5-2013

Adoção de normas de segurança da informação em Institutos de Pesquisas no setor público: uma proposta de análise explorando as possibilidades da Teoria Institucional

Antônio Eduardo de Albuquerque Junior
Universidade Federal da Bahia e Fundação Oswaldo Cruz, aealbuquerque@gmail.com

Ernani Marques dos Santos
Universidade Federal da Bahia, emarques@ufba.br

Adoção de normas de segurança da informação em Institutos de Pesquisas no setor público: uma proposta de análise explorando as possibilidades da Teoria Institucional

Antônio Eduardo de Albuquerque Junior
Universidade Federal da Bahia e Fundação Oswaldo Cruz
aealbuquerque@gmail.com

Ernani Marques dos Santos
Universidade Federal da Bahia
emarques@ufba.br

Resumo

Este artigo objetiva propor um modelo para análise da adoção de normas de Segurança da Informação em institutos de pesquisas do setor público, utilizando a Teoria Institucional como lente teórica, considerando os mecanismos de isomorfismo mimético, normativo e coercitivo como condicionadores desta adoção. A proposição do modelo justifica-se por haver uma necessidade de realizar estudos sobre Segurança da Informação a partir de uma abordagem social, e sua aplicação poderá ajudar a compreender o processo de adoção das referidas normas. Nestas instituições, a necessidade de proteger a informação está regulada por legislação específica, e vem sendo alvo de auditorias e regulamentações de órgãos de controle do poder público, pois possuem obrigação de proteger informações sensíveis, como dados de pesquisas clínicas, patentes, projetos, conhecimentos produzidos, propriedade intelectual e a continuidade das atividades, considerando para isso necessidades diferentes de pesquisadores, estudantes e demais funcionários, ampliando a teoria sobre o tema. Dessa forma, o modelo proposto poderá permitir a compreensão da institucionalização da Segurança da Informação nesse tipo de organizações.

Palavras-chave

Normas, Segurança da Informação, organizações públicas.

1. Introdução

As organizações têm evoluído com o passar do tempo e, em todas as fases de sua evolução, tiveram a informação como elemento importante desse processo (Donner & Oliveira, 2008), o que culminou em mudanças na forma de gestão e no surgimento de um novo modelo de economia que tem a informação como base (Mello, Vasconcellos, Bragança & Motta, 2010). A informação é atualmente um ativo intangível que pode estar entre os bens mais valiosos de uma organização (Nobre, Ramos & Nascimento, 2010), participando da composição do seu valor econômico (Kayo, Kimura, Martin & Nakamura, 2006).

A importância da informação tem aumentado com as facilidades trazidas pelos avanços tecnológicos, que contribuem para sua disseminação e disponibilização entre organizações e dentro das organizações (Sêmola, 2003). Por outro lado, expuseram as organizações a novas ameaças (Alexandria, 2009) que podem comprometer a segurança das próprias informações, das suas transações e das pessoas envolvidas nos processos a elas relacionados (Marciano, 2006).

Segundo Mendonça (2007), as ameaças relacionadas à tecnologia e às facilidades de comunicação em rede aumentam a importância da Segurança da Informação, seja ela privada ou pública. Alexandria (2009) afirma que há a necessidade de promover a Segurança da Informação em organizações públicas, e para Cepik, Canabarro, Possamai e Sebben (2010), isto deve ser tratada de forma prioritária, visando minimizar perdas e acessos indevidos às informações tanto do Governo quanto dos cidadãos.

Albuquerque Junior & Santos (2011) enfatizam que a Segurança da Informação no setor público vem sendo regulada por diferentes atos normativos (incluindo leis, decretos, instruções normativas e normas complementares do Governo Federal, que define um contexto de obrigatoriedade de conformidade.

Quando se trata de institutos de pesquisa, a informação é considerada um diferencial competitivo (Pimenta & Sousa Neto, 2010) que pode estar entre os ativos mais valiosos, tendo como exemplos técnicas de gestão, análises de dados, projetos e patentes (Caminha, Leal, Marques Junior & Nascimento, 2006). As organizações que desenvolvem pesquisas científicas, que tem a informação como um importante insumo ou produto (Albuquerque Junior & Santos, 2011), precisam proteger o conhecimento produzido em suas atividades (Alexandria, 2009) e a propriedade intelectual, além de garantir a continuidade do seu funcionamento (Bernaschi, D'Aiutolo & Rughetti, 1999; Albuquerque Junior & Santos, 2011). Assim, seja por obrigação legal ou pela necessidade de proteger a informação e a continuidade do negócio, as organizações públicas de pesquisa necessitam de controles apropriados de Segurança da Informação, o que leva à necessidade de estudar o tema nesse contexto.

