risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 22/09/2018
Aceitação/Acceptance: 16/11/2018

A Adopção de Medidas Formais, Informais e Técnicas de Segurança da Informação e sua Relação com as Pressões do Ambiente Institucional

Antonio Eduardo de Albuquerque Junior[1], Ernani Marques dos Santos[2], Rodrigo César Reis de Oliveira[3], Adriano Santos Rocha Silva[4], Laercio Moura de Almeida[5]

eduardo.albuquerque@fiocruz.br, emarques@ufba.br, rodrigo.oliveira@feac.ufal.br, adrianorocha70@gmail.com, laercio@prospectati.com

[1] Fundação Oswaldo Cruz – IGM, R. Waldemar Falcão 121, 40296-710, Salvador, Brasil

[2] Universidade Federal da Bahia – NPGA, Av. Reitor Miguel Calmon, 40110-903, Salvador, Brasil

[3] Universidade Federal de Alagoas – FEAC, Av. Lourival Melo Mota, 57072-900, Maceió, Brasil

[4] Universidade Federal da Bahia – NPGA, Av. Reitor Miguel Calmon, 40110-903, Salvador, Brasil

[5] Prospecta Tecnologia de Informação, Av. Vasco da Gama 4615, 40230-731, Salvador, Brasil

DOI: 10.17013/risti.30.17–33

Resumo: Para proteger suas informações, as organizações podem adoptar medidas de Segurança da Informação, mas a adopção pode ser influenciada pelo seu ambiente externo através de regulamentos, contratos, acordos e fiscalização, conhecimentos profissionais tidos como certos sobre tecnologias, normas e padrões internacionais, e da imitação de constituintes considerados bem-sucedidos. No entanto, não se sabe quais pressões influenciam a adopção dos diferentes tipos de medidas de Segurança da Informação. Este trabalho teve o objectivo de identificar quais pressões coercitivas, miméticas e normativas influenciam a adopção de medidas formais, informais e técnicas de Segurança da Informção em universidades públicas brasileiras, que têm o desafio de divulgar conhecimento enquanto precisam proteger informações de pesquisa e dados privados. A pesquisa envolveu um levantamento com gestores e profissionais de Segurança da Informação das universidades e pesquisa documental. Os resultados evidenciam que a adopção de medidas técnicas e informais é influenciada principalmente por pressões normativas enquanto medidas formais são adoptadas devido a pressões coercitivas.

Palavras-chave: universidades públicas; segurança da informação; pressões; ambiente institucional.

The Adoption of Formal, Informal, and Technical Information Security Measures and their Relation with Institutional Environment Pressures

Abstract: Organizations may adopt Information Security measures to protect information, but adoption may be influenced by external environment through

regulations, contracts, agreements, and inspection, professional knowledge about international standards and technologies that are taken for granted, and imitation of successful constituents of environment. However, it is not known what pressures influence adoption of different types of Information Security measures. This paper aimed to identify which coercive, mimetic, and normative pressures influence adoption of formal, informal, and technical Information Security measures in Brazilian public universities, which have the challenge of disseminating knowledge while need to protect research information and private data. The research involved a survey with universities' Information Security managers and professionals, and research in documents. The results show adoption of technical and informal measures is influenced mainly by normative pressures while formal measures are adopted due to coercive pressures.

Keywords: public universities; information security; pressures; institutional environment.

1. Introdução

Há um consenso sobre a necessidade de proteger informações organizacionais, mas características próprias levam a necessidades específicas de medidas de Segurança da Informação (Sêmola, 2014). Nesse contexto, as universidades precisam proteger informações acadêmicas, científicas e pessoais, que estão expostas a riscos de Segurança da Informação decorrentes de suas características e actividades e que podem sofrer incidentes com consequências graves (Perkel, 2010).

Para que se tenha Segurança da Informação, diferentes medidas técnicas, formais e informais podem ser aplicadas (Dhillon, 1999), mas a literatura recomenda uma análise e avaliação de riscos para que medidas apropriadas às necessidades e requisitos organizacionais sejam adoptadas (Fontes, 2006; Sêmola, 2014). O argumento para isso é que a simples adopção de medidas previstas em padrões e modelos de Segurança da Informação não garante a mitigação dos riscos (Dresner, 2011). Entretanto, a adopção dessas medidas pode acontecer como uma resposta a pressões do ambiente no qual as organizações estão inseridas, o que pode resultar na adopção de regulamentos internos, tecnologias, estruturas organizacionais, políticas e programas que não atendem às necessidades organizacionais (Albuquerque Junior & Santos, 2015). Para compreender a adopção de medidas de Segurança da Informação como resposta a pressões ambientais, Björck (2004) recomenda a Teoria Institucional, abordagem que enfatiza o comportamento organizacional como resultado de pressões do ambiente externo (Meyer & Rowan, 1977; DiMaggio & Powell, 1983).

Esta pesquisa teve o objectivo de identificar os factores do ambiente institucional que pressionam a adopção de medidas de Segurança da Informação em universidades públicas brasileiras. A literatura mais recente que aborda o tema sob a perspectiva da Teoria Institucional enfatiza principalmente a conformidade com regulamentos e leis (Kam, Katerattanakul, Gogolin, & Hong, 2013; Anthony, Appari, & Johnson, 2014; Lopes & Sá-Soares, 2014; Alkalbani, Deng, Kam, & Zhang, 2017; Hou, Gao, & Nicholson, 2018) e a difusão de estruturas de Segurança da Informação (Hsu, Lee, & Straub, 2012; Williams, Hardy, & Holgate, 2013). Diferentemente desses estudos, esta pesquisa busca relacionar a adopção de medidas formais, informais e técnicas de Segurança da

Informação a pressões institucionais miméticas, normativas ou coercitivas (DiMaggio & Powell, 1983). Para isso, este estudo envolveu a identificação dos constituintes do ambiente institucional, das pressões que eles exercem e das medidas de Segurança da Informação adoptadas em resposta a essas pressões.

