REFERÊNCIA

MIRANDA, Rhoxanna Crhistianth Farago; BARBALHO, Sanderson César Macêdo. Análise da sistemática de homologação e certificação de produtos cibernéticos: estudo de caso comparativo entre empresas e órgãos reguladores. In: CONGRESSO BRASILEIRO DE INOVAÇÃO E GESTÃO DE DESENVOLVIMENTO DO PRODUTO, 11., 2017, São Paulo. **Proceedings** [...]. São Paulo: Blucher, 2017. DOI: 10.5151/cbgdp2017-107. Disponível em: https://www.proceedings.blucher.com.br/article-details/anlise-da-sistemtica-de-homologao-e-certificao-de-produtos-cibernticos-estudo-de-caso-comparativo-entre-empresas-e-rgos-reguladores-27570. Acesso em: 29 maio 2020.

ANÁLISE DA SISTEMÁTICA DE HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS CIBERNÉTICOS: ESTUDO DE CASO COMPARATIVO ENTRE EMPRESAS E ÓRGÃOS REGULADORES

Rhoxanna Crhistianth Farago Miranda (rhoxanna@gmail.com) – Engenharia de Produção, Universidade de Brasília (UnB)

Sanderson César Macêdo Barbalho (sandersoncesar@unb.br) – Engenharia de Produção, Universidade de Brasília (UnB)

RESUMO

As empresas, independentemente da área de atuação, dependem extremamente de tecnologias de informação e comunicação na realização de suas atividades. O objetivo deste trabalho é a realização de um diagnóstico da sistemática de homologação e certificação de produtos cibernéticos e identificação dos requisitos de segurança utilizados nas empresas e organismos de certificação através da comparação com um modelo de referência em desenvolvimento de produtos. Este artigo busca responder três questões: 1. Que adaptações seriam necessárias a um modelo de referência em desenvolvimento de produtos para que possa ser aplicado em empresas cujos produtos são cibernéticos? 2. Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho? 3. Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho? O trabalho utiliza dois procedimentos de pesquisa: a pesquisa bibliográfica e estudo de caso. A utilização do diagnóstico serviu para identificar as práticas de homologação e certificação empregadas pelas empresas e órgãos públicos. Além disso, contribui na elaboração de estratégias de certificação e homologação de produtos cibernéticos.Palavras-chave: Cibernética; Homologação; Certificação; Processo de desenvolvimento de produtos; ISO/IEC-15408

Área: Gestão do Processo de Desenvolvimento de Produtos e Serviços

1. INTRODUÇÃO

A cibernética se encontra inserida no mundo moderno, tecnológico, presente no cotidiano da vida das pessoas e das organizações, seja através das aplicações em um ambiente de rede corporativa ou na utilização de dispositivos tecnológicos. Esses produtos apresentam grande influência tanto no aspecto de privacidade como de forma mais macro, do controle do Estado sobre as ações de empresas e indivíduos, o que leva o Brasil a aceitar uma legislação que impõe a disponibilização das informações produzidas por essas tecnologias para o uso do Governo, em aspectos de segurança e combate ao terrorismo (BARBALHO, 2006). Essa problemática enfrentada pelo Brasil acontece também com outras potências, como a União Europeia que busca uma regulamentação do uso desses sistemas e tecnologias estrangeiras. Esses produtos apresentam características de integração de diversas tecnologias de controle e projetos de engenharia inteligente, o que os tornam também, vulneráveis a ataques cibernéticos. Por outro lado, diversos fatores contribuem com o aumento das vulnerabilidades, como a pressa no lançamento de um produto, crescente número de atacantes, integração tecnológica, dentre outros (NAKAMURA; GEUS, 2007). Alguns autores como Shafqat e