Para Silva e Stein (2007), a Segurança da Informação não deve ser tratada exclusivamente sob a ótica da tecnologia, enquanto a *Information Systems Audit and Control Association* [ISACA] (2009) afirma que somente a tecnologia não pode corrigir as falhas de segurança que são resultado de governança ou gestão inadequada, ou provocadas por razões culturais ou por despreparo do pessoal. Para Björck (2004), pesquisadores e técnicos da área de TI têm conseguido criar sistemas razoavelmente ou suficientemente seguros, mas, ao considerar o comportamento humano, a ocorrência de uma vulnerabilidade é uma questão de tempo. Alexandria (2009) alerta que um erro comum na construção da Segurança da Informação é não considerar os aspectos sociais e humanos. Dentro do contexto de uma abordagem social, Björck (2004) destaca a possibilidade do uso da Teoria Institucional, que, segundo Scott (2005), trata da criação, difusão, adoção e adaptação de estruturas, esquemas, regras, normas e rotinas ao longo do espaço e do tempo. Essas características, segundo DiMaggio e Powell (1983), são assimiladas pelas organizações através de três formas de isomorfismo: coercitivo, normativo e mimético.

A partir deste cenário, este artigo objetiva propor um modelo de análise da adoção de normas de segurança em institutos de pesquisas do setor público, explorando as possibilidades do uso da

Teoria Institucional como lente teórica, considerando os processos de isomorfismo como condicionadores desta adoção.

A proposição do modelo justifica-se por haver uma necessidade de realizar estudos sobre Segurança da Informação a partir de uma abordagem social, conforme proposto por Björck (2004). Sua aplicação poderá ajudar a compreender a Segurança da Informação em organizações públicas, cuja necessidade de proteger a informação está regulada por legislação específica e que vem sendo alvo de auditorias e regulamentações de órgãos de controle do poder público. Além disto, o foco em institutos de pesquisas procura contemplar a necessidade ou obrigação de proteger informações sensíveis, como dados de pesquisas clínicas, patentes, projetos, conhecimentos produzidos, propriedade intelectual e a continuidade das atividades. Um ponto a considerar é que esta análise deve ser feita considerando as necessidades de pesquisadores e estudantes, que precisam de liberdade para realizar suas atividades, ao mesmo tempo em que necessitam seguir normas, ampliando assim, a teoria sobre o tema. Dessa forma, o modelo proposto poderá permitir a compreensão da institucionalização da Segurança da Informação nesse tipo de organização.

2. Segurança da informação

Ao estudar segurança da informação, é preciso conceituar o termo "informação". Allen (1996) define informação como um processo de codificação e transmissão das estruturas cognitivas entre duas partes. Para Machlup e Mansfield (1983), informação é o meio necessário para a extração e construção do conhecimento.

A possibilidade de divulgação não autorizada de informações foi potencializada pelas facilidades de troca e armazenamento trazidas pela tecnologia, o que aumentou a exposição das organizações a ameaças (Alexandria, 2009). Por dependerem da TI, as organizações precisam de uma estrutura de Segurança da Informação para se protegerem das ameaças do mundo globalizado (Eloff & Von Solms, 2000), que incluem a portabilidade de equipamentos e as facilidades de conexão em rede, que podem comprometer a segurança das informações, das transações e das pessoas envolvidas com essas informações (Marciano, 2006). Essa opinião é partilhada pela a ABNT (2005), segundo a qual o aumento da interconectividade expôs a informação à grande variedade de ameaças e vulnerabilidades, que pode levar a organização a enormes prejuízos financeiros e a um impacto negativo na sua imagem, como observaram Posthumus e Von Solms (2004).

A Segurança da Informação é definida por Beal (2005) como o processo de proteção dos ativos de informação contra ameaças à sua integridade, confidencialidade e disponibilidade. A ABNT (2005) apresenta duas definições: proteção da informação de ameaças para minimizar o risco e garantir a continuidade do negocio, maximizar as oportunidades de negócio e o retorno sobre os investimentos; e como a preservação dos seus três componentes, que são a confidencialidade, a integridade e a disponibilidade.