2. Fundamentação Teórica

A Segurança da Informação é uma área de conhecimento que visa à protecção da informação contra alterações ou acessos indevidos e indisponibilidade para seus utilizadores (Sêmola, 2014), o que pede acções, políticas, procedimentos, normas e orientações para esta finalidade (Fontes, 2006). Chamados de medidas (Sêmola, 2014) ou controlos (Lopes, 2012) de Segurança da Informação, esses mecanismos podem impedir ou limitar a exploração de vulnerabilidades ou seu impacto, minimizando ou mesmo evitando os riscos relacionados (Sêmola, 2014).

Incidentes de Segurança da Informação podem ser técnicos, ambientais e sociais (Belasco & Wan, 2006), e para combatê-los ou mitigá-los, são recomendadas medidas técnicas, formais e informais (Dhillon, 1999) (Tabela 1). No entanto, cada organização tem características próprias e, portanto, necessidades particulares de Segurança da Informação (Dresner, 2011; Sêmola, 2014) e a simples adopção de medidas padronizadas não garante a mitigação dos riscos aos quais as informações estão expostas (Dresner, 2011), o que significa que devem ser adoptadas as medidas que atendem aos requisitos organizacionais.

Há um entendimento de que as decisões sobre a adopção de medidas de Segurança da Informação precisam atender a princípios, requisitos e riscos específicos da organização (Sêmola, 2014). No entanto, essas decisões podem ser tomadas em resposta ao ambiente externo à organização, pois elementos do ambiente podem obrigar ou recomendar a adopção de diferentes medidas que definem papéis, responsabilidades, estratégias, processos, estruturas organizacionais, políticas e tecnologias (Albuquerque Junior & Santos, 2015), mas que podem não ser adequadas às suas necessidades e requisitos.

Tipo	Objetivo
Técnicos	Limitar acesso a prédios, salas, computadores e sistemas (Dhillon, 1999; Dhillon & Moores, 2001) ou mudar o ambiente físico no qual as informações e outros ativos são armazenados para protegê-los por meios físicos ou através da operação em sistemas computacionais com o objetivo de proteger os recursos tecnológicos utilizados no processamento e armazenamento das informações (Björck, 2005)
Formais	Mudar o comportamento dos indivíduos e da organização formalmente através de regras e da conformidade com leis e regulamentos (Dhillon & Moores, 2001), e estão relacionados à Política de Segurança da Informação e a processos, regulamentos e estruturas organizacionais (Björck, 2005)
Informais	Mudar o comportamento dos indivíduos através de ações de treinamento e educação (Björck, 2005), envolvendo a comunicação de atitudes e comportamentos apropriados e das responsabilidades dos indivíduos (Dhillon & Moores, 2001)

Tabela 1 – Medidas técnicas, formais e informais de Segurança da Informação

Para investigar a influência do ambiente externo sobre a adopção de medidas de Segurança da Informação, é recomendada a Teoria Institucional (Björck, 2004; Kam et al., 2013), abordada a seguir.

2.1. Teoria Institucional

Investigações sobre a influência do ambiente externo na adopção de medidas técnicas, formais e informais de Segurança da Informação precisam considerar as pressões que esse ambiente exerce sobre as organizações. Esse entendimento é consistente com a Teoria Institucional (Kam et al., 2013), que trata da criação, difusão, adopção e adaptação de estruturas, esquemas, regras, normas e rotinas nas organizações e no ambiente e preconiza que as organizações e ambiente se influenciam mutuamente (Quinello, 2007).

Quinello (2007) destaca o desenvolvimento da Teoria Institucional em duas escolas: a Velha Escola Institucional, que tem o foco na organização e na legitimação do poder ou interesses das lideranças através de alianças, acordos e da influência do ambiente externo; e a Nova Escola Institucional, cujo foco está no campo organizacional e entende que as organizações buscam se legitimar para sobreviver no ambiente através da conformidade com regras institucionais. DiMaggio e Powell (1983) argumentam que ambas as escolas baseiam-se na relação entre organização e ambiente, mas Busanelo (2010) enfatiza que, após o trabalho de Meyer e Rowan (1977), houve uma proliferação de estudos da Nova Escola Institucional, que Powell e Bromley (2015) entendem ter se tornado dominante.

O campo organizacional, unidade de análise da Nova Escola Institucional, é um conjunto de organizações que constituem uma área reconhecida de vida institucional, entre fornecedores-chave, consumidores, agências reguladoras e prestadores de serviços (DiMaggio & Powell, 1983), e sua utilização como unidade de análise permite considerar seus atores relevantes em um estudo científico (Lopes, 2012). Em um campo organizacional, as regras, práticas, procedimentos, políticas e programas são disseminados e vistos como apropriados e eficientes, e são incorporados pelas organizações para se legitimarem e sobreviverem (Meyer & Rowan, 1977), mas essa assimilação as torna semelhantes, em um processo chamado isomorfismo institucional, que pode ser coercitivo, mimético e normativo (DiMaggio & Powell, 1983), mecanismos esses descritos na Tabela 2.

