UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA DE ADMINISTRAÇÃO
NÚCLEO DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
DOUTORADO EM ADMINISTRAÇÃO

ANTONIO EDUARDO DE ALBUQUERQUE JUNIOR

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO: A INFLUÊNCIA DAS RESPOSTAS ESTRATÉGICAS DAS SUBUNIDADES NA CONFORMIDADE ORGANIZACIONAL

Salvador
2017

ANTONIO EDUARDO DE ALBUQUERQUE JUNIOR

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO: A INFLUÊNCIA DAS RESPOSTAS ESTRATÉGICAS DAS SUBUNIDADES NA CONFORMIDADE ORGANIZACIONAL

Tese apresentada ao curso de Doutorado em Administração do Núcleo de Pós-Graduação em Administração da Escola de Administração da Universidade Federal da Bahia, como requisito parcial para a obtenção do título de Doutor em Administração.

Orientador: Prof. Dr. Ernani Marques dos Santos

Salvador
2017

Escola de Administração – UFBA

A345 Albuquerque Junior, Antonio Eduardo.
Adoção de medidas de segurança da informação: a influência das subunidades na conformidade organizacional / Antonio Eduardo de Albuquerque Junior. – 2017.
367 f.

Orientador: Prof. Dr. Ernani Marques dos Santos.
Tese (doutorado) – Universidade Federal da Bahia, Escola de Administração, Salvador, 2017.

1. Tecnologia da informação – Medidas de segurança. 2. Gerenciamento de recursos de informação. 3. Comportamento organizacional. 4. Estudantes universitários – Ensino auxiliado por computador. I. Universidade Federal da Bahia. Escola de Administração. II. Título.

CDD – 658.472

UNIVERSIDADE FEDERAL DA BAHIA
ESCOLA DE ADMINISTRAÇÃO
NÚCLEO DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
DOUTORADO EM ADMINISTRAÇÃO

ANTONIO EDUARDO DE ALBUQUERQUE JUNIOR

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO: A INFLUÊNCIA DAS RESPOSTAS ESTRATÉGICAS DAS SUBUNIDADES NA CONFORMIDADE ORGANIZACIONAL

Tese apresentada ao curso de Doutorado em Administração do Núcleo de Pós-Graduação em Administração da Escola de Administração da Universidade Federal da Bahia, como requisito parcial para a obtenção do título de Doutor em Administração.

Banca Examinadora:

_____
Prof. Dr. Ernani Marques dos Santos
Doutor em Administração – Universidade Federal da Bahia
Orientador

_____
Prof. Dr. Antônio Carlos Gastaud Maçada
Doutor em Administração – Universidade Federal do Rio Grande do Sul

_____
Profa. Dra. Edimara Mezzomo Luciano
Doutora em Administração – Pontifícia Universidade Católica do Rio Grande do Sul

_____
Prof. Dr. João Gualberto Rizzo Araújo
Doutor em Administração – Centro de Pesquisas em Informática

_____
Profa. Dra. Maria do Carmo Lessa Guimarães
Doutora em Administração – Universidade Federal da Bahia

Salvador
2017

A Elaine e Breno, pessoas que amo.

AGRADECIMENTOS

A Elaine, amor da minha vida, e a Breno, meu filho amado, agradeço o apoio, a alegria e a paciência.

A Antonio Eduardo e Ivanete, meus amados pais, agradeço a educação que me proporcionaram, o que iniciou a trilha que me trouxe aqui.

Ao meu orientador, Prof. Dr. Ernani Marques dos Santos, agradeço a orientação e paciência que vem tendo comigo desde o mestrado.

Aos Professores Alexandre Reis Graeml, Antônio Carlos Gastaud Maçada, Edimara Mezzomo Luciano, João Gualberto Rizzo Araújo e Maria do Carmo Lessa Guimarães, agradeço a todas as contribuições que deram para este trabalho.

Aos colegas da FIOCRUZ, agradeço tanto àqueles que participaram da pesquisa como entrevistados quanto aos gestores e demais colegas que me apoiaram.

A Adriano Rocha Silva, Emmanuelle Daltro, Ivo Pedro Gonzalez Junior, Laercio Almeida, Larissa Queiroz, Morjane Armstrong Miranda, Platini Fonseca, Rodrigo César Oliveira, colegas de grupo de pesquisa e de orientação, agradeço a amizade e as contribuições.

Aos professores, pesquisadores e especialistas em Segurança da Informação e em Sistemas de Informações Amarolinda Klein, Anatália Ramos, Gabriela Figueiredo, Marcos Sêmola, Petruska Araújo, Rômulo Souza Neto e Violeta Sun agradeço as valorosas contribuições.

I am very grateful to Professor Christine Oliver and Professor Terence Tsai for the help they gave me when I contacted them.

Agradeço a todos os professores do NPGA, que me ajudaram direta e indiretamente, especialmente a Mônica Mac-Allister, Sandro Cabral, Francisco Teixeira, Adriano Leal Bruni, José Célio Andrade e Elizabeth Loiola.

A Dacy Andrade, Anaelia Almeida, Ernani Dórea, Artur Coêlho e Cristina Araújo, amigos do NPGA, toda a disponibilidade e dedicação.

Aos colegas que frequentaram o NAPP/NEPAD no período em que esta tese foi produzida, especialmente a Daniella Barbosa, Doraliza Monteiro e Ives Tavares, e a todos os colegas da Turma Diferenciada 2013, agradeço a amizade e o companheirismo.

RESUMO

ALBUQUERQUE JUNIOR, Antonio Eduardo de. **Adoção de medidas de Segurança da Informação**: a influência das respostas estratégicas das subunidades na conformidade organizacional. Salvador, 2017. 368f. Tese (Doutorado em Administração) – Escola de Administração, Universidade Federal da Bahia, Salvador, 2017.

A informação é considerada um ativo crítico e, para protegê-la, as organizações dispõem de uma série de medidas de Segurança da Informação previstas na literatura e recomendadas por normas, modelos e padrões utilizados por organizações de todo o mundo. A literatura sobre Segurança da Informação preconiza que as medidas devem ser adotadas com base nas necessidades identificadas para a organização, mas parte da literatura aponta que a adoção é determinada por pressões do ambiente no qual a organização está inserida. O determinismo das pressões do ambiente externo é limitado pela capacidade de a organização responder conforme seus próprios interesses e julgamentos, o que pode fazer com que fique em conformidade com os requisitos externos, mas também em não conformidade ou em uma conformidade apenas aparente. Este estudo parte do pressuposto de que a conformidade da organização com os requisitos externos de Segurança da Informação depende de como suas subunidades respondem às pressões do ambiente para investigar como essas respostas influenciam a conformidade da organização com os requisitos. Para isto, o trabalho envolveu a identificação das medidas de Segurança da Informação adotadas por uma organização, as pressões institucionais que as subunidades organizacionais sofrem, as medidas que as subunidades adotaram atendendo a essas pressões, suas respostas estratégicas e os efeitos dessas respostas sobre as medidas adotadas pela organização. A pesquisa teve abordagem qualitativa e compreendeu a análise de documentos e a realização de entrevistas semiestruturadas com gestores e profissionais de TI e Segurança da Informação da administração central e de 17 subunidades de uma organização. A análise dos dados foi realizada a partir de um *framework* elaborado com base na Teoria Institucional e na tipologia de respostas estratégicas às pressões institucionais, que permitiu sua categorização utilizando o *software* NVivo 10. Os resultados mostram que as subunidades organizacionais respondem às pressões que recebem através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre a eficiência e adequação das medidas de Segurança da Informação. A pesquisa mostrou também que as pressões para adoção de medidas formais, informais e técnicas não estão necessariamente associadas a respostas estratégicas específicas das subunidades organizacionais. Por fim, as respostas das subunidades às pressões que sofrem influenciam no nível de conformidade da organização com os requisitos de Segurança da Informação do ambiente externo.

Palavras-chave: segurança da informação. adoção. medidas. respostas estratégicas. pressões institucionais.

ABSTRACT

ALBUQUERQUE JUNIOR, Antonio Eduardo de. **Adoption of Information Security measures**: the influence of subunits' strategic responses on organizational compliance. Salvador, 2017. 368f. Thesis (Doctorate in Administration) – School of Administration, Federal University of Bahia, Salvador, 2017.

Information is a critical asset, and organizations can use many information security measures prescribed in the literature and recommended by standards and models to protect it. Information Security literature recommends that adoption of information Security measures should be based on needs and risks identified for the organization, but part of the authors indicates that adoption is determined by pressures of the environment in which the organization is inserted. The determinism of external pressures is limited by organization's ability to respond to them according to its own interests and judgments. The organizational response to pressures has potential to make the organization non-comply or comply to external requirements, but compliance may be apparent. This study builds on the idea that the organization's compliance with external Information Security requirements depends on how its subunits respond to the pressures they receive. The research addresses the influence of the subunit's strategic responses on organization's compliance with the external requirements. Based on Institutional Theory, the research included the identification of the Information Security measures adopted by the organization, the institutional pressures on the organizational subunits, the Information Security measures adopted by subunits in response to these pressures, their strategic responses and the effects of these responses on the organization's Information Security measures. The research had a qualitative approach and involved the analysis of documents and semi-structured interviews with IT and Information Security managers and professionals of the organization's headquarters and 17 of its subunits. Data analysis used a framework based on the Institutional Theory and on the typology of strategic responses to institutional pressures, which allowed its categorization using NVivo 10 software. The results show that the organizational subunits respond to the pressures they receive through different strategies and attending to their own interests and judgments about the efficiency and adequacy of the Information Security measures. The research also showed that the pressures to adopt formal, informal and technical information security measures do not result in different strategic responses of the organizational subunits. Finally, the subunit responses to the institutional pressures influence the level of compliance of the organization with the Information Security requirements of the external environment.

Keywords: information security. adoption. measures. strategic responses. institutional pressures.

LISTA DE FIGURAS

LISTA DE QUADROS E TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AUDIN	Auditoria Interna
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
BIO-Manguinhos	Instituto de Tecnologia em Imunobiológicos
CAFE	Comunidade Acadêmica Federada
CAIS	Centro de Atendimento a Incidentes de Segurança
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCS	Coordenadoria de Comunicação Social
CDTS	Centro de Desenvolvimento Tecnológico em Saúde
CECAL	Centro de Criação de Animais de Laboratório
CGTI	Coordenação de Gestão de Tecnologia da Informação
CGU	Controladoria Geral da União
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
COBIT	*Control Objectives for Information and Related Technology*
COC	Casa de Oswaldo Cruz
CPD	Centro de Processamento de Dados
CRIS	Centro de Operações Internacionais em Saúde
DIPLAN	Diretoria de Planejamento Estratégico
DIRAC	Diretoria de Administração do *Campus*
DIRAD	Diretoria de Administração
DIREB	Diretoria Regional de Brasília
DIREH	Diretoria de Recursos Humanos
DMZ	Zona Desmilitarizada

DSIC	Departamento de Segurança da Informação e Comunicações
ENSP	Escola Nacional de Saúde Pública Sérgio Arouca
EPSJV	Escola Politécnica de Saúde Joaquim Venâncio
FARManguinhos	Instituto de Tecnologia em Fármacos
FIOCRUZ	Fundação Oswaldo Cruz
GESTEC	Coordenação de Gestão Tecnológica
GSI	Gabinete de Segurança Institucional
HIPAA	*Health Insurance Portability and Accountability Act*
HTTPS	*Hyper Text Transfer Protocol Secure*
IAM	Instituto Aggeu Magalhães
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
ICC	Instituto Carlos Chagas
ICICT	Instituto de Comunicação e Informação Científica e Tecnológica
IFF	Instituto Fernandes Figueira
IGM	Instituto Gonçalo Moniz
ILMD	Instituto Leônidas e Maria Deane
INCQS	Instituto Nacional de Controle e Qualidade em Saúde
INI	Instituto Nacional de Infectologia Evandro Chagas
IOC	Instituto Oswaldo Cruz
IPS	*Intrusion Prevention System*
IRR	Instituto René Rachou
ISO	*International Organization for Standardization*
MPOG	Ministério do Planejamento, Orçamento e Gestão
NDLTD	*Networked Digital Library of Theses and Dissertations*
NSC	Núcleo de Segurança e Credenciamento

OATD	*Open Access Theses and Dissertations*
POSIC	Política de Segurança da Informação e Comunicações
QDA	*Quality Data Analysis*
RNP	Rede Nacional de Ensino e Pesquisa
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SLTI	Secretaria de Logística e Tecnologia da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
UFBA	Universidade Federal da Bahia
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

A ampla utilização de novas tecnologias e as facilidades trazidas pelos meios de acesso e troca de informações expuseram as organizações a novas ameaças, que podem tornar mais difícil ou inviável o cumprimento dos objetivos organizacionais (ALEXANDRIA, 2009). Além disso, juntamente com o aumento do risco de ocorrência de divulgação e acesso não autorizados, houve também um aumento do impacto de incidentes que comprometem as informações (FACHINI, 2009), pois os processos organizacionais precisam de informações e a tecnologia está amplamente disseminada pelas organizações. Como agravante, incidentes podem comprometer, além da própria informação, a segurança das transações e das pessoas envolvidas nos processos organizacionais (MARCIANO, 2006).

A dependência com relação às informações e a ocorrência de incidentes que as comprometem têm levado à necessidade de proteger também outros ativos envolvidos no processamento, armazenamento e transmissão de informações, aumentando a prioridade de processos voltados a assegurar a continuidade das operações nas organizações (HERATH; HERATH; BREMSER, 2010).

> A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. (FONTES, 2006, p.16).

Esse é o mesmo entendimento da Associação Brasileira de Normas Técnicas (ABNT, 2013), que, através da norma NBR ISO/IEC 27002, apresenta diversas recomendações técnicas e administrativas de Segurança da Informação.

Segundo Silva e Stein (2007, p.47-48), Segurança da Informação é a "proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a confidencialidade e a integridade dessa informação são preservadas", e de acordo com Fontes (2006, p.26), para que se tenha Segurança da Informação, é necessário um "conjunto de orientações, normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada".

Esses procedimentos, orientações, normas, políticas e demais ações estão previstos na literatura científica e profissional sobre Segurança da Informação (BELASCO; WAN, 2006; GORAYEB, 2012; SÊMOLA, 2014) e podem ser adotados por qualquer

organização, não importando seu tamanho ou atividade (ABNT, 2013). Para isso, as necessidades organizacionais precisam ser identificadas em uma análise e avaliação de riscos, um processo previsto tanto na literatura voltada para gestores e profissionais de Segurança da Informação quanto em trabalhos acadêmicos (BACKHOUSE; DHILLON, 1996; ELKY, 2006; SCHMITTLING; MUNNS, 2010; SALEH; ALFANTOOKH, 2011; FENG; LI, 2011; RYAN *et al*.,2012; LO; CHEN, 2012; ABNT, 2013; AHMAD; MAYNARD; SHANKS, 2015; CAVUSOGLU *et al*., 2015; GUSMÃO *et al*., 2016).

Identificados os riscos de Segurança da Informação, as organizações devem adotar medidas apropriadas que atendam às necessidades de todos os seus departamentos e unidades de negócio, e essas medidas devem estar expressas em uma Política de Segurança da Informação e em outros regulamentos internos (QURESHI, 2011; ABNT, 2013; SÊMOLA, 2014), o que formaliza a obrigatoriedade ou a necessidade de cumprimento dessas medidas pelas suas subunidades organizacionais.

Cabe destacar que a adoção de medidas de Segurança da Informação deve ser compreendida de forma análoga à que Thong e Yap (1995) entendem como adoção de Tecnologia da Informação (TI). Esta compreensão da adoção de TI foi ratificada posteriormente por Thong (1999), Chieochan, Lindley e Dunn (2000), Al-Qirim (2005) e Hameed, Counsell e Swift (2012) e envolve tanto a aquisição quanto o uso da tecnologia adotada, o que é coerente com a ideia de adoção de Moore e Benbasat (1991), que criaram uma ferramenta para medir a percepção dos usuários quanto à adoção de inovações de TI em um processo que envolve a decisão de adotar, o uso e a difusão da tecnologia dentro da organização. Dessa forma, neste trabalho, a adoção de medidas de Segurança da Informação envolve a aquisição e o uso de equipamentos e sistemas e a formalização de práticas de gestão voltados para assegurar a confidencialidade, integridade e disponibilidade da informação, como entendem também Hameed e Arachchilage (2016).

Apesar de a literatura sobre o tema esclarecer que as medidas de Segurança da Informação devem ser orientadas por documentos formais e devem atender às necessidades da organização como um todo, a literatura de estudos organizacionais mostra que pode haver uma dissociação entre as políticas formalizadas e as práticas adotadas pelas organizações. Assim, regras e políticas podem ser estabelecidas pelas organizações para atender a requisitos externos sem serem respeitadas, o que configura uma dissociação entre política e prática, caracterizada por uma conformidade apenas aparente com os requisitos externos (MEYER;

ROWAN, 1977; INGERSOLL, 1993; WOOD JR.; CALDAS, 1997; VASCONCELOS; VASCONCELOS, 2003; BROMLEY; POWELL, 2012).

Parte dos trabalhos que tratam de dissociação entre política e prática tem por base a Teoria Institucional, abordagem teórica que assume que as organizações formalizam políticas, modificam estruturas e adotam práticas em resposta às pressões do ambiente. A abordagem institucional põe as organizações como elementos passivos com relação às pressões ambientais, e a conformidade com os requisitos do ambiente externo é uma forma de garantir sua legitimidade e sobrevivência (MEYER; ROWAN, 1977; DIMAGGIO; POWELL, 1983; TOLBERT; ZUCKER, 1983, 1999; SCOTT, 1992, 2005).

Sob essa ótica, a conformidade é a obediência ou incorporação inconsciente ou consciente de valores, normas e requisitos institucionais, segundo Oliver (1991). A organização pode obedecer e incorporar, mas pode também se recusar a obedecer e não incorporar esses valores, normas e requisitos, colocando-se em não conformidade com os requisitos institucionais. Se a conformidade for apenas aparente, quando organização parece seguir as políticas e regras institucionais sem que as práticas internas sofram grandes mudanças, há a dissociação entre política e prática, resultando no que Meyer e Rowan (1977) chamam de conformidade cerimonial, que, como ressaltam estes autores, é útil para obtenção e manutenção da legitimidade organizacional. Assim, as formas de comportamento organizacional quanto à obediência às regras institucionais podem ser organizadas em três níveis de conformidade: não conformidade, conformidade cerimonial e conformidade.

A partir da ideia da dissociação, políticas de Segurança da Informação também podem ser formalizadas sem que tenham qualquer reflexo sobre as atividades das organizações, como admitem Lopes e Sá-Soares (2014). Björck (2004) concorda que muitas organizações formalizam políticas e procedimentos ambiciosos, mas que esses documentos, no entanto, não são consultados. Essa desconexão entre as medidas implementadas e a Política de Segurança da Informação formulada contribui de forma relevante para a ocorrência continuada de incidentes, argumentam Lapke e Dhillon (2015). Portanto, além de formalizada, a política deve ser implantada de forma significativa, resultando na adoção de medidas de Segurança da Informação que atendam aos requisitos e necessidades organizacionais e que tenham reflexo nas suas atividades, sob pena de expor as informações organizacionais a riscos.

As organizações são pressionadas pelo ambiente externo a adotarem medidas de Segurança da Informação (BJÖRCK, 2004; BACKHOUSE; HSU; SILVA, 2006; HU; HART; COOKE, 2007; HSU; LEE; STRAUB, 2012; SPEARS; BARKI; BARTON, 2013; WILLIAMS; HARDY; HOLGATE, 2013; ANTHONY; APPARI; JOHNSON, 2014; LOPES; SÁ-SOARES, 2014; CAVUSOGLU *et al*., 2015; SHAFIU, 2015). Diante das pressões do ambiente, Björck (2004) argumenta que, sob a ótica da Teoria Institucional, a formalização de uma Política de Segurança da Informação pode ser resultado de uma resposta organizacional em busca da conformidade com os requisitos do ambiente institucional.

Como destaca Björck (2004), os mecanismos de pressão institucional podem ajudar a explicar as estruturas formais das organizações e, consequentemente, as estruturas de Segurança da Informação, mas Oliver (1991) e Delmas e Toffel (2008) ponderam que a abordagem institucional dá pouca ênfase à capacidade organizacional de responder a essas pressões atendendo aos seus próprios interesses.

Nesse sentido, além da adoção cerimonial, que resulta em uma dissociação intencional entre política e prática – portanto, uma resposta racional visando aos interesses organizacionais (MEYER; ROWAN, 1977; PRESSMAN; WILDAVSKY, 1984; BOXENBAUM; JONSSON, 2009) –, alguns autores argumentam que as organizações podem responder às pressões externas de maneiras distintas (OLIVER, 1991; WOOD JR.; CALDAS, 1997; MCKAY, 2001; CASILE; DAVIS-BLAKE, 2002; SÁ, 2004; DELMAS; TOFFEL, 2008; PACHE; SANTOS, 2010). Dentre esses, Oliver (1991) propõe um conjunto de respostas estratégicas que podem variar em um contínuo que vai da aquiescência passiva até uma resposta mais ativa. A autora argumenta que as pressões institucionais podem ser contrárias aos objetivos organizacionais ou prejudiciais à realização das atividades desenvolvidas pela organização, ou podem ser contraditórias entre si. Assim, pressões institucionais podem ser assimiladas passivamente, ou as organizações podem responder negociando, ignorando, desafiando ou mesmo manipulando as fontes de pressão ou as pressões institucionais buscando uma situação mais vantajosa.

A partir dessa ótica, quando uma organização formaliza políticas e regulamentos internos buscando a conformidade com requisitos institucionais, passa a exercer pressão sobre suas subunidades organizacionais, que podem também responder de forma a atender aos seus próprios interesses, em detrimento dos interesses da sua administração central (TEMPEL *et al*., 2006; DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015). Essa situação configura uma dissociação entre a política formalizada pela organização e as

práticas adotadas por suas subunidades organizacionais, o que contradiz a ideia da dissociação como uma resposta intencional da organização. Em outras palavras, a dissociação pode ser decorrente do comportamento das subunidades organizacionais.

Organizações com estrutura complexa e descentralizada buscam integração e interconexão entre suas várias subunidades organizacionais e unidades de negócio, argumenta Larson (2012). De acordo com Von Simson (1990), subunidades organizacionais compartilham informações e bancos de dados, e seus sistemas são interligados em redes de computadores. Nesse contexto, com base na ideia de dissociação como resultado do comportamento das subunidades organizacionais, uma Política de Segurança da Informação pode ser formalizada pela administração central sem ser implementada nas subunidades. Para Lapke e Dhillon (2015), essa dissociação entre a Política e as práticas adotadas pode pôr a organização em risco, o que reforça o argumento de que a ocorrência de incidentes de Segurança da Informação em uma organização cujo ambiente de TI é interconectado dessa forma pode prejudicar informações de toda a organização. Esse entendimento é o mesmo de Bowersox *et al*. (2014), que argumentam que a ocorrência de incidentes pode ter impacto sobre diferentes organizações interligadas, e é coerente com a ideia de Delmas e Toffel (2008) e Hernes e Erdvik (2014) de que as respostas das subunidades de uma organização podem ter influência sobre sua administração central quanto à conformidade com os requisitos institucionais.

Sabe-se que a adoção das diferentes categorias de medidas de Segurança da Informação está mais relacionada a umas pressões institucionais do que a outras: a adoção de tecnologias e ações de educação e conscientização está associada principalmente a pressões normativas, enquanto a formalização de políticas e regulamentos está mais relacionada a pressões coercitivas (ALBUQUERQUE JUNIOR *et al*., 2016). A adoção de tecnologias é responsabilidade de subunidades organizacionais que realizam atividades técnicas, enquanto decisões sobre medidas formais e informais devem ser tomadas por comitês, escritórios e gestores de Segurança da Informação (MARTIN; KHAZANCHI, 2006; SÊMOLA, 2014). Considerando que subunidades distintas de uma mesma organização sofrem diferentes influências externas e respondem a elas de maneiras distintas (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015), espera-se que essas subunidades organizacionais respondam de maneiras diferentes às pressões para adoção das diferentes medidas de Segurança da Informação.

A abordagem institucional permite explicar como as subunidades de uma organização são pressionadas pela sua administração central e pelo ambiente institucional a adotarem medidas de Segurança da Informação. Já a tipologia de respostas estratégicas permite compreender como as subunidades respondem às pressões do ambiente e de sua administração central, considerando que podem responder de acordo com seus próprios interesses e que podem, por consequência, influenciar a conformidade da organização como um todo (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015).

A compreensão das respostas estratégicas das subunidades pode explicar a dissociação entre as medidas por elas adotadas e a Política de Segurança da Informação como um resultado do seu comportamento, e não como uma escolha da organização.

1.1 QUESTÃO DE PESQUISA

Uma organização com estrutura descentralizada precisa proteger as informações com as quais lida, e devido à interconexão e ao compartilhamento de redes de computadores, sistemas e informações, essa proteção deve alcançar todas as suas subunidades organizacionais. O ambiente institucional pressiona a organização e suas subunidades para que adotem medidas de Segurança da Informação, e para estar em conformidade com essas pressões, a administração central da organização elabora políticas e regulamentos internos com o objetivo de orientar as ações de todos os seus departamentos e unidades de negócio descentralizadas. No entanto, essas subunidades podem responder às pressões do ambiente conforme seus próprios interesses, e não necessariamente para atender aos interesses da organização, o que pode expor a organização como um todo a riscos de Segurança da Informação.

Considerando que cada subunidade de uma organização pode responder às pressões do ambiente visando seus próprios interesses e que essas respostas podem influenciar a conformidade da organização quanto aos requisitos externos de Segurança da Informação, a seguinte questão de pesquisa foi formulada:

Como as respostas estratégicas das subunidades às pressões que sofrem influenciam a conformidade de uma organização com os requisitos externos de Segurança da Informação?

1.2 JUSTIFICATIVAS

Este estudo investiga a adoção de medidas de Segurança da Informação nas subunidades de uma organização e os efeitos das respostas estratégicas dessas subunidades sobre a sua administração central. Diferentes trabalhos da área de Sistemas de Informação tratam de TI em subunidades organizacionais e unidades de negócio descentralizadas (MARKUS, 1983; BROADBENT; BUTLER, 1997; GORDON; GORDON, 2002; KARIMI; KONSYNSKI, 2003; WILLSON; POLLARD, 2009; CARTON; ADAM, 2010; LARSON, 2012), mas os trabalhos identificados na literatura que abordam a Segurança da Informação nesse contexto são poucos e limitados a prescrever modelos para implantação de tecnologias, processos e estruturas (HOPPÉ, 1994; ANYANWU, 1997; KIELY; BENZEL, 2006), propor métodos ou realizar a avaliação da efetividade ou eficácia (BOOKER, 2006; QURESHI, 2011), ou descrever como está organizada a Segurança da Informação (CUMMINGS; GUYNES, 1994).

Além disso, o foco pode ser nas matrizes das organizações, sem alcançar suas subunidades organizacionais (ANYANWU, 1997; QURESHI, 2011), ou abordar a Segurança da Informação como uma das muitas funções desenvolvidas pelo serviço de TI de uma organização (CUMMINGS; GUYNES, 1994). Não foram identificados trabalhos investigando como subunidades organizacionais respondem às pressões para adoção de medidas de Segurança da Informação nem como as respostas dessas subunidades influenciam a Segurança da Informação e a conformidade da organização como um todo. Esta pesquisa avança no conhecimento sobre o tema por abordar a relação entre as subunidades organizacionais e sua administração central, colocando o comportamento da organização como resultado do comportamento de cada uma das suas subunidades quanto à adoção de medidas de Segurança da Informação. Em suma, o trabalho mostra como a dissociação entre a Política de Segurança da Informação organizacional e as medidas adotadas nas subunidades pode ser decorrente das diferentes respostas das subunidades às pressões do ambiente institucional e da sua administração central, e isso justifica a sua realização.

A administração central de uma organização representa uma fonte significativa de pressão coercitiva sobre suas subunidades (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003), mas o relacionamento entre matrizes e subsidiárias não é

necessariamente de uma dependência unidirecional (TEMPEL *et al*., 2006) e as subunidades podem se comportar de forma autônoma, visando seus próprios interesses e a despeito dos interesses da sua matriz (TEMPEL *et al*., 2006; DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015). Ao responder às pressões institucionais elaborando uma Política de Segurança da Informação e outros regulamentos internos, a organização pressiona suas subunidades a adotarem diferentes medidas, e a não adoção caracteriza uma dissociação entre política e prática (POWER, 2000; DELMAS; TOFFEL, 2008; BROMLEY; POWELL, 2012; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015). Essa dissociação faz com que a conformidade com os requisitos do ambiente institucional seja prejudicada (HERNES; ERDVIK, 2014). Isso justifica a realização desta pesquisa, que investiga não só como subunidades organizacionais respondem às pressões que sofrem para que adotem medidas de Segurança da Informação, mas também como essas respostas afetam a conformidade da organização com os requisitos institucionais, causando a dissociação entre política e prática. Além disso, a pesquisa avança ainda na compreensão sobre a dissociação entre política e prática ao tratar desse tópico em um estudo sobre Segurança da Informação, assunto pouco abordado na literatura sobre dissociação.

