SUSTENERE Publishing Corporation

RBADM REVISTA BRASILEIRA DE ADMINISTRAÇÃO CIENTÍFICA

Journals Homepage:
www.sustenere.co/journals

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO: UM MODELO DE ANÁLISE PARA INSTITUTOS DE PESQUISA PÚBLICOS

RESUMO

A informação é considerada um ativo crítico para muitas organizações, como institutos de pesquisa, e mais ainda da esfera pública. Essas organizações tem a informação como matéria prima e como um dos seus produtos, e de acordo com parte da literatura que trata do tema, medidas de Segurança da Informação são adotadas nessas organizações seguindo orientações da estrutura de Governança da Segurança da Informação, visando proteger a informação e garantir a continuidade de suas atividades. Essas organizações também atuam sob forte regulação por parte do Governo e de outros órgãos que fiscalizam sua atuação como organizações públicas e também suas atividades de pesquisa. Diante disso, as decisões sobre a adoção de medidas de Segurança da Informação podem ser tomadas não para seguir orientações da estrutura de Governança da Segurança da Informação, mas como uma resposta a forças do ambiente externo no qual essas organizações estão inseridas. Este artigo tem como objetivo propor um modelo de análise que permita investigar os fatores que levam à adoção de medidas de Segurança da Informação em institutos de pesquisa públicos, tendo uma dimensão Organizacional, cujos indicadores baseiam-se principalmente na Governança da Segurança da Informação, e uma dimensão Institucional, cujos indicadores baseiam-se na Teoria Institucional.

PALAVRAS-CHAVES: Segurança da Informação; Institutos de Pesquisa; Medidas de Segurança.

ADOPTION OF INFORMATION SECURITY PRACTICES: AN ANALYTICAL FRAMEWORK FOR PUBLIC RESEARCH INSTITUTES

ABSTRACT

Information is considered a critical asset for many organizations, like research institutes, and specially in the public sector. These organizations have the information as input and as one of its products, and according to many studies on the subject, Information Security measures are adopted in these organizations following Information Security Governance structure guidelines, aiming to protect the information and ensure continuity of its activities. These organizations also work under severe regulation from government and other public agencies that supervise their performance as public and as research organizations too. Thus, decisions about adoption of Information Security measures can be taken not to follow the Information Security Governance structure guidelines, but as a response to forces from the external environment of these organizations. This paper aims to propose an analytical model to investigate the factors that drive the adoption of Information Security measures in public research institutes, having an organizational dimension, whose indicators are mainly based on the Information Security Governance, and an institutional dimension, with indicators that are based on Institutional Theory.

KEYWORDS: Information Security; Research Institutes; Security Practices.

Revista Brasileira de Administração Científica,
Aquidabã, v.5, n.2, Out 2014.

*ISSN **2179-684X***

*SECTION: **Articles***
*TOPIC: **Sistemas e Tecnologia da Informação***

Anais do Simpósio Brasileiro de Tecnologia da Informação (SBTI 2014)

DOI: 10.6008/SPC2179-684X.2014.002.0004

Antônio Eduardo de Albuquerque Junior
Universidade Federal da Bahia, Brasil
http://lattes.cnpq.br/9293798825143859
emarques@ufba.br

Ernani Marques dos Santos
Universidade Federal da Bahia, Brasil
http://lattes.cnpq.br/5388965130432483
emarques@ufba.br

Received: 07/08/2014
Approved: 15/10/2014
Reviewed anonymously in the process of blind peer.

Referencing this:

*ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M.. Adoção de medidas de segurança da informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica**, Aquidabã, v.5, n.2, p.46-59, 2014. DOI: http://dx.doi.org/10.6008/SPC2179-684X.2014.002.0004*

INTRODUÇÃO

A informação é reconhecida por Sêmola (2014) como um ativo crítico para a continuidade operacional e saúde da organização. Para Fachini et al. (2011), a informação impulsiona o processo de tomada de decisões, enquanto Sêmola (2014) argumenta que há informações fundamentais que se revelam como importante diferencial competitivo para uma organização. A Associação Brasileira de Normas Técnicas (ABNT) (2005) entende a informação como um ativo organizacional essencial que, por esse motivo, precisa ser adequadamente protegido.

Para proteger esse ativo, medidas de Segurança da Informação podem ser aplicadas, considerando que cada organização tem características próprias que levam a necessidades particulares (SÊMOLA, 2014). Por suas características, institutos de pesquisa necessitam proteger a informação e também o conhecimento produzido em suas atividades (ALEXANDRIA, 2009), pois a informação é um diferencial competitivo (PIMENTA et al., 2010), além de uma matéria prima e também um dos seus produtos, sendo um dos seus ativos mais valiosos (CAMINHA et al., 2006).

Também organizações públicas necessitam promover a Segurança da Informação. Além de proteger informações sobre os cidadãos, estas organizações tem obrigação preservar e fornecer informações cujo acesso é de interesse público, bem como garantir a continuidade dos serviços prestados para a sociedade. Além disso, utilizam recursos públicos para se mantiver, seguem normas do Governo e são fiscalizadas por órgãos como o Ministério do Planejamento, Orçamento e Gestão (MPOG), Controladoria Geral da União (CGU) e Tribunal de Contas da União (TCU), inclusive com relação à Segurança da Informação. Cepik et al. (2010) observam que o TCU tem auditado as organizações públicas quanto a questões relativas à Segurança da Informação.