Tipo	Características
Isomorfismo mimético	Decorre do sucesso e prestígio de algumas organizações do campo organizacional, o que as torna mais legítimas e, consequentemente, imitadas pelas outras, que almejam alcançar os mesmos resultados diante das incertezas existentes
Isomorfismo normativo	Decorre da profissionalização no campo organizacional, que faz com que profissionais com conhecimentos e percepções semelhantes quanto a modelos, práticas, procedimentos e estruturas passem a trabalhar nas organizações
Isomorfismo coercitivo	Decorre do poder e da dependência entre organizações do mesmo campo organizacional e do estabelecimento de regras, práticas, estruturas e procedimentos cuja adoção é obrigatória

Fonte: DiMaggio e Powell (1983)

Tabela 2 – Os três mecanismos de isomorfismo institucional

Sob essa perspectiva, regulamentos governamentais, padrões e práticas tidas como certas ou eficientes e disseminados no campo organizacional pressionam as organizações a adoptarem medidas formais, informais e técnicas de Segurança da Informação para se legitimarem (Albuquerque Junior & Santos, 2015).

2.2. Modelo de Pesquisa

A abordagem institucional foi utilizada recentemente em trabalhos sobre o tema (Tejay & Barton, 2013; Anthony et al., 2014; Lopes & Sá-Soares, 2014; Alkalbani, Deng & Kam, 2015; Angst, Block, D'Arcy, & Kelley, 2017; Alkalbani et al., 2017; Hou et al., 2018; Choi, Lee, & Hwang, 2018), mas, se analisados em conjunto, esses trabalhos são inconclusivos quanto aos mecanismos institucionais que pressionam as organizações a adoptarem medidas de Segurança da Informação, pois apontam para pressões normativas e miméticas (Tejay & Barton, 2013), coercitivas (AlKalbani et al., 2015; Hou et al., 2018), miméticas e coercitivas (Anthony et al., 2014; Alkalbani et al., 2017), e coercitivas e normativas (Kam et al., 2013; Lopes & Sá-Soares, 2014; Choi et al., 2018). Além disso, os trabalhos abordam principalmente medidas formais (Williams et al., 2013; Kam et al., 2013; Lopes & Sá-Soares, 2014; Anthony et al., 2014; Angst et al., 2017; Alkalbani et al., 2017; Hou et al., 2018; Choi et al., 2018), dando pouca atenção às medidas informais e técnicas.

Com base em diferentes trabalhos que aplicam a Teoria Institucional, Albuquerque Junior e Santos (2015) utilizaram sete indicadores relacionados ao ambiente institucional para realizar uma pesquisa com institutos de pesquisa: Leis, decretos, instruções normativas, normas complementares, resoluções publicadas pelo Governo; Convênios ou contratos firmados com outras organizações parceiras ou de financiamento; Normas e padrões internacionais de Segurança da Informação; Critérios de seleção de profissionais que exigem formação ou conhecimentos específicos em Segurança da Informação; Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos; Utilização de experiências de outras organizações públicas bem sucedidas como modelos; Utilização de experiências de outras organizações acadêmicas bem sucedidas como modelos.

Albuquerque Junior e Santos (2015) identificaram também três grupos de constituintes do ambiente institucional: Governo, Órgãos de Regulação e Organizações de Financiamento; Profissionais de Tecnologia da Informação (TI) e Segurança da Informação; e Outras Organizações do Campo Organizacional.

Os indicadores identificados por Albuquerque Junior e Santos (2015) foram associados aos constituintes de forma a permitir investigar de quê decorre a adopção de medidas de Segurança da Informação: obrigações, que são pressões coercitivas do governo e de organizações responsáveis pela regulação ou financiamento; profissionalização da Segurança da Informação, que resulta em pressões normativas que incidem sobre as organizações para adotarem medidas de Segurança da Informação; imitação de medidas adoptadas por outras organizações públicas ou acadêmicas consideradas bem sucedidas no ambiente institucional.

A Tabela 3 apresenta os constituintes do ambiente institucional associados aos indicadores de pressões coercitivas (PC01 e PC02), normativas (PN01, PN02 e PN03) e

miméticas (PM01 e PM02) utilizados por Albuquerque Junior e Santos (2015) com base na literatura sobre Segurança da Informação e Teoria Institucional.

Constituintes	Indicadores
Governo, órgãos de regulação, e organizações de financiamento	PC01 – Leis, decretos, instruções normativas, normas complementares, resoluções publicadas pelo Governo PC02 – Convênios ou contratos firmados com outras organizações parceiras ou de financiamento
Profissionais de TI e Segurança da Informação	PN01 – Normas e padrões internacionais de Segurança da Informação PN02 – Critérios de seleção de profissionais que exigem formação ou conhecimentos específicos em Segurança da Informação PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos
Outras organizações do campo organizacional	PM01 – Utilização de experiências de outras organizações públicas bem-sucedidas como modelos PM02 – Utilização de experiências de outras organizações acadêmicas bem-sucedidas como modelos

Fonte: Albuquerque Junior e Santos (2015)

Tabela 3 – Constituintes e pressões do ambiente institucional

As medidas de Segurança da Informação utilizadas neste estudo foram identificadas na literatura (Belasco & Wan, 2006; Juels, 2006; Thorpe, 2006; Panko, 2006; Sêmola, 2014) e agrupadas como técnicas, formais e informais, conforme proposto por Dhillon (1999) (Tabela 4).