Para estar em conformidade com os requisitos de Segurança da Informação provenientes do ambiente externo, uma organização precisa adotar medidas que devem atender às necessidades e orientar as ações de todas assuas subunidades organizacionais, incluindo unidades de negócio descentralizadas e departamentos funcionais, segundo Wood (2004), Qureshi (2011), Sêmola (2014) e a ABNT (2013). De acordo com Von Simson (1990) e Larson (2012), as organizações demandam interconexão entre suas várias subunidades organizacionais. Por compartilharem sistemas de informação integrados e por serem interligadas por redes de computadores, essas organizações são interconectadas e integradas, e o fato de uma parte da organização não estar em conformidade com os requisitos e necessidades organizacionais de Segurança da Informação (expressos em uma Política de Segurança da Informação e em outros regulamentos formalizados pela administração central) pode pôr em risco as informações da organização como um todo, como sustentam Bowersox *et al*. (2014). Esses argumentos corroboram com os de Delmas e Toffel (2008), de que o comportamento das subunidades de uma organização pode influenciar toda a organização, e com Lapke e Dhillon (2015), segundo os quais o fato de uma Política de Segurança da Informação ter sido formalizada e não ter sido implementada contribui para a ocorrência de

incidentes na organização. A compreensão do comportamento das subunidades nesse contexto justifica a realização desta pesquisa.

Departamentos técnicos são responsáveis pela realização de atividades técnicas de Segurança da Informação, devendo adotar medidas técnicas para atender aos requisitos organizacionais e externos de Segurança da Informação. Já comitês, escritórios e gestores de Segurança da Informação são responsáveis por decisões relacionadas a regulamentos e ações de conscientização e educação (MARTIN; KHAZANCHI, 2006; SÊMOLA, 2014). Considerando que a adoção dessas diferentes medidas de Segurança da Informação está relacionada mais a um tipo de pressão institucional do que aos outros (ALBUQUERQUE JUNIOR *et al*., 2016) e que as pressões incidem de maneiras distintas sobre as subunidades organizacionais, que podem responder de formas distintas (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015), esta pesquisa justifica-se por ampliar a compreensão sobre as diferenças na adoção das três categorias de medidas de Segurança da Informação. Com a pesquisa, fica reforçada também a justificativa para a utilização da tipologia de respostas estratégicas para investigar a Segurança da Informação, pois permite compreender como as subunidades organizacionais respondem às pressões institucionais para adoção dos diferentes tipos de medidas de Segurança da Informação em uma organização com estrutura descentralizada.

A Segurança da Informação é um assunto que tem sido alvo de debates nas organizações e no meio acadêmico e é vasta a quantidade de trabalhos científicos sobre o tema. Apesar de haver a necessidade de adotar medidas para mitigar riscos e ameaças de natureza técnica, ambiental e social (BELASCO; WAN, 2006; WORKMAN, 2007) e de ser necessário abordar a Segurança da Informação sob os pontos de vista organizacional, social e sociotécnico (DHILLON; BACKHOUSE, 2001; BJÖRCK, 2004; PUHAKAINEN, 2006; ALBRECHTSEN, 2008; COLES-KEMP, 2009; SILIC; BACK, 2014), boa parte da produção científica tem um enfoque tecnológico, com propostas de soluções tecnológicas ou de padrões e modelos administrativos para mitigar os riscos existentes, enquanto poucos trabalhos utilizam alguma abordagem teórica própria das ciências sociais para explicar fenômenos relacionados a Segurança da Informação (BJÖRCK, 2004; COLES-KEMP, 2009).

Ao analisar a produção científica brasileira sobre Segurança da Informação em eventos científicos do campo da Administração, Ciência da Informação e Engenharia de Produção e em periódicos científicos de Administração, constatou-se também que poucos trabalhos utilizam alguma abordagem teórica comum em estudos do campo da Administração

(ALBUQUERQUE JUNIOR; SANTOS, 2013, 2014a, 2014b). Ao contrário da maioria dos trabalhos identificados na literatura, este estudo não tem um enfoque tecnológico – ele foi realizado sob a ótica da Teoria Institucional, abordagem recomendada, mas pouco aplicada em pesquisas sobre o tema (BJÖRCK, 2004), embora seja comum em trabalhos do campo da Administração e da área temática de Sistemas de Informação (DEVAUJANY *et al*., 2014). No Brasil, nenhum estudo sobre Segurança da Informação foi identificado utilizando esta abordagem teórica (ALBUQUERQUE JUNIOR; SANTOS, 2013, 2014a, 2014b) e a pesquisa bibliográfica mostrou que poucos estudos podem ser identificados também na produção internacional. Assim, esta pesquisa avança no conhecimento sobre institucionalização da Segurança da Informação.

A pesquisa foi apoiada na tipologia de respostas estratégicas às pressões institucionais de Oliver (1991). Segundo a autora, a tipologia estende a Teoria Institucional ao reconhecer que esta abordagem pode abrigar uma variedade de respostas às pressões institucionais que vão além da aquiescência passiva. A utilização desta tipologia para analisar a adoção de medidas de Segurança da Informação permite verificar se a adoção é resultado da aquiescência organizacional às pressões institucionais, ou de uma tentativa de equilibrar, pacificar ou negociar demandas institucionais conflitantes em busca da conformidade.

A tipologia de respostas estratégicas também permite verificar se a organização busca evitar a conformidade com os requisitos externos de Segurança da Informação, mas mantendo uma conformidade aparente, ou distanciando suas atividades internas da inspeção externa, ou mudando suas atividades internas para evitar a necessidade de adotar medidas de Segurança da Informação.

Por fim, a tipologia de Oliver (1991) possibilita investigar se a organização desafia as pressões institucionais, recusando as medidas de Segurança da Informação exigidas pelo ambiente, ou se procura manipular as fontes de pressão institucional visando à utilização dos processos e relações institucionais de forma oportunista para neutralizar os constituintes do ambiente institucional ou mudar e redefinir os requisitos institucionais e os critérios de avaliação da conformidade.

O potencial da tipologia de Oliver (1991) pode ser percebido em uma variedade de trabalhos do campo da Administração (WAHYUDI, 2004; GRAEFF, 2005; BOSCHMAN, 2006; FREZATTI; AGUIAR; REZENDE, 2007; HANDGRAAF, 2012; LOPEZ, 2012; LUNDBERG, 2013; GUTIÉRREZ-RINCÓN, 2014; BORGES; DUTRA; SCHERER, 2014) e

também da área temática de Sistemas de Informação (OSMUNDSEN, 2005; MIGNERAT; RIVARD, 2009; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009; STANDING; SIMS; LOVE, 2009; AIER; WEISS, 2012).

As possibilidades apresentadas mostram como a tipologia de Oliver (1991) pode ajudar a investigar as respostas às pressões para adoção de medidas de Segurança da Informação, apresentando comportamentos que vão além da aquiescência passiva preconizada pela Teoria Institucional. Apesar disso, não foram identificados artigos, dissertações ou teses aplicando a tipologia em pesquisas sobre adoção de medidas de Segurança da Informação. Os trabalhos de Greenaway e Chan (2005) e Parks e Wigand (2014) se aproximam deste estudo, mas as autoras do primeiro analisam a aplicação de diferentes abordagens para investigar estratégias de privacidade de informações, entre elas a tipologia de Oliver (1991). Já o artigo de Parks e Wigand (2014), com base nas tipologias de Oliver (1991) e Miles e Snow (1978), investiga como organizações respondem aos riscos à privacidade de dados de pacientes.

Em suma, os trabalhos de Parks e Wigand (2014) e de Greenaway e Chan (2005) tratam de privacidade, sem abordar a Segurança da Informação como garantia da confidencialidade, integridade de disponibilidade. Assim, esta pesquisa amplia o conhecimento sobre respostas estratégicas às pressões institucionais por aplicar a tipologia de Oliver (1991) a um tema no qual ainda não havia sido utilizada.

Por fim, esta pesquisa contribui também para a gestão de Segurança da Informação, pois ajuda a identificar meios para promovê-la nas organizações através da compreensão do comportamento das suas subunidades, permitindo ampliar a conformidade entre as políticas e regulamentos internos e as medidas adotadas e, consequentemente, a conformidade da organização com seus requisitos externos de Segurança da Informação.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral desta pesquisa é explicar como as respostas estratégicas das subunidades organizacionais às pressões externas influenciam a conformidade de uma organização com os requisitos externos de Segurança da Informação. Para tanto, foi realizado

um estudo de caso único em uma organização com subunidades que gozam de autonomia administrativa e financeira e que estão geograficamente distribuídas.

1.3.2 Objetivos Específicos

Gil (2009) assevera que os objetivos devem cobrir os diferentes aspectos do problema da pesquisa para que sejam úteis e que estes devem ser expressos com verbos de ação. Seguindo essas orientações, foram estabelecidos os seguintes objetivos específicos, que permitiram que o objetivo geral deste trabalho fosse alcançado:

a) Identificar as medidas formais e informais adotadas pela organização devido às pressões institucionais;

b) Identificar as pressões institucionais sofridas pelas subunidades organizacionais para adoção de medidas de Segurança da Informação;

c) Identificar as medidas de Segurança da Informação adotadas pelas subunidades organizacionais;

d) Identificar as respostas das subunidades organizacionais às pressões para adoção de medidas de Segurança da Informação;

e) Analisar os efeitos das respostas das subunidades organizacionais sobre as medidas de Segurança da Informação adotadas pela organização.

1.4 ESTRUTURA DA TESE

Esta tese foi organizada em sete capítulos, cada um com suas respectivas seções e subseções, além das referências utilizadas no trabalho. Esta introdução apresenta a questão da pesquisa, as justificativas e os objetivos da tese. O capítulo seguinte traz a fundamentação teórica do trabalho, abordando Segurança da Informação, a Teoria Institucional e as respostas estratégicas às pressões institucionais, que compõem o referencial teórico da pesquisa. O terceiro capítulo apresenta as proposições e o *framework* utilizado para operacionalizar a

pesquisa, incluindo os indicadores verificados na análise dos dados. O quarto capítulo trata da metodologia, apresentando o desenho da pesquisa e os procedimentos utilizados na pesquisa bibliográfica, bem como a escolha do caso estudado, procedimentos de coleta e análise dos dados e procedimentos de garantia da qualidade da pesquisa. O quinto capítulo desta tese apresenta o caso – a organização estudada. O sexto capítulo trata da apresentação e análise dos dados coletados nos documentos e entrevistas, além de discutir a sustentação empírica das proposições da pesquisa. O capítulo sete traz as considerações finais, limitações e proposições de pesquisas futuras.

2 FUNDAMENTAÇÃO TEÓRICA

As organizações têm evoluído com o passar do tempo e em todas as fases dessa evolução a informação tem sido um elemento importante para o desempenho de suas atividades (DONNER; OLIVEIRA, 2008). Nesse contexto, a informação tem sido reconhecida como essencial para as organizações (AMORIM; TOMAÉL, 2011; ABNT, 2013) e considerada um ativo intangível importante em todas as áreas da atividade econômica (ALEXANDRIA, 2009), importância esta que tem crescido devido ao reconhecimento do seu valor (NOBRE; RAMOS; NASCIMENTO, 2011), que passou a compor o valor econômico das organizações (KAYO *et al*., 2006). A importância da informação para as organizações levou tanto a mudanças na gestão organizacional como ao surgimento de um novo modelo de economia, que tem justamente a informação como base (CASTELLS, 2005; MELLO *et al*., 2010).

Segundo Buckland (1991), a palavra informação tem sido utilizada de diferentes maneiras e o seu conceito é ambíguo. Alvarenga Neto (2005) argumenta que, apesar do grande esforço em torno do conceito de informação, ainda não se chegou a um consenso. Para Machlup e Mansfield (1983), a informação é o meio necessário para a extração e construção do conhecimento, enquanto Dretske (1983) argumenta que ela é capaz de gerar conhecimento. Davenport (1998) admite que a distinção entre dado, informação e conhecimento é imprecisa, mas propõe que dados são “simples observações sobre o estado do mundo” (DAVENPORT, 1998, p. 18) e que informação é um dado dotado de relevância e propósito, citando Drucker (1988). Já no entendimento de Allen (1996), informação é um processo de codificação e transmissão das estruturas cognitivas de um informante para um observador.

Mesmo com essa ambiguidade, a importância da informação tem aumentado, principalmente com as facilidades trazidas pelos avanços tecnológicos, sendo reconhecida como um ativo crítico para a continuidade operacional e saúde da organização, como argumenta Sêmola (2014).

Para Fachini, Fernandes e Faria (2011), a informação é relevante para a tomada de decisões, enquanto Sêmola (2014) esclarece que há informações fundamentais que se revelam como importante diferencial competitivo para uma organização. Já para a ABNT (2013), a informação é um ativo organizacional essencial que precisa ser adequadamente protegido. Com isso concorda Fontes (2006), segundo o qual a informação é um bem que tem valor para

a empresa, e por isso deve ser protegida por políticas e regras, como acontece com recursos financeiros e materiais.

Marciano (2006) ressalta que a informação tem sido cada vez mais compreendida como um recurso transformador que tem um papel essencial no atual contexto socio-econômico. Tratando do ciclo de vida da informação proposto por Borko (1968), Marciano (2006) argumenta que, em todas as etapas, a informação está sujeita a incidentes que podem comprometê-la, o que leva a uma preocupação com Segurança da Informação em todo o seu ciclo de vida. O autor ressalta a presença da tecnologia em todo o ciclo de vida da informação, o que pode ser observado inclusive em trabalhos mais antigos, como os de Borko (1968) e de Saltzer e Schroeder (1974), antes de a TI estar tão presente nos processos organizacionais.

De acordo com Wilson (2011), novas tecnologias são pervasivas e têm mudado a forma como o trabalho é realizado nas organizações. Apesar de observar que é crescente a aceitação dessas tecnologias e a compreensão de que elas precisam ser adotadas, este autor pondera que é necessário que seus requisitos de segurança sejam atendidos. Para Alexandria (2009), o desenvolvimento tecnológico, a importância da informação e as possibilidades que novas tecnologias trouxeram para seu armazenamento e transmissão expuseram as organizações a novos tipos de ameaças. Eloff e Von Solms (2000), Albertin (2001) e Karabacak e Sogukpinar (2005) argumentam que a TI traz benefícios, mas cria também uma relação de dependência nas organizações. Silva Netto e Silveira (2007) entendem que esta dependência está associada ao fato de os computadores armazenarem grande parte dos dados importantes de uma organização.

Karabacak e Sogukpinar (2005) destacam que a proteção das informações organizacionais se tornou mais crítica do que jamais havia sido. Para Williams (2001), os sistemas de informação podem trazer muitos benefícios diretos e indiretos para as organizações, mas podem trazer também muitos riscos, e segundo Fachini (2009), a facilidade de acesso às redes de computadores e a portabilidade dos equipamentos aumentam o risco de divulgação não autorizada de informações, o que, para Marciano (2006), pode comprometer a segurança de informações, transações e pessoas.

Diante do avanço tecnológico e dos riscos associados à informação, Eloff e Von Solms (2000) salientam que a Segurança da Informação é necessária para que as organizações se mantenham competitivas, enquanto Hedström *et al*. (2011) asseguram que a proteção da informação é uma questão estratégica. A necessidade de proteger a informação faz com que

os processos voltados para a continuidade das operações organizacionais e Segurança da Informação ganhem mais prioridade, argumentam Herath, Herath e Bremser (2010).

2.1 SEGURANÇA DA INFORMAÇÃO

Apesar da sua reconhecida necessidade e importância, os conceitos vigentes de Segurança da Informação são questionados em diferentes trabalhos (HITCHINGS, 1995; ALJAREH; ROSSITER, 2002; ANDERSON, 2003; STERGIOU; LEESON; GREEN, 2004), como observado por Marciano (2006). Apesar disso, diversos autores concordam que a Segurança da Informação é a garantia ou preservação da confidencialidade, integridade e disponibilidade da informação (BISHOP, 2003; BEAL, 2005; COOPER, 2009), concordando com a ABNT (2013).

Por exemplo, Cooper (2009) argumenta que Segurança da Informação é o processo de proteger recursos de informação do uso, divulgação, destruição, modificação ou desmembramento não autorizados, enquanto Peltier (2005) salienta que a Segurança da Informação visa garantir a utilização adequada de dados e ativos de informação, impedindo o acesso, modificação, destruição, divulgação ou perda não autorizada ou acidental de arquivos ou registros automáticos ou manuais. Com base em conceitos apresentados em diferentes trabalhos, Silva e Stein (2007, p.47-48) propõem que Segurança da Informação é a "proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a confidencialidade e a integridade dessa informação são preservadas".

Silva e Stein (2007) deixam claro quais são as três propriedades ou, como preferem Dhillon e Backhouse (2000), os três princípios sobre os quais a Segurança da Informação se sustenta: a confidencialidade, a integridade e a disponibilidade da informação. Os objetivos desses três princípios podem ser identificados na literatura:

a) Integridade: a informação deve manter todas as suas características originais estabelecidas pelo seu proprietário quando for manipulada, garantindo que não haja alteração não autorizada (LOPES, 2012). Visa garantir, portanto, a exatidão da informação contra mudanças não autorizadas (SILVA NETTO; SILVEIRA,

2007). Envolve a proteção contra mudanças não autorizadas, sejam elas acidentais ou intencionais (COOPER, 2009).

b) Disponibilidade: visa garantir que a informação possa ser acessada sempre que seus usuários precisarem (SILVA NETTO; SILVEIRA, 2007; COOPER, 2009). É o princípio que garante que a informação está sempre disponível para o uso legítimo, sempre que ela for necessária (LOPES, 2012).

c) Confidencialidade: visa garantir que o acesso à informação seja feito apenas por quem estiver legitimamente autorizado (SILVA NETTO; SILVEIRA, 2007; LOPES, 2012), ou, em outras palavras, envolve a proteção de recursos de informação do acesso não autorizado e/ou divulgação (COOPER, 2009).

Embora a literatura possa trazer outras características, propriedades, aspectos ou princípios da Segurança da Informação, como responsabilidade, confiança e ética (DHILLON; BACKHOUSE, 2000), legalidade, auditabilidade e não repúdio (FONTES, 2006), ou autenticidade (SÊMOLA, 2014), há um consenso quanto às três propriedades apresentadas acima, considerados tradicionais (DHILLON; BACKHOUSE, 2000).

Devido à portabilidade de equipamentos tecnológicos e às facilidades para estabelecer entre eles interconexões (MARCIANO, 2006; ABNT, 2013), essas três propriedades das informações podem estar vulneráveis e expostas a riscos e ameaças. Neste ponto, cabe distinguir vulnerabilidades, ameaças, ataques, incidentes e riscos, termos comumente encontrados em trabalhos sobre Segurança da Informação.

As vulnerabilidades são características que fazem com que um sistema seja suscetível a um ataque (MOREIRA, 2001), ou fragilidades que existem em ativos que manipulam ou processam informações ou que estão a eles associadas e que podem ser exploradas (SÊMOLA, 2014).

Ameaça é definida pela *International Organization for Standardization* (ISO, 2004) em sua norma ISO/IEC 13335-1:2004 como uma causa potencial de um incidente indesejado, que pode danificar um sistema ou prejudicar uma organização – a mesma definição encontrada na NBR ISO/IEC 27002 (ABNT, 2013). De acordo com Sêmola (2014), ameaças são condições ou agentes que provocam incidentes que comprometem tanto informações quanto ativos através da exploração de vulnerabilidades.

A literatura sobre Segurança da Informação apresenta diferentes ameaças, que foram classificadas por Whitman (2003) em categorias que incluem erros ou falhas humanas, atos deliberados de sabotagem, espionagem, vandalismo e extorsão, obsolescência tecnológica, erros e falhas de *software* e *hardware*, além de forças da natureza. Belasco e Wan (2006), por sua vez, classificaram as ameaças como: técnicas, que dependem da tecnologia; humanas, que envolvem o comportamento humano, mas não dependem de tecnologia; e naturais, provocadas por elementos da natureza (Quadro 1). Estas e outras classificações que podem ser identificadas na literatura mostram que as ameaças podem ser intencionais ou não, e que podem depender ou não do uso da tecnologia.

Quadro 1 – Classificação de ameaças.

TIPOS	EXEMPLOS
Técnicas	Códigos maliciosos, ataques e acessos não autorizados por *hackers* e terroristas, negação de serviços, abusos praticados por usuários internos ou externos, boatos e sondagem de informações utilizando recursos tecnológicos
Humanas	Visualização inadvertida de informações sensíveis, sabotagem de dispositivos físicos, terrorismo e roubo de informações ou documentos
Naturais	Gelo, fogo, terremoto, tornado e tempestade

Fonte: Belasco e Wan (2006).

Um ataque, segundo Marciano (2006, p.51), é a "concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante uma ação deliberada". Já um incidente, de acordo com a norma ISO/IEC TR 18044:2004 (ISO, 2004b), é um ou mais eventos indesejados ou inesperados que tenham uma grande probabilidade de comprometer a Segurança da Informação e as operações da organização. Dessa forma, infere-se que um incidente é uma ameaça que se concretizou, tendo comprometido ou não as operações do negócio e a Segurança da Informação, enquanto o ataque é um incidente deliberado, resultado de uma ação com intenção de provocar algum dano.

Já o risco, por estar incorporado a muitas disciplinas, tem diferentes definições, como mencionado por Damodaran (2008). Este autor aponta que, no contexto da engenharia, risco é o produto da probabilidade de um evento indesejável ocorrer e uma avaliação do dano esperado. Para Ozkan e Karabacak (2010), no contexto da TI (e consequentemente da Segurança da Informação), risco é a probabilidade de uma ameaça sobre um ativo se concretizar através de uma vulnerabilidade específica.

As possíveis consequências dos incidentes de Segurança da Informação para as organizações são diversas. Segundo Nakamura (2000), a ocorrência de incidentes pode

provocar a perda de negócios, mercado e capital. De acordo com Burd (2006), incidentes podem comprometer dados privados e propriedade intelectual, além de causar perdas financeiras e prejudicar a credibilidade e viabilidade da organização. Prejuízos financeiros e para a imagem da organização são consequências do comprometimento da exatidão, confidencialidade e atualidade da informação, para Posthumus e Von Solms (2004). Já Perkel (2010) acrescenta que, além do vazamento de senhas e informações pessoais e da perda de propriedade intelectual, patentes e recursos financeiros, incidentes de Segurança da Informação podem provocar ações judiciais e constrangimento público.

Parte dos incidentes de Segurança da Informação não está associada diretamente à tecnologia, mas às relações sociais e ao comportamento humano (MITNICK; SIMON, 2003; BELASCO; WAN, 2006; LUO *et al*., 2011). Se o comportamento humano, a portabilidade e as facilidades de interconexão de equipamentos expõem a informação a riscos, os meios para proteger sua integridade, disponibilidade e confidencialidade são orientações, normas, procedimentos, políticas e ações (FONTES, 2006). Considerando que a informação é um ativo tão importante, e diante dos riscos trazidos pela tecnologia e por ameaças ambientais, humanas e sociais, a literatura profissional e acadêmica tem apresentado uma variedade de medidas para garantir a Segurança da Informação.

2.2 MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

Para promover a Segurança da Informação, a norma NBR ISO/IEC 27002 (ABNT, 2013) e diversos autores que publicam sobre o tema (BJÖRCK, 2005; BELASCO; WAN, 2006; YEH; CHANG, 2007; GORAYEB, 2012; SÊMOLA, 2014; TAMJIDYAMCHOLO *et al*., 2014) recomendam não só recursos de *hardware* e *software*, mas também medidas relacionadas a aspectos organizacionais e humanos, como políticas, normas, práticas, processos, programas, planos, estratégias, procedimentos, ações de conscientização, treinamento e educação, definição de papéis e responsabilidades e estruturas organizacionais, além da conformidade, que, nesse contexto, foca no quanto os padrões organizacionais e as exigências legais são seguidos, de acordo com Maynard e Ruighaver (2006).

É comum encontrar na literatura trabalhos e documentos que chamam essas ações, mecanismos, orientações, políticas, processos, programas, procedimentos e estruturas

organizacionais de **controles** de Segurança da Informação, como faz a ABNT (2013). Entretanto, diversos autores preferem o termo **medidas** de Segurança da Informação (WINKLER; DEALY, 1995; SCHULTZ *et al*., 2001; WAWRZYNIAK, 2006; CHANG; HO, 2006; KRITZINGER; SMITH, 2008; HAGEN; ALBRECHTSEN; HOVDEN, 2008; WORKMAN; BOMMER; STRAUB, 2008; APPARI; JOHNSON, 2010; SUN; AHLUWALIA; KOONG, 2011; ADEBAYO; OMOTOSHO; ADEKUNLE, 2012; FRANGOPOULOS; ELOFF; VENTER, 2013; SÊMOLA, 2014), o que parece adequado diante do fato de a palavra medidas ser utilizada também ao tratar de segurança penal (LEBRE, 2013), segurança pública (KRAHMANN, 2011), segurança alimentar (BAPTISTA; PINHEIRO; ALVES, 2003; CORDEIRO, 2013), segurança nacional (WRIGHT, 1998) e segurança biológica (CASAL *et al*., 2007; PINHEIRO; ZEITOUNE, 2008).

Dessa forma, medidas de Segurança da Informação são práticas, procedimentos e mecanismos "usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, reduzir essas vulnerabilidades, limitar a probabilidade ou o impacto de sua exploração, minimizando ou mesmo evitando os riscos." (SÊMOLA, 2014, p.47).

Schaefer (2009) entende que a Segurança da Informação está associada a medidas que são basicamente ideias introduzidas por meio da cultura, costumes, educação e treinamento, e através da legislação. Para Carneiro (2002), a Segurança da Informação nas organizações exige a utilização de mecanismos diversos, que podem ser técnicos ou não. Segundo Höne e Eloff (2002), as medidas de Segurança da Informação envolvem soluções técnicas, normas, contratos e um trabalho de comunicação organizacional sobre riscos, ameaças e vulnerabilidades, orientados por uma Política de Segurança da Informação.

A Política de Segurança da Informação organizacional é um conjunto de regulamentos, regras e práticas que determinam como uma organização gerencia, protege e distribui recursos para alcançar objetivos específicos de Segurança da Informação (STERNE, 1991). Seu conteúdo inclui uma definição de Segurança da Informação (FORCHT; AYERS, 2001; HÖNE; ELOFF, 2002), atribuições de responsabilidades gerais e específicas (PATRICK, 2001; HÖNE; ELOFF, 2002; DOHERTY; FULFORD, 2006), requisitos de educação, conscientização e treinamento (FORCHT; AYERS, 2001), princípios de Segurança da Informação da organização (HÖNE; ELOFF, 2002), gestão da continuidade das operações e recuperação de desastres (FORCHT; AYERS, 2001; DOHERTY; FULFORD, 2006), consequências do seu descumprimento (HÖNE; ELOFF, 2002; DOHERTY; FULFORD,

2006), referências cruzadas com outras políticas, padrões, procedimentos, processos, leis e regulamentos, e uma declaração do compromisso de gestores e de alinhamento às estratégias e objetivos organizacionais (HÖNE; ELOFF, 2002), além de outras medidas de Segurança da Informação a serem adotadas pela organização (FORCHT; AYERS, 2001).

Lopes (2012) observou na literatura que as Políticas de Segurança da Informação são úteis para as organizações por diferentes razões, entre elas: por demonstrarem as iniciativas de Segurança da Informação da organização (SÁ-SOARES, 2005); por explicarem a importância da Segurança da Informação para a organização (HÖNE; ELOFF, 2002); por indicarem quais ativos devem ser protegidos e qual a proteção que precisam (KING; DALTON; OSMANOGLU, 2001); por servirem como guia na seleção, desenvolvimento e implementação de medidas apropriadas (BARMAN, 2001); e por contribuírem para a promoção de comportamentos coerentes dentro da organização (LEE, 2001).