Quando uma organização se enquadra tanto como instituto de pesquisa quanto como pública, assume as obrigações e necessidades relativas à Segurança da Informação desses dois contextos. Tais quais outras organizações públicas, os institutos de pesquisa necessitam garantir a continuidade dos serviços prestados à sociedade e são regulados e fiscalizados pelo TCU, CGU e MPOG ou órgãos correlatos das esferas estadual e municipal, e tal quais outros institutos de pesquisa, estão sujeitos à legislação que trata das atividades de pesquisa e tem a necessidade de proteger informações sensíveis e, como consequência, garantir a continuidade das pesquisas que desenvolvem. Mas a adoção de medidas de Segurança da Informação em institutos de pesquisa públicos pode ser resultado não de decisões tendo por objetivo a continuidade das operações e a proteção de informações sensíveis, e sim como resultado de forças existentes no ambiente em que essas organizações estão inseridas.

Assim, medidas de Segurança da Informação podem ser adotadas por institutos de pesquisa públicos para atender a obrigações legais e regulamentares e convênios firmados com outras organizações que desenvolvem ou financiam pesquisas científicas. A adoção de medidas de Segurança da Informação pode também ser resultado do reconhecimento e ampla utilização de

padrões e normas internacionais que trazem recomendações bem aceitas por organizações e governos de todo o mundo, e que estão também associadas a um mercado de treinamento e certificação que forma gestores e especialistas em Segurança da Informação que buscam a proteção da informação com base em suas recomendações. Experiências de outras organizações de pesquisa podem servir de modelo para ações de Segurança da Informação diante das incertezas e riscos relacionados, motivadas pelo sucesso dessas organizações na adoção de medidas de Segurança da Informação, ou apenas por terem destaque no campo em que atuam. Nesses casos, o objetivo da adoção das medidas pode ser alcançar reconhecimento diante do Governo, agências de fomento e outras organizações que desenvolvem ou financiam pesquisas científicas, e não a proteção da informação por si.

Diante dessa possibilidade, este artigo teve como objetivo propor um modelo de análise organizado em duas dimensões que permite investigar os fatores que levam à adoção de medidas de Segurança da Informação em institutos de pesquisa públicos. A primeira dimensão é voltada para fatores internos, que levam à adoção de medidas visando a continuidade das operações – a dimensão Organizacional, abordada pela ótica da Governança da Segurança da Informação. A segunda dimensão tem seu foco em fatores do ambiente, que levam à adoção de medidas para que a organização tenha legitimação em seu meio – a dimensão Institucional, amparada pela Teoria Institucional.

METODOLOGIA

Este artigo é motivado pela necessidade de identificar os fatores que levam à adoção de medidas de Segurança da Informação em institutos de pesquisa públicos. Os fatores podem ser organizados em duas dimensões: a dimensão Organizacional, que está associada aos conceitos de Governança da Segurança da Informação apresentados por Moulton e Coles (2003), Von Solms (2005) e Da Veiga e Eloff (2007); e a dimensão Institucional, associada às forças do ambiente institucional apontadas por DiMaggio e Powell (1983) que podem levar à adoção de medidas de Segurança da Informação nas organizações (KAM et al., 2013; HU et al., 2006; SPEARS et al., 2013; HOLGATE et al., 2012; LOPES, 2012; HSU et al., 2012; LUESEBRINK, 2011). A Figura 1 traz uma representação das dimensões e componentes do modelo de análise proposto.

A dimensão Organizacional tem como único componente a Governança da Segurança da Informação, que tem os 13 indicadores apresentados no Quadro 1. Os indicadores desta dimensão permite identificar os motivos que podem levar à adoção de medidas técnicas ou sociais de Segurança da Informação para atender aos objetivos e estratégias organizacionais, e por isso permitem identificar se nos institutos de pesquisa públicos as medidas são adotadas para atender a esses objetivos.

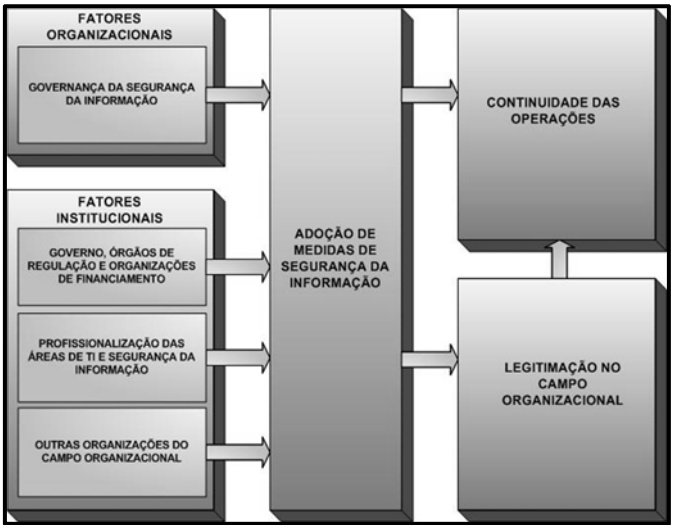

Figura 1: Modelo de análise proposto.