Tipo	Exemplos
Técnicas	Redundância de dados; Segregação de redes de computadores; Redundância de peças e equipamentos; Prevenção contra códigos maliciosos; Controlo de acesso lógico; Transmissão e armazenamento seguro de dados; Autenticação forte; Redundância de equipamentos; Controlo de acesso físico; Protecção ambiental
Formais	Política de Segurança da Informação; Comitê de Segurança da Informação; Regulamentos internos de Segurança da Informação; Processos e procedimentos de Segurança da Informação; Equipa de Tratamento de incidentes de Segurança da Informação; Escritório de Segurança da Informação; Processo de análise e avaliação de riscos; Classificação de informações; Sistema de Gestão de Segurança da Informação; Revisão da Política de Segurança da Informação
Informais	Programas de treinamento de profissionais de TI; Programas de treinamento de utilizadores de TI; Campanhas de divulgação de regulamentos e da Política de Segurança da Informação; Campanhas de conscientização

Tabela 4 – Medidas técnicas, formais e informais de Segurança da Informação

Decisões sobre a adopção de medidas formais e informais, como política, plano director, planeamento e estratégias de Segurança da Informação, devem ser tomadas nos mais altos níveis decisórios de Segurança da Informação, como em um Comitê criado para essa finalidade. Já questões relativas a implementação e execução de medidas técnicas devem ficar a cargo do Escritório de Segurança da Informação ou da equipa de tratamento

de incidentes (Sêmola, 2014). Entretanto, subunidades organizacionais distintas sofrem diferentes influências do ambiente institucional (Delmas & Toffel, 2008) e a adopção de medidas técnicas, normalmente realizada por departamentos de actuação técnica, pode estar sujeita a pressões institucionais diferentes das que incidem sobre estruturas organizacionais responsáveis pela adopção de medidas formais e informais. Assim, tipos diferentes de medidas (formais, informais e técnicas) podem ser adoptadas como respostas a diferentes pressões institucionais (coercitivas, normativas e miméticas).

Para investigar se a adopção de medidas formais, informais e técnicas está associada a pressões coercitivas, normativas e miméticas, foram estabelecidas relações hipotéticas entre os constituintes do ambiente institucional e as categorias de medidas de Segurança da Informação, permitindo a construção do modelo de pesquisa (Figura 1).

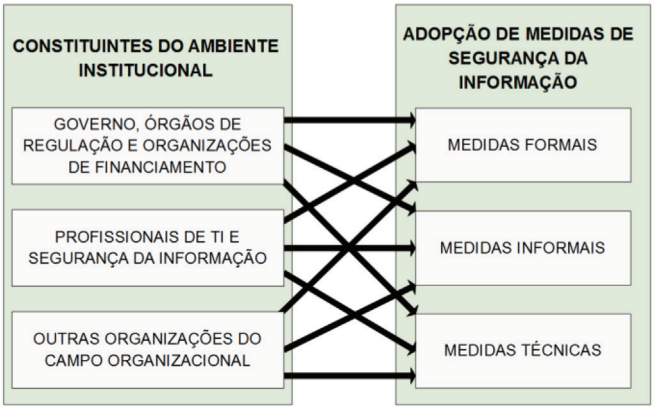

Figura 1 – Modelo de pesquisa

Dessa forma, constituintes que têm algum poder sobre o campo organizacional podem obrigar a adopção de medidas formais, informais e técnicas de Segurança da Informação por meio de leis, regulamentos, contratos ou acordos. A troca de informações e experiências em redes de profissionais de TI e Segurança da Informação ou a compreensão desses profissionais quanto às medidas necessárias pode levá-los a buscar a adopção em suas organizações também. Por fim, outras organizações públicas ou acadêmicas prestigiadas ou bem-sucedidas quanto à Segurança da Informação podem ser imitadas, e as medidas adoptadas por elas podem ser copiadas pelas universidades (Hsu et al., 2012; Lopes, 2012; Kam et al., 2013; Lopes & Sá-Soares, 2014).

3. Metodologia

Este trabalho envolveu a realização de pesquisa documental e um levantamento (*survey*) com gestores de Segurança da Informação ou TI de universidades públicas brasileiras, organizações que compõem um campo organizacional, conforme definido por DiMaggio e Powell (1983) e preconizado como unidade de análise da Teoria Institucional.

Essas organizações são também obrigadas a publicar documentos que tratam de Segurança da Informação, o que facilita o acesso aos dados. A pesquisa documental teve o objectivo de recolher dados para comparar com os dados oriundos do levantamento e envolveu a busca e análise de documentos que formalizam estruturas, processos, regulamentos internos, a Política de Segurança da Informação e o Plano Director de TI (PDTI) das universidades a fim de identificar evidências da adopção de medidas de Segurança da Informação. A busca pelos documentos foi realizada nos sítios *web* das universidades que responderam ao levantamento e na ferramenta de buscas Google, utilizando neste caso os termos "política de segurança da informação", "psi", "posic", "sistema de gestão de segurança da informação", "sgsi", "plano director de ti" e "pdti" junto ao nome e sigla das universidades.

Os dados foram recolhidos entre outubro de 2015 e janeiro de 2016. O levantamento utilizou um formulário electrónico disponibilizado através do sistema FormSUS (http://formsus.datasus.gov.br) contendo 32 perguntas organizadas em duas partes: a) oito perguntas com o objectivo de recolher informações sobre respondente, tipo de governo (federal, estadual ou local), organizações que regulamentam as actividades, organizações tidas como bem sucedidas quanto à Segurança da Informação, padrões e modelos que orientam a Segurança da Informação, as medidas adoptadas e a legislação que aborda Segurança da Informação; e b) 24 perguntas referentes às medidas técnicas, formais e informais (Dhillon, 1999). No formulário, os respondentes seleccionavam as pressões institucionais que influenciaram a adopção de cada medida na universidade, podendo ser marcadas mais de uma opção dentre as disponíveis. Parte das perguntas permitiu a escolha de apenas uma opção, enquanto outras permitiam a selecção de mais opções e o acréscimo de informações em texto para identificar os órgãos que regulamentam as actividades desenvolvidas na universidade, a legislação e os padrões e modelos considerados na adopção.

