeito das soluções de segurança implementadas pelo ativo sob avaliação, na medida em que são realizados testes funcionais que permitem avaliar, na prática, o comportamento do ativo em diversos casos de uso relevantes do ponto de vista de segurança da informação. A avaliação em nível operacional representa um nível adicional de confiança na segurança declarada pelo fabricante, ao passo que pode-se observar, na prática, o comportamento do ativo – e a sua consistência com as especificações de alto nível declaradas pelo fabricante. O nível operacional da CBSI é o primeiro nível em que ocorrem testes de penetração para avaliar a explorabilidade de falhas e vulnerabilidades de segurança.

A avaliação CBSI em nível formal consiste no nível mais elevado de confiança da CBSI, na medida em que a avaliação é subsidiada por toda uma documentação de engenharia de software do ativo sob avaliação – incluindo os códigos de software do ativo. A avaliação em nível formal permite atestar que o "conceito" proposto pelo fabricante do ativo foi adequadamente refletido em uma implementação adequada e consistente com as especificações de alto nível – com um nível de confiança ainda maior que aquele proporcionado pela avaliação em nível operacional.

3.4. Testes de Penetração e Explorabilidade de Vulnerabilidades

Um dos aspectos mais pragmáticos da CBSI é a previsão de realização de testes de penetração com o objetivo de se estimar a explorabilidade de eventuais vulnerabilidades do ativo sob avaliação. De fato, testes de penetração permitem reproduzir cenários de ataque típicos, oferecendo uma boa percepção a respeito da possibilidade de sucesso de ataques reais. A realização de testes de penetração é prevista nos níveis de avaliação operacional e formal.

4. Considerações Finais

No presente trabalho, apresentamos as bases para um programa de certificação básica de segurança da informação, o Programa CBSI. O CBSI permite aplicar as ferramentas da avaliação da conformidade a setores onde os custos e tempo de avaliação seriam impeditivos em programas tradicionais como o *Common Criteria* e o *Cryptographis*

Module Validation Program. O Programa CBSI foi concebido de tal maneira a estar compatível com os principais programas de avaliação da conformidade de segurança da informação atualmente em vigor no Brasil. Tal abordagem traz benefícios evidentes, na medida em que permite o aproveitamento, para diversos programas de avaliação da conformidade, de um mesmo arcabouço normativo, metodologias de ensaio e rede de laboratórios acreditados. Em particular, o modelo concebido está alinhado aos programas de avaliação da conformidade para Registradores Eletrônico de Ponto [INMETRO2011], para equipamento de certificação digital padrão ICP-Brasil [INMETRO2013] e para medidores inteligentes no âmbito da Metrologia Legal [INMETRO2012]. Adicionalmente, observam-se oportunidades de aplicação do Programa CBSI tanto nas esferas de Defesa Cibernética [BARBALHO2018] quanto na área de compras públicas da Administração Federal [EPING]. Finalmente, vislumbra-se a possibilidade de utilização do arcabouço do Programa por outros países da América Latina, o que pode ser viabilizado por meio do estabelecimento de acordos de reconhecimento mútuo.

Referências

[AISEP] Australasian Information Security Evaluation Program. [s.d.]. Disponível em: <https://www.asd.gov.au/infosec/aisep/faq.htm#acafunctions>. Acesso em: 23/maio/18.

[ANSSI-CSPN] Certification de Sécurité de Premier Niveau . [s.d.]. Disponível em: <https://www.ssi.gouv.fr/administration/produits-certifies/cspn/>. Acesso em: 10/janeiro/19.

[BARABANOV2014] BARABANOV, A.; MARKOV, A.; TSIRLOV, V. Russian IT Security Certification Scheme : Steps Toward Common Criteria Approach. [s.l.], p. 6–16, [s.d.].

[BARABANOV2015] BARABANOV, A.; MARKOV, A. Modern trends in the regulatory framework of the information security compliance assessment in Russia based on common criteria. In: Proceedings of the 8th International Conference on Security of Information and Networks - SIN '15. [s.l.]: [s.n.], 2015. Disponível em: <https://npo-echelon.ru/publications/cc_sinconf_2015.pdf>. Acesso em: 12/abr./18. ISBN: 9781450334532, DOI: 10.1145/2799979.2799980.

[BARBALHO2018] BARBALHO, Sanderson César Macêdo et al. Diagnóstico dos processos de homologação e certificação de produtos de natureza cibernética: perspectivas para a construção de um sistema nacional. **Revista Produção Online**, Florianópolis, v. 18, n. 2, p. 424-453, jun. 2018. ISSN 16761901..

[COMMONCRITERIA2017] COMMON CRITERIA. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model. Common Criteria, [s.l.], v. 3.1, no April, p. 1–106, 2017.

[EPING] Padrões de Interoperabilidade de Governo Eletrônico Documento de Referência. 2017. Disponível em https://www.governodigital.gov.br/documentos-e-arquivos/e-ping/e-PING_v2017_20161221.pdf. Última consulta 10/janeiro/2019.

[INMETRO2011] Portaria INMETRO / MDIC número 480 de 15/12/2011. Disponível em http://www.inmetro.gov.br/legislacao/detalhe.asp?seq_classe=1&seq_ato=1768. Última consulta 10/janeiro/2019.

Galoá { Este trabalho foi publicado utilizando o **Galoá** proceedings

[INMETRO2012] Portaria INMETRO / MDIC número 586 de 01/11/2012. Disponível em http://www.inmetro.gov.br/legislacao/detalhe.asp?seq_classe=1&seq_ato=1928. Última consulta 10/janeiro/2019.

[INMETRO2013] Portaria INMETRO / MDIC número 8 de 08/01/2013. Disponível em http://www.inmetro.gov.br/legislacao/detalhe.asp?seq_classe=1&seq_ato=1958. Última consulta 10/janeiro/2019.

[ISO2018] Using ISO/CASCO Standards in Regulation. Último acesso em outubro/2018: https://www.iso.org/sites/cascoregulators/documents/casco-regulators-fulltext.pdf.

[LEAMAN2013] LEAMAN, Dana. S.. NVLAP Cryptographic and Security Testing. http://dx.doi.org/10.6028/NIST.HB.150-17. 2013.

[LEAMAN2014] LEAMAN, Dana. S. NVLAP Common Criteria Testing. http://dx.doi.org/10.6028/NIST.HB.150-20 . 2014.

[MELLADO2007] MELLADO, D.; FERNÁNDEZ-MEDINA, E.; PIATTINI, M. A common criteria based security requirements engineering process for the development of secure information systems. Computer Standards & Interfaces, [s.l.], v. 29, no 2, p. 244–253, 2007. ISBN: 0920-5489, ISSN: 09205489, DOI: 10.1016/j.csi.2006.04.002.

[NIST_FIPS140-2] NIST FIPS 140-2. Change, [s.l.], v. 46, no 2, p. 69, 2001. ISBN: 140-2, ISSN: 03601315.

[VIANA2017] VIANA FILHO, Carlos; Machado, Raphael. Caminhos para a Segurança Normalização ou Adequação de Padrões. III Workshop sobre Regulação, Avaliação da Conformidade, Testes e Padrões de Segurança, 2017.

[ZHUOHUI2008] ZHUOHUI LIU, C. X. C. Common Criteria in China. 2008. Disponível em: <https://www.commoncriteriaportal.org/iccc/9iccc/pdf/A2311.pdf>. Acesso em: 07/maio/18.