Já a dimensão Institucional possui três componentes: Governo, Órgãos de Regulação e Organizações que Financiam Pesquisas, que tem dois indicadores; Profissionalização das Áreas de TI e Segurança da Informação, com três indicadores; e Outras Organizações do Campo Organizacional, que tem dois indicadores, conforme apresentado no Quadro 2. Esta dimensão possibilita a especificação de fatores que podem levar à adoção de medidas de Segurança da Informação em decorrência da obrigação de respeitar a legislação, ou de pressões da comunidade profissional de TI e Segurança da Informação, ou pela imitação de medidas adotadas por outras organizações do campo organizacional, para atender a uma necessidade de legitimação perante o Governo, agências de fomento e outras organizações de pesquisa. Os indicadores desta dimensão permitem identificar se fatores institucionais, como a legislação e obrigações contratuais, profissionalização dentro do campo e imitação de outras organizações, levam à adoção de medidas de Segurança da Informação.

Tanto fatores organizacionais quanto institucionais podem levar à adoção de medidas de Segurança da Informação: os fatores organizacionais através da orientação da Governança da Segurança da Informação, e os fatores institucionais por meio das forças coercitivas, normativas e miméticas existentes no campo organizacional. Como resultado da adoção dessas medidas, a organização pode tanto garantir a continuidade das suas operações quanto ter legitimação no campo organizacional. Ao mesmo tempo, a legitimação, como propuseram DiMaggio e Powell (1983), pode levar à sobrevivência da organização no campo, ou, em outras palavras, à continuidade das suas operações.

Quadro 1: Quadro teórico com os componentes e indicadores da dimensão Organizacional.

Dimensão Organizacional	
Componente	Indicadores
Governança da Segurança da Informação (MOULTON; COLES, 2003; VON SOLMS, 2005; DA VEIGA; ELOFF, 2007)	Existência de definição formal de papéis e responsabilidades sobre Segurança da Informação para gestores e demais membros da organização (MOULTON; COLES, 2003; NATIONAL..., 2006; DA VEIGA; ELOFF, 2007)
	Existência de estratégias e objetivos de Segurança da Informação definidos e documentados (MOULTON; COLES, 2003; NATIONAL..., 2006; DA VEIGA; ELOFF, 2007)
	Existência de processos de avaliação e gestão de riscos (MOULTON; COLES, 2003; VON SOLMS, 2005; DA VEIGA; ELOFF, 2007)

	Existência de processos de análise da gestão de recursos destinados à Segurança da Informação (MOULTON; COLES, 2003; VON SOLMS, 2005; DA VEIGA; ELOFF, 2007)
	Existência de mecanismos de fiscalização de conformidade das ações de Segurança da Informação com a legislação que trata do assunto (MOULTON; COLES, 2003; VON SOLMS; VON SOLMS, 2006; NATIONAL..., 2006; DA VEIGA; ELOFF, 2007)
	Existência de processos de comunicação sobre Segurança da Informação com agências de fomento, organizações parceiras e que financiam pesquisas (MOULTON; COLES, 2003; VON SOLMS, 2005)
	Existência de diretivas, ações ou de declaração formal de compromisso de gestores e líderes com a Segurança da Informação (MOULTON; COLES, 2003; VON SOLMS, 2005; VON SOLMS; VON SOLMS, 2006; NATIONAL..., 2006; DA VEIGA; ELOFF, 2007)
	Existência de estruturas organizacionais de Segurança da Informação (VON SOLMS, 2005; NATIONAL..., 2006; DA VEIGA; ELOFF, 2007)
	Existência de processos de conscientização para Segurança da Informação (VON SOLMS, 2005; DA VEIGA; ELOFF, 2007)
	Existência de uma Política de Segurança da Informação formal publicada (VON SOLMS, 2005; VON SOLMS; VON SOLMS, 2006; NATIONAL..., 2006)
	Existência de procedimentos organizacionais de Segurança da Informação documentados e seguidos (VON SOLMS, 2005; VON SOLMS; VON SOLMS, 2006; DA VEIGA; ELOFF, 2007)
	Existência de normas e padrões internos de Segurança da Informação documentados (VON SOLMS; VON SOLMS, 2006; DA VEIGA; ELOFF, 2007)
	Existência de mecanismos de fiscalização de conformidade das ações tomadas na organização com a Política de Segurança da Informação (VON SOLMS, 2005; VON SOLMS; VON SOLMS, 2006; DA VEIGA; ELOFF, 2007)

Quadro 2: Quadro teórico com os componentes e indicadores da dimensão Institucional.

Dimensão Institucional	
Componentes	Indicadores
Governo, Órgãos de Regulação e Organizações que Financiam Pesquisas (DIMAGGIO; POWELL, 1983; HU et al., 2006)	Existência de leis, decretos, Instruções Normativas, Normas Complementares e resoluções publicados pelo Governo obrigando a adoção de medidas de Segurança da Informação (HU et al., 2006; LOPES, 2012)
	Existência de convênios firmados com outras organizações de pesquisa ou que financiam pesquisas científicas obrigando a adoção de medidas de Segurança da Informação (LUESEBRINK, 2011)
Profissionalização das Áreas de TI e Segurança da Informação (DIMAGGIO; POWELL, 1983; HU et al., 2006; LOPES, 2012)	Utilização de normas e padrões de Segurança da Informação como modelo para a adoção de medidas de Segurança da Informação (LOPES, 2012; KAM et al., 2013)
	Existência de critérios de seleção de pessoal que exigem formação ou conhecimentos específicos em Segurança da Informação que fazem com que medidas de Segurança da Informação sejam adotadas (HU et al., 2006)
	Participação de profissionais que lidam com Segurança da Informação em redes de compartilhamento de informações e conhecimentos que fazem com que medidas de Segurança da Informação sejam adotadas (HU et al., 2006)
Outras Organizações do Campo Organizacional (DIMAGGIO; POWELL, 1983; HSU et al., 2012)	Utilização de experiências de outras organizações públicas bem sucedidas no campo organizacional como modelo para adoção de medidas de Segurança da Informação (HSU et al., 2012)
	Utilização de experiências de outras organizações que desenvolvem pesquisas científicas bem sucedidas no campo organizacional como modelo para adoção de medidas de Segurança da Informação (HSU et al., 2012)