Apesar de a Política de Segurança da Informação ser importante e abordar diferentes aspectos, Karyda, Kiountouzis e Kokolakis (2005) advertem que ela pode representar um obstáculo ao negócio caso seja rígida ou restritiva demais e que pode haver resistência dos membros da organização às mudanças e restrições que ela impõe. Sun, Ahluwalia e Koong (2011) concordam que quanto mais exigentes as medidas adotadas, mais pode haver resistência a elas. Também para Ellwanger (2009) uma Política de Segurança da Informação pode gerar resistência, mas isso pode ser evitado com ações de *endomarketing* e o envolvimento de pessoas não técnicas na sua elaboração. A implantação de uma Política de Segurança da Informação pode levar a conflitos entre os departamentos de uma organização em decorrência das diferentes perspectivas de riscos e objetivos organizacionais e de Segurança da Informação, de acordo com Abraham e Chengalur-Smith (2011). Björck (2005) concorda e observa que um aspecto central para a Segurança da Informação é estabelecer um canal de comunicação com os membros da organização com a finalidade de informar sobre as razões da adoção de medidas. Para este autor, medidas técnicas não acompanhadas de treinamento e educação tendem a não ser compreendidas e, como consequência, a não ser respeitadas.

De acordo com Lorens (2007), por desconsiderar as pessoas ao tratar da Segurança da Informação, a maioria das organizações enfrenta dificuldades na elaboração e formalização dos seus regulamentos, o que pode levar a um resultado ineficiente ou inexequível – a Política e os regulamentos podem se tornar meros formalismos sociais.

Segurança da Informação não é apenas uma questão tecnológica, e um viés técnico precisa ser evitado (ELLWANGER, 2009). Nesse sentido, abordagens puramente técnicas e simplistas para a Segurança da Informação têm grande possibilidade de fracassar (ANDERSON, 2001; POSEY *et al*., 2014), pois soluções técnicas de Segurança da Informação, embora necessárias, são insuficientes em ambientes sociotécnicos complexos e em constante mudança como são as organizações (HOLGATE; WILLIAMS; HARDY, 2012). Por isso, uma abordagem significativa deve incluir aspectos tecnológicos, humanos, administrativos e organizacionais (DHILLON; BACKHOUSE, 2001; BJÖRCK, 2004, 2005; ALBRECHTSEN, 2008; COLES-KEMP, 2009). Em outras palavras, a Política de Segurança da Informação deve orientar a adoção de medidas que incluem não só soluções técnicas, mas também normas, contratos e um trabalho de comunicação organizacional sobre riscos, ameaças e vulnerabilidades (HÖNE; ELOFF, 2002; ELLWANGER, 2009).

Exemplos de medidas de Segurança da Informação técnicas e não técnicas podem ser identificadas na literatura. Björck (2005) apresenta normas, estruturas organizacionais, processos, programas de treinamento e conscientização, planos, estratégias e a Política de Segurança da Informação, que visam mudar o comportamento das pessoas formalmente (estabelecendo metas, obrigações e responsabilidades) e informalmente (capacitando e conscientizando), além de medidas tecnológicas, que operam em sistemas computacionais, como controles de acesso lógico, antivírus, *backups*, biometria, criptografia e *firewalls*, e outras que procuram proteger a informação por meios físicos, como controles de acesso físico, sistemas de alarme e proteção contra fogo. Tamjidyamcholo *et al*. (2014) incluem ainda o estabelecimento de redes de troca de informações e conhecimentos entre profissionais, que têm o objetivo de aumentar o conhecimento dos membros da organização e que influenciam positivamente na expectativa de redução de riscos.

Essa diversidade levou diferentes autores a classificarem as medidas de Segurança da Informação (BJÖRCK, 2005; YEH; CHANG, 2007; SÊMOLA, 2014), podendo ser por sua finalidade, aproximação com a tecnologia ou pelas características que buscam afetar na organização. Dhillon (1999) as classificou com base no que afetam na organização:

a) Medidas técnicas: visam à limitação do acesso a prédios, salas, computadores e sistemas (DHILLON, 1999; DHILLON; MOORES, 2001), como mecanismos que operam em sistemas computacionais, controles de acesso lógico, antivírus,

correções de sistemas, *backup*, biometria, criptografia, *firewalls* e soluções de detecção de intrusos (BELASCO; WAN, 2006; SENTHILKUMAR; ARUMUGAM, 2011; GORAYEB, 2012), e aqueles que buscam proteger a informação por meios físicos, como soluções de controle de acesso físico, sistemas de alarme e proteção contra fogo (BJÖRCK, 2005).

b) Medidas formais: buscam afetar a organização e seus membros através de regras e da garantia da conformidade com leis e procedimentos. Envolvem a definição de funções, responsabilidades, planos, objetivos e papéis, como o Sistema de Gestão de Segurança da Informação, a Política de Segurança da Informação, o Escritório de Segurança da Informação e a equipe de tratamento de incidentes (DHILLON; MOORES, 2001; KILLCRECE *et al*., 2003; MANDIA; PROSISE; PEPE, 2003; FARN; LIN; FUNG, 2004; BJÖRCK, 2005; CASEY, 2005; MARTINS; SANTOS, 2005; PARK; JANG; PARK, 2010; MANOEL, 2014; SÊMOLA, 2014).

c) Medidas informais: visam afetar a organização e seus membros informalmente, promovendo o conhecimento e a conscientização sobre Segurança da Informação através de treinamento e educação (BJÖRCK, 2005). Envolvem a comunicação de responsabilidades, atitudes e comportamentos apropriados (DHILLON; MOORES, 2001), como programas de treinamento, educação e conscientização e ações de divulgação (DHILLON; MOORES, 2001; SÊMOLA, 2014).

A classificação de Dhillon (1999) foi utilizada neste trabalho e os tipos de medidas identificados em cada categoria estão no Quadro 2, enquanto o Apêndice B traz exemplos de medidas de cada tipo identificadas na literatura. Segundo o autor, é preciso evitar a adoção de medidas de Segurança da Informação de forma isolada, atendendo a situações específicas e sem considerar outras medidas necessárias e o contexto organizacional. Sveen, Torres e Sarriegi (2009) acrescentam que há uma interdependência entre as diferentes categorias de medidas. Segundo estes autores, medidas técnicas dependem de medidas formais, que afetam a organização através da imposição de regras, e as medidas formais dependem de medidas informais, que afetam as organizações por meio de ações de educação e conscientização. Os autores exemplificam: uma medida técnica, como a exigência de uma senha de acesso a um sistema, pode ser afetada pela violação de uma medida formal – a

divulgação da senha e, consequentemente, o descumprimento da obrigatoriedade do sigilo das senhas –, e essa violação pode ser uma decorrência de uma deficiência em uma medida informal – problemas em programas de educação e conscientização sobre a importância do sigilo da senha, ou a inexistência desses programas.

Quadro 2 – Tipos de medidas técnicas, formais e informais.

CATEGORIAS	TIPOS E EXEMPLOS
Formais	Política de Segurança da Informação; Comitê de Segurança da Informação; Regulamentos internos de Segurança da Informação; Processos e procedimentos de Segurança da Informação; Equipe 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 periódica da Política de Segurança da Informação.
Técnicas	Redundância de dados; Segregação e monitoramento de redes de computadores; Redundância de peças de equipamentos; Prevenção contra códigos maliciosos; Controle de acesso lógico; Transmissão e armazenamento seguros de dados; Autenticação forte; Redundância de equipamentos; Controle de acesso físico; Proteção ambiental.
Informais	Treinamento de profissionais de TI; Treinamento de usuários de TI; Divulgação de regulamentos e da Política de Segurança da Informação; Ações de conscientização.

Fonte: elaborado pelo autor com base em Dhillon e Moores (2001), Farn, Lin e Fung (2004), Björck (2005), Belasco e Wan (2006), Juels (2006), Doherty e Fulford (2006), Thorpe (2006), Panko (2006), Park, Jang e Park (2010), Gorayeb (2012), ABNT (2013), Casey (2005), Martins e Santos (2005), Manoel (2014) e Sêmola (2014).

Além da necessidade de considerar a relação de dependência entre diferentes medidas de Segurança da Informação, a ABNT (2013) e Sêmola (2014) concordam que as medidas não devem ser adotadas indistintamente, pois cada organização tem características próprias que exigem que a Segurança da Informação seja tratada de uma forma particular. De acordo com Dresner (2011), a simples adoção de medidas recomendadas por padrões e modelos de Segurança da Informação não garante a mitigação dos riscos.

Assim, para que sejam adotadas medidas apropriadas às necessidades e requisitos de Segurança da Informação das organizações, a literatura recomenda que seja realizada uma análise e avaliação de riscos (BACKHOUSE; DHILLON, 1996; KOTULIC; CLARK, 2004; PELTIER, 2005; FONTES, 2006; OSBORNE; SUMMITT, 2006; BERNARD, 2007;

CAVUSOGLU *et al*., 2015; GUSMÃO *et al*., 2016) e que as informações sejam classificadas quanto aos seus requisitos de Segurança da Informação (MARTINS; SANTOS, 2005).

É possível identificar em trabalhos anteriores uma diferenciação entre análise de riscos e avaliação de riscos: a primeira seria a identificação e caracterização dos riscos; e a segunda seria o processo de determinar a exposição aos riscos (BASKERVILLE, 1991; DHILLON; BACKHOUSE, 2001). Apesar dessa distinção, a literatura mais atual sobre Segurança da Informação tem tratado de análise e avaliação de riscos como um único processo, definido neste contexto como o uso sistemático de informações para identificar e estimar riscos (OZKAN; KARABACAK, 2010), ou como o processo de descoberta e avaliação de riscos para ativos de informação e de definição de linhas de ação alternativas para controlar esses riscos (CAVUSOGLU *et al*., 2015).

A análise e avaliação de riscos, no entendimento de Backhouse e Dhillon (1996), tornou-se um processo importante na gestão da Segurança da Informação pois possibilita justificar os gastos com novas tecnologias de Segurança da Informação, evitar a implementação de medidas caras e desnecessárias e prever criticamente os benefícios diante dos investimentos iniciais. Baskerville (1991) concorda que a análise e avaliação de riscos é um processo útil para mensurar a viabilidade de medidas e ressalta sua importância como ferramenta de comunicação entre os profissionais de Segurança da Informação e os gestores organizacionais.

Segundo Peltier (2005), a análise e avaliação de riscos orienta a tomada de decisões sobre as medidas que precisam ser implementadas para mitigar, eliminar ou aceitar riscos identificados. O autor observa também que o processo é útil mesmo após a ocorrência de incidentes, pois os documentos gerados permitem identificar os indivíduos envolvidos no processo de decisão, as discussões ocorridas, o que foi considerado por esses indivíduos e suas decisões, mostrando o caminho que levou às medidas adotadas. Por fim, o autor argumenta que o processo permite à organização adotar as medidas realmente necessárias.

Booker (2006) argumenta que, para que a Segurança da Informação seja eficaz, é necessário ter uma compreensão clara dos riscos associados, o que passa pela identificação das ameaças existentes e pela análise do impacto potencial da ocorrência de eventos que prejudiquem a confidencialidade, integridade ou disponibilidade das informações. O autor complementa que, caso os riscos ou o impacto da ocorrência de incidentes sejam considerados inaceitáveis, medidas de Segurança da Informação são necessárias.

As necessidades de Segurança da Informação identificadas em uma análise e avaliação de riscos variam de organização para organização, conforme orientam a ABNT (2013) e Sêmola (2014), mas Anyanwu (1997) ressalta que a garantia da disponibilidade, integridade e confidencialidade das informações não é uma meta que pode ser facilmente alcançada, principalmente em organizações que precisam lidar com ameaças a esses três pilares da Segurança da Informação ao mesmo tempo em que busca garantir autonomia às suas subunidades organizacionais, pois os gestores precisam lidar com questões de Segurança da Informação relativas à pirataria e direitos autorais, compatibilidade, garantia de acesso a sistemas remotos, redundância de dados e sistemas, bem como a transferência de grandes volumes de informações entre escritórios e unidades de negócio geograficamente distantes e sua sede.

De acordo com Larson (2012), organizações com estrutura descentralizada buscam integrar e interconectar suas várias unidades de negócio, e Von Simson (1990) complementa que essas organizações compartilham informações e bancos de dados e mantêm sistemas interligados em redes de computadores. Devido a essas características, um incidente em uma subunidade pode comprometer as outras, segundo o argumento apresentado por Bowersox *et al*. (2014) para organizações que experimentam essa integração.

Organizações com essas características também estão em constante mudança, demandam flexibilidade e lidam com informações muitas vezes conflitantes sobre os riscos de Segurança da Informação, de acordo com Booker (2006). Ainda segundo o autor, essas características não estão de acordo com a coerência e previsibilidade exigidas por um programa de Segurança da Informação. Acrescenta-se a isso o fato de que a Segurança da Informação precisa ser garantida em toda a organização, incluindo seus departamentos e subsidiárias, de acordo com Qureshi (2011) e Sêmola (2014) e conforme recomenda a ABNT (2013). Booker (2006) conclui que, além das dificuldades que enfrentam ao lidar com a necessidade de manter a conformidade com a Política de Segurança da Informação enquanto garantem autonomia às suas subunidades organizacionais, organizações com estrutura descentralizada muitas vezes respondem a auditorias e pedidos de informações sobre conformidade de forma reativa e não necessariamente representando a realidade.

Cabe salientar que é necessário promover a sensibilização e a conformidade de todas as subunidades da organização com sua Política e seus regulamentos (BOOKER, 2006), mas também que políticas podem ser formalizadas sem necessariamente serem respeitadas ou

consultadas (BJÖRCK, 2004; LOPES; SÁ-SOARES, 2014), uma desconexão que contribui para a ocorrência de incidentes de Segurança da Informação (LAPKE; DHILLON, 2015).

Apesar de as organizações terem necessidades de Segurança da Informação específicas e de ser imperativo realizar uma análise e avaliação de riscos para orientar suas decisões, a adoção de medidas de Segurança da Informação pode ser resultado das respostas organizacionais às pressões do ambiente externo (ANTHONY; APPARI; JOHNSON, 2014; ALKALBANI; DENG; KAM, 2014; ALBUQUERQUE JUNIOR; SANTOS, 2015; CAVUSOGLU *et al*., 2015; SHAFIU, 2015), o que pode levar à formalização e adoção de regulamentos internos, tecnologias, estruturas organizacionais, políticas e programas de Segurança da Informação que não atendem às necessidades e requisitos organizacionais (ALBUQUERQUE JUNIOR; SANTOS, 2014c).

A relação entre a adoção de medidas de Segurança da Informação e as pressões ambientais pode ser compreendida através da Teoria Institucional (BJÖRCK, 2004), abordagem que enfatiza que o comportamento organizacional é resultado de pressões do ambiente no qual a organização está inserida (MEYER; ROWAN, 1977; TOLBERT; ZUCKER, 1983, 1999; DIMAGGIO; POWELL, 1983).

2.3 TEORIA INSTITUCIONAL

Segundo Kam *et al*. (2013), pressões externas podem impulsionar o cumprimento de Políticas de Segurança da Informação nas organizações e essa noção é consistente com a Teoria Institucional. Para Björck (2004), o lado humano da Segurança da Informação deve conduzir a atenção para teorias que estudam o comportamento social, e a Teoria Institucional mostra-se adequada para compreender, explicar, controlar e prever questões de Segurança da Informação nas organizações.

Quinello (2007) aponta que, ao perceberem que as organizações não eram sistemas fechados às influências externas, pesquisadores do campo de estudo da Administração passaram a investigar diferentes abordagens teóricas após 1940. A partir dessa perspectiva, veio a compreensão de que as organizações influenciam e recebem influências do ambiente externo, que passou a ter destaque nos estudos organizacionais. Dentre as abordagens teóricas que consideram o ambiente como fator que influencia as organizações, o autor destaca a 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.

Weerakkody, Dwivedi e Irani (2009) argumentam que a Teoria Institucional é proeminente em pesquisas nos campos da sociologia, ciência política, economia e estudos organizacionais. Guarido Filho, Machado-da-Silva e Gonçalves (2009) observaram um crescimento da importância da Teoria Institucional no campo dos estudos organizacionais, com um aumento das publicações e adesão de novos pesquisadores a esta abordagem. Para Weerakkody, Dwivedi e Irani (2009), pesquisadores têm utilizado a perspectiva institucional para estudar as influências internas e externas sobre os padrões organizacionais e explicar por que algumas ideais e estruturas organizacionais perduram nas organizações.

Quinello (2007) esclarece que o desenvolvimento da Teoria Institucional se deu em dois movimentos: a Velha Escola Institucional, que tem seu foco na organização; e a Nova Escola Institucional, também conhecida como Escola Neo-Institucional, que tem um foco no campo organizacional. DiMaggio e Powell (1983) explicam que as duas escolas institucionais se baseiam na relação entre a organização e o ambiente em que ela está inserida, e Peci (2006) complementa que ambas são céticas quanto à racionalidade das decisões dos atores organizacionais.

De acordo com Quinello (2007), 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 a influência do ambiente, enquanto o neo-institucionalismo tem um foco nos conflitos entre grupos ou organizações e nas mudanças resultantes desses conflitos, com a institucionalização de estruturas no campo organizacional e a busca por legitimação da organização. Para Busanelo (2010), a vertente Neo-Institucional proliferou após a publicação do artigo seminal de Meyer e Rowan (1977).

Neste ponto, é necessário esclarecer o que é uma **instituição** no contexto dessa abordagem teórica. Peci (2006) denuncia o fato de o termo ser utilizado de forma controversa quanto à sua concepção teórica e aplicação prática. No contexto da Teoria Institucional, instituições são regras, práticas, procedimentos, políticas e programas que são incorporados pela sociedade e pelas organizações, de acordo com Meyer e Rowan (1977). Para estes autores, as organizações, inseridas no ambiente institucional, agem conforme aquilo que é considerado apropriado e eficiente dentro desse campo. Dessa forma, o ambiente no qual uma organização está inserida influencia fortemente suas estruturas organizacionais, de maneira

que práticas e processos já institucionalizados em um campo organizacional são incorporados pelas organizações que o compõem, legitimando-as nesse campo. Para Tolbert e Zucker (1983), a institucionalização é o processo através do qual os componentes de uma estrutura formal se tornam amplamente aceitos, considerados tanto adequados quanto necessários, servindo para legitimar as organizações.

Essas instituições existentes no ambiente no qual uma organização está inserida limitam ou definem como ela deve agir. Para DiMaggio e Powell (1983), o ambiente institucional força a organização a tornar-se semelhante às outras que atuam nesse mesmo campo. Estes autores explicam que campo organizacional é um conjunto de organizações que constituem uma área reconhecida de vida institucional. Eles citam como exemplos de organizações que compõem esse conjunto os fornecedores-chave, consumidores, agências reguladoras e outras organizações que prestam serviços, produzem ou fornecem produtos semelhantes. Segundo Scott (1992), campo organizacional é um conjunto de organizações que compartilham um sistema de significados comum e que interagem com uma frequência maior do que com organizações externas a ele.

De acordo com os autores que estudam a Teoria Institucional, as organizações dentro do mesmo campo organizacional assumem formas institucionalizadas semelhantes. Para DiMaggio e Powell (1983), um campo organizacional estabelecido tem tanta influência nas estruturas das organizações que o compõem que elas experimentam uma homogeneização, e essa semelhança leva a uma redução na diversidade do campo. Estes autores argumentam ainda que o conceito que melhor capta este processo é o de isomorfismo e sustentam que esse fenômeno pode ser de dois tipos: o isomorfismo competitivo, que é mais relevante para os campos em que há competição livre e aberta entre as organizações; e o isomorfismo institucional, relacionado não à competição por recursos e consumidores, mas por poder político e legitimidade institucional. DiMaggio e Powell (1983) asseveram que o isomorfismo institucional é a razão dominante pela qual as organizações assimilam determinadas estruturas ou assumem determinadas formas.

A mudança institucional provocada por isomorfismo ocorre através de três mecanismos, que nem sempre são empiricamente distintos e que tendem a ter origens em condições diferentes e a levar a resultados diferentes (DIMAGGIO; POWELL, 1983):

a) Isomorfismo coercitivo – que resulta de influências políticas formais e informais de outras organizações, tanto por dependência quanto por expectativas culturais do meio em que atuam. É o isomorfismo relacionado à necessidade de legitimidade e ao poder político.

b) Isomorfismo mimético – é o resultado de respostas das organizações a padrões de incerteza, seja por tecnologias organizacionais mal compreendidas, por objetivos ambíguos ou por soluções pouco claras.

c) Isomorfismo normativo – relacionado à profissionalização, é o isomorfismo que certas categorias ou grupos de profissionais forçam ou impõem às organizações através de crenças e comportamentos tidos como certos em sua categoria ou grupo.

No isomorfismo coercitivo, as pressões que uma organização sofre para se assemelhar às outras podem ser percebidas como força, persuasão ou convite para associação, podendo ser também uma determinação do Governo ou de quem regula certos tipos de atividade, de acordo com DiMaggio e Powell (1983). Portanto, os autores descrevem o isomorfismo coercitivo como resultado de pressões formais e informais existentes no campo organizacional. Com isso, a relação de dependência que uma organização tem de outra do mesmo campo organizacional é uma fonte de pressão que pode resultar em isomorfismo coercitivo. Políticas e regras adotadas pelas matrizes das organizações são também refletidas nas suas subsidiárias através de coerção, como mencionam DiMaggio e Powell (1983), reforçando o argumento de Holland *et al*. (1994) e Teo, Wei e Benbasat (2003) de que a administração central de uma organização é uma fonte relevante de pressão coercitiva. Além disso, a força que o Estado exerce sobre as organizações também pode levar ao isomorfismo, como observaram Meyer e Rowan (1977). Appari, Johnson e Anthony (2009) explicam que o ambiente legal pede mudanças significativas nas estruturas das organizações. Para eles, a regulação pode levar as organizações a uma padronização de processos, práticas e recursos, visando à legitimação no ambiente de negócio através da demonstração de conformidade. Assim, as regras institucionalizadas e legitimadas pelo Estado e no Estado acabam sendo refletidas nas organizações.

No isomorfismo mimético, uma organização imita a outra para resolver um problema comum cuja solução é incerta, o que pode ser mais viável e ter um custo menor do que descobrir ou criar a própria solução. As organizações tendem a imitar outras do seu

campo que são tidas como bem-sucedidas ou mais legítimas, e isso nem sempre ocorre de forma que a organização que serve como modelo saiba que está sendo imitada, e nem sempre as soluções são difundidas de forma intencional entre os demais constituintes do campo organizacional (DIMAGGIO; POWELL, 1983).

Já no isomorfismo normativo, certas categorias ou grupos de profissionais forçam ou impõem mudanças às organizações, tanto em decorrência da formação que tiveram em universidades e cursos voltados para formação profissional, quanto pelo surgimento e crescimento de redes profissionais que saem do contexto das organizações onde trabalham, esclarecem DiMaggio e Powell (1983). Os autores acrescentam que os profissionais também migram de uma organização para outra, levando consigo seus conhecimentos, e as empresas de consultoria, associações profissionais e industriais também têm um papel relevante ao difundir entre seus profissionais ou associados preceitos que podem levar as organizações a semelhanças, esclarecem os autores.

Nesse contexto, as pressões do ambiente institucional são aquelas exercidas pelos constituintes do ambiente institucional sobre as organizações que o compõem para que se conformem com as regras e valores institucionalizados. Com base nos mecanismos de isomorfismo institucional propostos por DiMaggio e Powell (1983) e nos pilares institucionais de Scott (2008), Handgraaf (2012) classifica essas pressões como regulativas, miméticas e normativas, limitando as pressões regulativas àquelas canalizadas por meio de documentos escritos, ignorando outras formas de coerção. Neste trabalho, essas pressões são chamadas de coercitivas em respeito à denominação dada por DiMaggio e Powell (1983) aos mecanismos de isomorfismo institucional.

Outro conceito importante para a abordagem institucional é o de **legitimidade**. De acordo com Suchman (1995), legitimidade é uma suposição ou percepção generalizada de que as ações de uma entidade são desejáveis ou apropriadas dentro de um sistema socialmente construído de normas, valores, crenças e definições. Segundo Tolbert e Zucker (1983), quando alguns elementos organizacionais se tornam institucionalizados – percebidos como necessários e apropriados para a eficiência organizacional –, as organizações são pressionadas a incorporar esses elementos em sua estrutura formal para que tenham legitimidade, pois, ao incorporá-los, demonstram que estão com uma conduta considerada apropriada e correta.

Para DiMaggio e Powell (1983), na perspectiva da abordagem institucional, a legitimidade frente às expectativas de partes interessadas é requisito para a sobrevivência das

organizações no seu campo organizacional. Segundo estes autores, mesmo que inovações sejam adotadas inicialmente por uma ou algumas organizações com o objetivo de melhorar o desempenho, estas vão sendo assimiladas pelos outros constituintes do ambiente institucional de forma que deixam de representar uma vantagem competitiva e tornam-se meios para obter legitimidade.

Embora a Teoria Institucional seja amplamente utilizada em estudos no campo da Administração, esta abordagem não está livre de críticas. Quinello (2007) identifica na literatura trabalhos críticos à Teoria Institucional, nos quais os autores argumentam que alguns dos trabalhos seminais se baseiam em considerações teóricas de múltiplos estudos, dificultando a reprodutibilidade dos resultados e sua categorização. Quinello (2007) aponta também críticas à ausência de métricas confiáveis, ao fato de a teoria não responder a questões como o porquê de algumas ideias e técnicas se tornarem reconhecidas e outras não, ou o porquê de alguns padrões serem persistentes nas organizações e outros não. Para os críticos, são necessários mais estudos empíricos e testes validados sobre o processo de institucionalização, e a abordagem institucional não explica de forma aprofundada como práticas e crenças racionalizadas levam à adoção de procedimentos e regras organizacionais.

Ao analisar criticamente a contribuição da Escola Neo-Institucional aos estudos organizacionais, Peci (2006) argumenta que o novo institucionalismo não consegue distanciar-se da "ortodoxia funcionalista" e apresenta ainda outros "pontos de estrangulamento", alguns dos quais estão aqui sintetizados: pouca atenção é dispensada à compreensão dos processos de institucionalização, sem que sejam questionados os motivos pelos quais algumas práticas são institucionalizadas e outras não; há pouca atenção a questões de criação e transformação que levam às mudanças nas organizações – o foco é sobre a durabilidade e persistência das instituições; o tratamento dado ao poder enfatiza o aspecto regulativo, não a distinguindo de outras abordagens funcionalistas. A autora conclui que os estudos dentro da abordagem neo-institucional são pouco preocupados com processos de mudança e transformação organizacional e institucional, tanto em termos teóricos quanto empíricos.

A despeito das críticas, Dwivedi, Wade e Schneberger (2012) entendem que a abordagem institucional traz bases teóricas que permitem realizar estudos na área de Sistemas de Informação. Já Hu, Hart e Cooke (2007) admitem que a abordagem pode contribuir em investigações sobre as forças que impulsionam a mudança ou a inércia nas organizações, o que tem sido demonstrado em diferentes estudos. Focando especificamente em Segurança da

Informação, Lorens (2007) considera que as organizações baseiam suas decisões em melhores práticas de mercado, experiências de outras organizações e modelos institucionalizados, o que é consistente com a Teoria Institucional.

Nesse sentido, Björck (2004) e recomenda a utilização da Teoria Institucional em pesquisas no campo dos estudos organizacionais, explicando que esta abordagem não é um sistema coerente de regras, mas um conjunto de ideias que formam uma perspectiva de mecanismos que apoiam ou restringem o comportamento social. O autor vai além e considera a Teoria Institucional adequada para explicar a relação entre o ambiente externo e a Segurança da Informação nas organizações, com o que concordam Kam *et al*. (2013).

2.4 A ABORDAGEM INSTITUCIONAL E A SEGURANÇA DA INFORMAÇÃO

Embora a conformidade com requisitos de Segurança da Informação seja tradicionalmente visto como uma questão estratégica, relacionada aos interesses e objetivos da organização (HONG *et al*., 2003; POSTHUMUS; VON SOLMS, 2004; DOHERTY; FULFORD, 2006; HEDSTRÖM *et al*., 2011; WU; SAUNDERS, 2011), uma série de trabalhos tem mostrado que as decisões sobre Segurança da Informação têm sido influenciadas ou determinadas pelo ambiente externo – alguns desses utilizam a Teoria Institucional como lente teórica (ver Quadro 3).

Apesar de a Teoria Institucional já ter sido utilizada em trabalhos de Sistemas de Informação (DEVAUJANY *et al*., 2014), sua aplicação nessa área temática é considerada incipiente, havendo ainda muito potencial de aplicação (WEERAKKODY; DWIVEDI; IRANI, 2009), situação que se repete em trabalhos do tema Segurança da Informação (BJÖRCK, 2004; KAM *et al*., 2013; ALBUQUERQUE JUNIOR; SANTOS, 2013, 2014a, 2014b).