2.1. Segurança da informação em organizações do setor público

As mudanças constantes nas ameaças e riscos às informações fizeram da Segurança da Informação uma função essencial, que precisa ser gerida e governada para reduzir os riscos às

operações do Governo. No Brasil, a preocupação com esta segurança vem sendo demonstrada através de diversas ações do Governo Federal. Segundo Cepik, Canabarro e Possamai (2010), o tema foi objeto de auditoria do TCU em 2007, onde foi identificado que normalmente não há Políticas de Segurança da Informação na Administração Pública Federal, ou que essas políticas, quando existem, não são efetivas, e não há cultura de gestão de riscos nem planos de continuidade dos negócios. Ainda para eles, a Segurança da Informação foi um dos itens priorizados na Estratégia Geral de TI elaborada pelo Governo Federal para todos os órgãos do Poder Executivo Federal, o que demonstra sua importância no âmbito da Administração Pública brasileira.

Reforçando a necessidade de proteger informações em organizações públicas, atos normativos foram publicados com esse objetivo, como: a Lei nº 8.159/1991, que cria a obrigação para as organizações públicas de proteger seus documentos para apoiar o desenvolvimento científico e servir como elemento de prova e informação; a Lei nº 9.983/2000, que alterou o Código Penal brasileiro, tipificando a violação indevida e proposital da confidencialidade e integridade dos dados armazenados em sistemas computacionais como crime; o Decreto nº 4.553/2002, que trata especificamente da segurança de informações sigilosas da Administração Pública Federal; e o Decreto nº 3.505/2000, que institui a Política de Segurança da Informação na Administração Pública Federal. Além dessas leis e decretos, outras normas tratam da Segurança da Informação na esfera pública: a Instrução Normativa GSI/PR nº 1/2008, que disciplina a gestão da Segurança da Informação e Comunicações na Administração Pública Federal; a Norma Complementar 02/IN01/ DSIC/GSIPR, de 2008, que define uma metodologia de gestão de Segurança da Informação e Comunicações na Administração Pública Federal; a Norma Complementar 03/IN01/DSIC/GSIPR, de 2009, que estabelece diretrizes para criação e manutenção de Políticas de Segurança da Informação; a Norma Complementar 04/IN01/DSIC/GSIPR, de 2009, que estabelece diretrizes para o processo de gestão de riscos de Segurança da Informação e Comunicações na Administração Pública Federal; a Norma Complementar 05/IN01/DSIC/GSIPR, de 2009, que busca disciplinar a criação de Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais na Administração Pública Federal; a Norma Complementar 06/IN01/DSIC/GSIPR, de 2009, que visa estabelecer diretrizes para Gestão de Continuidade de Negócios; a Norma Complementar 07/IN01/DSIC/GSIPR, de 2010, que estabelece diretrizes de controles de acesso nos órgãos e entidades da Administração Pública Federal; e a Norma Complementar 08/IN01/DSIC/GSIPR, de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores. Apesar dessas normas, Alexandria (2009) aponta que as organizações públicas não estão entre aquelas que têm uma preocupação maior em adotar controles e boas práticas de Segurança da Informação.

2.2. Segurança de informação em organizações de pesquisas

Segundo Pimenta e Sousa Neto (2010), a informação é um diferencial competitivo para os institutos de pesquisa tecnológica, e na opinião de Caminha *et al*. (2006), a informação é um dos ativos mais valiosos para institutos de pesquisa. Bernaschi *et al*. (1999) afirmam que os institutos de pesquisa científica precisam aprimorar a Segurança da Informação para reduzir os riscos associados.

A questão da Segurança da Informação em organizações que desenvolvem pesquisas científicas também pode ser analisada a partir do contexto presente nas universidades, que desempenham

um papel relevante na produção científica e no desenvolvimento tecnológico. Ao estudar as políticas de Segurança da Informação em 122 universidades, Doherty, Anastasakis e Fulford (2009) identificaram que 50% delas não possuem um documento formal de Política de Segurança da Informação, apenas 42% contam com norma sobre uso aceitável de recursos de TI, pouco mais de 28% têm norma que regula a utilização de correio eletrônico e aproximadamente 14% contam com norma que trata de direitos autorais. Por fim, os autores argumentam que essas políticas e normas regulam uma pequena gama de questões específicas e refletem uma visão muito técnica.

Van der Leeden (2010), ao investigar Segurança da Informação em cinco universidades holandesas, concluiu que três delas tinha uma política definida. Apesar disso, nenhuma das realizava gestão de riscos, o que pode levar ao tratamento errado e à dificuldades de justificar os investimentos necessários para mitigá-los. O autor conclui também que os usuários têm baixo nível de conscientização e representam a maior causa de incidentes de segurança, o que fortalece a opinião de Mitnick e Simon (2003), que afirmam que o homem é a maior causa de incidentes desse tipo. Silva e Stein (2007) complementam afirmando que pouco tem sido feito para identificar as causas que levam os usuários a comportamentos inseguros.