Do total de 113 universidades públicas brasileiras, foram seleccionadas para participar da pesquisa as 55 que tinham profissionais ou estruturas organizacionais de Segurança da Informação, conforme informações divulgadas na Internet. Os possíveis respondentes e seus meios de contacto foram também identificados na Internet. O endereço electrónico do formulário foi enviado por correio electrónico, juntamente com esclarecimentos sobre a pesquisa, para os possíveis participantes ou para os departamentos de Segurança da Informação ou de TI. Os dados do levantamento foram analizados de forma descritiva, enquanto a análise qualitativa do conteúdo dos documentos foi fundamentada na teoria.

4. Apresentação e Análise dos Dados

Dentre os possíveis respondentes que receberam o convite, 27 (ou 49%) preencheram totalmente o formulário, sendo três de universidades estaduais e 24 de federais. Os respondentes são coordenadores de TI (17) e de Segurança da Informação (2), ou desempenham actividades técnicas (8) relacionadas.

Na busca por documentos, foram identificadas 17 Políticas de Segurança da Informação, 15 PDTIs, dois Sistemas de Gestão de Segurança da Informação (SGSI), oito normas e regulamentos, 152 acordos e convênios com outras organizações, mas nenhum Plano de Continuidade do Negócio.

Diferentes leis brasileiras preveem a adopção de medidas de Segurança da Informação em organizações públicas e privadas, e por desenvolverem actividades de ensino e pesquisa, universidades brasileiras estão sujeitas a regulamentos e fiscalização de diferentes órgãos, como Ministério do Planejamento, Orçamento e Gestão (MPOG), Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), Controladoria Geral da União (CGU), Tribunal de Contas da União (TCU) e governos e tribunais de contas estaduais. Os respondentes de 22 universidades federais confirmaram TCU e SISP como fontes de pressão para adopção de medidas de Segurança da Informação, enquanto o MPOG foi apontado por 20 e a CGU por 16 respondentes, enquanto as três universidades estaduais confirmaram a pressão dos governos e tribunais de contas estaduais. Como as universidades brasileiras recebem financiamento de pesquisas de organizações governamentais, como a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), elas têm suas actividades de pesquisa e pós-graduação regulamentadas por essas organizações também, que podem impor exigências quanto à segurança de informações de pesquisa. Apesar disso, somente um respondente incluiu o CNPq, enquanto a CAPES foi apontada por 21 respondentes como fonte de pressão institucional.

Os respondentes informaram quais organizações consideram bem sucedidas quanto à Segurança da Informação, e os resultados mostram que há mais organizações públicas do que universidades, destacando-se o TCU (apontado por todos os respondentes), o MPOG (26 respondentes), a CGU (25 respondentes), o Banco Central do Brasil (BACEN) (24 respostas), além da Universidade de São Paulo (USP) (19 respostas) e da Universidade de Campinas (UNICAMP) (19 respostas), sinalizando a incidência de pressões miméticas.

O modelo de Segurança da Informação mais utilizado é a norma ISO/IEC 27002, segundo 25 respondentes, enquanto o *Control Objectives for Information and Related Technology* (COBIT), voltado para Governança de TI, é adoptado por 18 universidades. As normas de Segurança da Informação ISO/IEC 27001 e ISO/IEC 27005 foram apontadas por 15 e 10 respondentes, respectivamente. Esses resultados mostram que as universidades recebem pressões normativas de modelos bem conhecidos pelos profissionais de TI e Segurança da Informação.

Diferentes leis, decretos e regulamentos relacionados a Segurança da Informação foram indicados nos formulários (Tabela 5) e confirmadas em 13 Políticas de Segurança da Informação analisadas na pesquisa documental, o que evidencia pressões coercitivas sobre as universidades.

Além da medida informal “Programas de treinamento de profissionais de TI”, quatro medidas técnicas compõem a lista das que são adoptadas por todas as universidades: “Segregação de redes de computadores”, “Redundância de peças de equipamentos”, “Prevenção contra códigos maliciosos” e “Protecção ambiental”. A mais adoptada entre as formais é “Política de Segurança da Informação” (23 respondentes). A Tabela 6 mostra as medidas e quantas universidades as adoptam.

Leis, Decretos e Regulamentos	Objetivo ou Assunto	Quantidade
Lei nº 12.527/2011	Lei de Acesso à Informação, que dispõe sobre garantia de acesso a informações públicas	19
Decreto nº 7.724/2012	Regulamenta a Lei de Acesso à Informação	19
Decreto nº 3.505/2000	Institui a Política de Segurança da Informação da administração pública federal	17
NC 03/IN01/DSIC/GSIPR	Norma Complementar que dispõe sobre a elaboração de políticas de Segurança da Informação na administração pública federal	17
IN 01 GSI/PR/2008	Instrução Normativa que disciplina a gestão da Segurança da Informação na administração pública federal	16
NC 07/IN01/DSIC/GSIPR	Norma Complementar que regulamenta a implantação de controlos de acesso sobre a elaboração de políticas de Segurança da Informação na administração pública federal	14
NC 02/IN01/DSIC/GSIPR	Norma Complementar que estabelece uma metodologia de gestão da Segurança da Informação para a administração pública federal	13
NC 17/IN01/DSIC/GSIPR	Norma Complementar que estabelece diretrizes de actuação de profissionais de Segurança da Informação nos órgãos públicos federais	13

Tabela 5 – Legislação brasileira apontada pelos respondentes

Medida	Categoria	Quantidade
Segregação de redes de computadores	Técnica	27
Redundância de peças e equipamentos	Técnica	27
Prevenção contra códigos maliciosos	Técnica	27
Protecção ambiental	Técnica	27
Programas de treinamento de profissionais de TI	Informal	27
Redundância de dados	Técnica	24
Política de Segurança da Informação	Formal	23
Controlo de acesso lógico	Técnica	22
Transmissão e armazenamento seguro de dados	Técnica	20
Comitê de Segurança da Informação	Formal	19
Redundância de equipamentos	Técnica	19
Regulamentos internos de Segurança da Informação	Formal	18
Equipa de tratamento de incidentes	Formal	18
Processos e procedientos de Segurança da Informação	Formal	16
Autenticação forte	Técnica	16
Programas de treinamento de utilizadores de TI	Informal	16