Para Björck (2004), a Teoria Institucional é adequada para estudar Segurança da Informação, pois permite identificar quais forças institucionais afetam a maneira como as políticas são desenvolvidas, de onde vêm essas forças institucionais, como essas instituições são difundidas entre as organizações e em que medida afetam as estruturas formais de Segurança da Informação. O autor sustenta ainda que as instituições afetam as organizações, subgrupos organizacionais e indivíduos, e a Teoria Institucional pode explicar o que determina as escolhas que implicam em questões de Segurança da Informação nesses

contextos, quais forças institucionais incidem sobre esses grupos e indivíduos, quem exerce as pressões institucionais, como as instituições são difundidas nesses grupos e em que medida afetam a Segurança da Informação.

Quadro 3 – Trabalhos sobre Segurança da Informação sob a ótica da Teoria Institucional.

AUTORES	TIPO	OBJETIVO
Björck (2004)	Teórico	Propor a Teoria Institucional como abordagem para pesquisas sobre Segurança da Informação
Backhouse, Hsu e Silva (2006)	Empírico	Analisar o desenvolvimento e institucionalização da norma BS7799 (norma internacional ISO/IEC 27002)
Hu, Hart e Cooke (2006)	Empírico	Identificar o papel das influências externas nas ações de Segurança da Informação
Hu, Hart e Cooke (2007)	Empírico	Identificar o papel das influências internas e externas nas ações de Segurança da Informação
Appari, Johnson e Anthony (2009)	Empírico	Propor um modelo para estudar a conformidade regulamentar com a norma *Health Insurance Portability and Accountability Act* (HIPAA) do Governo dos Estados Unidos e testar empiricamente
Appari, Anthony e Johnson (2009)	Empírico	Investigar a variação da conformidade das organizações com a norma HIPAA
Luesebrink (2011)	Empírico	Avaliar o impacto do ambiente regulatório sobre a Governança da Segurança da Informação
Nasution (2012)	Empírico	Compreender como se deu a institucionalização das medidas e da Governança da Segurança da Informação
Lopes (2012)	Empírico	Estudar o processo de adoção de Políticas de Segurança da Informação
Hsu, Lee e Straub (2012)	Empírico	Investigar a adoção da gestão da Segurança da Informação como uma inovação moderada por fatores organizacionais
Holgate, Williams e Hardy (2012)	Empírico	Examinar como são organizados na prática os arranjos de Governança da Segurança da Informação
Spears, Barki e Barton (2013)	Empírico	Estudar os aspectos simbólicos para aumentar a aceitação da Gestão de Riscos e da Segurança da Informação
Tejay e Barton (2013)	Empírico	Investigar como influências externas motivam a alta gestão a se comprometer com a Segurança da Informação
Williams, Hardy e Holgate (2013)	Empírico	Examinar como surgem as variações de arranjos de Governança da Segurança da Informação
Kam, Katerattanakul e Emerick (2013)	Empírico	Examinar como as pressões externas conduzem ao cumprimento de Políticas de Segurança da Informação
Kam *et al*. (2013)	Empírico	Examinar como as expectativas externas impulsionam o cumprimento de Políticas de Segurança da Informação
Anthony, Appari e Johnson (2014)	Empírico	Examinar a conformidade com a norma HIPAA
Lopes e Sá-Soares (2014)	Empírico	Estudar os fatores que condicionam a adoção de Políticas de Segurança da Informação
AlKalbani, Deng e Kam (2014)	Empírico	Propor um modelo para conformidade de iniciativas de Governo Eletrônico e testar empiricamente
AlKalbani, Deng e Kam (2015)	Empírico	Explicar como a cultura organizacional influencia a conformidade com a Segurança da Informação
Cavusoglu *et al*. (2015)	Empírico	Explicar por que existem diferenças de recursos de controle de Segurança da Informação entre as organizações

Fonte: elaborado pelo autor.

Backhouse, Hsu e Silva (2006) estudaram como se deu a institucionalização da norma britânica BS 7799, que viria a se tornar a norma internacional ISO/IEC 17799, posteriormente nomeada ISO/IEC 27002 e adotada como norma brasileira pela ABNT (2013) como NBR ISO/IEC 27002. Para os autores, a adoção da norma no Reino Unido e sua internacionalização podem ser explicadas pelo mimetismo institucional: a adoção dentro do país no qual foi criada foi feita com a intenção de demonstrar bons controles internos nas organizações, embora não houvesse obrigação; depois de ter sido adotada pela ISO como norma internacional, diversos países passaram a adotá-la também ao invés de desenvolverem suas respectivas normas.

A possibilidade de ocorrência de incidentes que afetam iniciativas de governo eletrônico motivou AlKalbani, Deng e Kam (2014) a proporem um modelo de conformidade de Segurança da Informação para organizações públicas. Segundo os autores, expectativas externas impõem pressões sobre as organizações públicas no sentido de empreender esforços para atender aos requisitos de Segurança da Informação. Os autores identificaram pressões coercitivas de leis e regulamentos, em um contexto de aumento de intervenções de órgãos do Governo para que essas organizações estejam em conformidade. A pressão coercitiva também pode vir da sociedade, que espera que seus dados em posse do Governo estejam seguros, segundo os autores. O modelo proposto foi validado em outro estudo (ALKALBANI; DENG; KAM, 2015) e os autores concluem que promover uma cultura de Segurança da Informação na organização pode aumentar a conformidade organizacional com os requisitos externos de Segurança da Informação.

Spears, Barki e Barton (2013) estudaram a Segurança da Informação e a Gestão de Riscos em um contexto regulatório sob a lente da Teoria Institucional em seis organizações e concluíram que elas são incentivadas por fatores externos, destacando a regulamentação à qual estão sujeitas e as auditorias externas sofridas para avaliar a conformidade.

Nasution (2012) estudou a institucionalização de medidas de Segurança da Informação no setor bancário da Indonésia e notou que o Banco Central do país tem uma participação significativa na adoção de medidas devido ao seu poder regulamentar – em outras palavras, poder coercitivo. O autor ressalta o apoio do alto escalão de gestores e o impacto positivo que o cumprimento da Política de Segurança da Informação tem sobre a adoção de outras medidas. Outro destaque apresentado é o impacto da ocorrência de

incidentes de Segurança da Informação, que, apesar de ser um fato negativo, impulsiona a adoção ou revisão de medidas de Segurança da Informação.

Tejay e Barton (2013) investigaram como influências externas motivam o comprometimento de gestores de pequenas e médias empresas com a Segurança da Informação e concluíram que as crenças desses gestores são influenciadas principalmente por mecanismos normativos e miméticos, mas também por regulamentos do Governo como mecanismos coercitivos, o que influencia positivamente na assimilação da Segurança da Informação nas organizações.

Holgate, Williams e Hardy (2012) estudaram a influência do ambiente institucional na Governança da Segurança da Informação em organizações de infraestrutura crítica da Austrália e identificaram algumas variações nos arranjos de governança, além de isomorfismo por influências institucionais, como normas internacionais, relações estabelecidas com outras organizações, indústrias com quem têm relações de dependência e seu campo organizacional. Ao examinar como surgem as variações em arranjos de Governança da Segurança da Informação nessas organizações, Williams, Hardy e Holgate (2013) perceberam que elas estavam sujeitas a pressões coercitivas de órgãos do Governo, além de pressões normativas referentes à adoção da norma ISO/IEC 27002 como modelo.

Kam *et al*. (2013) estudaram como as organizações acadêmicas dos Estados Unidos são influenciadas por expectativas externas para cumprirem Políticas de Segurança da Informação e a influência dessas forças externas na conscientização sobre Segurança da Informação. A pesquisa mostrou que pressões institucionais regulatórias (coercitivas) e normativas influenciam de forma significativa a conformidade dessas organizações com as Políticas de Segurança da Informação, embora essas pressões sejam moderadas pela liberdade existente no ambiente acadêmico, que pode ser reduzida com a adoção de medidas de Segurança da Informação.

Kam, Katerattanakul e Emerick (2013) estudaram ainda como pressões externas afetam a conformidade com Políticas de Segurança da Informação no setor bancário e concluíram que essas organizações cumprem suas políticas principalmente para atender a expectativas normativas.

Documentos que formalizam Políticas de Segurança da Informação da administração pública municipal de Portugal foram analisados e como resultado foi feita uma proposta de um modelo aplicável aos diferentes municípios daquele país. O modelo pôde ser

institucionalizado por meio de um processo que envolve regulação, aprovação como padrão e criação da obrigação de adotá-lo. A institucionalização envolve ainda fazer do modelo uma obrigação social por meio da formação das pessoas e interiorização dos benefícios da Política de Segurança da Informação (LOPES, 2012; LOPES; SÁ-SOARES, 2014).

Hsu, Lee e Straub (2012) estudaram a Segurança da Informação como uma inovação administrativa e concluíram que as organizações sofrem pressões isomórficas miméticas e coercitivas, ainda que moderadas por fatores organizacionais e econômicos: 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.

Luesebrink (2011) avaliou o impacto de iniciativas de regulação sobre as estruturas de gestão de Segurança da Informação de organizações acadêmicas a partir da perspectiva institucional. O autor observou que a contratação de profissionais com conhecimentos sobre Governança da Segurança da Informação e a compreensão por parte dos gestores de que é prioridade alcançar e manter a conformidade com regulamentos e normas fez com que as organizações adotassem medidas de Segurança da Informação, o que mostra que mecanismos normativos e coercitivos de pressão institucional influenciaram na adoção de medidas de Segurança da Informação.

Cavusoglu *et al*. (2015) investigaram os investimentos que diferentes organizações fazem em Segurança da Informação e concluíram que estas sofrem pressões institucionais normativas e coercitivas. A pressão normativa recai principalmente sobre os investimentos em capacitação dos membros da organização em Segurança da Informação, mas influencia também a adoção de tecnologias e a qualificação dos profissionais. A pressão coercitiva também influencia a decisão de investir na aquisição de tecnologia e contratação de profissionais de Segurança da Informação, o que ocorre para atender a regulamentos governamentais. Os autores observaram também que há pressão coercitiva de organizações parceiras quanto às medidas necessárias para mitigar riscos comuns.

Ao estudarem a importância de fatores que influenciam a conformidade de serviços de saúde com a *Health Insurance Portability and Accountability Act* (HIPAA), lei dos Estados Unidos que regula, entre outros aspectos, a privacidade e a segurança de informações eletrônicas de pacientes, Appari, Johnson e Anthony (2009) argumentam que o ambiente legal pede mudanças significativas nas estruturas das organizações e essa regulação

pode levar a uma padronização de processos, práticas e recursos, com o objetivo de ganhar legitimidade no ambiente de negócio através da demonstração de conformidade. Os autores argumentam ainda que a relação de dependência (ou afiliação) entre duas organizações que atuam no mesmo mercado e a imitação de outras organizações que tiveram sucesso quanto a incertezas comuns no ambiente de negócio podem também levar a mudanças tendo como objetivo a legitimação.

Appari, Anthony e Johnson (2009) investigaram a variação da conformidade de hospitais dos Estados Unidos com a norma HIPAA e descobriram que a aderência dessas organizações à legislação é influenciada pela abrangência de outros regulamentos do Governo e pelo apoio de estruturas internas voltadas à conformidade organizacional.

Em outro trabalho, Anthony, Appari e Johnson (2014) perceberam que organizações que atuam no mesmo negócio, se submetidas a ambientes institucionais distintos – serviços de saúde com e sem fins lucrativos, no caso –, produzem resultados distintos quanto à conformidade com as medidas de Segurança da Informação presentes na norma HIPAA.

As influências externas nos investimentos em Segurança da Informação foram estudadas por Hu, Hart e Cooke (2006), que argumentam que os investimentos em tecnologias de Segurança da Informação e o desenvolvimento de políticas de Segurança da Informação têm baixa prioridade para os gestores. Em contrapartida, os autores observaram que os meios mais eficazes para impulsionar os investimentos em tecnologia e os esforços para desenvolver políticas 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.

Hu, Hart e Cooke (2007) mostraram que, além de pressões ambientais, a organização está sujeita também a forças internas. Entre as pressões coercitivas do ambiente para que a organização adote medidas de Segurança da Informação, os autores identificaram as auditorias e a legislação. Como pressões normativas, os resultados da pesquisa apontam as interações entre os profissionais que atuam na Segurança da Informação, que acontecem através de associações profissionais, atualizações sobre modelos e padrões e publicações sobre o tema.

Hu, Hart e Cooke (2007) também apontam dificuldade em identificar influências miméticas e atribuem essa dificuldade à natureza da Segurança da Informação: relatos de sucesso na implantação de medidas de Segurança da Informação raramente são divulgados, enquanto relatos de incidentes são mais comuns. Com isso, os autores argumentam que é mais difícil imitar casos de sucesso, já que esses não são divulgados. Quanto às forças internas, os autores concluem que a busca pela eficiência pode motivar a resistência às medidas de Segurança da Informação adotadas pela organização.

Uma pesquisa anterior com o objetivo de analisar se a adoção de medidas de Segurança da Informação pelas organizações era fruto de pressões institucionais ou da estrutura de Governança da Segurança da Informação (ALBUQUERQUE JUNIOR; SANTOS, 2015) mostrou que a adoção é resultado de pressões do ambiente institucional, exercidas principalmente por meio de leis, decretos e outros regulamentos e pela interação de profissionais de TI e Segurança da Informação com seus pares em redes profissionais, mas também pela imitação de medidas adotadas por outras organizações públicas e pelos padrões e normas internacionais de Segurança da Informação, evidenciando que pressões coercitivas, normativas e miméticas influenciam a adoção. A pesquisa mostrou também que normas e padrões internos previamente adotados pela organização influenciam a adoção de outras medidas de Segurança da Informação, e que são adotadas principalmente medidas técnicas.

A relação entre as pressões institucionais e a adoção de medidas técnicas, formais e informais foi analisada em outra pesquisa (ALBUQUERQUE JUNIOR *et al.*, 2016) que mostrou que a adoção acontece devido a pressões coercitivas e miméticas, mas principalmente devido a pressões normativas. A participação de profissionais de TI e Segurança da Informação em redes de troca de informações e conhecimentos foi a pressão institucional mais associada à adoção de medidas técnicas, e a publicação de normas e padrões internacionais de Segurança da Informação foi a pressão mais associada à adoção de medidas formais e informais. A pesquisa evidenciou também que a adoção de medidas técnicas e informais está mais associada a pressões normativas, enquanto a adoção de medidas formais está mais associada a pressões coercitivas. Por fim, a pesquisa mostrou que as medidas técnicas são as mais difundidas pelas organizações, muitas delas adotadas por todas as organizações que participaram da pesquisa, e que a Política de Segurança da Informação e o Comitê de Segurança da Informação são as medidas formais mais adotadas, enquanto os treinamentos de profissionais de TI são as medidas informais mais comuns.

Os trabalhos que abordam a Segurança da Informação sob a lente da Teoria Institucional enfatizam principalmente a conformidade com regulamentos e leis (LOPES, 2012; KAM *et al*., 2013; KAM; KATERATTANAKUL; EMERICK, 2013; ALKALBANI; DENG; KAM, 2014, 2015; ANTHONY; APPARI; JOHNSON, 2014; LOPES; SÁ-SOARES, 2014) e a institucionalização e difusão de políticas, normas e estruturas de Segurança da Informação (BACKHOUSE; HSU; SILVA, 2006; LUESEBRINK, 2011; HOLGATE; WILLIAMS; HARDY, 2012; HSU; LEE; STRAUB, 2012; LOPES, 2012; NASUTION, 2012; WILLIAMS; HARDY; HOLGATE, 2013; LOPES; SÁ-SOARES, 2014).

Embora reconheçam o potencial da Teoria Institucional em estudos a respeito das influências externas sobre as ações organizacionais visando à Segurança da Informação, alguns trabalhos críticos a esta abordagem são citados por Hu, Hart e Cooke (2007), que resumem as críticas à ideia de que, se as organizações são tão diferentes sob diversos aspectos, as pressões externas talvez não sejam tão poderosas a ponto de causar a homogeneização do ambiente institucional.

Isso é reforçado por estudos que admitem fatores internos como fontes de pressão para adoção de medidas de Segurança da Informação. Esses estudos mostram que as organizações estão sujeitas a pressões institucionais coercitivas, normativas e miméticas para que adotem medidas de Segurança da Informação, mas mostram também que a adoção depende da percepção interna quanto ao ganho ou perda de eficiência no desenvolvimento das atividades da organização (HU; HART; COOKE, 2007; HSU; LEE; STRAUB, 2012; KAM *et al*., 2013), do apoio de subunidades organizacionais, o que implica na conformidade com os requisitos externos de Segurança da Informação das organizações (APPARI; ANTHONY; JOHNSON, 2009), da existência de estruturas de governança da Segurança da Informação e das decisões tomadas no contexto dessas estruturas (ALBUQUERQUE JUNIOR; SANTOS, 2015) ou da disponibilidade de recursos e do resultado de avaliações das necessidades internas de Segurança da Informação (CAVUSOGLU *et al*., 2015).

Nesse sentido, e apesar de não tratarem de Segurança da Informação, Boxenbaum e Jonsson (2009) argumentam que, embora as pressões institucionais possam causar isomorfismo entre as organizações, estas podem também fazer escolhas quando as pressões são conflitantes entre si ou quando são contrárias às suas necessidades de eficiência interna, e que isso resulta em uma dissociação entre a estrutura formal adotada pela organização e as ações e práticas do dia a dia.

2.5 DISSOCIAÇÃO ENTRE POLÍTICA E PRÁTICA

A dissociação entre o comportamento real e as políticas e estruturas formais adotadas pelas organizações tem diversos exemplos na literatura. Mais conhecido como dissociação entre política e prática (WESTPHAL; ZAJAC, 2001; BROMLEY; POWELL, 2012; HERNES; ERDVIK, 2014), esse comportamento também é chamado de adoção simbólica (BROMLEY; POWELL, 2012; ALHIRZ; SAJEEV, 2013; HERAS-SAIZARBITORIA; BOIRAL, 2015), adoção cerimonial (BOIRAL, 2007; HERAS-SAIZARBITORIA, 2011), baixo acoplamento (WEICK, 1976; ORTON; WEICK, 1990; INGERSOLL, 1993), implementação instrumental (VASCONCELOS; VASCONCELOS, 2003) e comportamento "para inglês ver" (WOOD JR.; CALDAS, 1997).

Orton e Weick (1990) identificam três causas para a ocorrência da dissociação: pouca clareza quanto às conexões entre meios e fins; fragmentação do ambiente interno, em que os participantes estão envolvidos em operações específicas dentro das organizações; e fragmentação do ambiente externo, com estímulos dispersos e expectativas incompatíveis. Boxenbaum e Jonsson (2009) argumentam que as organizações, ao serem pressionadas a se adaptarem a mitos institucionalizados, enfrentam dois problemas: esses mitos podem não ser soluções eficientes e podem ser simultâneos e contraditórios. Assim, a defesa da organização para esses problemas, para Meyer e Rowan (1977), é cumprir superficialmente as exigências institucionais – manter uma dissociação entre a estrutura formal e a prática.

Vários trabalhos sobre dissociação têm por base a Teoria Institucional, e apresentam ou citam evidências empíricas de que a dissociação está relacionada à imagem de sucesso e à legitimidade organizacional (POWELL, 1988; OLIVER, 1991; ELSBACH; SUTTON, 1992; BEVERLAND; LUXTON, 2005; VOXTED; LIND, 2010; BROMLEY; POWELL, 2012; BROMLEY; HWANG; POWELL, 2012; HERAS-SAIZARBITORIA; BOIRAL, 2015). Como exemplo, Voxted e Lind (2010) apontam um paradoxo ao argumentarem que as organizações buscam descentralizar decisões ao mesmo tempo em que adotam tecnologias de gestão que implicam em aumento de controle e supervisão, dissociando a estrutura das práticas de fato adotadas nas organizações. Também a partir da perspectiva institucional, Bromley e Powell (2012) explicam que a dissociação entre política e prática acontece quando as políticas são adotadas de maneira simbólica pela organização. A

Figura 1 apresenta uma comparação entre a situação que Bromley e Powell (2012) consideram ideal e a dissociação entre política e prática, como compreendida por estes autores.

De acordo com Meyer e Rowan (1977), a dissociação entre a estrutura formal e a prática é uma maneira racional de a organização garantir sua legitimidade. Nesse sentido, Power (2000) argumenta que a dissociação minimiza os efeitos das pressões institucionais, embora seja importante para a legitimidade externa da organização. O resultado da dissociação entre política e prática, segundo Meyer e Rowan (1977), é uma **conformidade cerimonial** com os requisitos do ambiente institucional.

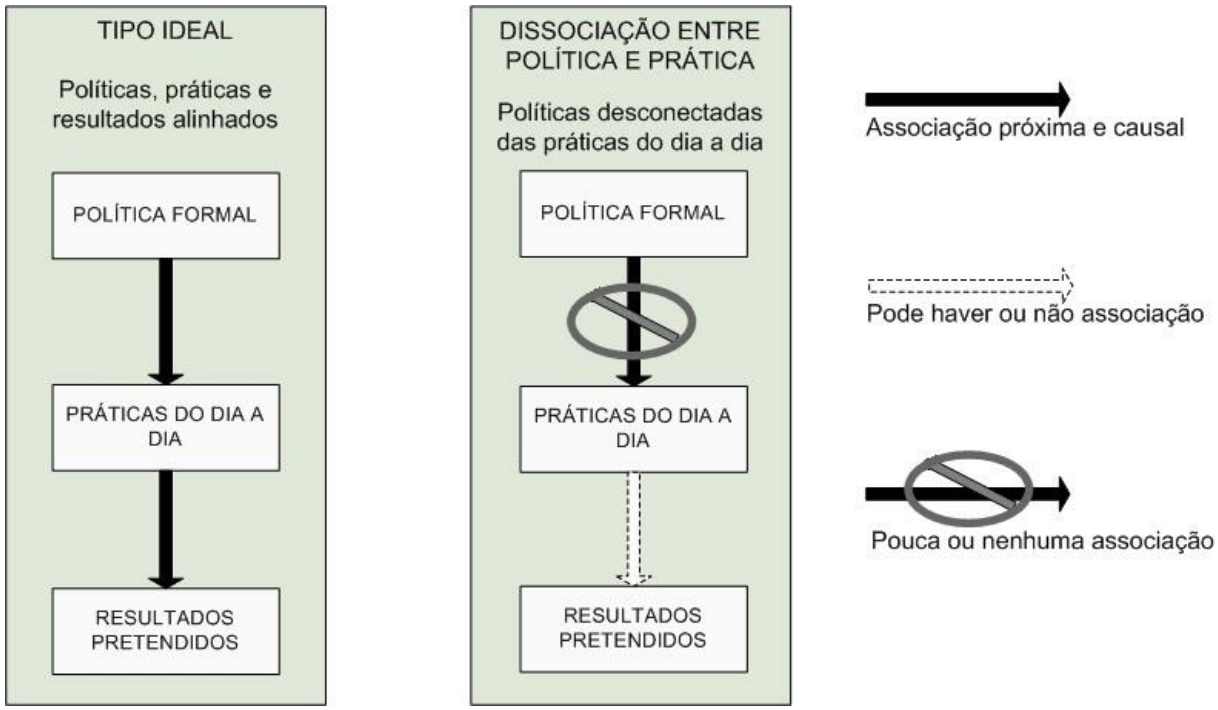


Figura 1 – Situação ideal versus dissociação entre política e prática.
Fonte: Bromley e Powell (2012).
Traduzido pelo autor.

Apesar de normalmente ser abordada como uma decisão racional da organização, a literatura sobre dissociação entre política e prática também mostra que ela pode acontecer ainda que a organização tenha a intenção de estar em conformidade com as exigências externas. Cole (2005, 2012) e Lim e Tsutsui (2012), por exemplo, perceberam que a dissociação entre política e prática pode ser decorrente tanto da falta de interesse em adotar a

política em profundidade quanto da falta de capacidade da organização, concordando com Bromley e Powell (2012).

Diversos exemplos de trabalhos que tratam de dissociação não intencional entre política e prática são apresentados por Bromley e Powell (2012), que explicam que ela é mais provável quando: a adoção é motivada pela legitimidade ao invés de exigências técnicas; o processo de adoção está ainda no início; há pouca capacidade para implementar as políticas; ou as pressões do ambiente institucional não são reforçadas internamente. Os autores esclarecem ainda que, em contextos com demandas institucionais concorrentes, as organizações podem adotar diferentes práticas, muitas vezes conflitantes, sem interromper ou alterar suas operações na tentativa de implementá-las, causando a dissociação.

Neste trabalho, argumenta-se que a causa para a dissociação não intencional entre política e prática é o comportamento das subunidades das organizações. Aguilera-Caracuel *et al*. (2012) notaram que a padronização de práticas de gestão em uma organização com estrutura descentralizada é impactada pelo fato de a administração central e as subsidiárias estarem sujeitas a demandas institucionais diferentes, o que, segundo os autores, tem grande influência sobre a adesão das subunidades às práticas adotadas pela sede.

Delmas e Toffel (2008) ampliam essa ideia ao argumentarem que as demandas institucionais concorrentes podem pressionar não só a administração central da organização, mas também os setores internos individualmente, e que as organizações são diferentes quanto à receptividade às pressões de diferentes constituintes do ambiente institucional devido ao fato de suas subunidades normalmente se envolverem com conjuntos diferentes de constituintes e sofrerem pressões institucionais distintas. Como consequência, diferentes subunidades da mesma organização podem responder de maneiras distintas às pressões que sofrem e podem também influenciar suas sedes de formas variadas.

> Nós sustentamos que as organizações canalizam pressões [...] a diferentes departamentos funcionais, e que estes departamentos funcionais, por sua vez, influenciam a sensibilidade e as respostas dos gestores às pressões institucionais. Por isso, defendemos que diferenças na adoção de práticas de gestão pelas organizações refletem não apenas diferentes níveis de pressões institucionais [...], mas também diferenças na influência de seus departamentos funcionais. (DELMAS; TOFFEL, 2008, p.1027, traduzido pelo autor).

Já para Hernes e Erdvik (2014), a conformidade e a não conformidade com uma política instituída por uma organização hierarquicamente superior podem ser resultantes de decisões tomadas de maneira descentralizada, balizadas por interesses próprios, distintos dos

interesses gerais da organização. Os autores sustentam que a dissociação pode acontecer quando subordinados utilizam seu próprio julgamento sobre o que é melhor para a organização, em detrimento do julgamento dos superiores hierárquicos. Assim, as diretrizes gerenciais podem ser consideradas ineficazes ou percebidas como puramente simbólicas e retóricas e, portanto, como algo que não precisa ser cumprido ou que pode ser cumprido apenas superficialmente, o que leva à dissociação em subunidades organizacionais.

Pilato e Pedrini (2015) observam na literatura estudos que enfatizam que as subsidiárias de uma organização sofrem pressões externas (interorganizacionais) e internas (organizacionais) para que cumpram políticas de responsabilidade social corporativa. Segundo os autores, as pressões internas sobre as unidades descentralizadas são principalmente da matriz da organização, e a resposta às pressões internas ou externas depende da autonomia administrativa das subunidades organizacionais e da necessidade destas de legitimação perante os constituintes do ambiente institucional em que estão e perante sua matriz. As pressões institucionais internas são chamadas neste trabalho de pressões da administração central da organização.

Netland e Aspelund (2014) entendem que práticas importantes para as organizações nem sempre são implementadas pelas suas subunidades organizacionais porque elas precisam lidar com pressões institucionais que competem entre si, provenientes tanto da sede quanto do ambiente institucional. Segundo os autores, ainda que a sede defenda e busque a adoção em todas as suas subunidades, não significa que as práticas serão consideradas eficientes por todas elas, o que pode levar à dissociação.

A literatura sobre dissociação entre política e prática mostra que o fenômeno pode acontecer mesmo quando a organização busca a conformidade com os requisitos institucionais e que a causa pode ser o fato de suas subunidades organizacionais sofrerem pressões institucionais distintas e respondem de maneiras distintas a essas pressões. A dissociação foi abordada em pesquisas sobre gestão ambiental (DELMAS; TOFFEL, 2008; AGUILERA-CARACUEL *et al*., 2012), melhoria operacional (NETLAND; ASPELUND, 2014), gestão de saúde (HERNES; ERDVIK, 2014) e responsabilidade social (PILATO; PEDRINI, 2015), mas nenhum trabalho abordando dissociação entre políticas e práticas de Segurança da Informação foi identificado na bibliografia consultada.

Entretanto, em um trabalho sobre Segurança da Informação, Appari, Anthony e Johnson (2009) mostram que a conformidade organizacional com regulamentos externos

depende do apoio das estruturas internas da organização, o que reforça o entendimento de que o comportamento das subunidades pode causar a dissociação. Além disso, para Hu, Hart e Cooke (2007), pode haver resistência interna às medidas de Segurança da Informação adotadas por uma organização, e essa resistência pode ser motivada pela busca pela eficiência, concordando com o entendimento de que a conformidade vai depender de como a política adotada pela organização é julgada internamente.