Citando diversas pesquisas e casos de incidentes de Segurança da Informação em ambiente de pesquisa científica, Perkel (2010) afirma que a proteção de dados de pesquisa representa um desafio, pois os profissionais de TI procuram adotar práticas de segurança que podem ser contrárias às opiniões ou necessidades de pesquisadores, estudantes e colaboradores. Para o autor, alguns pesquisadores preferem não contar com a segurança, mas ter a liberdade que julgam necessária para desempenhar suas atividades.

Caminha *et al*. (2006) estudaram o processo de implantação da gestão da Segurança da Informação em um instituto de pesquisa tecnológica privado e, para eles, a natureza das atividades realizadas e o fato de a informação ser um insumo e grande parte dos produtos dessas organizações fazem necessária a implantação da gestão da segurança, o que envolve superar dificuldades como a liberdade que os pesquisadores precisam e a necessidade de implantar controles.
Ao realizar um estudo em um instituto de pesquisa, Alexandria (2009) identificou lacunas na administração da Segurança da Informação que representam uma vulnerabilidade grave para a organização. O autor identificou também práticas não recomendadas, ausência de procedimentos de gestão de riscos e de tratamento de incidentes, e ausência de políticas formalmente definidas, o que indica gestão incipiente ou inexistente. Nesta organização os usuários percebem a segurança como uma necessidade apenas dos sistemas e informações institucionais, e responsabilidade de quem administra esses sistemas e informações, não sendo aplicável, portanto, para informações e computadores de uso individual. Em uma pesquisa realizada em 14 institutos públicos de pesquisa tecnológica (Alexandria, 2012), apenas três deles tinha um departamento de Segurança da Informação estruturado conforme as normas e modelos de boas práticas mais amplamente adotados e, nestes casos, o departamento está subordinado à área de TI, o que pode indicar que há um viés tecnológico nas ações desses institutos.

3. A Teoria Institucional

Diferentes autores defendem a necessidade de investigações científicas de fenômenos de Segurança da Informação sob uma abordagem social (Dhillon & Backhouse, 2001; Silva & Stein, 2007; Albrechtsen, 2008; Coles-Kemp, 2009). Frangopoulos, Eloff e Venter (2008) afirmam que, de maneira geral, as normas de Segurança da Informação são incompletas por não tratarem corretamente das relações humanas, embora sejam completas do ponto de vista técnico. Nesse sentido, pesquisas sobre o tema vêm sendo realizadas tradicionalmente nos campos da tecnologia e da matemática, indicando que há necessidade de mais estudos sob uma abordagem social, embora tenha havido um crescimento da importância da dimensão humana nessas pesquisas (Coles-Kemp, 2009). Apesar disso, os estudos têm sido direcionados principalmente para problemas e soluções tecnológicas, com pouca atenção para aspectos sociais, organizacionais e humanos (Dhillon & Backhouse, 2001). Sendo a adoção de normas de Segurança da Informação uma área em que os aspectos sociais e organizacionais são relevantes, e ainda observando recomendação de Björck (2004), a Teoria Institucional desenha-se como uma base teórica bastante pertinente para análise deste fenômeno.

A Teoria Institucional é considerada um novo campo de estudo para a Administração (Quinello, 2007), não sendo um sistema coerente de regras, mas um conjunto de idéias que formam uma perspectiva um pouco consistente de mecanismos que apóiam ou restringem o comportamento social, podendo ser utilizada em diferentes áreas de conhecimento, com destaque em pesquisas no campo dos estudos organizacionais (Björck, 2004).

Quinello (2007) afirma que há necessidade de criar métodos de mensuração, variáveis e metodologias de pesquisa para investigação mais aprofundada, e que essa situação levou ao surgimento de duas vertentes de estudiosos da Teoria Institucional: um grupo que o autor chama de "velha escola institucional", que investigou a interação informal nas organizações, as macroestruturas institucionais, os sistemas políticos e a linguagem e o sistema legal, e cujo foco está na organização; e a "nova escola institucional" ou escola "neo-institucionalista", cujos autores estudam os princípios institucionais nas organizações, considerados os elos de conexão entre os indivíduos e a sociedade, e que têm foco no campo organizacional – um conjunto de organizações que compõem uma área reconhecida de vida institucional, que inclui fornecedores, consumidores, outras organizações que prestam serviços, produzem ou fornecem produtos semelhantes e agências reguladoras, segundo DiMaggio e Powell (1983).