DISCUSSÃO TEÓRICA

Segurança da Informação é definida por Fontes (2006) como as orientações, normas, procedimentos, políticas e demais ações que visam proteger a informação, possibilitando que a organização realize seu negócio e alcance sua missão. Esta definição é ampla e mostra que a Segurança da Informação vai além de questões técnicas, como defende Albrechtsen (2008), segundo o qual uma abordagem significativa para a Segurança da Informação deve considerar aspectos tecnológicos, humanos, administrativos e organizacionais.

A relevância do componente humano para a Segurança da Informação pode ser observado nos resultados de uma pesquisa com 575 executivos de empresas brasileiras conduzidas pela empresa de consultoria e auditoria. A pesquisa mostrou que 37% dos incidentes tem origem em funcionários, 36% tem origem em ex-funcionários e 16% tem origem em prestadores de serviços terceirizados das organizações. Em uma pesquisa com 400 profissionais de TI, aponta que 52%

deles estão mais concentrados em prevenir ataques de gente da organização do que provocados por agentes externos e que 59% das infecções por vírus e outros programas maliciosos são provocadas por empregados das organizações. Mitnick e Simon (2003) e Silva e Stein (2007) argumentam que a maior fragilidade da Segurança da Informação está no homem, o que leva a uma preocupação com questões sociais.

Mitnick e Simon (2003) e Sêmola (2014) estabelecem que é impossível extinguir por completo os riscos de Segurança da Informação, enquanto Silva e Stein (2007, p.47) atribuem essa impossibilidade aos aspectos sociais relacionados, pois, ainda segundo estas autoras, "o comportamento humano é complexo e envolve variáveis que não podem ser controladas". Como agravante. Svensson (2013) argumenta que os ataques mais comuns à informação se iniciam através da exploração de fraquezas humanas.

Essas questões sociais da Segurança da Informação aplicam-se a todas as organizações de forma indistinta, mas algumas têm a informação como um dos seus ativos mais importantes, e entre elas, destacam-se as que desenvolvem pesquisas científicas (CAMINHA et al., 2006; ALEXANDRIA, 2009).

Caminha et al. (2006) citam como exemplos de informações importantes com que essas organizações lidam as técnicas de gestão, as análises de dados, os projetos e as patentes. Pode-se adicionar a essa lista informações sobre pesquisadores, colaboradores, participantes das pesquisas (entrevistados, respondentes de questionários e pacientes de pesquisas clínicas) e qualquer outra informação cujo sigilo ou guarda sejam obrigatórios por lei ou qualquer regulamento que trate de questões éticas em pesquisa. A falta de uma informação essencial pode inviabilizar uma pesquisa, e a divulgação de uma informação sigilosa pode levar a problemas éticos e legais. Essas características já justificam a preocupação com Segurança da Informação no meio acadêmico.

Mas a Segurança da Informação é crucial também para organizações públicas. Na Administração Pública brasileira, a Segurança da Informação vem sendo regulada por diferentes atos normativos, incluindo leis, decretos e normas complementares (BRITTO, 2011; ARAÚJO, 2012; ALBUQUERQUE JUNIOR & SANTOS, 2013). "Os problemas de vazamento de informações, ou quebra de sigilo em organizações públicas são recorrentes", o que tem levado o Governo Federal a regulamentar a Segurança da Informação em seus órgãos e entidades (ARAÚJO, 2012, p.15). Além disso, a proteção de informações críticas deve ser estabelecida na Administração Pública, pois boa parte dela pode estar vulnerável a interrupções de serviços e funções essenciais, perda de dados e fraudes, que podem afetar a sociedade como um todo (BRITTO, 2011). Aliam-se a isso o fato de a pesquisa científica no Brasil ser realizada principalmente em organizações públicas, com destaque para institutos de pesquisa (HILU & GISI, 2011), e o fato de organizações públicas serem reguladas e fiscalizadas por órgãos como MPOG, CGU e TCU, inclusive quanto à Segurança da Informação.

É discutível a necessidade de garantir a confidencialidade de toda informação de uma organização que desenvolve pesquisas, que nem sempre são patentes, segredos industriais, inovação, direitos autorais ou dados de colaboradores, pacientes ou participantes de pesquisas. Alexandria e Quoniam (2010) apontam isso como um aparente contrassenso, pois a Segurança da Informação procura dificultar a divulgação e o acesso à informação, frustrando a disseminação do conhecimento gerado nas pesquisas científicas, consequentemente. Mas os autores esclarecem que, na realidade, o objetivo é definir o quanto a informação é sensível e sua confidencialidade é necessária. Ainda para eles, mesmo que nem toda a informação seja confidencial, quase sempre é necessário garantir sua integridade e disponibilidade. Assim, a proteção da informação em institutos de pesquisa públicos é crucial para cumprimento das obrigações legais e éticas e para a continuidade das suas atividades. Nesse contexto, a Segurança da Informação exige estruturas e processos organizacionais, políticas e normas, serviços e tecnologia de Segurança da Informação orientados por estratégias e objetivos claros e em conformidade com as estratégias e objetivos da própria organização e do Governo. Em outras palavras, exige que seja estabelecida uma estrutura de Governança da Segurança da Informação.