Escritório de Segurança da Informação	Formal	11
Controlo de acesso físico	Técnica	11
Revisão da Política de Segurança da Informação	Formal	10
Campanhas de conscientização	Informal	10
Sistema de Gestão de Segurança da Informação	Formal	9
Campanhas de divulgação de regulamentos e da Política	Informal	8
Classificação de informações	Formal	7
Processo de análise e avaliação de riscos	Formal	6

Tabela 6 – Medidas adoptadas e quantidade de universidades que as adotam

Apesar de os dados mostrarem que 27 universidades adoptam "Programas de treinamento de profissionais de TI", a pesquisa documental não identificou evidências nos 15 PDTIs analisados, nem de "Programas de treinamento de utilizadores de TI", adoptado por 16 universidades. Os dados mostram que, embora tenha havido capacitação de funcionários, houve poucas "Campanhas de conscientização" (10 universidades) e "Campanhas de divulgação de regulamentos e da Política de Segurança da Informação" (oito universidades).

Dentre as medidas formais, a "Política de Segurança da Informação" é a mais comum, adoptada por 23 universidades. Como quatro universidades não têm esse documento, outras medidas podem ser adoptadas sem seguir princípios e diretrizes organizacionais. Foram localizadas apenas 17 Políticas para análise, possivelmente porque não foram divulgadas em seis universidades, o que pode contribuir para o descumprimento de suas diretrizes devido ao seu desconhecimento interno.

O "Comitê de Segurança da Informação" é a segunda medida formal mais adoptada, segundo 19 respondentes, mas sua formalização está documentada em 12 universidades. Por ser responsável por elaborar e revisar a Política de Segurança da Informação (Sêmola, 2014), e considerando que 23 universidades formalizaram Políticas e 19 têm Comitês instituídos, infere-se que as Políticas não são elaboradas nem revisadas por Comitês em quatro universidades.

Entre as medidas formais menos adoptadas está "Processo de Análise e Avaliação de Riscos" (adoptada por seis universidades), imprescindível para identificar requisitos de Segurança da Informação (Sêmola, 2014) e cujo facto de não ser adoptada implica em perda da capacidade de identificar informações sensíveis e as medidas necessárias para protegê-las.

A adopção de "Política de Segurança da Informação" foi mais associada a regulamentos do Governo, evidenciado pelo indicador "PC01 – Leis, decretos, Instruções Normativas, Normas Complementares e resoluções publicadas pelo Governo" (21 respondentes), assim como "Comitê de Segurança da Informação" (19 respondentes) e "Regulamentos internos de Segurança da Informação" (16 universidades), sendo que quatro universidades adoptam regulamentos internos sem ter uma Política de Segurança da Informação como base, o que pode resultar em rejeição por parte dos utilizadores.

A Política de Segurança da Informação deve orientar a elaboração de processos e procedimentos internos (Sêmola, 2014). A adopção de "Processos e Procedimentos de Segurança da Informação" nas universidades foi associada por 15 respondentes a "PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos", o que aponta que são adoptadas destacadamente devido a pressões normativas, mas os documentos não foram localizados. Duas universidades têm processos e procedimentos internos, mas não têm uma Política de Segurança da Informação.

A adopção da medida formal "Equipa de tratamento de incidentes" foi associada por 15 respondentes ao indicador "PM01 – Utilização de experiências de outras organizações públicas bem-sucedidas como modelos", evidenciando que sua existência decorre do mimetismo institucional, sendo, portanto, uma imitação de experiências de outras organizações públicas. Já a medida formal "Escritório de Segurança da Informação" foi adoptada devido ao indicador "PN01 – Utilização de normas e padrões internacionais de Segurança da Informação como modelo" (11 respondentes), o que evidencia uma associação com pressões normativas. Da mesma forma, as poucas universidades que adoptam a medida formal "Processo de Análise e Avaliação de Riscos" o fazem devido a padrões normativos internacionais.

As medidas formais "Classificação de Informações" e "Sistema de Gestão de Segurança da Informação" foram mais associadas a pressões coercitivas do ambiente institucional: a primeira foi associada por sete e a segunda por nove respondentes ao indicador "PC01 – Leis, decretos, Instruções Normativas, Normas Complementares e resoluções publicados pelo Governo".

A "Revisão da Política de Segurança da Informação" permite que o documento seja actualizado devido a mudanças nos requisitos de Segurança da Informação (Sêmola, 2014). Nove respondentes associaram esta medida formal ao indicador "PN01 – Normas e padrões internacionais de Segurança da Informação", o que a relaciona a pressões normativas. Todas as 17 Políticas de Segurança da Informação analisadas previam revisões, mas somente dez respondentes informaram que são realizadas e apenas duas universidades publicaram versões revisadas.

Os resultados mostram que as medidas formais são adoptadas principalmente devido a pressões coercitivas, mas também a pressões normativas e miméticas. Das dez medidas formais, cinco são adoptadas em resposta a pressões coercitivas ("PC01 – Leis, decretos, Instruções Normativas, Normas Complementares e resoluções publicadas pelo Governo") provenientes do Governo e de órgãos que regulam e financiam as actividades das universidades.

Quatro medidas formais foram relacionadas a pressões normativas, sendo três ao indicador "PN01 – Utilização de normas e padrões internacionais de Segurança da Informação como modelo" e um a "PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos", o que mostra a relevância das normas e padrões internacionais e do compartilhamento de informações e conhecimentos entre profissionais, que são pressões normativas para adopção de medidas de Segurança da Informação.