Por tratar da criação, difusão, adoção e adaptação de estruturas, esquemas, regras, normas e rotinas ao longo do espaço e do tempo, a Teoria Institucional considera os processos pelos quais essas características se estabelecem como diretrizes obrigatórias para o comportamento social (Scott, 2005). Essas regras institucionais são assimiladas pelas organizações através de diferentes formas de isomorfismo (DiMaggio & Powell, 1983; Quinello, 2007; Lopes, 2012),

O isomorfismo pode ser do tipo competitivo, que é mais relevante para os campos em que há competição livre e aberta entre as organizações; e do tipo institucional, relacionado não à competição por recursos e consumidores, mas por poder político e legitimação institucional. O isomorfismo institucional ocorre através de três mecanismos: o coercitivo, o mimético e o normativo. No isomorfismo coercitivo, estão incluídas as pressões sofridas por uma organização para se assemelhar às outras por força, persuasão ou convite para associação (DiMaggio &

Powell, 1983), ou por regulação pelo Estado (DiMaggio & Powell, 1983; Meyer & Rowan, 1977). No isomorfismo mimético, há uma busca por resolver um problema comum às organizações de um mesmo campo e cuja solução é incerta para a maioria delas, de maneira que o mimetismo aparenta ser mais viável e ter um custo menor do que inovar para encontrar a solução (DiMaggio & Powell, 1983), ou a imitação ocorre porque uma organização pretende ser reconhecida como legítima em seu campo (Hsu, Lee & Straub, 2012). Já no isomorfismo normativo, certas categorias profissionais ou grupos de profissionais forçam ou impõem mudanças às organizações, influências coletivas resultantes do desenvolvimento da profissionalização de determinado campo (Hsu *et al*., 2012). Assim, os três mecanismos de isomorfismo podem ser úteis em investigações sobre os fatores que condicionam a adoção de normas de Segurança da Informação em organizações que realizam pesquisas científicas.

4. Isomorfismo e segurança de informação

Björck (2004) afirma que a Teoria Institucional é uma importante ferramenta de análise de problemas de Segurança da Informação, mas complementa que há pouca teoria sobre este tema voltada para os estudos sobre o comportamento social.

Hu, Hart e Cooke (2007) pesquisaram a promoção da Segurança da Informação em uma empresa multinacional e descobriram evidências de processos coercitivos, normativos e miméticos. Já Hsu *et al*. (2012), ao estudarem 140 organizações coreanas, concluíram que há considerável pressão para que as organizações adotem e assimilem a Gestão da Segurança da Informação.

Para Björck (2004), organizações investem em Políticas de Segurança da Informação que não são postas em prática e sugere estudos sobre os efeitos de forças institucionais coercitivas, miméticas e normativas na elaboração e aceitação de políticas, normas e procedimentos de Segurança da Informação. O autor sugere também o estudo utilizando a abordagem institucional sobre os fatores que determinam como os funcionários de uma organização fazem escolhas que implicam na Segurança da Informação.

Sendo assim, é possível estabelecer um modelo de análise considerando esses três tipos de isomorfismo como fontes de fatores condicionantes da adoção de normas de Segurança da Informação em institutos de pesquisas no setor público. Nesse contexto, propõe-se o modelo de análise apresentado na Figura 1, baseado na Teoria Institucional. Nele, o Governo e os órgãos de regulação que orientam a atuação das organizações desse campo organizacional aparecem como origem de forças institucionais coercitivas. O Governo regula a atividade de organizações públicas através de leis, decretos e instruções normativas que obrigam essas organizações a instituírem comitês, a criarem sistemas e elaborarem normas e políticas de Segurança da Informação, ao mesmo tempo em que procura aumentar a transparência das informações públicas. Por realizarem pesquisas científicas, essas organizações estão sujeitas também a normas da Comissão Nacional de Ética em Pesquisa (CONEP), a regulamentos e normas do Ministério da Educação, do Ministério da Ciência, Tecnologia e Inovação, do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e a exigências da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