Embora a dissociação seja um fenômeno relevante para a Teoria Institucional, como ressaltado por Westphal e Zajac (2001), estes autores consideram difícil observá-la em grandes amostras de organizações. Além disso, ainda segundo estes autores, poucas pesquisas têm procurado explicar a variação nas formas como as organizações respondem a determinados conjuntos de pressões institucionais. Nesse sentido, alguns autores propõem que, além da adoção, rejeição e adoção cerimonial, as organizações podem dispor ainda de uma variedade de respostas às pressões institucionais.

2.6 RESPOSTAS ORGANIZACIONAIS ÀS PRESSÕES DO AMBIENTE

As pressões do ambiente institucional têm sido tradicionalmente associadas a respostas de inércia e passividade, mas tem surgido uma ênfase em ações estratégicas e na interação de pressões diferentes dentro do pensamento institucional (NAIDOO, 2010). Diversos autores concordam que as organizações podem responder de diferentes formas às pressões, modelos e demandas do ambiente externo (PFEFFER; SALANCIK, 1978; OLIVER, 1991; WOOD JR.; CALDAS, 1997; MCKAY, 2001; CASILE; DAVIS-BLAKE, 2002; SÁ, 2004; PACHE; SANTOS, 2010; NETLAND; ASPELUND, 2014).

Na visão de Wood Jr. e Caldas (1997), as organizações buscam imitar de forma pouco crítica as práticas e tecnologias gerenciais comumente adotadas por outras organizações. Isto parece consistente com a ideia de isomorfismo mimético institucional, pois organizações passam a imitar práticas que são adotadas por organizações percebidas como eficientes e que atuam em países desenvolvidos, mas, segundo os autores, o mimetismo não acontece de maneira tão simples e as organizações tendem a se comportar de três formas: adotando as práticas “para inglês ver”, comportamento considerado típico, no qual a adoção é parcial, sem que mudanças substanciais sejam realizadas – em outras palavras, um comportamento de dissociação, que deixa a organização em conformidade cerimonial;

negando, comportamento que acontece quando a organização sofre resistência ou pressões internas ou quando as práticas mostram-se incompatíveis com a realidade organizacional e a adoção "para inglês ver" mostra-se insuficiente ou impossível; adaptando de maneira criativa, que acontece quando a organização não busca fingir que adota nem rejeita as práticas, mas as adapta às suas necessidades e realidade.

Netland e Aspelund (2014) apresentam respostas semelhantes às propostas por Wood Jr. e Caldas (1997), acrescentando, entretanto, a adoção em conformidade com as pressões externas, comportamento que estes não admitem devido a questões culturais das organizações que são foco do seu trabalho. Segundo Netland e Aspelund (2014), diante das pressões institucionais sofridas, as respostas podem ser: adotar práticas em conformidade com a política; adaptar as práticas de forma a atender melhor às suas contingências locais; atuar, fingindo estar em conformidade; e evitar, mantendo suas práticas e rotinas atuais inalteradas.

Como crítica às propostas destes autores, é possível destacar que tanto Wood Jr. e Caldas (1997) quanto Netland e Aspelund (2014) não consideraram a possibilidade de a organização enfrentar as fontes de pressão externa ou manipulá-las com base no poder que tem sobre recursos dos quais os constituintes institucionais dependem. Os autores também não consideraram a possibilidade de a organização responder de alguma outra forma entre a aceitação passiva e o comportamento dissimulado, como ao assumir o compromisso de implementar as regras impostas pelo ambiente ou implementá-las parcialmente.

A partir da perspectiva institucional, uma tipologia de respostas às pressões e expectativas do ambiente foi proposta por Sá (2004). O autor busca vincular os três mecanismos de isomorfismo institucional de DiMaggio e Powell (1983) com diferentes respostas, apresentadas conforme aumenta a resistência organizacional às pressões institucionais. As respostas propostas pelo autor são: conformidade institucional, que se apresenta em discursos, decisões e ações consistentes com os requisitos externos e que pode acontecer através de rotina, imitação, convicção e negociação; hipocrisia institucional, conceito consistente com a dissociação e a conformidade cerimonial, pois é uma resposta organizacional a pressões contraditórias e incompatíveis que envolve desarticulação entre discurso e prática, e que pode ser dos tipos cronológica, ambiental, estrutural e temática; infidelidade institucional, resposta contrária à conformidade (aparente ou não), que pode ser verificada em discursos e práticas de transgressão à norma, e se apresenta nas formas defensiva, assumida e ofensiva; e endoutrinamento institucional, que, por anulação, conversão

ou liquidação, tenta eliminar as pressões que não estão de acordo com os interesses organizacionais.

Outra forma de compreender as relações entre organizações e constituintes do ambiente é através da Teoria da Dependência de Recursos. Diferentemente da perspectiva institucional, Pfeffer e Salancik (1978) defendem que as organizações não são tão passivas diante do ambiente, pois tentam gerir dificuldades e incertezas resultantes da necessidade de recursos externos para garantir sua sobrevivência e, visando à obtenção desses recursos, precisam interagir com as outras organizações que as controlam. Sob a ótica da dependência de recursos, as organizações que controlam recursos críticos ou escassos apresentam maior poder de influenciar o ambiente e as outras organizações.

Pfeffer e Salancik (1978) argumentam que as capacidades da organização de influenciar o ambiente e responder ao controle externo e às suas dependências definem suas possibilidades de sobreviver. Essas capacidades se apresentam através de estratégias que envolvem a diversificação de suas relações de dependência, a manipulação de informações para aumentar sua influência externa e a negação da sua dependência. Pfeffer e Salancik (1978) ressaltam ainda que essa relação de interdependência e influência pode ser determinada pela regulamentação governamental. Mas a Teoria da Dependência de Recursos limita as pressões externas ao controle e acesso a recursos, dando pouca atenção a questões como a adoção de modelos e normas tidos como necessários sem que haja uma crítica quanto à sua adequação à realidade organizacional, o poder da profissionalização como mecanismo de adoção de normas sociais, a imitação como solução frente a incertezas ambientais ou a busca pela legitimidade como forma de sobrevivência em detrimento da necessidade de garantir a eficiência organizacional.

As abordagens da dependência de recursos e institucional já foram utilizadas em trabalhos que investigam as respostas organizacionais às pressões do ambiente (MCKAY, 2001; AGUILERA-CARACUEL *et al*., 2012). McKay (2001) argumenta que a Teoria da Dependência de Recursos tem uma preocupação central com o quanto uma organização depende de constituintes do ambiente externo. A autora enfatiza que o ambiente é dinâmico, em parte negociado e em parte coercitivo, e introduz mudanças nas organizações. Já a Teoria Institucional, para a autora, é uma abordagem ideal para estudar as pressões do ambiente externo e como as organizações respondem a elas, além de dar atenção às fontes de pressão e na interação dessas fontes com as organizações a fim de garantir a conformidade. Mas a Teoria Institucional tem como fraqueza o fato de assumir que as organizações não buscam os

benefícios da não conformidade ao serem pressionadas pelo ambiente institucional, destaca a autora. Em dois estudos de casos que investigaram como as organizações respondem a uma nova regulamentação de direitos ambientais, McKay (2001) utilizou a tipologia de respostas estratégicas de Oliver (1991).

Segundo Frezatti, Aguiar e Rezende (2007), a abordagem de Tolbert e Zucker (1999) se preocupou em explicar a institucionalização, sem prever a possibilidade de não haver institucionalização, enquanto Oliver (1991) focou nas respostas dos agentes, tratando inclusive da não institucionalização e da não conformidade. Sem descartar a relevância do ambiente institucional ao pressionar as organizações para que estejam em conformidade, Oliver (1991) postula que, em resposta a essas pressões, as organizações podem se comportar de diferentes formas, em um contínuo que vai da passividade e conformidade à resistência ativa e manipulação das pressões e fontes de pressão institucional. Assim, a autora se opõe aos preceitos da Teoria Institucional quanto à passividade organizacional ao utilizar ideias desta abordagem e da Teoria da Dependência de Recursos para argumentar que as organizações também buscam alcançar seus próprios interesses ao responderem às pressões institucionais.

Autores das abordagens institucional e da dependência de recursos concordam que os ambientes são coletivos e interconectados e que as organizações devem responder às demandas e expectativas externas para sobreviver através da estabilidade e legitimidade, confrontando muitas vezes demandas incompatíveis de uma variedade de atores externos (DOWLING; PFEFFER, 1975; MEYER; ROWAN, 1977; PFEFFER; SALANCIK, 1978; DIMAGGIO; POWELL, 1983).

Oliver (1991) destaca que as duas abordagens reconhecem que são limitadas as escolhas organizacionais diante das pressões externas, mas pondera que, se na Teoria Institucional o comportamento organizacional é limitado à aceitação ou não das demandas e expectativas ambientais, pela Teoria da Dependência de Recursos, as organizações podem adotar uma variedade maior de comportamentos para garantir a alocação e disponibilização dos recursos que necessitam. Assim, se na abordagem institucional a ênfase está na imposição de regras e na transformação organizacional, a ênfase da dependência de recursos é no controle de recursos escassos do ambiente. Além disso, pela Teoria da Dependência de Recursos, a ligação entre as organizações e o ambiente é um meio de fluxo e troca de recursos, e na Teoria Institucional, a ligação é um meio para incorporação de regras e isomorfismo, argumenta Oliver (1991).

Para Tsai e Child (1997), a busca pela legitimidade no ambiente faz com que uma organização atenda às demandas institucionais essenciais, sejam elas formais ou informais, de forma que as duas teorias – a institucional e da dependência de recursos – se complementam na descrição do comportamento organizacional,

A partir dessas duas abordagens, Oliver (1991) integrou o potencial de variação do comportamento organizacional da Teoria da Dependência de Recursos com o potencial que o ambiente tem de impor mudanças no comportamento e nas estruturas organizacionais da Teoria Institucional, estabelecendo as bases conceituais para apresentar alternativas estratégicas em resposta às pressões do ambiente institucional sobre as organizações. A autora propôs cinco respostas estratégicas, cada uma com três táticas: aquiescência, compromisso, esquiva, desafio e manipulação.

A **aquiescência** é uma resposta de consentimento e aceitação passiva dos requisitos institucionais. Oliver (1991) associa esta estratégia a três táticas: **hábito**, que ocorre quando as normas, valores, ações e práticas institucionais são percebidas com fatos sociais, tidos como certos e reproduzidos de forma inconsciente entre as organizações (DIMAGGIO; POWELL, 1983); **imitação**, que ocorre quando modelos institucionalizados adotados por algumas organizações são copiados de forma consciente ou inconsciente por outras, de forma consistente com o isomorfismo mimético de DiMaggio e Powell (1983); **conformidade**, que ocorre quando a organização incorpora ou obedece de forma consciente a normas, valores ou requisitos externos com o objetivo de obter apoio social ou recursos (PFEFFER; SALANCIK, 1978). A resposta de aquiescência está associada à busca pela eficiência (aptidão econômica) ou pela legitimidade (aptidão social) (ESTERHAZY, 2014) e suas três táticas levam à conformidade com os requisitos institucionais, visto que são táticas de aceitação e adoção (OLIVER, 1991).

Segundo Oliver (1991), **compromisso** é a estratégia de acolhimento parcial das regras, normas e valores institucionais devido à possibilidade de serem conflitantes ou inconsistentes com os objetivos organizacionais, como sugerem Meyer e Rowan (1977). A resposta estratégica está entre a aceitação e a resistência às pressões institucionais e tem as seguintes táticas: **equilíbrio**, que busca acomodar expectativas conflitantes com os interesses internos e demandas de múltiplos constituintes institucionais (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009); **pacificação**, que ocorre quando a organização se esforça para minimizar as pressões que sofre e com as quais não concorda, embora precise respeitá-las (SCOTT, 1983); **barganha**, tática utilizada para obter concessões dos constituintes do

ambiente institucional quanto ao nível de conformidade exigido através de negociação (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009).

Para manter a aparência de conformidade, as organizações que dissociam suas políticas formais das práticas internas se esforçam para evitar inspeções por agentes externos ou para controlar essas inspeções com o objetivo de não serem expostas como fraudes (BOXENBAUM; JONSSON, 2009). Isso conduz à resposta estratégica de **esquiva**, cujo nome já foi traduzido do texto original de Oliver (1991) para o português como dissimulação (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009) e fuga (BORGES; DUTRA; SCHERER, 2014). Trata-se de uma tentativa de evitar a conformidade com os requisitos do ambiente institucional através das seguintes táticas: **ocultação**, que envolve disfarçar a não conformidade atrás de uma conformidade cerimonial, presumindo que seja suficiente para se ter legitimidade (MEYER; ROWAN, 1977); **amortecimento**, também chamada de absorção (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009) ou proteção (BORGES; DUTRA; SCHERER, 2014), é uma tentativa de reduzir o quanto a organização é inspecionada, controlada ou avaliada externamente através de um distanciamento entre as atividades internas e o ambiente externo (PFEFFER; SALANCIK, 1978), o que pode ser compreendido como uma redução nos vínculos institucionais (PARKS; WIGAND, 2014) ou uma dissociação entre o que é inspecionado externamente e o que é implementado internamente (AIER; WEISS, 2012); **fuga** (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009) ou escape (BORGES; DUTRA; SCHERER, 2014), que acontece quando, motivada pelo desejo de contornar as condições que tornam o comportamento de conformidade necessário, uma organização sai do domínio no qual a pressão institucional é exercida ou altera suas atividades ou objetivos (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). É importante estabelecer uma distinção entre as táticas de ocultação e amortecimento: elas são semelhantes e difíceis de distinguir, pois ambas põem a organização em uma conformidade aparente com os requisitos externos, mas a ocultação significa que a organização formalizou políticas internas sem implementá-las, enquanto o amortecimento significa um afastamento entre as práticas internas e a inspeção externa, sem que tenha havido a formalização de políticas de fachada.

A estratégia de **desafio**, também chamada de oposição (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009), é uma resposta de resistência mais ativa, uma rejeição inequívoca das normas e expectativas institucionais (OLIVER, 1991). Suas três táticas são: **rejeição**, que consiste em ignorar regras e valores institucionais como uma opção estratégica (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009); **contestação**, que é uma insurreição,

um afastamento mais ativo das regras, normas ou expectativas institucionais, uma vez que, além de desafiar a conformidade, a organização ainda declara esta posição, segundo Armênio Neto e Machado-da-Silva (2009), que preferem chamá-la de desafio; **ataque**, que é uma oposição mais agressiva, onde a organização minimiza ou denuncia os valores institucionalizados ou os constituintes do ambiente institucional que os defendem (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009).

Manipulação é a resposta estratégica mais ativa de resistência, na qual a organização busca exercer poder sobre as expectativas ou os constituintes institucionais de forma oportunista (OLIVER, 1991). Pode ocorrer através de três táticas: **cooptação**, que visa neutralizar a oposição dos constituintes institucionais através da persuasão para que se aliem à organização (PFEFFER, 1974); **influência**, tática que busca alterar a percepção de constituintes institucionais a fim de mudar valores, crenças e critérios de aceitação quanto a práticas e desempenho (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009); **controle**, tática mais agressiva, relacionada ao poder e à dominação sobre os constituintes do ambiente institucional que aplicam as pressões sobre a organização (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009).

As respostas de aquiescência e compromisso, segundo Oliver (1991) e Frezatti, Aguiar e Rezende (2007), são de conformidade com as pressões institucionais, ainda que parcial (no caso do compromisso). A esquiva é apresentada como uma resposta divisora entre a aceitação e a resistência. Já o desafio e a manipulação são respostas de resistência ou rejeição mais ativa. A autora apresenta um quadro com exemplos relacionados a cada uma das táticas associadas às respostas estratégicas que propõe (Quadro 4).

A tipologia de Oliver (1991) se assemelha à de Sá (2004), que também propõe respostas às pressões institucionais em um contínuo que vai da passividade a uma resistência mais agressiva, mas, ao contrário de Oliver (1991), esse autor não menciona a possibilidade de a organização mudar seus objetivos, atividades ou domínios para evitar a inspeção externa ou as pressões institucionais, como também não trata da possibilidade de a organização amortecer as pressões através de um distanciamento entre as atividades desenvolvidas e as fontes de pressão institucional. A tipologia proposta pela autora, além de anterior, prevê um conjunto mais completo de respostas às pressões institucionais.

As respostas estratégicas de Oliver (1991) já foram utilizadas por diferentes autores do campo da Administração em trabalhos sobre temas diversos, como adoção de

práticas contábeis (WAHYUDI, 2004), políticas de direitos humanos (BOSCHMAN, 2006), adoção de práticas e tecnologias agrícolas (GRAEFF, 2005), internacionalização de operações organizacionais (OSMUNDSEN, 2005), elaboração de orçamento e alcance de metas (FREZATTI; AGUIAR; REZENDE, 2007), ações de responsabilidade social (HANDGRAAF, 2012), atuação sindical (LOPEZ, 2012), gestão de desempenho organizacional (LUNDBERG, 2013), processos de decisão (GUTIÉRREZ-RINCÓN, 2014) e práticas de proteção ambiental (BORGES; DUTRA; SCHERER, 2014).

Quadro 4 – Respostas estratégicas às pressões institucionais.

ESTRATÉGIAS	TÁTICAS	EXEMPLOS
Aquiescência	Hábito	Seguir normas invisíveis tidas como certas.
	Imitação	Imitar modelos institucionais.
	Conformidade	Obedecer a regras e aceitar normas.
Compromisso	Equilíbrio	Equilibrar expectativas de múltiplos constituintes do ambiente.
	Pacificação	Aplacar e acomodar elementos institucionais.
	Barganha	Negociar com partes interessadas do ambiente institucional.
Esquiva	Ocultação	Disfarçar não conformidades.
	Amortecimento	Reduzir vínculos institucionais.
	Fuga	Mudar metas, atividades e domínios.
Desafio	Rejeição	Ignorar normas e valores explícitos.
	Contestação	Contestar normas e requisitos.
	Ataque	Agredir as fontes de pressão institucional.
Manipulação	Cooptação	Importar constituintes influentes.
	Influência	Moldar valores e critérios.
	Controle	Dominar constituintes e processos institucionais.

Fonte: Oliver (1991, p.152).
Traduzido pelo autor.

Frezatti, Aguiar e Rezende (2007) analisaram a potencialidade da tipologia de Oliver (1991) para compreender as respostas estratégicas à demanda pelo processo de elaboração de orçamento organizacional. Para os autores, o sucesso no alcance de metas orçamentárias depende das respostas estratégicas daqueles que estão submetidos às pressões institucionais para elaboração do orçamento. Ainda na perspectiva desses autores, a conformidade e institucionalização desse processo nas organizações só acontecem se as respostas às pressões institucionais forem de aquiescência ou compromisso, enquanto outras respostas levam à não institucionalização.

Wahyudi (2004) notou que as respostas estratégicas às pressões para adoção de práticas contábeis levaram uma organização a adotar um discurso de conformidade com as

pressões do ambiente institucional ao mesmo tempo em que manteve as práticas internas dissociadas desse discurso. Como consequência, foram adotadas práticas consideradas ineficientes, não relacionadas às necessidades organizacionais, mas aos interesses de grupos internos, o que prejudicou a gestão e o controle da organização.

Graeff (2005) estudou a mudança de tecnologias de plantio utilizando a tipologia de Oliver (1991) e notou que as mudanças decorrentes das pressões institucionais podem ou não acontecer, a depender da percepção das organizações quanto às pressões sofridas e das influências internas e externas, que podem ser conscientes ou inconscientes. Além disso, a autora notou que as respostas variam com o tempo, a depender de como as pressões se conformam. Embora todas as respostas estratégicas previstas por Oliver (1991) tenham sido identificadas pela autora, a aquiescência e o compromisso foram as mais comuns.

Handgraaf (2012) também observou que as respostas das organizações às pressões que sofrem podem variar com o tempo, a depender da origem e do tipo de pressões sofridas: pressões normativas tiveram respostas de desafio, esquiva, compromisso e aquiescência; pressões coercitivas (ou regulativas, com prefere a autora) tiveram como respostas desafio, aquiescência, manipulação, esquiva e compromisso. A autora concluiu que a organização que estudou não sofreu pressões miméticas.

A fim de compreender como os bancos respondem às pressões institucionais, Lundberg (2013) argumenta que as organizações interpretam as pressões que sofrem, e a depender de como fazem isso, incorporam mudanças em seus sistemas de gestão de desempenho, afetando estratégias, estrutura organizacional, procedimentos e sistemas, ações de treinamento e desenvolvimento, além da cultura organizacional. Ao mesmo tempo, o autor sustenta que esses sistemas de gestão de desempenho também influenciam as respostas organizacionais, e que a organização também pressiona o ambiente, a depender de como responde, mostrando que as pressões não são unidirecionais.

A adoção de práticas de gestão ambiental como resposta a pressões institucionais foi estudada por Borges, Dutra e Scherer (2014). Os autores utilizaram a tipologia de Oliver (1991) e concluíram que essas práticas de gestão são adotadas devido a pressões do Governo e dos consumidores. Os autores concluem que as pressões coercitivas levam as organizações a responderem com aquiescência, principalmente através de imitação devido a incertezas e à dependência que elas têm dos órgãos de regulação e fiscalização. Essa dependência faz com

que as organizações busquem manter um bom relacionamento com os órgãos de fiscalização das suas atividades, segundo os autores.

Alguns estudos que aplicaram as respostas estratégicas às pressões institucionais propostas por Oliver (1991) abordam organizações com estrutura descentralizada tanto administrativamente quanto geograficamente. Essas organizações têm funções internas diferenciadas, sofisticadas e especializadas, com suas próprias estruturas de poder e algum controle sobre as atividades, como no conceito de organizações complexas de Mechanic (1962) e Perrow (1993). Essas organizações são compreendidas como sistemas abertos a influências do ambiente, formados por entidades autônomas (suas subunidades organizacionais), interconectadas de diferentes maneiras e com diferentes intensidades, conforme Fontana e Iarozinski Neto (2009). As respostas estratégicas das subunidades de organizações com estrutura descentralizada é o tópico abordado a seguir.

2.7 O COMPORTAMENTO DAS SUBUNIDADES ORGANIZACIONAIS FRENTE ÀS PRESSÕES INSTITUCIONAIS

As respostas estratégicas de Oliver (1991) permitem explicar não só o comportamento das organizações, mas também das suas subunidades organizacionais. Por estar submetida a pressões institucionais, a administração central de uma organização pode buscar a conformidade com essas pressões. Segundo Boschman (2006), as pressões institucionais para que organizações multinacionais adotem condutas coerentes com políticas internacionais e locais de direitos humanos as levam a responderem buscando a conformidade através da formalização de códigos de conduta próprios, que a princípio precisam ser respeitados por suas unidades descentralizadas. Osmundsen (2005) enfatiza que, por estar exposta a regras, normas e crenças provenientes do seu próprio ambiente institucional, a administração central de uma organização pode difundi-las para suas subunidades organizacionais. Boschman (2006) conclui que as subunidades dessas organizações respondem com aquiescência, através de táticas de conformidade ou imitação das práticas adotadas por outras organizações do mesmo ambiente institucional. Além disso, uma parte dessas organizações responde às pressões que sofrem imitando o comportamento das outras organizações, o que também configura uma estratégia de aquiescência. Outro comportamento comum observado pela autora é a esquiva através da tática de ocultação, que se apresenta por

meio de uma aparente conformidade demonstrada em códigos de conduta formalizados, mas que não são operacionalizados.

Além das respostas estratégicas propostas por Oliver (1991), Boschman (2006) identificou também a cooperação, que fora apresentada por Tsai e Child (1997) e que envolve a definição de objetivos comuns e a resolução conjunta de problemas. A partir das perspectivas institucional, da dependência de recursos e da escolha estratégica, Tsai e Child (1997) propuseram uma adaptação ao modelo de Oliver (1991) para estudar como organizações multinacionais mudam seu comportamento diante das pressões ambientais para que adotem práticas de gestão ambiental. A cooperação, segundo os autores, é um meio para garantir que organizações diferentes alcancem seus objetivos ao longo prazo ao invés de tentar alcançá-los individualmente em curto prazo. Assim, a cooperação entre as organizações e as fontes de pressão institucional pode levá-las a atender de forma mais eficaz às expectativas institucionais, especialmente quando estão dispostas a contribuir com seus conhecimentos tecnológicos em prol do alcance dos objetivos comuns.

As pressões institucionais incidem também sobre as unidades descentralizadas das organizações. Osmundsen (2005) argumenta que as unidades de negócio de organizações com estrutura descentralizada sofrem múltiplas influências institucionais e que, devido a isso, são confrontadas com pressões conflitantes. A autora utilizou a tipologia de respostas estratégicas para analisar as dificuldades de integração entre unidades de negócio diferentes em um processo de internacionalização de operações de uma organização. As subsidiárias de uma organização com estrutura descentralizada podem estar localizadas em regiões diferentes, podem ter interesses distintos e precisam buscar legitimidade entre constituintes dos diferentes ambientes institucionais, além de sofrerem pressões que têm origem não só na sua administração central (ambiente institucional pai), mas também de seus respectivos e diferentes ambientes institucionais (ambientes institucionais locais) e do ambiente institucional global, que incide sobre a organização como um todo. As estruturas e processos organizacionais das subsidiárias, consequentemente, são desenhados por diferentes pressões desses múltiplos ambientes institucionais e podem responder a essas pressões de diferentes formas. Os resultados obtidos pela autora confirmam os de Kostova e Zaheer (1999), que identificaram que as subunidades organizacionais precisam ter legitimidade interna enquanto parte de uma organização maior, o que se soma à necessidade de ter legitimidade no seu próprio ambiente institucional.

Tempel *et al*. (2006) notaram que, ao responderem às pressões tanto da sua matriz quanto do seu ambiente, as subsidiárias utilizaram toda a gama de respostas estratégicas apresentadas por Oliver (1991) para adotar práticas de recursos humanos, incluindo o desafio aos requisitos da sua administração central e a manipulação. Para os autores, a resposta variou a depender das diferenças entre os domínios institucionais locais e os das respectivas matrizes, e também conforme aumenta ou diminui a dependência que as subsidiárias têm do ambiente institucional e da administração central.

Pache e Santos (2010) criticam os modelos de respostas estratégicas demonstrando que esses tratam as organizações como entidades unitárias que respondem estrategicamente às pressões externas, ignorando o papel da dinâmica intraorganizacional. A partir do modelo de Oliver (1991), os autores propõem que a natureza das demandas e a representação interna dentro das organizações afetam a mobilização das diferentes estratégias quando as organizações são confrontadas por demandas institucionais conflitantes. Segundo os autores, a natureza das demandas institucionais é determinada pela sua relação com os meios ou os fins: quando as pressões incidem sobre práticas e processos, sua natureza é de nível funcional; quando incidem sobre objetivos e metas organizacionais, são de nível ideológico.

Na visão de Pache e Santos (2010), a natureza dos conflitos institucionais interage com suas representações internas para influenciar as estratégias organizacionais. Dessa forma, os autores reforçam o entendimento de que as respostas organizacionais às pressões institucionais dependem do comportamento das suas subunidades. O modelo de Pache e Santos (2010) é comparado à tipologia de Oliver (1991) por Gutiérrez-Rincón (2014), que conclui que o primeiro complementa o segundo, tornando-o mais operacional. Entretanto, nota-se que Pache e Santos (2010) não incluem a aquiescência como resposta em seu modelo, pois esta não é possível em situações de pressões conflitantes, como argumentam.

Segundo Osmundsen (2005), os estudos que abordam o relacionamento entre sede e subunidades organizacionais tendem a destacar a influência da primeira sobre as outras, mas a autora argumenta que há razão para esperar que também haja influência das subunidades sobre sua administração central. Embora não tenham utilizado a tipologia de Oliver (1991), outros trabalhos reforçam o entendimento de que as pressões externas incidem sobre subunidades organizacionais e que essas respondem de maneiras distintas.

Delmas e Toffel (2008), por exemplo, consideram que as respostas organizacionais às pressões institucionais para adoção de práticas de gestão refletem não somente diferentes pressões, mas também diferentes influências internas oriundas das suas subunidades organizacionais. Segundo estes autores, as pressões de diferentes constituintes do ambiente institucional podem penetrar nas organizações não só por suas matrizes, mas também através de seus departamentos. Considerando que as subunidades organizacionais têm interesses específicos, as diferentes pressões institucionais incidem sobre elas de maneiras distintas, e suas respostas podem ser também distintas, esclarecem os autores.

Hernes e Erdvik (2014) salientam que a autonomia das subunidades organizacionais pode levá-las a julgarem determinadas políticas adotadas por instâncias decisórias superiores como mais ou menos eficientes, como barreiras ao cumprimento de suas metas ou mesmo como políticas puramente simbólicas, e consequentemente pode levá-las a adotarem comportamentos distintos daqueles esperados por quem formalizou as políticas.