Massod (2016) relatam a ausência de uma padronização em segurança cibernética em vários países de diferentes regiões do mundo, incluindo estratégias e planos de ação. Relatam ainda a Malásia como o país mais experiente em cibernética, porém, assim como o Irã e Israel, não compartilham suas estratégias de segurança cibernética. Este trabalho busca responder três questões: 1. Que adaptações seriam necessárias a um modelo de referência em desenvolvimento de produtos para que possa ser aplicado em empresas cujos produtos são cibernéticos? 2. Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho? 3. Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho? O presente trabalho se encontra alinhado ao Modelo de Referência Mecatrônico (MRM), um modelo analítico para dar suporte ao desenvolvimento de produtos mecatrônicos, proposto por Barbalho (2006). Apresenta-se a visão dos processos das fases de homologação e validação do MRM, assim como alguns requisitos de segurança do produto propostos pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). O modelo analítico construído será utilizado para realizar estudos de caso em cinco empresas públicas e privadas no âmbito da cidade de Brasília, sendo a base para sugerir melhorias para as empresas analisadas e diretrizes para órgãos públicos.

2. METODOLOGIA

Quanto à natureza da pesquisa este estudo caracteriza-se pela pesquisa aplicada sendo dirigida a soluções de problemas específicos. Quanto aos objetivos gerais é possível classificar este estudo como pesquisa exploratória, segundo Gil (2008), pode envolver levantamento bibliográfico, entrevistas com pessoas experientes no problema pesquisado. É exploratória principalmente pelo fato de ser um tema pouco explorado, com pouca bibliografia científica à respeito. Os procedimentos utilizados neste estudo caracterizam-se pela pesquisa bibliográfica e estudo de caso. Sob os aspectos da abordagem do problema classificou-se este estudo como pesquisa qualitativa.

Para realização do diagnóstico do estudo de caso utiliza-se três formulários: Formulário de Análise do Processo de Homologação do Produto, Formulário de Análise do Processo de Certificação do Produto e Formulário de Análise dos requisitos de segurança do produto. Os estudos de casos realizados na pesquisa em campo incluem dois tipos distintos: três órgãos públicos e duas empresas do setor privado instaladas em Brasília. Definiu-se que as empresas privadas deveriam fornecer ou desenvolver produtos/serviços cibernéticos. No caso dos órgãos públicos deveriam apresentar procedimentos de homologação e certificação para produtos cibernéticos desenvolvidos por empresas privadas. A Empresa A do estudo de caso é desenvolvedora de uma solução integrada de segurança da informação em *Software* do tipo IDS/IPS e filtro de aplicações, cujo objetivo é proteger a integridade da rede de ameaças cibernéticas. O produto cibernético da Empresa B é uma tecnologia embarcada para rastreamento veicular, sendo o mesmo fornecido diretamente pelo fabricante.

No caso dos Órgãos reguladores, o produto cibernético em estudo no Órgão Regulador A são os Veículos Aéreos Não Tripulados (VANT), também conhecidos como "Drones". Já no Órgão Regulador B são os Módulos de Segurança Criptográficos (MSC, também conhecidos como HSM – *Hardware Security Modules*) e podem ser definidos como dispositivos de criptografia baseado em *hardware* (ICP Brasil, DOC-ICP-10.05). Já o Órgão regulador C especifica serviços cibernéticos no âmbito da Administração Pública Federal - APF, como por exemplo, VoIP, correio eletrônico, dentre outros.

A coleta dos dados foi realizada através da aplicação dos formulários e as questões propostas nos mesmos tiveram como objetivo a realização do diagnóstico da sistemática de homologação e certificação utilizada pelas empresas/órgãos para produtos cibernéticos. Além disso, possibilita identificar se os mesmos incluem em seus processos alguns dos requisitos para segurança do produto previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

O Formulário de Análise do Processo de Homologação do Produto é composto por 24 perguntas baseadas na fase de homologação do produto do MRM proposto por Barbalho (2006) e referentes ao processo de verificação e validação de software. A coleta de dados do Formulário de Homologação inclui os seguintes itens: Protótipo; Carregamento e Teste do *Software*; Configurações no *Hardware*; Características de *Hardware*; Integração *Software/Hardware*; Especificação dos Componentes Mecânicos e Interfaces Elétrica/Eletrônica; Montagem e manufatura dos Componentes Mecânicos e Eletrônicos; Revisão dos Componentes Mecânicos e Eletrônicos; Falhas; Recursos de Produção; Fornecedores; Instalação, Criticidade, Validação/Verificação e Desenvolvimento do *Software*; Testes; Documentação; Impactos de mudanças; Projeto; Qualidade; Conclusão da Homologação e Documentação.