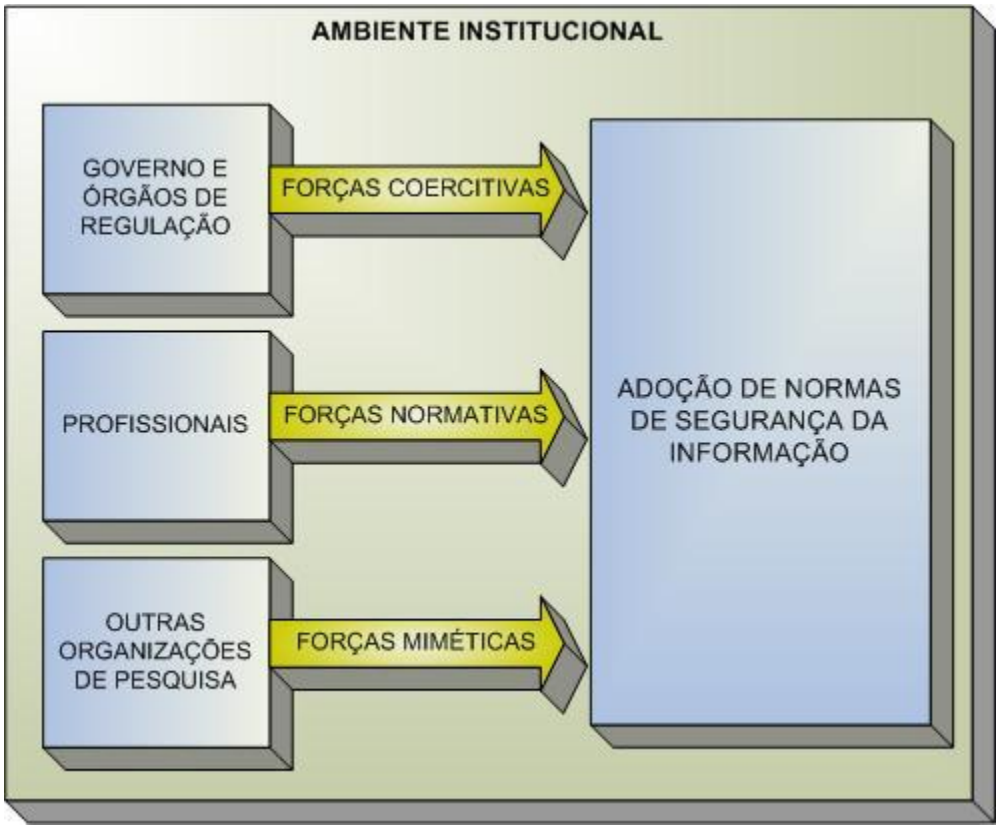

Figura 1: Modelo de análise proposto
Fonte: Elaborado pelos autores

Os profissionais de TI aparecem como fontes de forças institucionais normativas, uma vez que a Segurança da Informação está em evidência, principalmente após os escândalos financeiros que levaram à aprovação da Lei Sarbanes-Oxley nos Estados Unidos, e há uma preocupação com boas práticas de governança de TI e Segurança da Informação em organizações de todo o mundo. Dessa forma, os profissionais de TI levam para as organizações em que exercem suas atividades as práticas e processos em que vêm assimilando em cursos e certificações, como *Certified Information Systems Auditor* (CISA), promovida pela ISACA, *Modulo Certified Security Officer* (MCSO) e *Modulo Certified Risk Manager* (MCRM), ambas promovidas pela empresa *Modulo Security*.

As outras organizações de ensino e pesquisa consideradas bem sucedidas em sua área de atuação aparecem neste modelo como origem de forças institucionais miméticas. As políticas, normas e práticas em uso nessas organizações, que em muitos casos são baseadas em modelos publicados por organizações reconhecidas internacionalmente, como a *International Organization for Standardization* (IOS) e o *Britsh Standands Institute* (BSI), são utilizadas como modelos para a elaboração de políticas, normas e práticas em outras organizações que atuam no mesmo campo organizacional.

Assim, essas três forças isomórficas condicionam a adoção de normas de Segurança da Informação em organizações públicas que realizam pesquisas científicas, como resultado de um processo de institucionalização.

5. Conclusões

A partir deste modelo proposto, objetiva-se compreender a adoção de normas de segurança em organizações públicas que desenvolvem pesquisas científicas, que devem proteger suas informações para atender a obrigações legais e éticas, e que precisam garantir também a continuidade de suas atividades e a proteção do conhecimento e da propriedade intelectual, frutos de suas atividades. Sua utilização poderá ajudar a identificar os fatores que condicionam as organizações públicas de pesquisa a criar, adotar e manter políticas, normas, processos e procedimentos de Segurança da Informação. Isto considerando que neste tipo de organização as necessidades de pesquisadores, estudantes e demais funcionários podem ser muito diferentes e que a área de TI precisa seguir normas e responder a auditorias operacionais de órgãos de controle do Governo.