Dentre as medidas técnicas, a adopção de "Redundância de dados" e "Prevenção contra códigos maliciosos" acontece com base em experiências de outras universidades ("PM02 – Utilização de experiências de outras organizações acadêmicas bem-sucedidas como modelos"), segundo 23 e 26 respondentes, respectivamente, o que sugere que são implantadas tecnologias utilizadas por outras universidades, evidenciando o mimetismo institucional.

As medidas técnicas "Segregação de redes de computadores" e a "Redundância de peças de equipamentos" foram associadas pela maioria dos respondentes ao indicador "PN02 – Utilização de critérios de seleção de pessoal que exigem formação ou conhecimentos específicos em Segurança da Informação". A primeira foi associada por todos os 27 respondentes e a segunda por 23. Estas medidas são adoptadas, portanto, em resposta a pressões normativas, pois estão associadas aos conhecimentos e formação dos profissionais, o que pode ser explicado pela exigência de conhecimentos específicos de Segurança da Informação.

As demais medidas técnicas foram todas associadas ao indicador "PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos": "Protecção ambiental", por 25 respondentes; "Transmissão e armazenamento seguros de dados", por 19 respondentes; "Controlo de acesso lógico", por 18 pessoas; "Redundância de equipamentos", por 17 pessoas; "Autenticação forte", associado por 15 pessoas; e "Controlo de acesso físico", associada por 11 pessoas. A adopção de medidas técnicas está mais relacionada a pressões normativas, sendo que este indicador foi associado a cinco medidas, e "PN02 – Utilização de critérios de seleção de pessoal que exigem formação ou conhecimentos específicos em Segurança da Informação" a duas medidas, o que destaca a actuação dos profissionais em suas redes de relacionamentos e a importênia de conhecimentos específicos prévios como pressões para a adopção de medidas técnicas.

Dentre as medidas informais, a mais adoptada é "Programas de treinamento de profissionais de TI", sendo que 26 universidades a adoptam devido às pressões normativas "PN01 – Normas e padrões internacionais de Segurança da Informação" e "PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos", o que leva a inferir que a capacitação dos profissionais de TI resulta da troca de conhecimentos e da influência de normas e padrões de Segurança da Informação. A medida informal "Programas de treinamento de utilizadores de TI" também é adoptada principalmente devido a pressões normativas, mas foi associada por 16 respondentes apenas ao indicador "PN03 – Participação de profissionais de TI e Segurança da Informação em redes de compartilhamento de informações e troca de conhecimentos". Esses treinamentos para utilizadores podem ser realizados, portanto, devido ao facto de que os profissionais de TI e Segurança da Informação os entendem como necessários. A adopção da medida informal "Campanhas de divulgação de regulamentos e da Política de Segurança da Informação" foi também resultado das mesmas pressões normativas, segundo oito respondentes.

Por fim, dez respondentes associaram a medida informal "Campanhas de conscientização" aos indicadores "PM01 – Utilização de experiências de outras

organizações públicas bem-sucedidas como modelos" e "PM02 – Utilização de experiências de outras organizações acadêmicas bem sucedidas como modelos", ambos de pressões miméticas, o que evidencia a imitação de organizações consideradas bem sucedidas no ambiente. Assim, medidas informais foram adoptadas principalmente em resposta a pressões normativas, mas também devido à imitação de experiências bem-sucedidas, enquanto a adoção de medidas formais está mais relacionada a pressões coercitivas, e as técnicas a pressões normativas.

5. Conclusões

Esta pesquisa mostrou que as universidades públicas brasileiras estão sujeitas a pressões normativas, coercitivas e miméticas de diferentes constituintes do campo organizacional, como grupos de profissionais de Segurança da Informação, organizações que regulamentam e fiscalizam suas actividades e organizações públicas ou acadêmicas bem-sucedidas quanto à Segurança da Informação.

Os dados evidenciam que a adopção de medidas de Segurança da Informação acontece devido principalmente a pressões normativas, sendo que a participação de profissionais de TI e Segurança da Informação em redes de trocas de informações foi o indicador mais seleccionado, que influencia destacadamente a adopção de medidas técnicas. Já as normas e padrões de Segurança da Informação tiveram influência relevante sobre a adopção de medidas informais, sendo que as medidas formais foram mais associadas a pressões coercitivas.

O trabalho mostrou também que as medidas técnicas são as mais difundidas, sendo que algumas delas foram adoptadas por todas as universidades, tendo sido mais associadas a pressões normativas, com destaque para a troca de informações entre profissionais e a contratação de profissionais com conhecimentos específicos em Segurança da Informação. Entre as informais, os "Programas de treinamento de profissionais de TI" também foram adoptadas por todas as universidades e foram associadas à contratação de profissionais com conhecimentos específicos e à participação deles em redes de profissionais. Entre as medidas formais, as mais adoptadas são a "Política de Segurança da Informação" e o "Comitê de Segurança da Informação" em resposta a pressões coercitivas de organizações que regulamentam a actuação das universidades.

Os resultados deixam claro que as informações das universidades não estão classificadas, o que pode levar a um tratamento inadequado e exposição a riscos. Outro resultado relevante é o facto de poucas universidades realizarem análises e avaliações de riscos, o que pode resultar na adopção de medidas de Segurança da Informação desnecessárias, insuficientes ou inapropriadas, expondo informações sensíveis ou protegendo excessivamente informações que necessitam de medidas menos rigorosas. Esses resultados e o facto de as medidas formais serem adoptadas devido a pressões coercitivas levam a questionar se a adopção visa à eficiência da Segurança da Informação ou à legitimidade das universidades no ambiente, tendo em vista que a conformidade com requisitos do ambiente externo é tida como meio para obter legitimidade e ter acesso a recursos.