Já o Formulário de Análise do Processo de Certificação do Produto é composto por seis perguntas baseadas na fase de validação do produto do MRM proposto por Barbalho (2006). A coleta de dados do Formulário de Certificação inclui os seguintes itens: Planejamento e Documentação da Certificação; Documentação do Produto; Conformidade do Produto aos Requisitos Normativos; Testes e Certificação do Produto.

Já o Formulário de Análise baseado na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) é composto por oito perguntas relativas aos requisitos de segurança de produtos de TI. A coleta de dados do Formulário dos requisitos de segurança do produto inclui os seguintes itens: Perfil de Proteção; Documentação de Desenvolvimento e Usuário Final; Controles de Desenvolvimento e Manutenção; Segurança; Testes; Vulnerabilidades e Níveis de Avaliação do Produto. Cada nível corresponde a um pacote de requisitos de garantia de segurança envolvendo itens das respectivas classes.

3. REFERENCIAL TEÓRICO

Os principais temas dentro dos quais o trabalho está inserido incluem cibernética, segurança, mecatrônica, Processo de Desenvolvimento de Produtos (PDP) e MRM. O tema principal do trabalho encontra-se no processo de desenvolvimento de produtos (PDP). É sobre essa sistemática que se justifica o desenvolvimento do trabalho e para a qual pretende agregar contribuição. No trabalho de Boccardo et al. (2015), é apresentado um modelo de segurança para ambientes de avaliação e testes de *software* através da implementação de controles lógicos. No trabalho de Al-Ahmad (2013) são apresentadas soluções estratégicas de segurança contra ataques de guerra cibernética para proteção de infraestruturas de TI, tanto para o setor público como para o privado. Conforme o autor, as soluções devem ser revisadas periodicamente para lidar com novas ameaças.

A falta de uma padronização em segurança cibernética assim como o compartilhamento de informações pertinentes às estratégias adotadas é um problema enfrentado por muitos países, conforme mostra o trabalho de Shafqat e Massod (2016), no qual os autores realizam uma comparação das estratégias nacionais de segurança cibernética em 20 países distintos. É essa lacuna existente na literatura em relação à padronização para o desenvolvimento de produtos

cibernéticos que este trabalho busca suprir. É possível encontrar diferentes abordagens para o desenvolvimento de produtos, sendo a abordagem simultânea de Cooper (1993) a que se encaixa melhor no propósito deste trabalho, uma vez que possibilita o aumento do paralelismo entre as atividades de desenvolvimento, com destaque na realização simultânea das tarefas de projeto e planejamento de processo, Rozenfeld (2006). Existem outras abordagens para o desenvolvimento de produtos, como por exemplo, a definida por Barbalho (2006), como suporte ao desenvolvimento de produtos mecatrônicos, a qual foi escolhida uma vez que esses produtos segundo Wiener (1968) são considerados essencialmente cibernéticos o que viabilizou sua utilização.

4. ANÁLISE DOS CASOS ESTUDADOS

Os estudos de casos deste trabalho, considerando os órgãos públicos, apresentam critérios distintos em relação ao processo de homologação e certificação de produtos. Entretanto, considerando as empresas privadas, apresentam procedimentos semelhantes para homologar e certificar seus produtos. Além disso, as práticas de segurança adotadas pelas empresas/órgãos dos estudos de casos, em sua grande maioria, refletem boa parte dos requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Os órgãos públicos analisados neste estudo apresentam procedimentos sistematizados para a homologação e certificação de produtos de natureza cibernética. Nos Órgãos B e C algumas atividades do processo de homologação são recomendadas ao fabricante, como por exemplo, protótipos, especificação de componentes, validação do *software*, testes, etc. No caso o órgão B recomenda ao fabricante a utilização do padrão FIPS-1402 (NIST, 2001).