Segundo Netland e Aspelund (2014), ainda que a sede da organização busque e defenda a adoção de políticas gerenciais tidas como necessárias por suas subunidades, isso não significa que essas políticas serão eficientes em todas elas, o que pode levá-las a responderem às pressões que sofrem da sede de maneiras distintas.

Esses estudos mostram que as subunidades organizacionais estão sujeitas a pressões do ambiente institucional e das suas respectivas matrizes para adotarem práticas administrativas. Considerando sua autonomia, ainda que limitada, essa situação enseja investigar como as subunidades respondem a essas pressões. A aplicação da tipologia de respostas estratégicas à adoção de TI e de práticas de gestão de Sistemas de Informação será abordada a seguir.

2.8 RESPOSTAS ESTRATÉGICAS ÀS PRESSÕES PARA ADOÇÃO DE TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO

A realização de estudos sobre a adoção de TI pelas organizações a partir da ótica da Teoria Institucional – portanto, como consequência de forças ambientais que afetam o comportamento e a tomada de decisões organizacionais – permite compreender além da adoção, difusão e uso da tecnologia, também sua rejeição (STANDING; SIMS; LOVE, 2009).

Como uma extensão da Teoria Institucional, a tipologia de Oliver (1991) já foi utilizada também em trabalhos na área temática de Sistemas de Informação visando explicar o comportamento organizacional frente às pressões para adoção de tecnologia, mas Mignerat e Rivard (2009) notaram que o foco desses trabalhos é principalmente na estratégia de aquiescência e, mais especificamente, na tática de conformidade, de maneira que tem havido pouca atenção a estratégias de compromisso, manipulação e esquiva, que as autoras também consideram possíveis ao tratar de adoção e implantação de TI.

Apesar disso, outros trabalhos mostram que as organizações podem responder de outras maneiras também. Armênio Neto e Machado-da-Silva (2009) estudaram a substituição de uma tecnologia mais antiga por outra em uma organização que atua no mercado de telefonia. Para isso, os autores utilizaram o processo de desinstitucionalização (OLIVER, 1992) e a tipologia de respostas estratégicas (OLIVER, 1991) para analisar como aconteceu a institucionalização de uma tecnologia e a desinstitucionalização da outra. Os autores concluíram que, sob pressões institucionais distintas, diferentes respostas estratégicas foram adotadas: esquiva, através da fuga da necessidade de adotar a nova tecnologia; compromisso, através da tática de equilíbrio, que permitiu a manutenção das duas tecnologias paralelamente; e aquiescência por conformidade, com a aceitação da nova tecnologia e a finalização dos investimentos na tecnologia mais antiga. Com isso, mostraram que, para uma mesma situação, as pressões institucionais mudam com o tempo e podem levar a respostas distintas.

Ao estudarem a adoção e rejeição de tecnologia, Standing, Sims e Love (2009) assumem que as respostas às pressões institucionais podem mudar com o passar do tempo. Os autores utilizam os pilares institucionais de Scott (2008) para argumentar que as respostas estratégicas podem variar com o tempo, a depender do escopo (pessoal, organizacional, local, global ou sobre o sistema), do tipo (normativa, regulatória ou cultural-cognitiva), do nível de influência das autoridades que exercem as pressões institucionais (externa ou interna) e de antecedentes identificados no artigo de Oliver (1991): o nível de autoridade que exerce as pressões; a consistência da tecnologia com os objetivos organizacionais; os níveis de controle existentes no ambiente institucional; a incerteza existente no ambiente institucional; a dependência da organização para com outros constituintes do ambiente institucional; a quantidade de constituintes do ambiente institucional; a multiplicidade de demandas institucionais; e a eficiência da tecnologia.

A pesquisa de Standing, Sims e Love (2009) mostrou que as organizações são pressionadas a adotarem determinada tecnologia e que respondem inicialmente com

aquiescência, mas que não necessariamente vão permanecer em conformidade, podendo evoluir para uma estratégia de compromisso ou manipulação, e posteriormente para esquiva, compromisso ou manipulação. O estudo mostrou que essa evolução pode acompanhar a mudança do comportamento da manipulação em direção à aquiescência, em uma aceitação crescente, ou indo da aquiescência para a manipulação, em uma resistência crescente, como é possível inferir a partir do contínuo de respostas estratégicas. Os autores identificaram um padrão de crescente não conformidade, que envolve uma aquiescência inicial devido a pressões regulatórias e culturais-cognitivas e a pressões internas, seguida de um compromisso devido a limitações e problemas técnicos apresentadas pelo sistema adotado, e finalmente com uma resposta de esquiva, devido às mesmas limitações e problemas apresentados. A aquiescência inicial pode também dar lugar a uma resposta de compromisso, devido às limitações apresentadas pelo sistema, e posteriormente a um comportamento de manipulação, o que configura outro padrão de resistência crescente. Standing, Sims e Love (2009) identificaram ainda um padrão que parte de uma resposta de aquiescência, mas que é seguida de manipulação devido às incertezas causadas pelos problemas apresentados pelo sistema e, no último momento, de uma resposta de compromisso, demonstrando que os padrões de respostas estratégicas não necessariamente são de resistência crescente.

A tecnologia adotada e questões relacionadas a sua eficiência, seus problemas ou a sua adequação às atividades desenvolvidas na organização foram a maior razão para as respostas de compromisso, segundo Standing, Sims e Love (2009). Os autores concluíram também que laços institucionais fracos fizeram com que as subunidades organizacionais desafiassem abertamente o uso da tecnologia adotada pela sua administração central, pois não havia temor quanto às consequências do descumprimento, configurando o desafio como um padrão de comportamento. Os autores complementaram que a má qualidade do sistema (como problemas técnicos e de usabilidade) legitimou a resistência e que a adoção foi resultado do alinhamento entre as camadas de autoridade institucional (que exercem as pressões internamente e externamente).

A tipologia de Oliver (1991) já foi aplicada também em trabalhos sobre adoção de práticas de gestão de Sistemas de Informações. Aier e Weiss (2012) abordaram a gestão de arquitetura organizacional como uma disciplina que apoia os programas de transformação nas organizações. Com base na tipologia de Oliver (1991), os autores argumentam que o sucesso da implementação das transformações previstas em um programa baseado em práticas de gestão de arquitetura organizacional depende de como as pressões institucionais internas e

externas são compreendidas e de quais estratégias as organizações utilizam em resposta a essas pressões.

Embora não tenham sido identificados na bibliografia consultada trabalhos sobre Segurança da Informação que utilizam a tipologia de Oliver (1991), foram encontrados dois artigos que tratam de privacidade. Cabe registrar que a privacidade não deve ser confundida com Segurança da Informação. O conceito de privacidade depende do contexto e varia com as experiências de vida dos indivíduos, segundo Xu *et al*. (2008). Sheenan e Hoy (2000) complementam que a privacidade está relacionada a garantias quanto aos dados e informações pessoais e que tem os seguintes princípios: a consciência sobre as informações a seu respeito e sobre como estas são utilizadas; a escolha, que trata da possibilidade de o indivíduo escolher quanto ao uso e à divulgação das suas informações pessoais; o acesso, que garante ao indivíduo o acesso às suas informações pessoais; a segurança, que trata da garantia de que as informações privadas são guardadas de maneira segura; e o recurso, que dá ao indivíduo o direito de recorrer quanto a violações à sua privacidade. Segurança da Informação, por sua vez, tem como princípios clássicos a confidencialidade, a integridade e a disponibilidade da informação, como já discutido neste trabalho. Apesar de ser possível tratar de segurança em um estudo sobre privacidade ou de privacidade em um estudo sobre Segurança da Informação, não cabe tratá-los como sinônimos, mas aceitar que há interseções entre esses dois temas.

Dento dessa perspectiva, Greenaway e Chan (2005) realizaram um estudo bibliográfico sobre privacidade nas organizações buscando identificar uma lacuna de pesquisa através da análise de trabalhos sobre o tema. Os autores apresentaram as respostas estratégicas de Oliver (1991) como uma maneira dentro da abordagem institucional para investigar as respostas organizacionais às pressões institucionais, considerando que as organizações precisam gerenciar suas atividades técnicas em oposição às exigências do ambiente institucional.

Parks e Wigand (2014) citam Bélanger e Crossler (2011), Pavlou (2011) e Smith, Dinev e Xu (2011) para justificar a necessidade de estudar como as pressões institucionais e os tipos estratégicos organizacionais estão impactando nas estratégias adotadas pelas organizações em resposta às ameaças à sua privacidade. Os autores se baseiam na ideia de Culnan e Williams (2009) de que a necessidade de garantir a privacidade permite outras respostas organizacionais além da conformidade e resistência. Utilizando as cinco respostas estratégicas propostas por Oliver (1991) e os quatro tipos organizacionais de Miles e Snow

(1978), que caracterizam as organizações quanto à capacidade de se ajustarem ao ambiente (prospectoras, defensivas, analíticas e reativas), os autores propõem um modelo que permite classificar as organizações a partir das estratégias que adotam em resposta aos riscos à privacidade de informações.

Os trabalhos que utilizam as respostas estratégicas de Oliver (1991), tanto do campo da Administração quanto de Sistemas de Informação, mostram que as organizações podem responder de diferentes maneiras às pressões institucionais tanto para adoção de tecnologias (GRAEFF, 2005; STANDING; SIMS; LOVE, 2009; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009) quanto de práticas de gestão (WAHYUDI, 2004; FREZATTI; AGUIAR; REZENDE, 2007; AIER; WEISS, 2012; LUNDBERG, 2013; BORGES; DUTRA; SCHERER, 2014; GUTIÉRREZ-RINCÓN, 2014; PARKS; WIGAND, 2014). A partir desses trabalhos e de outros sobre respostas estratégicas às pressões institucionais, Teoria Institucional e Segurança da Informação, foram construídas as proposições da pesquisa e identificados os indicadores utilizados na sua operacionalização.

3 PROPOSIÇÕES E *FRAMEWORK* DE PESQUISA

A adoção de medidas de Segurança da Informação pelas organizações pode acontecer em resposta a diferentes pressões do ambiente externo. Trabalhos anteriores mostram que as pressões para adoção vêm de diferentes organizações, como organizações governamentais de regulação e controle, organizações que financiam as atividades desenvolvidas no ambiente institucional, órgãos nacionais e internacionais de normatização que publicam modelos e padrões de Segurança da Informação, profissionais de TI e Segurança da Informação e outras organizações de destaque no ambiente institucional.

As pressões institucionais se apresentam nas formas de leis e regulamentos, auditorias e fiscalizações de conformidade (coercitivas), publicações de normas, padrões e modelos de Segurança da Informação e a difusão de experiências e conhecimentos entre os profissionais que atuam nessa área (normativas), além da imitação de organizações de prestígio do mesmo ambiente institucional (miméticas) e podem incidir em conjunto ou isoladamente, influenciando o comportamento organizacional quanto à Segurança da Informação (LUESEBRINK, 2011; HSU; LEE; STRAUB, 2012; LOPES, 2012; NASUTION, 2012; KAM *et al*., 2013; SPEARS; BARKI; BARTON, 2013; TEJAY; BARTON, 2013; ANTHONY; APPARI; JOHNSON, 2014; LOPES; SÁ-SOARES, 2014; ALKALBANI; DENG; KAM, 2014, 2015; ALBUQUERQUE JUNIOR; SANTOS, 2015; CAVUSOGLU *et al*., 2015; ALBUQUERQUE JUNIOR *et al*., 2016).

Em resposta às pressões do ambiente, as organizações elaboram políticas e regulamentos para influenciar o comportamento das suas subunidades organizacionais (OSMUNDSEN, 2005; DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014; PILATO; PEDRINI, 2015). Nesse sentido, a literatura tem exemplos de trabalhos que mostram a formalização de regulamentos e políticas de Segurança da Informação para atender a requisitos externos (BJÖRCK, 2004; LUESEBRINK, 2011; LOPES, 2012; NASUTION, 2012; LOPES; SÁ-SOARES, 2014; ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016).

Da mesma forma que a administração central de uma organização sofre pressões institucionais, suas subunidades também sofrem pressões dos ambientes nos quais estão inseridas. Além disso, a administração central pressiona suas subunidades a se comportarem de acordo com seus interesses através da formalização de políticas e regulamentos internos

(HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003; OSMUNDSEN, 2005; TEMPEL *et al*., 2006; DELMAS; TOFFEL, 2008; AGUILERA-CARACUEL *et al*., 2012; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014; PILATO; PEDRINI, 2015). Dessa forma, as subunidades organizacionais estão sujeitas a pressões tanto dos seus respectivos ambientes institucionais quanto da administração central.

A visão de que tanto a administração central quanto o ambiente institucional pressionam as subunidades leva à compreensão de que estas estão sujeitas a diferentes pressões institucionais, até porque, como sustentam Delmas e Toffel (2008), as pressões que incidem sobre a administração central podem ser diferentes das que incidem sobre suas subunidades. Segundo estes autores, matriz e subunidades se envolvem com conjuntos diferentes de constituintes do ambiente institucional, o que as expõem a demandas institucionais diferentes e as leva a responder de diferentes maneiras às pressões.

As políticas formalizadas pela administração central são uma importante fonte de pressão institucional sobre as subunidades organizacionais, cujas respostas vão variar a depender da autonomia e da necessidade de legitimar-se na organização e no ambiente, segundo Pilato e Pedrini (2015).

Para Boxenbaum e Jonsson (2009), os mitos institucionalizados no ambiente podem não ser considerados eficientes e podem ser simultâneos e contraditórios. Netland e Aspelund (2014) concordam que as pressões institucionais sobre as subunidades organizacionais podem ser conflitantes e obrigar as subunidades a adotarem praticas percebidas como ineficientes, o que as leva a se comportarem de maneiras distintas ao serem confrontadas por essas pressões.

Para Boschman (2006), sob diferentes pressões institucionais (tanto do ambiente quanto da matriz da organização), as subunidades respondem utilizando diferentes estratégias, como aquiescência, conformidade, esquiva, ou mesmo cooperando com as fontes de pressão institucional, como proposto por Tsai e Child (1997).

As decisões tomadas pelas subunidades organizacionais são descentralizadas e baseadas em interesses e julgamentos próprios sobre a necessidade de adotar práticas em conformidade com as políticas corporativas e de acordo com suas próprias percepções a respeito da sua eficácia, segundo Hernes e Erdvik (2014).

Esse comportamento leva a inferir que as subunidades organizacionais, ao serem pressionadas a adotar medidas de Segurança da Informação, respondem tendo em vista seus

próprios interesses e julgamentos, utilizando diferentes respostas estratégicas. Ao sofrerem pressões institucionais, as subunidades organizacionais podem, portanto, responder com aquiescência, compromisso, esquiva, desafio ou manipulação, segundo a tipologia de Oliver (1991). A cooperação identificada por Tsai e Child (1997) pressupõe que a subunidade buscou a conformidade tanto com sua matriz quanto com outras fontes de pressão, sendo, portanto, uma forma de responder com aquiescência, motivo pelo qual não foi contemplada neste estudo. Assim, a aquiescência, como proposto por Oliver (1991), seria a resposta de consentimento e aceitação passiva dos requisitos de Segurança da Informação do ambiente institucional. Se a subunidade organizacional percebe esses requisitos de Segurança da Informação como fatos tidos como certos e a adoção das medidas acontece de maneira inconsciente, houve a adoção por hábito. Se as medidas adotadas foram copiadas de outras organizações ou subunidades da mesma organização (conscientemente ou inconscientemente), a adoção aconteceu através de imitação. Se a incorporação das medidas de Segurança da Informação aconteceu de forma consciente, visando à obtenção de apoio social ou recursos da sede ou de outros constituintes do ambiente institucional, a subunidade utilizou a tática de conformidade.

Se foram adotadas pela subunidade apenas as medidas consideradas adequadas às suas atividades e objetivos, a estratégia utilizada foi o compromisso, como explica Oliver (1991). Pelo fato de parte das medidas de Segurança da Informação ser rígida ou restritiva, como destacam Karyda, Kiountouzis e Kokolakis (2005) e Ellwanger (2009), é de se esperar que algumas sejam consideradas conflitantes ou inconsistentes com os objetivos e atividades das subunidades organizacionais. Neste caso, a subunidade pode acomodar as expectativas conflitantes com seus interesses e objetivos ou inconsistentes entre si, ajustando a implantação das medidas ao ponto de não haver o descumprimento total, o que caracteriza uma tática de equilíbrio. Se a subunidade se esforça para minimizar essas pressões conflitantes enquanto há uma compreensão de que é necessário respeitá-las, adotando parte das medidas exigidas e rejeitando outras, a tática utilizada é de pacificação. A barganha acontece quando a subunidade negocia com sua administração central ou com os constituintes do ambiente institucional o nível de conformidade exigido ou o momento em que deve estar em conformidade, tanto devido à incapacidade de adotar as medidas naquele momento quanto por incompatibilidade das medidas com seus objetivos e atividades.

A subunidade pode também buscar evitar a conformidade com os requisitos de Segurança da Informação da sua sede e do ambiente institucional através da esquiva, resposta

que tem como táticas previstas por Oliver (1991) a ocultação, o amortecimento e a fuga. A ocultação pode ocorrer através da implantação de tecnologias sem as configurações necessárias, ou sem executar as ações necessárias para seu funcionamento como previsto na política ou nos regulamentos de Segurança da Informação da organização, ou através da formalização de regulamentos previstos na Política de Segurança da Informação sem que seu cumprimento seja cobrado, causando a dissociação entre a política organizacional e as práticas adotadas nas subunidades, como argumentam Björck (2004), Lopes e Sá-Soares (2014) e Lapke e Dhillon (2015). Assim, a ocultação é uma forma de a subunidade estar intencionalmente em conformidade cerimonial com os requisitos da administração central e do ambiente institucional.

A tática de amortecimento significa que a subunidade busca reduzir o quanto a sua sede ou outras organizações controlam, avaliam ou inspecionam suas atividades de Segurança da Informação, mantendo um distanciamento com relação às fontes de pressão institucional, tanto escondendo da sede e dos órgãos de fiscalização a ocorrência de incidentes de Segurança da Informação, como descrito por Dhillon (2001), quanto escondendo quais medidas adotou e quais ainda precisa adotar para estar em conformidade. A fuga é uma tática cuja exemplificação é mais difícil em se tratando de subunidades organizacionais, pois elas têm uma aparente dificuldade em mudar suas atividades, seus objetivos ou o domínio no qual sofrem pressões institucionais, visto que estão diretamente ligadas a uma organização maior e têm sua discricionariedade limitada. No entanto, argumenta-se que uma subunidade pode deixar de participar de iniciativas da sua administração central ou de outras organizações, fugindo, por exemplo, de um projeto ou não adotando tecnologias por não haver possibilidade, tanto por incapacidade quanto por inconsistência das medidas com outras atividades desenvolvidas ou com seus objetivos.

Se a subunidade responder rejeitando de forma inequívoca os requisitos de Segurança da Informação formalizados pela administração central ou do ambiente institucional, sua estratégia é o desafio, que é associado à falta de controle por parte das autoridades internas e externas que exercem as pressões institucionais, à multiplicidade de demandas e à percepção de que as medidas não são eficientes, segundo Standing, Sims e Love (2009). Com base nas táticas propostas por Oliver (1991), a subunidade pode: rejeitar as medidas, ignorando os requisitos da sede e do ambiente externo, como a própria Política de Segurança da Informação da organização, tecnologias, modelos e padrões utilizados no mercado e leis e regulamentos governamentais; contestar ativamente os requisitos de

Segurança da Informação do ambiente e da administração central, criticando-os por não serem considerados eficientes ou por serem restritivos demais; atacar os requisitos de Segurança da Informação ou os constituintes do ambiente institucional que a pressionam, adotando uma postura agressiva contra leis, regulamentos, tecnologias, fabricantes, fornecedores, membros do Comitê ou a Política de Segurança da Informação. Assim, argumenta-se que a ausência de cobranças ou restrições por não estar em conformidade com as exigências de Segurança da Informação, a baixa autoridade das fontes de pressão institucional ou a existência de exigências inconsistentes ou percebidas como ineficientes pode levar as subunidades a responderem desafiando as pressões ou as fontes de pressão.

A resposta mais ativa de resistência é a manipulação, que está associada à baixa autoridade das fontes de pressão institucional, à multiplicidade de demandas institucionais, à baixa eficiência percebida dos requisitos do ambiente institucional e à baixa incerteza quanto às consequências da não conformidade (STANDING; SIMS; LOVE, 2009). As táticas que levam à resposta de manipulação são cooptação, influência e controle (OLIVER, 1991). Ao ser pressionada a adotar medidas de Segurança da Informação, uma subunidade organizacional pode cooptar membros influentes da sua administração central ou constituintes do ambiente institucional para participar das suas decisões sobre Segurança da Informação, não com a intenção de estar em conformidade, mas buscando neutralizar as pressões que esses exercem. A subunidade pode também utilizar seu prestígio sobre a sede ou mesmo sobre o ambiente institucional para influenciar os constituintes a mudarem os requisitos de Segurança da Informação conforme suas necessidades ou mudarem critérios de conformidade. Por fim, o poder sobre as fontes de pressão institucional pode dar à subunidade organizacional oportunidade para controlá-las em benefício próprio, mudando os requisitos de Segurança da Informação conforme seus próprios interesses ou fazendo com que as medidas exigidas as beneficiem. O Quadro 5 mostra a associação entre as respostas de Oliver (1991) e exemplos no contexto da Segurança da Informação.

Anthony, Appari e Johnson (2014) notaram que pressões de diferentes ambientes institucionais podem resultar em diferenças quanto à conformidade com os requisitos institucionais de Segurança da Informação, o que apoia a ideia de que pressões institucionais distintas levam a respostas organizacionais distintas quanto à Segurança da Informação. Além disso, a compreensão de que a conformidade depende do quanto os requisitos institucionais são julgados eficientes é amparada pelos argumentos de Hu, Hart e Cooke (2007), para quem

o comportamento de resistência às pressões institucionais para adoção de medidas de Segurança da Informação pode ser motivado pela busca pela eficiência.

Quadro 5 – Respostas às pressões para adoção de medidas de Segurança da Informação.

ESTRATÉGIAS	TÁTICAS	EXEMPLOS EM SEGURANÇA DA INFORMAÇÃO
Aquiescência	Hábito	Adotar medidas percebidas como indiscutivelmente necessárias para garantir a Segurança da Informação na organização.
	Imitação	Copiar conscientemente ou inconscientemente medidas adotadas por outras organizações ou subunidades da mesma organização.
	Conformidade	Adotar medidas conscientemente para obter apoio ou recursos da organização ou de constituintes do ambiente institucional.
Compromisso	Equilíbrio	Adotar medidas que são conflitantes entre si, equilibrando inconsistências existentes através de ajustes na implementação.
	Pacificação	Minimizar pressões inconsistentes com os interesses e objetivos da subunidade através da adoção parcial das medidas.
	Barganha	Negociar a quantidade de medidas a serem adotadas e o prazo para adoção, sem rejeitá-las.
Esquiva	Ocultação	Implantar tecnologias sem atender aos requisitos de Segurança da Informação, ou formalizar políticas e regulamentos sem que isso resulte em mudanças nas práticas do dia a dia.
	Amortecimento	Reduzir a sujeição da subunidade ao controle ou inspeção da sede ou dos constituintes do ambiente institucional, escondendo o quanto está em conformidade e a ocorrência de incidentes.
	Fuga	Não executar ou aderir a projetos que impliquem na adoção de medidas que a subunidade não pretende ou não pode adotar.
Desafio	Rejeição	Ignorar deliberadamente a Política de Segurança da Informação, normas, padrões e a legislação que exigem a adoção, além de tecnologias utilizadas.
	Contestação	Criticar a eficiência ou a rigidez das medidas ou da Política de Segurança da Informação.
	Ataque	Atacar leis, regulamentos, modelos, tecnologias, constituintes do ambiente institucional, o Comitê e a Política de Segurança da Informação.
Manipulação	Cooptação	Fazer com que pessoas da administração central ou constituintes do ambiente institucional participem das decisões da subunidade.
	Influência	Utilizar o prestígio que tem para alterar requisitos e critérios de conformidade de acordo com suas necessidades.
	Controle	Utilizar o poder que tem para controlar a administração central ou constituintes do ambiente institucional em benefício próprio,

Fonte: elaborado pelo autor

A possibilidade de as subunidades responderem de diferentes maneiras às pressões institucionais para adoção de medidas de Segurança da Informação conduz à primeira proposição deste trabalho:

Proposição 1: As subunidades organizacionais respondem às pressões institucionais através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre a eficiência e adequação das medidas de Segurança da Informação.

As subunidades organizacionais podem responder de maneiras distintas às diferentes pressões que recebem porque as respostas atendem às necessidades e interesses das próprias subunidades, em detrimento das necessidades e interesses da administração central da organização (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014), ou porque as pressões são conflitantes com os objetivos e necessidades organizacionais (BOXENBAUM; JONSSON, 2009; NETLAND; ASPELUND, 2014), ou mesmo porque são contraditórias entre si (BOXENBAUM; JONSSON, 2009), um comportamento relacionado à autonomia e à necessidade de legitimar-se tanto em seu ambiente institucional quanto perante sua matriz (PILATO; PEDRINI, 2015).

Os trabalhos que investigam as respostas organizacionais às pressões para adoção de tecnologias ou de práticas de gestão de TI mostram que essas respostas vão depender do tipo de pressão institucional (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009; STANDING; SIMS; LOVE, 2009) e da percepção sobre essas pressões quanto a sua eficiência e utilidade (AIER; WEISS, 2012).

Medidas técnicas de Segurança da Informação são basicamente recursos tecnológicos e barreiras físicas, medidas formais são políticas, regulamentos e processos de gestão, e medidas informais são ações de conscientização, divulgação e educação. Sabe-se que medidas técnicas e informais são adotadas principalmente devido a pressões normativas, e que medidas formais são adotadas devido a pressões coercitivas (ALBUQUERQUE JUNIOR *et al*., 2016). A adoção de medidas técnicas é realizada principalmente por subunidades ou grupos de profissionais responsáveis por desenvolver atividades mais técnicas de Segurança da Informação, e as decisões sobre adoção de medidas formais e informais são tomadas pelos responsáveis por decisões de gestão ou governança de Segurança da Informação (SÊMOLA, 2014). No entanto, ao tomar decisões sobre adoção, deve-se considerar a interdependência entre as medidas informais, formais e técnicas (DHILLON, 1999; SVEEN; TORRES; SARRIEGI, 2009), o que pode ser dificultado pelo fato de grupos diferentes estarem responsáveis por medidas técnicas, formais e informais.

Considerando que pressões diferentes levam a respostas diferentes e que categorias de medidas de Segurança da Informação distintas são responsabilidades de grupos diferentes dentro das organizações, espera-se que as pressões para adoção de medidas formais, informais e técnicas resultem em diferentes respostas estratégicas, conforme os interesses e as percepções das subunidades sobre as pressões que sofrem. Assim, fica estabelecida a segunda proposição da tese:

Proposição 2: Pressões para adoção de medidas formais, medidas informais e medidas técnicas vão resultar em diferentes respostas estratégicas, para cada categoria de medida, por parte das subunidades organizacionais.

Para Osmundsen (2005) e Delmas e Toffel (2008), o comportamento das subunidades organizacionais influencia suas matrizes. De acordo com Hernes e Erdvik (2014), a conformidade ou não conformidade organizacional depende de decisões tomadas de maneira descentralizada pelas subunidades organizacionais, com base em seus próprios interesses e julgamentos. Dessa forma, as práticas previstas na política e nos regulamentos formalizados pela sede podem ser consideradas ineficientes pelas subunidades organizacionais, de acordo com Netland e Aspelund (2014). Como têm alguma autonomia administrativa e precisam legitimar-se na organização à qual pertencem e em seus respectivos ambientes institucionais, as respostas das subunidades às pressões – por vezes conflitantes – podem variar, complementam Pilato e Pedrini (2015).

O comportamento esperado pela administração central da organização é a conformidade das subunidades com seus requisitos de Segurança da Informação, o que põe a organização em conformidade com os requisitos do ambiente institucional. Mas pode ocorrer que a adoção das práticas reconhecidas como eficientes pela administração central não aconteça em todas as subunidades, mesmo que a sede da organização busque e defenda a adoção, como argumentam Netland e Aspelund (2014). Nesse sentido, Boschman (2006) e Aguilera-Caracuel *et al*. (2012) entendem que as diferentes respostas das subunidades podem prejudicar as tentativas de padronização de práticas em uma organização.