Governança da Segurança da Informação

No entendimento de Da Veiga e Eloff (2007), a Governança da Segurança da Informação trata de vulnerabilidades, privacidade e implementação de ferramentas de aprimoramento, do estabelecimento de métricas e de avaliações da efetividade da Segurança da Informação, bem como da elaboração de uma estratégia de Segurança da Informação. Já para Von Solms (2006), a Governança da Segurança da Informação envolve questões tanto técnicas quanto não técnicas: é resultado da percepção da alta direção de que, apesar dos recursos gastos com medidas técnicas, a solução para o problema não é exclusivamente técnica, pois os incidentes envolvem questões sociais e os riscos com os quais as organizações lidam pedem decisões estratégicas.

Para Moulton e Coles (2003), Governança da Segurança da Informação é a criação e manutenção do ambiente de controle necessário para gerenciar os riscos relacionados à confidencialidade, integridade e disponibilidade das informações e dos seus processos e sistemas de apoio, envolvendo a definição de responsabilidades e a execução de práticas pelos gestores visando a proteção da informação, a definição de estratégias e objetivos, a avaliação e gestão de riscos, a gestão racional de recursos, a busca pela conformidade com leis, regulamentos, políticas e regras, e as atividades de comunicação e relacionamento com investidores sobre Segurança da Informação. Von Solms (2005) complementa propondo que a Governança da Segurança da Informação consiste no compromisso de gestão e liderança, estruturas organizacionais, conscientização e compromisso dos usuários de TI, políticas, procedimentos, processos, tecnologias e mecanismos de fiscalização de conformidade.

O modelo de Governança da Segurança da Informação proposto por Von Solms e Von Solms (2006) envolve diretivas, políticas, normas organizacionais, procedimentos e operação ou execução de medidas de Segurança da Informação. Já o modelo do *National Institute of Standards and Technology* (NIST) (2006) associa determinações estratégicas superiores a políticas, estratégias, estrutura organizacional, arquitetura, papéis e responsabilidades de Segurança da Informação. Da Veiga e Eloff (2007) também apresentam um modelo que combina componentes técnicos, processuais e orientados às pessoas: compromisso dos líderes, estratégia de Segurança da Informação, avaliação de riscos, métricas e medidas de efetividade da Segurança da Informação, direcionamento de investimentos, estrutura organizacional, respeito à legislação e outros regulamentos, políticas, procedimentos, padrões, guias, certificação e conformidade, auditorias e monitoramento, conscientização e educação, proteção da privacidade, estabelecimento de uma relação de confiança com os membros da organização, gestão de ativos de informação, desenvolvimento de sistemas, gestão de incidentes, operações técnicas, atividades relacionadas ao ambiente físico e continuidade das operações.

Observa-se que a Governança da Segurança da Informação trata de aspectos técnicos e sociais. Marciano e Lima-Marques (2006) também argumentam que a Segurança da Informação é uma questão não só técnica, mas também social. Para estes autores, não existe solução puramente tecnológica conhecida para problemas sociais de Segurança da Informação e, para que o tema seja corretamente abordado, deve ser tratado por uma visão embasada em teorias sociais. Dentre as diferentes abordagens teóricas sociais existentes, Björck (2004) sugere que estudos sobre Segurança da Informação sejam realizados sob a ótica da Teoria Institucional.

Teoria Institucional

Segundo Quinello (2007), a Teoria Institucional é uma abordagem teórica utilizada em estudos sociais que parte do princípio de que as organizações influenciam e recebem influências do ambiente em que estão inseridas. Este autor lembra ainda que a Teoria Institucional desenvolveu-se em dois movimentos: a Velha Escola Institucional, que tem um foco na organização; e a Nova Escola Institucional, também conhecida como Escola Neo-Institucional, que tem um foco no campo organizacional.

As duas escolas institucionais baseiam-se na relação entre a organização e o ambiente em que ela está inserida (DIMAGGIO & POWELL, 1983) e são céticas quanto ao pressuposto do ator racional (PECI, 2006), mas, para a velha escola, há uma busca por legitimar os interesses pessoais ou o poder das lideranças por meio de acordos e alianças políticas internas e da influência do ambiente, enquanto que para o Neo Institucionalismo, há um foco nos conflitos entre grupos ou organizações e nas mudanças nas estruturas resultantes desses conflitos, com a institucionalização de estruturas no campo organizacional e a busca por legitimação da organização dentro do campo (QUINELLO, 2007). Dentro da abordagem Neo Institucional, a

legitimação frente às expectativas de partes interessadas é requisito para a sobrevivência das organizações no seu campo organizacional (DIMAGGIO & POWELL, 1983). Neste trabalho, em que se propõe um modelo de análise para investigar se a adoção de medidas de Segurança da Informação é decorrente de decisões racionais tomadas pela estrutura de Governança da Segurança da Informação ou se a adoção dessas medidas se dá para atender a pressões externas visando a legitimação das organizações no seu campo, a Escola Neo Institucional mostra-se mais adequada.