Este modelo poderá ajudar também a compreender questões relacionadas a diferenças entre o comportamento real das pessoas que trabalham ou estudam nessas organizações e o comportamento exigido nessas estruturas formais de segurança, bem como a identificar mecanismos de controle do comportamento nessa área. Compreendendo questões como essas a partir da perspectiva institucional, vislumbra-se ser possível melhorar a gestão da Segurança da Informação nesse tipo de organizações.

Como próximos passos, é necessária a definição dos indicadores de cada uma das dimensões propostas, de modo a operacionalizar a aplicação do modelo para sua validação e/ou ajustes necessários.

Referências

Albrechtsen, E. (2008). Friend of foe? Information security management of emplyees. Tese de Doutorado, University of Science and Technology, Trondheim.

Albuquerque Junior, A. E. and E. M. dos Santos (2011) "Controles e Práticas de Segurança da Informação em um Instituto de Pesquisa Federal", Anais do VIII Simpósio de Excelência em Gestão e Tecnologia – SEGET 2011, Resende.

Albuquerque Junior, A. E. and E. M. dos Santos (2012) "Segurança da Informação em Hospitais: A Percepção da Importância de Controles para Gestores e Profissionais de TI", Revista Gestão & Saúde, (4)2, pp. 1-14.

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

Alexandria, J. C. S. de (2012) "A Picture of Information Security in Public Institutions of Scientific Research in Brazil", Proceedings of 9th International Conference on Information System and Technology Management – CONTECSI 2012, São Paulo, pp. 4209-4215.

Allen, B. L. (1996) Information Tasks: Toward a User-Centered Approach to Information Systems, 1st. edition, Orlando, FL: Emerald.

Associação Brasileira de Normas Técnicas (2005). NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, RJ: ABNT.

Beal, A. (2005). Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações, São Paulo, SP: Atlas.

Bernaschi, M., E. D'Aiutolo and P. Rughetti (1999). "Enforcing Network Security: a Real Case Study in a Research Organization", Computers & Security, (18)6, pp. 533-543.

Björck, F. (2004). "Institutional Theory: A new perspective for research into IS/IT security in organisations", Proceedings of 37th Hawaii International Conference on System Sciences – HICSS 2004, Big Island.

Britto, T. D. e (2011). Levantamento e Diagnóstico de Maturidade da Governança da Segurança de Informação na Administração Direta Federal Brasileira. Dissertação de Mestrado, Universidade Católica de Brasília, Brasília, DF.

Buckland, M. K. (1991). Information and Information Systems, New York, NY: Greenwood.

Caminha, J., R. T. Leal, R. O. P. C. Marques Junior, M. G. do Nascimento (2006). "Implantação da Gestão da Segurança da Informação em um Instituto de Pesquisa Tecnológica", Anais do Congresso da Associação Brasileira das Instituições de Pesquisa Tecnológica e Inovação 2006 – ABIPTI 2006, Campinas, SP.

Cepik, M., D. R. Canabarro, A. J. Possamai (2010). "A Institucionalização do SISP e a Era Digital no Brasil" in Cepik, M. and D. R. Canabarro (eds.) Governança de TI: Transformando a Administração Pública no Brasil, Porto Alegre, RS: WS Editor, pp. 37-74.

Cepik, M., D. R. Canabarro, A. J. Possamai, F. D. Sebben (2010). "Alinhando TI e Políticas Públicas: quatro temas prioritários" in Cepik, M. and D. R. Canabarro (eds.) Governança de TI: Transformando a Administração Pública no Brasil, Porto Alegre, RS: WS Editor, pp. 157-204.

Coles-Kemp, L. (2009). "Information Security management: An entangled research challenge", Information Security Technical Report, (14)4, pp. 181-185.

Corporate Governance Task Force (2004). Information Security Governance: A Call to Action. Washington DC: National Cyber Security Partnership.

Davenport, T. H. (1998). Ecologia da Informação: por que só a tecnologia não basta para o sucesso na era da informação, São Paulo, SP: Futura.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: towards socioorganizational perspectives", Information Systems Journal, (11)2, pp. 127-153.

DiMaggio, P. J. and W. W. Powell (1983). "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", American Sociological Review, (48)2, pp. 147-160.

Doherty, N. F., L. Anastasakis, H. Fulford (2009). "The information security policy unpacked: A critical study of the content of university policies", International Journal of Information Security Management, (29)6, pp.449-457.

Donner, M. L. and L. R. de Oliveira (2008) "Análise de Satisfação com a Segurança no Uso de Internet Banking em Relação aos Atuais Recursos Disponíveis no Canal Eletrônico", Anais do XXXII Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração – EnANPAD 2008, Rio de Janeiro.