Em relação às atividades de certificação do produto, os órgãos reguladores A e B apresentam procedimentos semelhantes. O Órgão Regulador A possui regulamento específico para homologar e certificar os produtos que regula. No caso do Órgão Regulador B, os critérios para homologação e certificação consolidam as políticas estabelecidas pela Infraestrutura de Chaves Públicas Brasileira do ICP-Brasil (2012). Entretanto, o Órgão Regulador C encontra-se em processo de desenvolvimento e atualização do Programa Nacional de Homologação e Certificação de Ativos de TIC's. Ao adotar o padrão *Common Criteria* (CC) na especificação dos serviços para a APF o Órgão C está emitindo um requisito de certificação para esse tipo de produto. Observou-se que os Órgãos Reguladores B e C utilizam os requisitos previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). No caso do órgão C, verificou-se uma maior cobertura das classes, devido à grande necessidade de segurança na prestação do serviço público ao cidadão, assim como aos riscos que os problemas de segurança possam impactar na Disponibilidade, Integridade, Confidencialidade e Autenticidade.

Entretando, observou-se que o Órgão Regulador A apresenta um pequeno escopo para cobertura dos requisitos previstos na referida norma como por exemplo, *Protection Profile* (PP), documentação para o usuário, segurança e testes. Outros itens ficam a cargo do fabricante do produto, como, por exemplo, documentação e controles para o desenvolvimento do produto, análise de vulnerabilidades e níveis de garantia para avaliação do produto, concluindo que o referido órgão não suporta a Norma ISO/IEC_15408 (COMMON CRITERIA, 2012).

Considerando as empresas privadas analisadas neste estudo, verificou-se que a Empresa A apresenta procedimentos bem definidos para o processo de homologação do produto, desde a definição de protótipos até a documentação para homologação, com exceção apenas de procedimentos para os componentes mecânicos. A Empresa B recebe o produto diretamente do fabricante, ou seja, o produto já passou por todo o ciclo de desenvolvimento, porém necessita de algumas configurações iniciais realizadas no *Hardware* para o funcionamento do

Software, como por exemplo, parâmetros do APN (*Access Point Name*) protocolo de comunicação das redes GSM e configurações no endereço do SIMCard. Em relação ao processo de certificação do produto as empresas privadas analisadas apresentam procedimentos semelhantes. A certificação na Empresa A segue a Metodologia de Avaliação da CERTICS para *Software* (CTI ARCHER, 2013) e a estrutura do modelo segue os requisitos previstos na Norma ISO/IEC 15504-2 (ABNT, 2008). No caso da Empresa B existem três órgãos envolvidos no processo: a Anatel, a Cesvi Brasil e o Denatran.

Em relação a utilização dos requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012), foram observadas algumas diferenças de utilização pelas empresas privadas do estudo. A Empresa A desenvolve parte do *Software* do produto cibernético e importa alguns componentes do *hardware*, utiliza documentação para descrever o produto, incluindo alguns dos itens previstos no Perfil de Proteção (PP) da referida norma, como, por exemplo, documentação de requisitos, segurança, RFC-2547 (SEMERIA, 2001), análise da segurança do código. Entretanto, a Empresa B não apresenta documentação para o desenvolvimento do produto, apenas verifica se os parâmetros de segurança do mesmo são atendidos.

5. DISCUSSÃO

Os resultados dos estudos de casos demonstraram que a metodologia utilizada permitiu identificar a sistemática de homologação e certificação utilizadas pelas empresas privadas e órgãos públicos pesquisados. Além disso, possibilitou a identificação de requisitos de segurança necessários aos produtos cibernéticos em estudo como por exemplo os sugeridos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). As questões de pesquisa foram respondidas da seguinte forma: 1. Que adaptações seriam necessárias ao MRM para que possa ser aplicado em empresas cujos produtos são cibernéticos? Segundo Wiener (1984), os produtos mecatrônicos são considerados essencialmente cibernéticos. Diante deste fato tornou-se viável a utilização do MRM desenvolvido por Barbalho (2006) complementado por requisitos do *Common Criteria* (ISO/IEC_15480) e da Norma IEEE 1012-2012 na realização do diagnóstico da sistemática de homologação e certificação dos produtos cibernéticos. Verificou-se que o MRM proposto por Barbalho (2006) poderia ser adaptado para ser utilizado em produtos cibernéticos incluindo questionamentos mais específicos em relação ao *Software*, como, por exemplo, as características para que o *Hardware* funcione com o mesmo, pois muitos produtos cibernéticos requerem uma grande quantidade de *Hardware* para o seu funcionamento.