Neste ponto, é necessário definir os termos 'instituição' e 'campo organizacional' no contexto da Teoria Institucional. Meyer e Rowan (1977) definem instituições como regras, práticas, procedimentos, políticas e programas que são incorporados pela sociedade e pelas organizações, que, inseridas no ambiente institucional, agem conforme essas instituições (que são consideradas apropriadas e capazes de torná-las eficientes ou bem sucedidas dentro desse campo). Assim, no entendimento destes autores, o ambiente onde a organização está inserida influencia fortemente suas estruturas organizacionais, de forma que, dentro de um mesmo campo organizacional, as estruturas, práticas e processos já institucionalizados são incorporados pelas organizações.

Já campo organizacional é apresentado por DiMaggio e Powell (1983) como um conjunto de organizações que constituem uma área reconhecida de vida institucional. Estes autores citam como exemplos de organizações que compõem um campo organizacional fornecedores-chave, consumidores, agências reguladoras e outras organizações que prestam serviços, produzem ou fornecem produtos semelhantes. Lopes (2012) aponta como virtude de ter o campo organizacional como unidade de análise a atenção dada a todos os atores relevantes do campo, em contraste com o foco apenas na organização.

O campo organizacional tem grande influência nas estruturas das organizações que o compõem, pois, mesmo que inovações organizacionais sejam adotadas inicialmente por uma ou algumas organizações visando a melhoria do seu desempenho, estas vão sendo assimiladas pelas outras organizações de forma que deixam de representar uma vantagem competitiva e tornam-se meios para legitimação no campo, observam DiMaggio e Powell (1983). Com isso, estes autores postulam que, dentro do campo organizacional, as organizações ficam expostas a três diferentes tipos de mecanismos de mudanças que as tornam semelhantes entre si: o isomorfismo coercitivo, decorrente de pressões exercidas por meio de uma relação de poder e dependência entre organizações, como no caso do poder regulador que o Governo exerce, por exemplo, sobre organizações públicas ou sobre as que desenvolvem pesquisas científicas; isomorfismo mimético, derivado das incertezas inerentes às atividades desenvolvidas em um campo organizacional, que podem levar organizações a imitarem outras de maior prestígio, mais bem-sucedidas ou mais legítimas; isomorfismo normativo, que vem da profissionalização dentro do campo organizacional, que se mostra através da seleção de pessoal de outras organizações do mesmo campo, ou de profissionais que tenham sido treinados da mesma forma ou nas

mesmas escolas, ou mesmo do compartilhamento e troca de opiniões dentro de redes profissionais que atravessam organizações e ajudam na difusão de novos modelos e inovações.

A Segurança da Informação normalmente está associada a normas governamentais, padrões internacionais e práticas tidas como necessárias, que levam as organizações a implantarem, definirem ou estabelecerem papéis e responsabilidades, estratégias, processos, estruturas organizacionais, políticas, tecnologias e outras medidas de Segurança da Informação. Assim, as organizações estão sujeitas a pressões externas que podem levar à adoção de medidas de Segurança da Informação, e, segundo Kam et al. (2013), essa noção é consistente com a Teoria Institucional.

Abordagem Institucional em Estudos sobre Segurança da Informação

Para Björck (2004), embora a abordagem institucional seja amplamente utilizada em pesquisas de Sistemas de Informações e TI, pouco vem sendo aplicada em trabalhos de Segurança da Informação. Kam et al. (2013) argumentam que poucos estudos tem sido realizados tratando da influência de pressões externas para o cumprimento de Políticas de Segurança da Informação em organizações acadêmicas.

Apesar disso, a aproximação entre a Teoria Institucional e a Segurança da Informação pode ser identificada em algumas pesquisas. A influência de forças externas na Segurança da Informação pode ser observada no trabalho de Spears et al. (2013). Estes autores utilizaram a Teoria Institucional para estudar a aceitação social da garantia da Segurança da Informação e a melhoria da capacidade e eficácia das medidas de gestão de riscos de Segurança da Informação em um contexto regulatório, e concluíram que fatores externos incentivaram a adoção de medidas de Segurança da Informação. Além disso, segundo os autores, a garantia da Segurança da Informação está mais baseada na sua representação simbólica do que na eficácia das medidas adotadas – em outras palavras, mais para se ter legitimação do que para proteger a informação.

Holgate et al. (2012) estudaram a influência do ambiente institucional em arranjos de Governança da Segurança da Informação e observaram isomorfismo por influência de forças institucionais no mesmo campo organizacional.

Hu et al. (2006) apontam que gestores atribuem baixa prioridade aos investimentos em tecnologias de Segurança da Informação e ao desenvolvimento de políticas de Segurança da Informação. Em contrapartida, os autores observaram que os meios mais eficazes para impulsionar os investimentos em tecnologia e os esforços para desenvolver políticas de Segurança da Informação são forças institucionais coercitivas e normativas, oriundas da legislação e da profissionalização dentro do campo em que as organizações estão inseridas. Os autores observaram também que os profissionais de TI sofrem maior influência de forças normativas, devido à sua formação profissional e à participação em redes profissionais de Segurança da Informação. Kam et al. (2013) estudaram como as organizações acadêmicas dos

Estados Unidos são influenciadas por expectativas externas institucionais para cumprirem Políticas de Segurança da Informação e a influência dessas forças externas na conscientização sobre Segurança da Informação. A pesquisa mostrou que pressões externas influenciam de forma significativa a conformidade dessas organizações com as Políticas de Segurança da Informação, principalmente pressões regulatórias e normativas.