Da mesma forma que a conformidade das subunidades resulta na conformidade da organização, ao responderem às pressões para adotar medidas de Segurança da Informação atendendo aos seus próprios interesses, as subunidades podem pôr a organização em uma situação de dissociação entre a política e prática, pois podem não adotar as medidas previstas e, consequentemente, não atender aos requisitos presentes nos regulamentos e na Política de Segurança da Informação da administração central (BJÖRCK, 2004; LOPES; SÁ-SOARES, 2014; LAPKE; DHILLON, 2015), ainda que eles tenham sido criados com a intenção de estar em conformidade (NETLAND; ASPELUND, 2014). Nesse contexto, a dissociação entre as medidas adotadas e a Política de Segurança da Informação pode ser uma decorrência de respostas de esquiva ou desafio, pois essas estratégias caracterizam uma adoção apenas aparente ou a rejeição. Assim, a organização pode ficar em conformidade cerimonial com os requisitos do ambiente institucional. Neste caso, é conveniente esclarecer que, de forma

diferente da prevista por Meyer e Rowan (1977), a conformidade cerimonial não é resultado de uma decisão racional da administração central da organização, mas do fato de parte das subunidades não estar em conformidade.

Além do efeito indireto do conjunto das respostas, a influência sobre a administração central pode ser também uma consequência direta da resposta estratégica da subunidade. Se em resposta às pressões institucionais, uma subunidade adota uma estratégia de manipulação, através das táticas de cooptação, influência ou controle sobre as fontes de pressão, é possível que mude a maneira como as pressões são exercidas sobre a subunidade ou mesmo sobre a organização, visto que, segundo Oliver (1991), a cooptação é uma tática que visa à redução da incidência ou dos efeitos da pressão institucional sobre a organização, enquanto a influência envolve o uso do prestígio sobre as fontes de pressão institucional para alterar requisitos externos para atender aos interesses organizacionais, e o controle é uma tática que envolve a utilização do poder para controlar o ambiente e as pressões institucionais em benefício próprio.

Considerando a ideia de conformidade com os requisitos externos de Segurança da Informação como sendo a aderência ou demonstração de aderência a padrões, regulamentos e exigências legais (MAYNARD; RUIGHAVER, 2006; AL-HAMDANI, 2011) e a obediência ou incorporação desses requisitos externos à organização (OLIVER, 1991), tem-se que as diferentes respostas das subunidades podem pôr a organização em conformidade cerimonial ou mesmo em não conformidade. Fica, então, estabelecida a terceira e última proposição do trabalho:

Proposição 3: As respostas das subunidades às pressões que sofrem influenciam no nível de conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional.

As três proposições da pesquisa estão compiladas no Quadro 6. O referencial teórico e as proposições apontam que a organização que busca a conformidade com os requisitos de Segurança da Informação do ambiente institucional pressiona suas subunidades para que adotem medidas de Segurança da Informação, e as subunidades podem responder com diferentes estratégias, adotando as medidas conforme suas necessidades, interesses e percepções, influenciando a conformidade da organização com os requisitos do ambiente institucional.

Quadro 6 – Proposições da pesquisa.

PROPOSIÇÃO	CONTEÚDO
Proposição 1	As subunidades organizacionais respondem às pressões institucionais através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre a eficiência e adequação das medidas de Segurança da Informação
Proposição 2	Pressões para adoção de medidas formais, medidas informais e medidas técnicas vão resultar em diferentes respostas estratégicas por parte das subunidades organizacionais
Proposição 3	As respostas das subunidades às pressões que sofrem influenciam no nível de conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional

Fonte: Elaborado pelo autor.

Essas proposições foram construídas a partir das relações entre os construtos apresentadas na fundamentação teórica. A Figura 2 mostra as relações entre as pressões institucionais do ambiente e da administração central, respostas estratégicas e adoção de medidas de Segurança da Informação, relações essas que determinam o nível de conformidade da organização com os requisitos de Segurança da Informação.

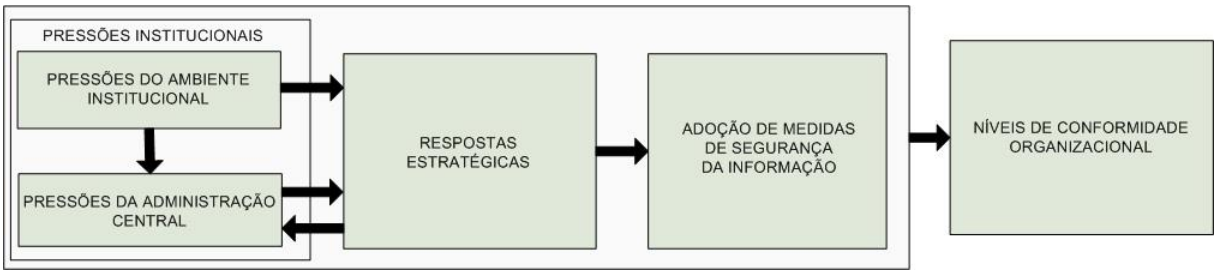


Figura 2 – Relações entre os construtos da pesquisa.
Fonte: elaborada pelo autor.

As relações apresentadas na Figura 2 podem ser replicadas para cada subunidade, uma vez que ocorrem nesse nível da estrutura organizacional. A depender da resposta, cada subunidade pode influenciar ou manipular a administração central da organização, e o conjunto das respostas das subunidades determina a conformidade da organização como um todo com os requisitos externos de Segurança da Informação. A Figura 3 ilustra as pressões sobre as subunidades, a influência das suas respostas sobre a administração central, a relação entre as respostas e a adoção de medidas de Segurança da Informação e como o comportamento das subunidades determina o nível de conformidade da organização com os requisitos institucionais.

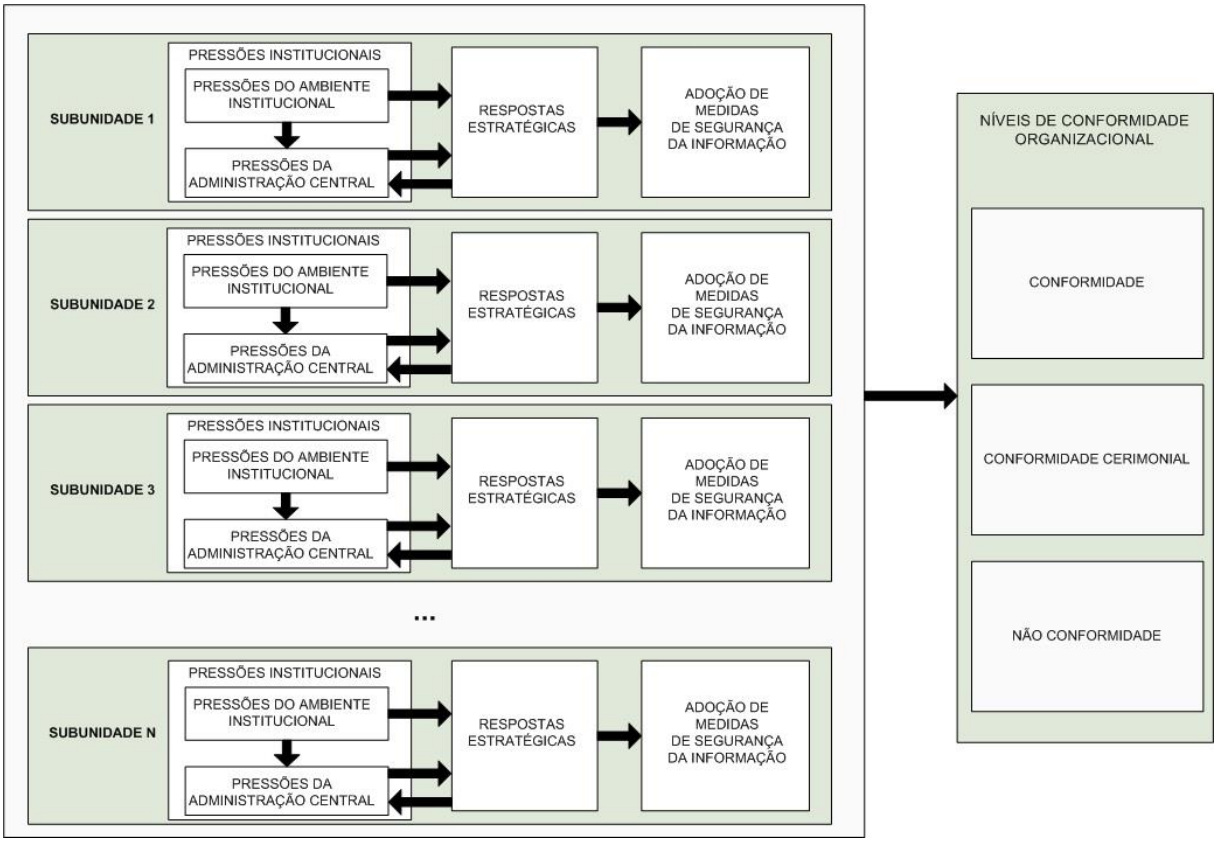


Figura 3 – O comportamento das subunidades e o nível de conformidade organizacional.
Fonte: elaborada pelo autor.

A partir das proposições e do referencial teórico, foi elaborado um *framework* para operacionalização da pesquisa. Nele estão representadas as pressões do ambiente institucional para adoção de medidas de Segurança da Informação, que podem ser coercitivas (na forma de leis, regulamentos, convênios ou contratos), miméticas (modelos adotados por organizações de prestígio, incluindo outras subunidades da organização), ou normativas (medidas tidas como certas por profissionais de Segurança da Informação) (ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016).

Partindo da compreensão de que as pressões institucionais para adoção de tecnologias e práticas administrativas incidem não só sobre as organizações, mas também sobre suas subunidades organizacionais, incluindo unidades de negócio (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003; OSMUNDSEN, 2005; BOSCHMAN, 2006), e que essas são pressionadas também por suas respectivas matrizes (DELMAS; TOFFEL, 2008; AGUILERA-CARACUEL *et al*., 2012; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014; PILATO; PEDRINI, 2015), entende-se que a administração central pode pressionar as subunidades organizacionais através de programas de conscientização,

regulamentos internos e da Política de Segurança da Informação. O ambiente institucional pressiona também as subunidades organizacionais através de leis, regulamentos, modelos e conhecimentos difundidos entre os profissionais, e as subunidades podem responder a essas pressões com aquiescência, compromisso, esquiva, desafio ou manipulação, segundo a tipologia de respostas estratégicas (OLIVER, 1991), o que pode resultar na adoção ou rejeição de medidas técnicas, formais e informais.

O *framework* utilizado na pesquisa (Figura 4) mostra a relação entre a adoção de medidas de Segurança da Informação pelas subunidades e o nível de conformidade da organização com os requisitos do ambiente institucional: a adoção atendendo aos requisitos institucionais de Segurança da Informação (respostas de aquiescência ou compromisso) põe a organização em conformidade; a adoção cerimonial ou rejeição (respostas de esquiva ou desafio) põem a organização em conformidade cerimonial; a alteração de requisitos de Segurança da Informação da administração central devido à atuação das subunidades (resposta de manipulação) põe a organização em não conformidade.

Considerando que o comportamento das subunidades influencia o comportamento da matriz (DELMAS; TOFFEL, 2008; PACHE; SANTOS, 2010), espera-se que uma subunidade possa exercer poder sobre seus recursos para manipular a matriz através de uma resposta estratégica de manipulação, alterando requisitos de Segurança da Informação impostos pela matriz (política, regulamentos e programas), o que pode fazer com que a organização deixe de estar em conformidade com o ambiente institucional. Em suma, o nível de conformidade da organização pode ser um resultado tanto da adoção (ou não adoção) das medidas de Segurança da Informação pelas subunidades organizacionais quanto da influência que essas exercem sobre sua matriz.

Leis, regulamentos, convênios e contratos, modelos adotados por outras organizações de prestígio e medidas tidas como certas por profissionais de Segurança da Informação são pressões coercitivas, miméticas e normativas que o ambiente institucional exerce sobre as organizações (LOPES, 2012; LOPES; SÁ-SOARES, 2014; ALBUQUERQUE JUNIOR; SANTOS, 2015).

Ações e programas de conscientização em Segurança da Informação e a formalização de regulamentos e de uma Política de Segurança da Informação como resultados de respostas às pressões do ambiente externo são indicadores de que a administração central da organização exerce pressões sobre suas subunidades organizacionais. As ações de

conscientização em Segurança da Informação são uma forma de fazer com que as pessoas tenham consciência sobre o comportamento considerado adequado e das habilidades que precisam desenvolver (ELLWANGER, 2009), pois têm a finalidade de mudar crenças, atitudes e cultura organizacional em prol da Segurança da Informação (EMINAGAOGLU; UÇAR; EREN, 2009; SHAW; CHEN; HARRIS, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010; ALKALBANI; DENG; KAM, 2015). Portanto, as ações de conscientização em Segurança da Informação têm o objetivo de difundir na organização crenças e comportamentos racionalizados no ambiente institucional, sendo uma forma de exercer pressão normativa sobre as subunidades organizacionais.

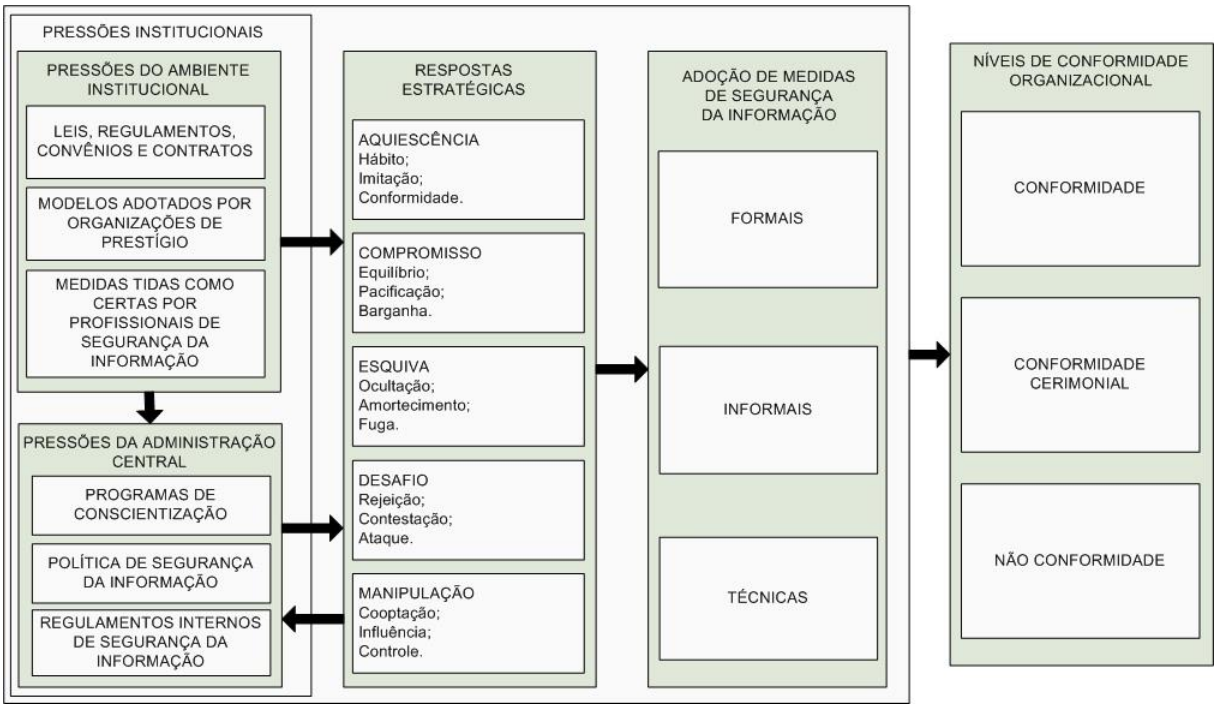


Figura 4 – *Framework* da pesquisa.
Fonte: elaborado pelo autor.

Já os regulamentos e a Política de Segurança da Informação indicam os ativos de informação que devem ser protegidos e qual a proteção que precisam (KING; DALTON; OSMANOGLU, 2001) e orientam a escolha, o desenvolvimento e a implementação de medidas de Segurança da Informação (BARMAN, 2001), além de divulgarem e promoverem comportamentos desejados (LEE, 2001) e difundirem medidas consideradas necessárias (QURESHI, 2011; ABNT, 2013; SÊMOLA, 2014), sendo, portanto, meios através dos quais a

organização exerce significativa pressão coercitiva sobre suas subunidades (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003) e indicadores da ocorrência dessas pressões.

Dentre as respostas estratégicas, a aquiescência é a mais passiva e tem como táticas o hábito, a imitação e a conformidade, como proposto por Oliver (1991). A autora esclarece que o hábito significa que a organização não tem consciência das influências institucionais e, por este motivo, é impedida de responder estrategicamente, passando a reproduzir os requisitos do ambiente institucional que são percebidos como fatos sociais. Dessa forma, a adoção inconsciente (por hábito) de medidas de Segurança da Informação pode ser identificada se não foi fruto da imitação consciente do comportamento de outras organizações ou mesmo de outras subunidades da mesma organização, e se as medidas adotadas não estavam previstas em leis, regulamentos e padrões de Segurança da Informação cuja conformidade seja obrigatória, como retratado por Chou, Liu e Hammitt (2004) em um estudo que compara a adoção de uma tecnologia antes e depois de a obrigação legal ser estabelecida, e por Turner, Gotze e Bernus (2010), que estudaram a adoção inconsciente de práticas de arquitetura organizacional. A adoção através desta tática de aquiescência está associada, portanto, à percepção de que as medidas de Segurança da Informação são tidas como certas pelos responsáveis pela adoção, necessárias para a garantia da confidencialidade, integridade e disponibilidade, sem que tenha havido alguma obrigação ou avaliação quanto à obtenção de benefícios junto à administração central ou ao ambiente institucional, e que não tenham sido copiadas de outras organizações ou subunidades.

Em uma organização composta por diferentes subunidades com algum grau de autonomia e sujeitas a diferentes pressões institucionais, espera-se que uma ou mais despontem como exemplos a serem seguidos e gozem de prestígio entre seus pares, da mesma forma que ocorre entre organizações do mesmo ambiente institucional, seguindo os argumentos de DiMaggio e Powell (1983). Se organizações de destaque no ambiente institucional são imitadas por outras quanto à adoção de medidas de Segurança da Informação, como previsto por teóricos da abordagem institucional e observado em trabalhos anteriores (ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016), fica clara a possibilidade de que as subunidades consideradas bem sucedidas de uma organização sejam imitadas pelas outras. Devido ao fato de estarem expostas a pressões não só da sua administração central, mas também do ambiente institucional, como argumentam Delmas e Toffel (2008), Hernes e Erdvik (2014) e Pilato e Pedrini (2015), as subunidades organizacionais podem imitar o comportamento de outras subunidades e de outras

organizações do ambiente institucional. A imitação é uma tática de aquiescência, mas Oliver (1991) considera que ela pode ser tanto inconsciente quanto consciente. Assim, medidas de Segurança da Informação adotadas por outras subunidades ou organizações podem ser imitadas de maneira inconsciente ou consciente pelas subunidades, e evidências dessa imitação são indicadores dessa tática, como a utilização de documentos e políticas de outras organizações ou outras subunidades como modelos, a adoção de processos e procedimentos iguais ou semelhantes ou a aquisição das mesmas tecnologias.

Oliver (1991) considera que uma organização pode responder com aquiescência visando benefícios para si. Neste caso, a tática apresentada pela autora é a conformidade, através da qual a organização aceita e respeita os requisitos externos de forma consciente, visando à obtenção de benefícios, apoio ou recursos do ambiente. A autora explica que esta tática é mais ativa do que o hábito e a imitação, pois a organização escolhe estrategicamente aceitar as pressões institucionais antecipando os benefícios decorrentes da conformidade.

Em se tratando de Segurança da Informação, que é tida por diferentes autores como uma questão estratégica (HONG *et al*., 2003; POSTHUMUS; VON SOLMS, 2004; DOHERTY; FULFORD, 2006; HEDSTRÖM *et al*., 2011; WU; SAUNDERS, 2011), a proteção dos sistemas e informações contra incidentes e ataques (e, consequentemente, a sobrevivência da organização) apresenta-se como benefício dos esforços em prol da Segurança da Informação (RYAN; RYAN, 2006).

No entanto, esses benefícios são considerados como parte dos mitos institucionalizados a respeito da Segurança da Informação. A caracterização da tática de conformidade se dá quando a organização visa à obtenção de benefícios outros, decorrentes da legitimidade perante os constituintes do ambiente institucional alcançada através da conformidade, pois esta é reconhecida como um meio para obtenção de recursos externos e sobrevivência da organização (DIMAGGIO; POWELL, 1983). Nesse sentido, a conformidade com os requisitos externos de Segurança da Informação apresenta-se como um meio para legitimação da organização com base no fato de que a ocorrência de incidentes pode prejudicar sua imagem e credibilidade (POSTHUMUS; VON SOLMS, 2004) e o acesso a recursos financeiros (PERKEL, 2010). Assim, a organização e suas subunidades podem intencionalmente escolher estar em conformidade com os requisitos externos de Segurança da Informação visando à obtenção de recursos e benefícios do ambiente institucional. O indicador da tática de conformidade, portanto, é a adoção de medidas com o objetivo

inequívoco de obter benefícios de constituintes do ambiente institucional decorrentes da conformidade.

A resposta estratégica de compromisso, que tem como táticas o equilíbrio, a pacificação e a barganha, demonstra que a organização tem ressalvas quanto aos requisitos institucionais. A conformidade, nesse caso, pode ser impraticável devido ao fato de as demandas institucionais serem conflitantes entre si ou inconsistentes com os objetivos, a eficiência ou a autonomia organizacionais (OLIVER, 1991). Nesse sentido, uma Política de Segurança da Informação rígida pode ser considerada um obstáculo para a organização e medidas muito rigorosas podem ser rejeitadas (KARYDA; KIOUNTOUZIS; KOKOLAKIS, 2005; ABRAHAM; CHENGALUR-SMITH, 2011; SUN; AHLUWALIA; KOONG, 2011). A literatura mostra também que diferentes constituintes do ambiente institucional podem exercer pressões para adoção de medidas de Segurança da Informação, como o Governo, órgãos de regulação e fiscalização, organizações que realizam as mesmas atividades, organizações parceiras e de financiamento, além de grupos de profissionais (TEJAY; BARTON, 2013; ALKALBANI; DENG; KAM, 2014; ANTHONY; APPARI; JOHNSON, 2014; LOPES; SÁ-SOARES, 2014). Se as pressões que esses múltiplos constituintes exercem são conflitantes entre si, espera-se que as organizações e suas subunidades adotem as medidas parcialmente, utilizando a tática de equilíbrio para atender pelo menos parcialmente às diferentes demandas. Para identificar esse tipo de tática, os indicadores são a existência de pressões conflitantes e evidências de que as subunidades respondem adotando as medidas parcialmente.

Pressões institucionais para adoção de medidas rígidas ou rigorosas demais, ou consideradas como obstáculos ou empecilhos para a realização das atividades na organização ou para o alcance dos seus objetivos, como descrito por Karyda, Kiountouzis e Kokolakis (2005), Abraham e Chengalur-Smith (2011) e Sun, Ahluwalia e Koong (2011), podem resultar em respostas que levam a uma conformidade parcial. Segundo Oliver (1991), organizações que experimentam pressões para adotarem comportamentos ou estruturas considerados desnecessários ou prejudiciais à sua eficiência ou aos seus objetivos tendem a impor alguma resistência, mas aceitam estar em conformidade com um mínimo de requisitos institucionais para atender em parte às pressões que sofrem, o que caracteriza a resposta estratégica de compromisso utilizando a tática de pacificação. Portanto, a utilização dessa tática tem como indicadores a existência de pressões para adoção de medidas de Segurança da Informação percebidas como prejudiciais ou incoerentes para as subunidades organizacionais, bem como a adoção parcial dessas medidas.

As organizações têm investido cada vez mais em Segurança da Informação, mas é difícil estimar o montante de investimentos que pode ser considerado ótimo, como argumentam Gordon e Loeb (2002). Em outro trabalho, Gordon e Loeb (2006) apontam que é difícil elaborar orçamentos para a Segurança da Informação, pois raramente é possível utilizar modelos racionais baseados na relação entre custo e benefício para justificar os gastos nessa área. Há também uma relação entre o rigor das medidas a serem adotadas e a propensão da organização a resistir a elas, segundo Sun, Ahluwalia e Koong (2011), e a adoção pode ainda exigir o desenvolvimento de competências para habilitar a organização a investir, planejar, organizar e executar processos, tecnologias e projetos de Segurança da Informação, de acordo com Chang e Ho (2006). Assim, a adoção das medidas requeridas pelos constituintes do ambiente institucional ou pela administração central da organização pode exigir que condições anteriores sejam satisfeitas, como a realização de investimentos prévios cuja justificativa é difícil, ou o desenvolvimento anterior de competências internas, o que leva tempo, e as medidas podem ainda ser consideradas demasiadamente rigorosas, o que torna necessário estabelecer negociações entre as subunidades organizacionais e quem demanda a adoção das medidas de Segurança da Informação. Oliver (1991) exemplifica que uma organização pode negociar com as fontes de pressão institucional a frequência ou o âmbito da conformidade com requisitos recém instituídos. A autora cita Pfeffer e Salancik (1978) para argumentar que o ambiente institucional é aberto a negociações entre seus componentes. Nesse sentido, a tática de barganha para responder com compromisso às demandas institucionais para adoção de medidas de Segurança da Informação tem como indicadores as evidências de que houve negociação entre a subunidade e sua administração central ou outros constituintes do ambiente institucional quanto ao momento da adoção das medidas ou o quanto as medidas exigidas devem ser adotadas, ou para postergar inspeções de conformidade.

A esquiva é a resposta estratégica que representa uma tentativa de evitar a necessidade ou obrigatoriedade de estar em conformidade, cujas táticas são ocultação, amortecimento e fuga, de acordo com Oliver (1991). A ocultação, que a autora explica envolver o disfarce da não conformidade com uma fachada de aquiescência e representações de rituais que demonstrem a aceitação das normas institucionais, é uma tática que a organização pode utilizar para intencionalmente alcançar a conformidade cerimonial apontada por Meyer e Rowan (1977). Segundo Parks e Wigand (2014), uma organização pode escrever políticas e regulamentos que não têm reflexo nas atividades desenvolvidas na organização. Da

mesma forma, uma subunidade organizacional pode elaborar e formalizar regulamentos e adotar medidas técnicas e informais de Segurança da Informação sem que isso não se reflita em mudanças nas suas práticas internas, com intenção de estar apenas em uma aparente conformidade com os requisitos institucionais. Assim, o indicador da tática de ocultação é a adoção de medidas que respeitam as exigências da administração central ou de outros constituintes do ambiente institucional, mas que não se refletem nas práticas do dia a dia das subunidades organizacionais, seja através de tecnologias que não tenham sido devidamente implantadas, seja através de políticas e regulamentos que não são cumpridos.

A tática de amortecimento, que significa uma tentativa de reduzir a inspeção, controle ou avaliação externa por meio da redução dos vínculos institucionais, afastando o que está implementado do que é visto externamente (OLIVER, 1991; AIER; WEISS, 2012; PARKS; WIGAND, 2014), pode ser utilizada por uma subunidade organizacional tanto para evitar as pressões exercidas pela sua sede quanto pelos constituintes do ambiente institucional. Nesse sentido, uma subunidade pode reduzir o quanto é inspecionada externamente escondendo do ambiente as medidas de Segurança da Informação que estão de fato implementadas e as que não foram. Isso se aproxima da ideia de segurança por obscuridade, que se baseia no fato de que agentes externos não podem atacar o que não conhecem (OSBORNE; SUMMITT, 2006), sendo que, neste caso, é possível esconder o nível de conformidade interna da inspeção externa para evitar críticas e sanções por parte dos constituintes do ambiente institucional – se a não conformidade não é conhecida, não pode ser criticada ou punida. Outra forma de amortecer a inspeção externa é escondendo a ocorrência de incidentes de Segurança da Informação. O fato de as organizações esconderem incidentes levou à publicação de leis nos Estados Unidos as obrigando a comunicarem as ocorrências aos interessados (HASAN; YURCIK, 2006; ADEBAYO; OMOTOSHO; ADEKUNLE, 2012). Assim, uma subunidade pode esconder a ocorrência de incidentes com a intenção de proteger sua imagem dentro e fora da organização à qual pertence (DHILLON, 2001). Portanto, esconder o nível real de conformidade e a ocorrência de incidentes de Segurança da Informação da administração central e do ambiente institucional indica que a subunidade adotou uma tática de amortecimento.