2. Em Órgãos Reguladores há adequação dos requisitos para homologação e certificação de produtos cibernéticos aos propostos no trabalho ? Nos Órgãos reguladores do estudo de caso observou-se que algumas recomendações ao fabricante estavam descritas em documentação específica de cada órgão, direcionando o processo de homologação e certificação. O Órgão Regulador B obteve maior cobertura quanto aos itens de homologação do produto. No caso do órgão A não foi verificado procedimentos para integração do *software* ao *hardware*, especificação dos componentes mecânicos, procedimentos de montagem e manufatura dos componentes mecânicos e eletrônicos, além dos itens não contemplados pelo Órgão Regulador B, como por exemplo, criticidade do *software*, recursos de produção do produto, dentre outros. Observou-se que Órgão C contempla a grande maioria dos itens do Formulário de Homologação, porém outros itens não são contemplados, como por exemplo, protótipos, montagem de componentes mecânicos, impactos de mudança no *software*, dentre outros. Observou-se que apenas os Órgãos reguladores B e C adotam em grande parte os requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Os processos

de homologação e certificação adotados pelos órgãos reguladores neste estudo mesmo considerando suas especificidades inerentes às características de cada produto cibernético, proporcionaram uma visão do entendimento do processo e dos requisitos do produto.

3. Em empresas desenvolvedoras de produtos cibernéticos, há atendimento aos requisitos de homologação e certificação propostos no trabalho ? Nas empresas privadas do estudo de caso foram identificadas várias atividades relacionadas ao processo de homologação e certificação de produtos cibernéticos. Porém, quando componentes do produto eram adquiridos de fornecedores, as atividades relacionadas com o ciclo de desenvolvimento do produto não eram conhecidas. Foi o caso observado na Empresa B. Observou-se que a certificação do produto na Empresa A segue a Metodologia de Avaliação CERTICS para *Software*, porém, na Empresa B o planejamento da certificação fica a cargo do fabricante. Observou-se que apenas a Empresa A adota em sua grande maioria os requisitos de segurança previstos na Norma ISO/IEC_15408 (COMMON CRITERIA, 2012). Assim, considera-se que a resposta para esta pergunta é diferenciada para as empresas, havendo conhecimento do cumprimento dos requisitos de homologação e certificação do produto com maior cobertura apenas pela Empresa A.

O estudo permitiu identificar as lacunas existentes entre os requisitos de segurança relacionados à defesa cibernética e as práticas de homologação e certificação adotadas pelas Empresas/Órgãos. Além disso, alguns autores (SHAFQAT; MASSOD, 2016), reconhecem a lacuna existente na literatura da ausência de uma padronização em segurança cibernética. Através da pesquisa foi possível contribuir cientificamente para a elaboração de estratégias de certificação e homologação de produtos cibernéticos, tendo como base o MRM proposto por Barbalho (2006) com as devidas adptações sugeridas aos produtos cibernéticos. Além disso, a adoção de requisitos de segurança propostos pela Norma ISO/IEC_15408 (COMMON CRITERIA, 2012) viabiliza o desenvolvimento de produtos cibernéticos com maior grau de confiabilidade.

6. CONCLUSÕES

O estudo se delimitou na realização do diagnóstico da sistemática de homologação e certificação de produtos cibernéticos. A implementação dos requisitos de segurança propostos pela norma ISO/IEC_15408 (COMMON CRITERIA, 2012) nas empresas dos estudos de caso, não é escopo deste trabalho. Nesse sentido, devido a apresentação de restrições de publicidade de informações internas consideradas por algumas empresas como sigilosas, muitas organizações não permitem uma intervenção mais profunda em seus processos. Portanto, embora não seja possível realizar de fato a implementação dos requisitos de segurança no processo de desenvolvimento do produto nas empresas deste estudo, o trabalho contribuiu com o fornecimento de recomendações de melhorias e diretrizes para o desenvolvimento de tais produtos (especificamente no que tange à homologação e certificação) com base na realização do diagnóstico.