Ao estudar as Políticas de Segurança da Informação da administração pública municipal de Portugal, Lopes (2012) analisou as Políticas documentadas e elaborou um modelo aplicável aos diferentes municípios daquele País. Para a autora, a Teoria Institucional oferece as bases para a institucionalização de seu modelo, o que pode ocorrer através de regulação, por meio da aprovação do modelo como padrão e consequentemente da obrigação de adotar o padrão, ou através de pressões normativas, que podem fazer com que o modelo proposto se torne um valor ou obrigação social, ou por meio de pressões culturais-cognitivas, relacionadas à formação das pessoas e interiorização dos benefícios da Política de Segurança da Informação.

A gestão da Segurança da Informação foi tratada por Hsu et al. (2012) como uma inovação administrativa em organizações da Coréia do Sul. Os autores propuseram um modelo de análise para investigar o quanto as capacidades organizacional e econômica influenciam a adoção e assimilação institucional da gestão da Segurança da Informação como uma inovação administrativa. Os autores concluem que as organizações sofrem pressões isomórficas miméticas e coercitivas, ainda que moderadas pelos fatores organizacionais e econômicos, a saber: percepção quanto a incertezas ambientais e ao ganho de vantagem competitiva; disponibilidade de recursos; apoio da alta gestão; capacidade em prover recursos de TI; e aceitabilidade cultural de inovações. A pesquisa de Luesebrink (2011) analisou a Governança da Segurança da Informação em organizações acadêmicas públicas dos Estados Unidos sob a lente da Teoria Institucional, avaliando o impacto de iniciativas de regulação sobre as estruturas de gestão de Segurança da Informação das organizações estudadas. O autor observou que as estruturas de gestão da Segurança da Informação sofrem influência de mecanismos normativos e coercitivos de mudança institucional.

A literatura de forma geral indica que as medidas de Segurança da Informação são (ou deveriam ser) adotadas para proteger a informação e garantir a continuidade das operações, e como resultado de decisões racionais tomadas pela estrutura de Governança da Segurança da Informação ou com base em suas orientações. Já os trabalhos que tratam do tema sob a ótica institucional mostram que os gestores das organizações de um mesmo campo tomam decisões sobre Segurança da Informação com base em pressões externas – coercitivas, normativas e miméticas – e visando principalmente a legitimação da organização dentro do seu campo organizacional. Como diferencial, e com base no referencial teórico apresentado até aqui, o modelo de análise proposto permite realizar trabalhos empíricos visando identificar se as medidas são adotadas com base em decisões de Governança ou se são resultado de fatores institucionais.

CONCLUSÕES

A partir do modelo de análise proposto, pretende-se compreender empiricamente, em um segundo momento, o que leva à adoção de medidas de Segurança da Informação em institutos de pesquisa públicos. Além da obrigação legal de proteger a informação sobre participantes de pesquisas científicas e o conhecimento resultante de suas atividades de pesquisa, essas organizações precisam garantir a continuidade de suas atividades. O modelo proposto permite analisar quantitativamente os fatores que levam à adoção de medidas de Segurança da Informação no campo organizacional, ou analisar de forma qualitativa uma ou mais organizações específicas deste campo.

A dimensão Organizacional, cujos indicadores estão associados à Governança da Segurança da Informação e sua capacidade de direcionar as ações para atender aos objetivos e estratégias da organização, e a dimensão Institucional, cujos indicadores estão associados às forças presentes no ambiente institucional em que as organizações estão inseridas, não são mutuamente excludentes. Assim, medidas de Segurança da Informação podem ser adotadas tanto para atender a objetivos definidos pela estrutura de Governança da Segurança da Informação quanto por força de pressões isomórficas do campo organizacional, como pode ser observado na literatura. A questão que se coloca é o quanto fatores organizacionais e institucionais levam institutos de pesquisa públicos à adoção dessas medidas. Embora seja baseado em trabalhos científicos que tratam do tema, o modelo de análise proposto precisa ser validado empiricamente, o que possivelmente levará a ajustes. Uma vez validado, poderá ser útil na compreensão dos fatores que levam à adoção de medidas de Segurança da Informação, e pode ajudar na gestão da Segurança da Informação nessas organizações. Por fim, além de servir para diagnósticos em institutos de pesquisa, este modelo poderá ser utilizado também em estudos em universidades e outras organizações acadêmicas públicas ou privadas, bem como organizações de outras áreas de atuação, desde que sejam realizados os ajustes necessários.

REFERÊNCIAS

ALBRECHTSEN, E.. **Friend or foe**: Information security management of employees. Tese (Doutorado em Economia Industrial e Gestão da Tecnologia) – Norwegian University of Science and Technology, Trondheim, 2008.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M.. Adoção de normas de segurança da informação em Institutos de Pesquisas no setor público: uma proposta de análise explorando as possibilidades da Teoria Institucional. In: INTERNATIONAL CONFERENCE ON INFORMATION RESOURCES MANAGEMENT, 6. **Anais**. Natal: AIS, 2013.

ALEXANDRIA, J. C. S.. **Gestão de Segurança da Informação**: Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

ALEXANDRIA, J. C. S.; QUONIAM, L. M.. Proposta para a estruturação da gestão da segurança da informação em um ambiente de pesquisa científica. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT, 7. **Anais**. São Paulo: FEA/USP, 2010.

ARAÚJO, W. J.. Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal. **Informação & Sociedade**, v.22, p.13-24, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, 2005.

BRITTO, T. D.. **levantamento e diagnóstico de maturidade da governança da segurança de informação na administração direta federal brasileira**. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2011.

BJÖRCK, F. J.. Institutional Theory: A new perspective for research into IS/IT security in organisations. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 37. **Annals**. Big Island: HICSS, 2004.