Eloff, M. M., S. H. Von Solms (2000). "Information Security Management: A Hierarchical Framework for Various Approaches", Computers & Security, (19)3, pp. 243-256.

Frangopoulos, E. D., M. M. Eloff, L. M. Venter (2008). "Social Aspects of Information Security", Proceedings of ISSA 2008 Innovative Minds Conference – ISSA 2008, Johannesburgo: ICSA.
Grant, I. (2007). "Public Sector Staff 'ignore IT security", ComputerWeekly.com, 06 dec. 2007.
Hsu, C., J. Lee, D. W. Straub (2012). "Institutional Influences on Information Systems Security Innovations", Information Systems Research, (23)3, pp. 918-939.
Hu, Q., P. Hart, D. Cooke (2007). "The role of external and internal influences on information systems security – a neo-institutional perspective", Journal of Strategic Information Systems, (16)2, pp. 153-172.
Kayo, E. K., H. Kimura, D. M. L. Martin, W. T. Nakamura. (2006). "Ativos Intangíveis, Ciclo de Vida e Criação de Valor", RAC, (10)3, pp. 73-90.
Lopes, I. M. (2012). Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal. Tese de Doutorado, Universidade do Minho, Braga.
Machlup, F., U. Mansfield (1983). "Semantic Quirks in Studies of Information" in Machlup, F., U. Mansfield (eds.) The Study of Information: Interdisciplinary Messages, New York, NY: John Wiley, pp. 641-671.
Mandarini, M. (2005). Segurança Corporativa Estratégica: Fundamentos, Barueri, SP: Manole.
Marciano, J. L. P. (2006). Segurança da Informação – uma abordagem social. Tese de Doutorado, Universidade de Brasília, Brasília.
Marques, P. E. P. C. and T. W. Baptista (2012). "Tecnologia da Informação na Fundação Oswaldo Cruz", RECIIS, (6)1, pp. 62-76.
Mello, L. B. B., L. A. Vasconcellos, L. de R. Bragança, O. M. Motta (2010) "Contribuição para Gestão de Ativos Intangíveis Organizacionais: Proposição de Um Modelo Baseado no Balenced Scorecard", Anais do VI Congresso Nacional de Excelência em Gestão – CNEG 2010, Niterói.
Mendonça, M. C. S. de (2007). A Percepção Gerencial Sobre o Modelo de Gestão da Segurança da Informação de uma Empresa Pública de TIC: Perspectiva da evolução para um modelo de governança. Dissertação de Mestrado, Universidade Católica de Brasília, Brasília, DF.
Meyer, J. W. and B. Rowan (1977). "Institutionalized Organizations: Formal Structure as Myth and Ceremony", The American Journal of Sociology, (83)2, pp. 340-363.
Mitnick, K. D. and W. L. Simon (2003). Mitnick – A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação, São Paulo, SP: Makron Books.
Nobre, A. C. dos S., A. S. M. Ramos, T. C. Nascimento (2010). "Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil", Anais do XXXIV Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração – EnANPAD 2010, Rio de Janeiro.
North, D. C. (1990). Institutions, Institutional Change and Economic Performance, New York, NY: Cambridge University Press.
Perkel, J. (2010). "Cybersecurity: How Safe Are Your Data?", Nature, 464, pp. 1260-1261.
Pimenta, R. C. Q. and M. V. Sousa Neto (2010). "Gestão da Informação: um estudo de caso em um instituto de pesquisa tecnológica", Prisma.com, 9.
Posthumus, S. and R. Von Solms (2004). "A Framework for the Governance of Information Security", Computers & Security, (23)8, pp. 638-646.
Quinello, R. (2007). A Teoria Institucional Aplicada à Administração: Entenda como o mundo invisível impacta na gestão dos negócios, São Paulo, SP: Novatec Editora.

Scott, W. R. (2005). “Institutional Theory: Contributing to a Theoretical Research Program” in Smith, K., M. A. Hitt (eds.) Great Minds in Management: The Process of Theory Development, Oxford: Oxford University Press, pp. 460-484.
Sêmola, M. (2003). Gestão da Segurança da Informação: uma visão executiva, Rio de Janeiro, RJ: Campus.
Silva, D. R. P. and L. M. Stein (2007). “Segurança da Informação: uma reflexão sobre o componente humano”, Ciências & Cognição, 10, pp. 43-56.
Van Der Leeden, K. (2010). Security without risk? Investigating information security among Dutch universities. Dissertação de Mestrado, University of Twente, Twente.