A principal limitação do estudo está na quantidade de universidades que participou da pesquisa, o que inviabilizou a realização de análises estatísticas mais profundas e

limitou as conclusões. Procurou-se minimizar essa limitação cruzando os dados do levantamento e os da pesquisa documental, mas a pequena quantidade de documentos disponibilizados pelas universidades também se mostrou uma limitação. Organizações do mercado de TI não aparecem como constituintes do campo organizacional nesta pesquisa, o que restringe os resultados e é também uma limitação. A partir desse contexto, há uma necessidade de investigar a adopção de medidas observando um escopo maior de constituintes do campo organizacional e questionar a finalidade ou motivação da adopção de medidas de Segurança da Informação: se a eficiência ou legitimidade no campo organizacional.

Referências

Albuquerque Junior, A. E., & Santos, E. M. (2015). Adoption of Information Security measures in public research institutes. *Journal of Information Systems and Technology Management*, 12(2), 289–316.

Al-Kalbani, A, Deng, H., & Kam, B. (2015). Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure. In: *Proceedings of the 19th Pacific Asia Conference on Information Systems, Singapore*, 5–9 July 2015, pp. 1–11.

Al-kalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security compliance in organizations: an institutional perspective. *Data and Information Management*, 1(2), 104–114.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, 41(3), 893–916.

Anthony, D. L., Appari, A., & Johnson, M. E. (2014). Institutionalizing HIPAA compliance: organizations and competing logics in U.S. health care. *Journal of Health and Social Behavior*, 55(1), 108–124.

Belasco, K., & Wan, S.-P. (2006). Online retail banking: security concerns, breaches, and controls. In Bidgoli, H. (Org.). *Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management* (v.1, pp. 37-48). New Jersey: John Wiley & Sons.

Björck, F. J. (2004). Institutional Theory: A new perspective for research into IS/IT security in organisations. In *Proceedings of Hawaii International Conference on System Sciences* (pp. 37). Big Island, HI, USA: IEEE.

Björck, F. J. (2005). *Discovering Information Security management*. Tese de Doutoramento, Stockholm University, Estocolmo, Suécia.

Busanelo, E. C. (2010). Um estudo epistemológico da Teoria Neo-Institucional. In *Anais do Encontro de Estudos Organizacionais da Associação Nacional de Pós-Graduação e Pesquisa em Administração*,(pp. 6). Florianópolis, SC, Brasil: ANPAD.

Choi, M., Lee, J., & Hwang, K. (2018). Information Systems Security (ISS) of e-government for sustainability: a dual path model of ISS influenced by institutional isomorphism. *Sustainability*, 10(5*), 1555*.

Delmas, M. A., & Toffel, M. W. (2008). Organizational responses to environmental demands: opening the black box. *Strategic Management Journal*, 29(10), 1027–1055.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security*, 7(4), 171–175.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, 20(8), 715–723.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160.

Dresner, D. G. (2011). *A study of standards and the mitigation of risk in Information Systems*. Tese de Doutoramento, The University of Manchester, Manchester, Reino Unido.

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

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: the case of a Chinese hospital. *Technological Forecasting and Social Change*, 126, 64–75.

Hsu, C. W., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on Information Systems Security innovations. *Information Systems Research*, 23(3), 918–939.

Juels, A. (2006). Encryption basics. In Bidgoli, H. (Org.). *Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management* (v.2, pp. 469–478). Nova Jersey: John Wiley & Sons.

Kam, H.-J., Katerattanakul, P., Gogolin, G., & Hong, S. (2013). Information Security Police compliance in higher education: a neo-institutional perspective. In *Proceedings of Pacific Asia Conference on Information Systems* (pp.17), Jeju Island, Coreia do Sul.

Lopes, I. M. (2012). *Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública local em Portugal*. Tese de Doutoramento, Universidade do Minho, Braga, Portugal.

Lopes, I. M., & Sá-Soares, F. (2014). Institutionalization of Information Systems Security Policies adoption: factors and guidelines. *International Journal on Computer Science and Information Systems*, 9(2), 82–95.

Luesebrink, M. (2011). *The institutionalization of Information Security Governance structures in academic institutions: a case study*. Tese de Doutoramento, Florida State University, Tallahassee, FL, Estados Unidos da América.

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *The American Journal of Sociology*, 83(2), 340–363.

Panko, R. R. (2006). Digital signatures and electronic signatures. In Bidgoli, H. (Org.). *Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management* (v.3, pp. 562-570). Nova Jersey: John Wiley & Sons.

Perkel, J. (2010). Cybersecurity: how safe are your data? *Nature*, 464, 1260–1261.

Powell, W. W., & Bromley, P. (2015). New Institutionalism in the analysis of complex organizations. In Wright, J. D. (Org.). *International encyclopedia of the social & behavioral sciences* (Vol. 2, 2ª ed., pp. 764–769). Amsterdão: Elsevier.

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

Sêmola, M. (2014). *Gestão da Segurança da Informação: uma visão executiva* (2a ed.). Rio de Janeiro: Campus.

Tejay, G. P. S., & Barton, K. A. (2013). Information System Security commitment: a pilot study of external influences on senior management. In *Proceedings of Hawaii International Conference on System Sciences* (pp. 46), Manoa, HI, Estados Unidos da América.

Thorpe, S. W. (2006). Extranets: applications, development, security, and privacy. In Bidgoli, H. (Org.). *Handbook of Information Security: threats, vulnerabilities, prevention, detection, and management* (v.1, pp. 215–225). Nova Jersey: John Wiley & Sons.

Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information Security Governance practices in critical infrastructure organizations: a socio-technical and institutional logic perspective. *Electronic Markets*, 23(4), 341–354.