CAMINHA, J.; LEAL, R. T.; MARQUES JUNIOR, R. O. P. C.; NASCIMENTO, M. G.. Implantação da Gestão da Segurança da Informação em um Instituto de Pesquisa Tecnológica. In: CONGRESSO DA ASSOCIAÇÃO BRASILEIRA DAS INSTITUIÇÕES DE PESQUISA TECNOLÓGICA E INOVAÇÃO. 4. **Anais**. Brasília: ABIPTI, 2006.

CEPIK, M.; CANABARRO, D. R.; POSSAMAI, A. J. A.. **Institucionalização do SISP e a Era Digital no Brasil**. Porto Alegre: WS Editor, 2010.

DA VEIGA, A.; ELOFF, J. H. P.. An information security governance framework. **Information Systems Management**, v.24, n.4, p.361-372, 2007.

DIMAGGIO, P. J.; POWELL, W. W.. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. **American Sociological Review**, v.48, n.2, p.147-160, 1983.

FACHINI, G. J.; FERNANDES, F. C.; FARIA, A. C.. Análise das políticas de segurança da informação à luz da NBR ISO/IEC 17799:2005 em empresas de tecnologia da informação: evidências obtidas em organizações de Blumenau (SC). In: ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, 3. **Anais**. Rio de Janeiro: ANPAD, 2011.

FONTES, E. L. G.. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

HILU, L.; GISI, M. L.. Produção científica no Brasil: um comparativo entre as universidades públicas e privadas. In: CONGRESSO NACIONAL DE EDUCAÇÃO, 10. **Anais**. Curitiba: PUC-PR, 2011.

HOLGATE, J.; WILLIAMS, S. P.; HARDY, C. A.. Information security governance: investigating diversity in critical infrastructure organizations. In: BLED ECONFERENCE, 25. **Annals**. Bled, 2012.

HSU, C.; LEE, J. N.; STRAUB, D. W.. Institutional influences on information systems security innovations. **Information Systems Research**, v.23, n.3, p.1-22, 2012.

HU, Q.; HART, P.; COOKE, D.. The role of external influences on organizational information security practices: an institutional perspective. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 39. **Annals**. Big Island: HICSS, 2006.

KAM, H. J.; KATERATTANAKUL, P.; GOGOLIN, G.; HONG, S.. Information security police compliance in higher education: a neo-institutional perspective. In: PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS, 17. **Annals**. Seoul: KMIS, 2013.

LOPES, I. M.. **Adopção de políticas de segurança de sistemas de informação na administração pública local em Portugal**. Tese (Doutorado em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação) – Universidade do Minho, Braga, 2012.

LUESEBRINK, M.. **The institutionalization of information security governance structures in academic institutions**: A Case Study. Tese (Doutorado em Comunicação e Informação) – Florida State University, Tallahassee, 2011.

MARCIANO, J. L. P.; LIMA MARQUES, M.. O enfoque social da segurança da informação. **Ciência da Informação**, v.35, n.3, p.89-98, 2006.

MEYER, J. W.; ROWAN, B.. Institutionalized organizations: formal structure as myth and ceremony. **American Journal of Sociology**, v.83, n.2, p.340-363, 1977.

MITNICK, K. D.; SIMON, W. L.. **mitnick – a arte de enganar – ataques de hackers**: Controlando o Fator Humano na Segurança da Informação. São Paulo: Makron Books, 2003.

MOULTON, R.; COLES, R. S.. Applying information security governance. **Computers & Security**, v.22, n.7, p.580-584, 2003.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Information Security Handbook**: A Guide for Managers – Recommendations of the National Institute of Standards and Technology. Gaithersburg, 2006.

PECI, A. A.. Nova Teoria Institucional em Estudos Organizacionais: Uma Abordagem Critica. **Cadernos EBAPE**, v.4, n.1, 2006.

PIMENTA, R. C. Q.; SOUSA NETO, M. V.. Gestão da Informação: um estudo de caso em um instituto de pesquisa tecnológica. **Prisma**, n.9, 2010.

QUINELLO, R.. **A Teoria Institucional aplicada à Administração**: entenda como o mundo invisível impacta na gestão dos negócios. São Paulo: Novatec, 2007.

SÊMOLA, M.. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2 ed, 2014.

SILVA, D. R. P.; STEIN, L. M.. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, v.10, p.43-56, 2007.

SPEARS, J. L.; BARKI, H.; BARTON, R. R.. Theorizing the concept and role of assurance in information systems security. **Information & Management**, v.50, n.7, p.598-605, 2013.

SVENSSON, G.. **Auditing the Human Factor as a Part of Setting up an Information Security Management System**. Dissertação (Mestrado em Sistemas de Informação e Controle Industrial) – Stockholm University, Estocolmo, 2013.

VELLOSO, J.. Mestres e Doutores no País: Destinos Profissionais e Políticas de Pós-Graduação. **Cadernos de Pesquisa**, v.34, n.123, p.583-611, 2004.

VON SOLMS, B.. Information security governance: compliance management vs operational management. **Computers & Security**, v.24, n.6, p.443-447, 2005.

VON SOLMS, B.. Information security: the fourth wave. **Computers & Security**, v.25, n.3, p.165-168, 2006.

VON SOLMS, R.; VON SOLMS, S. H.. Information security governance: a model based on the direct–control cycle. **Computers & Security**, v.25, n.6, p.408-412, 2006.