No decorrer do trabalho algumas considerações tornaram-se relevantes, como por exemplo, a necessidade de parceria entre as empresas públicas e privadas para realização dos testes nos serviços de TICs para a APF, além da criação de uma entidade que certifique empresas a prestarem serviços que possam comprometer a segurança nacional, conforme constatado pela literatura no trabalho de Min, Chai e Han (2015). Como direções para pesquisas futuras sugere-se a definição dos testes específicos para validação dos requisitos dos ativos de TICs utilizados pela APF. Neste caso, sugere-se explorar os tipos de testes realizados pelos

laboratórios acreditados, o que requer uma análise mais profunda e específica. Além disso, pode-se adicionar perguntas ao Formulário de homologação do produto, envolvendo características mínimas do ambiente para o funcionamento do mesmo, pois alguns produtos, devido à sua complexidade podem exigir condições específicas do ambiente para sua operação.

7. REFERÊNCIAS

AL-AHMAD, W. A detailed strategy for managing corporation cyber war security. International Journal of Cyber-Security and Digital Forensics, v.2, n. 4, p.1-9, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 15504-2: Tecnologia da informação: Avaliação de processo: Parte 2: Realização de uma avaliação. Rio de Janeiro, 2008.

BARBALHO, S. C. M. Modelo de referência para o desenvolvimento de produtos mecatrônicos: proposta e aplicações. Tese (Doutorado em Engenharia Mecânica) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2006.

BOCCARDO, D. R. et al. Modelo de segurança para ambientes de avaliação e testes de segurança de software. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 15., 2015, Florianópolis. Anais... . Florianópolis: Sociedade Brasileira de Computação, 2015. p. 501 – 509

CENTRO DE TECNOLOGIA DA INFORMAÇÃO RENATO ARCHER. Metodologia de Avaliação da CERTICS para Software. Campinas, 2013. Disponível em: <http://www.certics.cti.gov.br/downloads/Definicao_MetodologiaCERTICS.pdf>. Acesso em: 31 out. 2016.

COOPER, R. Winning at New Product: accelerating the process from idea to launch. Massachussetts: Addison-Wesley Publishing Company, 1993.

COMMON CRITERIA. Common Criteria for information technology security evaluation: part 3: Security assurance components. S. L, 2012. Disponível em: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf>. Acesso em: 04 jun. 2015.

GIL, A. C. Métodos e técnicas de pesquisa social. 6.ed. São Paulo: Atlas, 2008.

INFRAESTRUTURA DE€ CHAVES€ PÚBLICAS€ BRASILEIRA. DOC-ICP 10.05: Padrões e procedimentos técnicos a serem observados nos processos de homologação de Módulos de Segurança Criptográfica (MSC) no âmbito da ICP-Brasil. 2007. Disponível em: <http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/DocIcp/DOC-ICP-10.05_-_v_1.0.pdf>. Acesso em: 20 out. 2016

MIN, K.; CHAI. S.; HAN, M. An international comparative study on cyber security strategy. International Journal of Security and Its Applications. v. 9, n. 2, p. 13-20, 2015.

NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes em Ambientes Cooperativos - Fundamentos, Técnicas, Tecnologias, Estratégias. São Paulo/SP. Editora Novatec, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. FIPS PUB 140-2: Security requirements for cryptographic modules. 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Acesso em: 12 ago. 2016

ROZENFELD, H. Gestão de Desenvolvimento de Produtos. São Paulo/SP: Editora Saraiva, 2006.

SEMERIA, Chuck. RFC 2547bis: BGP/MPLS VPN Fundamentals. Sunnyvale: Juniper Networks, 2001. Disponível em: <https://pdfs.semanticscholar.org/d274/2676bc8c35b3e9700143d938ecf6f285a885.pdf>. Acesso em: 02 nov. 2015.

SHAFQAT, N.; MASSOD, A. Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security. v. 14, n. 1, p. 129-136, 2016.

WIENER, N. Cibernética e sociedade: o uso humano de seres humanos. 3.ed., São Paulo: Cultrix, 1968.

ROZENFELD, H. et al. Gestão de Desenvolvimento de Produtos: uma referência para a melhoria do processo. São Paulo: Saraiva, 2006. 542 p.