A tipologia de respostas estratégicas às pressões institucionais prevê a tática de fuga, através da qual a organização busca contornar a necessidade de estar em conformidade através de mudanças nas suas atividades ou objetivos a fim de não se sujeitar às pressões institucionais (OLIVER, 1991; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). Uma

estratégia mais agressiva, como o desafio, pode não ser possível para a organização ao se deparar com pressões institucionais (PARKS; WIGAND, 2014), o que pode levá-la a escolher fugir da obrigatoriedade de estar em conformidade. Embora possa parecer difícil comprovar empiricamente que houve a tática de fuga em subunidades organizacionais, como já discutido, as subunidades podem escolher não participar de projetos ou não se envolver em ações promovidas por sua matriz ou por outras organizações caso exijam a adoção de medidas de Segurança da Informação incoerentes com suas atividades. Subunidades podem também não adotar uma tecnologia importante para a sua produtividade pelo fato de esta ter como requisito a adoção dessas medidas de Segurança da Informação. A ocorrência de tentativas deliberadas de não participar de iniciativas que impliquem na adoção de medidas de Segurança da Informação por este motivo é um indicador de que houve uma resposta de esquiva através da tática de fuga.

O desafio é uma resposta estratégica em que a organização se recusa a estar em conformidade com os requisitos institucionais e declara este comportamento. Suas três táticas são a rejeição, a contestação e o ataque (OLIVER, 1991; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). A rejeição está associada à falta de controle externo, multiplicidade de demandas e percepção de que os requisitos institucionais não são eficientes (STANDING; SIMS; LOVE, 2009) e as organizações são mais propensas a utilizá-la quando há baixo potencial para aplicação das regras institucionais, ou quando há fortes divergências ou conflitos entre essas regras e os objetivos internos das organizações (OLIVER, 1991). A propensão a ignorar a autoridade ou a força das expectativas institucionais aumenta quando há uma compreensão interna diferente quanto à racionalidade por trás das pressões e quanto às consequências da não conformidade (OLIVER, 1991). Se a subunidade organizacional rejeita inequivocamente estar em conformidade com a obrigação de adotar medidas de Segurança da Informação ou a adoção de tecnologias, procedimentos e processos tidos como necessários por outras organizações do ambiente institucional, sua tática de desafio é a rejeição. Assim, o indicador de que houve rejeição dos requisitos institucionais é a tentativa deliberada das subunidades de ignorar as exigências de Segurança da Informação da organização ou do ambiente institucional, apesar de haver o conhecimento da existência dessas exigências.

A contestação, em que a organização não só rejeita, mas também declara a rejeição ou mesmo se vangloria dela, segundo Armênio Neto e Machado-da-Silva (2009), demonstrando os motivos ou benefícios da não conformidade, é uma postura mais ofensiva sobre as pressões institucionais, como destaca Oliver (1991). A percepção de que os

requisitos institucionais não são eficientes é uma motivação para a sua contestação, explicam Standing, Sims e Love (2009). Parks e Wigand (2014) complementam que as organizações podem se opor a regras de privacidade e segurança impostas pelo ambiente institucional. Uma subunidade organizacional pode, portanto, contestar diante da sua administração central ou dos constituintes do ambiente institucional a eficiência ou a adequação das exigências que fazem diante das incoerências dessas com relação às suas atividades e objetivos. Pode também contestar a rigidez das medidas requisitadas pela sua matriz ou por outras organizações que compõem o ambiente institucional. Portanto, o comportamento de contestação, em que a eficiência ou a adequação dos requisitos institucionais de Segurança da Informação são postos em dúvida perante as fontes de pressão institucional, é o indicador de que a organização adotou uma postura de desafio através da contestação dos requisitos institucionais.

Um comportamento mais agressivo do que a contestação caracteriza a tática de ataque, segundo Oliver (1991). O ataque pode ser contra as pressões institucionais e contra os constituintes que exercem essas pressões, complementam Armênio Neto e Machado-da-Silva (2009), podendo ser uma tentativa de ferir, denunciar ou destruir as entidades que exercem as pressões, de acordo com Aier e Weiss (2012). Dentro dessa perspectiva, uma subunidade organizacional pode atacar as leis e os regulamentos que obrigam a adoção de medidas de Segurança da Informação. Pode atacar também os modelos e padrões de Segurança da Informação existentes no mercado ou adotados pela sua administração central e que preconizam medidas de Segurança da Informação, bem como a eficiência e adequação das tecnologias existentes ou adotadas pela sua administração central ou outras organizações. Pode atacar ainda as organizações que exigem a adoção de medidas de Segurança da Informação ou que fiscalizam a sua conformidade com essas exigências, bem como o Comitê de Segurança da Informação e outros órgãos da estrutura organizacional que promovem ou obrigam a adoção das medidas e a conformidade da organização. As evidências de que a subunidade atacou requisitos de Segurança da Informação, constituintes do ambiente institucional ou a própria organização são indicadores de que adotou a estratégia de desafio utilizando a tática de ataque.

A manipulação é a resposta estratégica mais ativa dentro da proposta de Oliver (1991), e segundo a autora, envolve o exercício do poder da organização sobre as fontes de pressão ou sobre as pressões institucionais com a intenção de obter benefícios. Standing, Sims e Love (2009) associam esta resposta a diferentes fatores: a falta de autoridade dos

constituintes do ambiente institucional; a percepção de que as consequências da não conformidade não são tão graves; a existência de múltiplos requisitos do ambiente institucional; e a percepção de que esses requisitos não são tão eficientes. Oliver (1991) apresenta como táticas a cooptação, influência e controle. Pfeffer (1974) argumenta que uma organização, ao utilizar a tática de cooptação, usa seu poder de persuasão para que constituintes do ambiente institucional se aliem a ela. Armênio Neto e Machado-da-Silva (2009) complementam que a intenção, neste caso, é neutralizar as pressões institucionais que a organização sofre.

Considerando que Sêmola (2014) explica que, além de um Comitê de Segurança da Informação, o Sistema de Gestão de Segurança da Informação pode prever a existência de subcomitês nas subunidades organizacionais, argumenta-se que uma delas pode se esforçar para que seu subcomitê de Segurança da Informação tenha membros influentes do Comitê corporativo visando neutralizar as pressões que sofre. Pode também chamar constituintes do ambiente institucional para participar das suas decisões sobre adoção de medidas de Segurança da Informação com a intenção de legitimar decisões que podem ser contrárias aos interesses das fontes e pressão. Como indicadores da tática de cooptação, tem-se a ocorrência de tentativas de trazer para o grupo que toma decisões nas subunidades membros do Comitê de Segurança da Informação da organização, ou atores de outras organizações do ambiente institucional que exercem pressões para adoção de medidas de Segurança da Informação, sendo que com a intenção de eliminar as pressões institucionais.

Uma organização utiliza a tática de influência para mudar a forma como os constituintes institucionais percebem os requisitos institucionais e a necessidade de estar em conformidade (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). A influência pode ser no sentido de mudar definições e critérios de aceitação, metas de desempenho aceitável, regulamentos e acesso a recursos, pois esses requisitos institucionais são muitas vezes abertos a reinterpretação e manipulação (OLIVER, 1991). A ocorrência de eventos em que as subunidades organizacionais exercem influência sobre o comportamento das suas sedes já é um fenômeno reconhecido na literatura (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014). Assim, uma subunidade organizacional pode utilizar seu prestígio para tentar influenciar sua administração central ou outras fontes de pressão institucional com a intenção de mudar requisitos de Segurança da Informação ou de alterar regulamentos corporativos ou a Política de Segurança da Informação da organização, o que configura uma tática de

influência. Portanto, as tentativas das subunidades de influenciar as fontes de pressão para que mudem requisitos institucionais indicam a tática de influência.

O controle, como a forma mais ativa de manipulação, significa um esforço para dominar as fontes de pressão institucional, o que é mais agressivo do que cooptar ou influenciar, como descreve Oliver (1991). A autora ressalta que a tática de controle é mais facilmente utilizada quando as expectativas institucionais são incipientes, localizadas ou fracamente promovidas. Armênio Neto e Machado-da-Silva (2009) relacionam a tática de controle ao exercício do poder e à dominação de uma organização sobre os constituintes do ambiente institucional que aplicam as pressões sobre ela. O controle pode ser também exercido pela subunidade sobre sua administração central.

Tempel *et al*. (2006) consideram que o relacionamento de poder entre a matriz e as subunidades nem sempre se apresenta de forma unidirecional, de maneira que uma subunidade, que está em uma posição de inferioridade hierárquica, pode ter recursos ou conhecimentos, ou uma capacidade ou desempenho que conferem a ela poder sobre sua administração central ou sobre o ambiente institucional. Com isto, os autores argumentam que a relação de dependência pode dar à subunidade oportunidade de controlar ou influenciar a sede ou o ambiente em benefício próprio ao não concordar com requisitos de Segurança da Informação. Assim, a ocorrência de tentativas de alteração, extinção ou criação de medidas pela administração central ou por outras organizações do ambiente institucional para atender aos interesses de subunidades organizacionais são indicadores da tática de controle.

As pressões institucionais incidem de formas distintas sobre as subunidades de uma organização, que respondem a essas pressões de diferentes maneiras, a depender do tipo de pressão institucional, da forma como interpretam essas pressões e da coerência delas com seus próprios interesses (DELMAS; TOFFEL, 2008; AIER; WEISS, 2012; HERNES; ERDVIK, 2014; PILATO; PEDRINI, 2015). Diferentes pressões institucionais estão também relacionadas à adoção de medidas técnicas, formais e informais de Segurança da Informação de maneiras distintas (ALBUQUERQUE JUNIOR *et al*., 2016). Além disso, há o entendimento na literatura de que as decisões sobre adoção de medidas técnicas, formais e informais são responsabilidades de diferentes subunidades organizacionais, que podem ter atribuições mais técnicas e operacionais, de gestão ou estratégicas (SÊMOLA, 2014). Considerando que as subunidades organizacionais têm relativa autonomia administrativa e muitas vezes contam com equipes técnicas e estruturas próprias de gestão e governança da Segurança da Informação, as pressões para adoção de medidas técnicas, formais e informais

podem incidir sobre departamentos e grupos de profissionais distintos, que podem perceber essas pressões de diferentes maneiras, levando suas respectivas subunidades a responderem de formas distintas.

A ocorrência de tratamentos diferenciados destinados às pressões para adoção de medidas técnicas, formais e informais pode ser uma decorrência da percepção de que a conformidade não é obrigatória ou que medidas de uma categoria são mais importantes do que as de outras. Da mesma forma, a identificação de medidas formais, informais e técnicas que foram adotadas pelas subunidades em detrimento dos objetivos e interesses da administração central indica que a adoção é para atender aos interesses das subunidades, independentemente dos interesses da organização.

Se decisões tomadas nas subunidades organizacionais, com base em seus próprios interesses e julgamentos, podem determinar a conformidade ou não conformidade da organização com requisitos externos (HERNES; ERDVIK, 2014), é possível que políticas e regulamentos organizacionais sejam desrespeitados pelas subunidades por julgarem desnecessários ou ineficientes, ainda que a administração central da organização promova a adoção das práticas previstas na política e nos regulamentos formalizados por considerá-los eficientes, como destacam Netland e Aspelund (2014). A diversidade de julgamentos e de respostas das subunidades organizacionais prejudicam a uniformidade na adoção das práticas em toda a organização, de acordo com Boschman (2006) e Aguilera-Caracuel *et al*. (2012).

Quanto à Segurança da Informação, os efeitos do comportamento das subunidades sobre suas matrizes podem ser tanto diretos, como uma decorrência de respostas estratégicas de manipulação, quanto indiretos, provocados por respostas de aquiescência, compromisso, esquiva e desafio. Se uma ou mais subunidades não adotam as medidas exigidas em políticas e regulamentos organizacionais, o resultado da dissociação entre política e prática é a conformidade cerimonial, pois a organização busca a conformidade e os gestores e responsáveis deixam isso claro em seu discurso, embora ela não esteja sendo alcançada.

Cabe ressaltar que a conformidade cerimonial, neste caso, não é intencional, mas uma consequência de diferentes respostas, que podem variar da aquiescência passiva à resistência aos requisitos de Segurança da Informação, diferentemente daquela descrita por Meyer e Rowan (1977). Além disso, caso uma ou mais subunidades tenham controle sobre recursos importantes para a organização e influenciem ou exerçam o poder que têm sobre a sua administração central, é possível que políticas e regulamentos sejam alterados conforme

seus interesses, e como consequência, a organização, que formalizou uma Política e outros regulamentos de Segurança da Informação para estar em conformidade com os requisitos institucionais, pode não conseguir ficar em conformidade ou mesmo deixar de estar.

Dessa forma, a ocorrência de respostas de conformidade e não conformidade por parte das subunidades pode indicar que a organização está em conformidade cerimonial com os requisitos de Segurança da Informação do ambiente institucional. Já a ocorrência de alterações em regulamentos e na Política de Segurança da Informação da organização para atender aos interesses das subunidades devido às influências que exercem ou ao poder que têm indica que a organização pode não estar em conformidade com os requisitos institucionais de Segurança da Informação. Por fim, a ocorrência de respostas exclusivamente de conformidade por parte das subunidades indica que a organização como um todo está também em conformidade com os requisitos de Segurança da Informação do ambiente institucional. O Quadro 7 compila todos os construtos da pesquisa e seus indicadores.

Quadro 7 – Construtos e indicadores da pesquisa.

CONSTRUTOS		INDICADORES	AUTORES DE REFERÊNCIA
Pressões Institucionais		Programas de conscientização, regulamentos e Política de Segurança da Informação formalizados na organização	Ellwanger (2009), Eminagaoglu, Uçar e Eren (2009), Shaw, Chen e Harris (2009), Bulgurcu, Cavusoglu e Benbasat (2010), Alkalbani, Deng e Kam (2015)
Resposta Estratégica de Aquiescência	Hábito	Adoção inconsciente de medidas tidas como certas pelas subunidades, independentemente de terem sido adotadas por outras organizações ou subunidades	Chou, Liu e Hammitt (2004), Standing, Sims e Love (2009), Turner, Gotze e Bernus (2010), Parks e Wigand (2014)
	Imitação	Cópia inconsciente ou consciente pelas subunidades das medidas adotadas por outras organizações ou subunidades	Standing, Sims e Love (2009), Hsu, Lee e Straub (2012), Tejay e Barton (2013), Parks e Wigand (2014), Albuquerque Junior e Santos (2015), Albuquerque Junior *et al*. (2016)
	Conformidade	Adoção consciente pelas subunidades das medidas exigidas visando à obtenção benefícios decorrentes da conformidade	Posthumus e Von Solms (2004), Ryan e Ryan (2006), Standing, Sims e Love (2009), Perkel (2010), Parks e Wigand (2014)
Resposta Estratégica de Compromisso	Equilíbrio	Adoção pelas subunidades de medidas conflitantes com outras medidas ou com seus objetivos e atividades realizando ajustes na implementação para que não haja descumprimento	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Sun, Ahluwalia e Koong (2011), Abraham e Chengalur-Smith (2011), Parks e Wigand (2014)

CONSTRUTOS (cont.)		INDICADORES (cont.)	AUTORES DE REFERÊNCIA (cont.)
Resposta Estratégica de Compromisso	Equilíbrio	Adoção pelas subunidades de medidas conflitantes com outras medidas ou com seus objetivos e atividades realizando ajustes na implementação para que não haja descumprimento	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Sun, Ahluwalia e Koong (2011), Abraham e Chengalur-Smith (2011), Parks e Wigand (2014)
	Barganha	Negociações entre as subunidades e as fontes de pressão visando à alteração do quando ou o quanto as medidas devem ser adotadas	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Esquiva	Ocultação	Implantação de tecnologias pelas subunidades sem realizar as configurações e ações necessárias ou previstas nos regulamentos e na Política de Segurança da Informação da organização; criação de políticas e regulamentos nas subunidades sem que haja cobrança quanto ao seu cumprimento	Björck (2004), Standing, Sims e Love (2009), Parks e Wigand (2014), Lopes e Sá-Soares (2014), Lapke e Dhillon (2015)
	Amortecimento	Ações da subunidade com o objetivo de esconder das fontes de pressão o nível real de conformidade e a ocorrência de incidentes	Dhillon (2001), Hasan e Yurcik (2006), Standing, Sims e Love (2009), Aier e Weiss (2012), Adebayo, Omotosho e Adekunle (2012), Parks e Wigand (2014)
	Fuga	Ações da subunidade para não participar de iniciativas que exijam a adoção de medidas de Segurança da Informação	Armênio Neto e Machado-da-Silva (2009), Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Desafio	Rejeição	Rejeição das medidas exigidas ou tidas como certas pela administração central e outras organizações	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Contestação	Ações da subunidade para desafiar as pressões através de críticas à sua eficiência ou rigor	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Ataque	Ataques deferidos pela subunidade às fontes de pressão ou às próprias pressões por considerá-las ineficientes ou rigorosas demais	Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Manipulação	Cooptação	Tentativas de fazer com que membros do Comitê ou do Escritório de Segurança da Informação da administração central ou membros de outras fontes de pressão participem das decisões sobre Segurança da Informação da subunidade para neutralizar as pressões sofridas	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Influência	Utilização pela subunidade de prestígio para influenciar a administração central ou outras fontes de pressão para mudarem requisitos de Segurança da Informação	Delmas e Toffel (2008), Standing, Sims e Love (2009), Parks e Wigand (2014), Hernes e Erdvik (2014)

CONSTRUTOS (cont.)		INDICADORES (cont.)	AUTORES DE REFERÊNCIA (cont.)
Resposta Estratégica de Manipulação	Controle	Utilização pela subunidade de poder sobre a administração central ou outras fontes de pressão para que exijam a adoção de medidas que a beneficiem	Tempel *et al*. (2006), Standing, Sims e Love (2009), Parks e Wigand (2014)
Adoção de Medidas de Segurança da Informação		Medidas técnicas, formais e informais adotadas pelas subunidades	Farn, Lin e Fung (2004), Björck (2005), Casey (2005), Martins e Santos (2005), Belasco e Wan (2006), Juels (2006), Doherty e Fulford (2006), Thorpe (2006), Panko (2006), Park, Jang e Park (2010), Gorayeb (2012), Manoel (2014), Sêmola (2014)
Níveis de Conformidade Organizacional		Tratamentos distintos às pressões para adoção de medidas formais, informais e técnicas nas subunidades; adoção pelas subunidades de medidas formais, informais e técnicas contrárias aos objetivos e interesses da administração central; ocorrência de respostas de conformidade e não conformidade pelas subunidades; ocorrência de alterações em regulamentos e na Política de Segurança da Informação devido a ações promovidas pelas subunidades para atender aos seus interesses; discurso de conformidade da administração central	Björck (2004), Sá (2004), Wahyudi (2004), Boschman (2006), Armênio Neto e Machado-da-Silva (2009), Standing, Sims e Love (2009), Aguilera-Caracuel *et al*. (2012), Aier e Weiss (2012), Lopes e Sá-Soares (2014), Netland e Aspelund (2014), Hernes e Erdvik (2014), Lapke e Dhillon (2015), Pilato e Pedrini (2015)

Fonte: elaborado pelo autor.

A partir desses construtos e indicadores, foi possível construir o instrumento de pesquisa e operacionalizar a codificação dos trechos dos documentos e das transcrições das entrevistas no *software* de análise qualitativa NVivo, como descrito no capítulo seguinte.

4 MÉTODO

Esta pesquisa caracteriza-se quanto ao objetivo como explanatória, pois busca responder a uma pergunta "como", segundo a classificação de Yin (2010), ou como explicativa, segundo Gil (2009), uma vez que tem o objetivo de explicar como o comportamento das subunidades organizacionais frente às pressões para adotarem medidas de Segurança da Informação influencia a conformidade de uma organização com os requisitos de Segurança da Informação do ambiente institucional.

Yin (2010) explica que questões de pesquisa do tipo "como", por serem explanatórias, levam ao uso do estudo de caso como método de pesquisa. Dentro da área temática de Sistemas de Informações, Benbasat, Goldstein e Mead (1987) corroboram com esse entendimento, pois os estudos de caso lidam com ligações operacionais a serem traçadas ao invés de frequência ou incidência, permitindo compreender a natureza e a complexidade dos processos organizacionais. Estes autores concordam que estudos de caso podem ser também explicativos, o que reforça a caracterização deste trabalho. Ainda para estes autores, outras razões para realizar estudos de caso em Sistemas de Informações são: a possibilidade de estudar o tema em um ambiente natural e gerar teorias a partir dele; e a possibilidade de realizar pesquisas em um tema pouco estudado, o que não é incomum em Sistemas de Informação, área temática que evolui rapidamente e na qual podem surgir novos temas de pesquisa. Não foram encontrados trabalhos utilizando a tipologia de respostas estratégicas para investigar a adoção de medidas de Segurança da Informação na bibliografia consultada, como também não foram encontrados trabalhos que tratem das causas para a dissociação entre Política de Segurança da Informação e as medidas adotadas. Estes fatos justificam a realização de um estudo de caso.

Segundo Yin (2010), além da questão e objetivo da pesquisa, o estudo de caso é caracterizado por ter seu foco em eventos contemporâneos, concordando com Benbasat, Goldstein e Mead (1987). Creswell (2010) e Gil (2009) complementam que estudos de caso buscam ainda obter conhecimento detalhado sobre o objeto de pesquisa. Cooper e Schindler (2016) acrescentam que este método enfatiza a análise contextual profunda de poucos eventos ou condições e permite obter detalhes a partir de múltiplas fontes de informação. Para Yin (2010), o estudo de caso permite conhecer características amplas de eventos da vida real, entre eles os processos organizacionais, reforçando a compreensão de Benbasat, Goldstein e

Mead (1987). A utilização do estudo de caso para a realização desta pesquisa permitiu compreender de forma profunda como as subunidades organizacionais respondem às pressões que sofrem e os efeitos dessas respostas sobre a conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional, o que reitera essa adequação do método à pesquisa realizada.

Parte dos dados foi coletada no local em que o fenômeno ocorre, através de entrevistas semiestruturadas com as pessoas que estão envolvidas diretamente com ele, o que caracteriza o trabalho como uma pesquisa predominantemente de campo, segundo Flick (2009). De acordo com Cooper e Schindler (2016), estudos de caso combinam diferentes métodos de pesquisa, e segundo Yin (2010), contam também com múltiplas fontes de evidência. Benbasat, Goldstein e Mead (1987) concordam que estudos de caso da área de Sistemas de Informação examinam fenômenos em ambiente natural e coletam dados através de múltiplos meios. Neste trabalho, além das entrevistas, foi realizada também pesquisa em documentos, tanto da organização quanto de suas subunidades. Os documentos foram acessados diretamente de *websites* da organização e subunidades, e quando o acesso não foi possível, foram solicitados aos gestores e responsáveis pela TI e Segurança da Informação, e a membros do setor de auditoria, o que garante os critérios de aceitação apresentados por Scott (1990), *apud* Flick (2009): autenticidade, credibilidade, representatividade e significação.

Como esta pesquisa foi realizada em apenas uma organização, trata-se de um estudo de caso único, pois, como destaca Gil (2009), estudos de casos únicos podem referir-se a uma organização ou um fenômeno, sendo a modalidade mais tradicional deste método de pesquisa. Benbasat, Goldstein e Mead (1987) apontam como característica dos estudos de caso o exame de uma ou mais entidades (pessoas, grupos ou organizações). Segundo Yin (2010), o estudo de caso único justifica-se quando: a) trata-se de um **caso crítico** no teste de uma teoria que tenha especificado um conjunto claro de proposições e circunstâncias em que essas proposições são verdadeiras, situação em que pode confirmar, desafiar ou ampliar a teoria; b) representa um **caso extremo** ou **peculiar**, quando o caso é tão raro que precisa ser documentado e analisado; c) é um **caso revelador**, quando permite investigar um fenômeno que, em outra situação ou momento, seria inacessível; d) representa um **caso longitudinal**, em que o mesmo caso é estudado em mais de um momento, situação em que a teoria especifica como o caso evoluirá com o tempo se determinadas condições forem satisfeitas; ou e) trata-se de um **caso típico** ou **representativo**, que tem o objetivo de captar as condições, circunstâncias ou características da maioria de um determinado tipo de caso. Esta última

justificativa é apresentada também por Gil (2009), que explica que este tipo de estudo tem o objetivo de investigar casos que pareçam ser a melhor expressão de um tipo ideal. Assim, com base nos tipos apresentados por Yin (2010) e Gil (2009), este trabalho é caracterizado como um estudo de caso típico, pois a organização em estudo atende aos requisitos e apresenta as condições ideais que para realizar esta pesquisa.

Yin (2010) acrescenta que um estudo de caso único pode ser ainda: **holístico**, quando examina a natureza global de uma organização e a teoria ou as subunidades lógicas do caso não podem ser identificadas; ou **integrado**, quando o caso envolve múltiplas unidades de análise, mesmo sendo sobre uma única organização. O estudo de caso integrado, segundo o autor, envolve resultados sobre uma ou mais subunidades da mesma organização (chamadas unidades integradas), que podem acrescentar oportunidades significativas para uma análise extensiva do caso único. Por envolver as unidades de análise integradas (as subunidades da organização) e os efeitos do seu comportamento sobre a organização em estudo, este trabalho é caracterizado como um estudo de caso integrado.

A abordagem metodológica deste trabalho é qualitativa, pois exige a interpretação das respostas ao invés do uso de técnicas e métodos estatísticos ao investigar uma relação dinâmica entre a realidade, o fenômeno e as pessoas envolvidas, de acordo com Silva e Menezes (2001). Creswell (2010) recomenda uma abordagem qualitativa quando pouca pesquisa foi realizada a respeito do fenômeno em estudo e quando ele precisa ser melhor compreendido. Na pesquisa bibliográfica, não foram identificados trabalhos investigando como as organizações respondem às pressões institucionais para adotarem medidas de Segurança da Informação nem como as respostas das subunidades influenciam a organização. Além disso, acredita-se que a utilização de métodos quantitativos para a realização desta pesquisa é dificultada pelo fato de determinados comportamentos, como a ocultação e o amortecimento, terem o objetivo de enganar o observador em uma análise pouco aprofundada – como a que seria possível utilizando apenas formulários. Embora a dissociação seja um fenômeno relevante para os estudos organizacionais e para a abordagem institucional, Westphal e Zajac (2001) consideram difícil observá-lo em grandes amostras de organizações. Nesse sentido, Moreira e Caleffe (2008) entendem que a pesquisa qualitativa explora características que não podem ser descritas facilmente com números.

Essa dificuldade em aplicar outros métodos é também uma justificativa para realizar estudos de caso, que em geral são qualitativos e “possibilitam investigar a complexidade de fenômenos cujas sutilizas não podem ser captadas por delineamentos cujo

planejamento é muito rígido, como é o caso dos levantamentos.” (GIL, 2009, p.17). Pesquisas qualitativas foram identificadas em trabalhos sobre dissociação (ELSBACH; SUTTON, 1992; BEVERLAND; LUXTON, 2005; BOIRAL, 2007; ULVIN, 2007; HERAS-SAIZARBITORIA, 2011; DIAS; HERAS, 2013; SPEARS; BARKI; BARTON, 2013; HERNES; ERDVIK, 2014; HERAS-SAIZARBITORIA; BOIRAL, 2015; LAPKE; DHILLON, 2015) e também sobre respostas organizacionais às pressões do ambiente externo (MCKAY, 2001; GRAEFF, 2005; BOSCHMAN, 2006; FREZATTI; AGUIAR; REZENDE, 2007; DELMAS; TOFFEL, 2008; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009; PAPADIMITRIOU; WESTERHEIJDEN, 2010; PARKS *et al*., 2011; AIER; WEISS, 2012; HANDGRAAF, 2012; JEWER; MCKAY, 2012; PARKS, 2012; LUNDBERG, 2013; BORGES; DUTRA; SCHERER, 2014; ESTERHAZY, 2014; PARKS; WIGAND, 2014), o que reforça a utilização de uma abordagem qualitativa neste trabalho.

4.1 DESENHO DA PESQUISA

A realização desta pesquisa envolveu três etapas principais:

a) Etapa 1: realização da pesquisa bibliográfica e a identificação do referencial teórico que permitiu elaborar o *framework* utilizado na operacionalização do estudo, incluindo a identificação dos indicadores que permitiram a elaboração do instrumento de pesquisa – roteiro de entrevistas semiestruturadas;

b) Etapa 2: identificação e acesso a documentos organizacionais relacionados a Segurança da Informação, realização de entrevistas semiestruturadas com responsáveis pela adoção de medidas de Segurança da Informação na administração central da organização e nas subunidades organizacionais, e transcrição das entrevistas para documentos eletrônicos e revisão das transcrições pelos entrevistados;

c) Etapa 3: categorização e análise dos documentos obtidos e dos dados coletados nas entrevistas e revisados pelos entrevistados, comparação dos dados dos documentos e das transcrições das entrevistas e conclusão do trabalho.

Por ter envolvido tanto dados de documentos quanto das entrevistas realizadas, esta pesquisa envolveu múltiplas fontes de dados, de forma coerente com o método de estudo de caso. A análise dos dados foi realizada utilizando o *software* de análise de dados

qualitativos (*quality data analysis* – QDA) NVivo 10, como descrito adiante. A Figura 5 apresenta de forma simplificada o desenho da pesquisa.

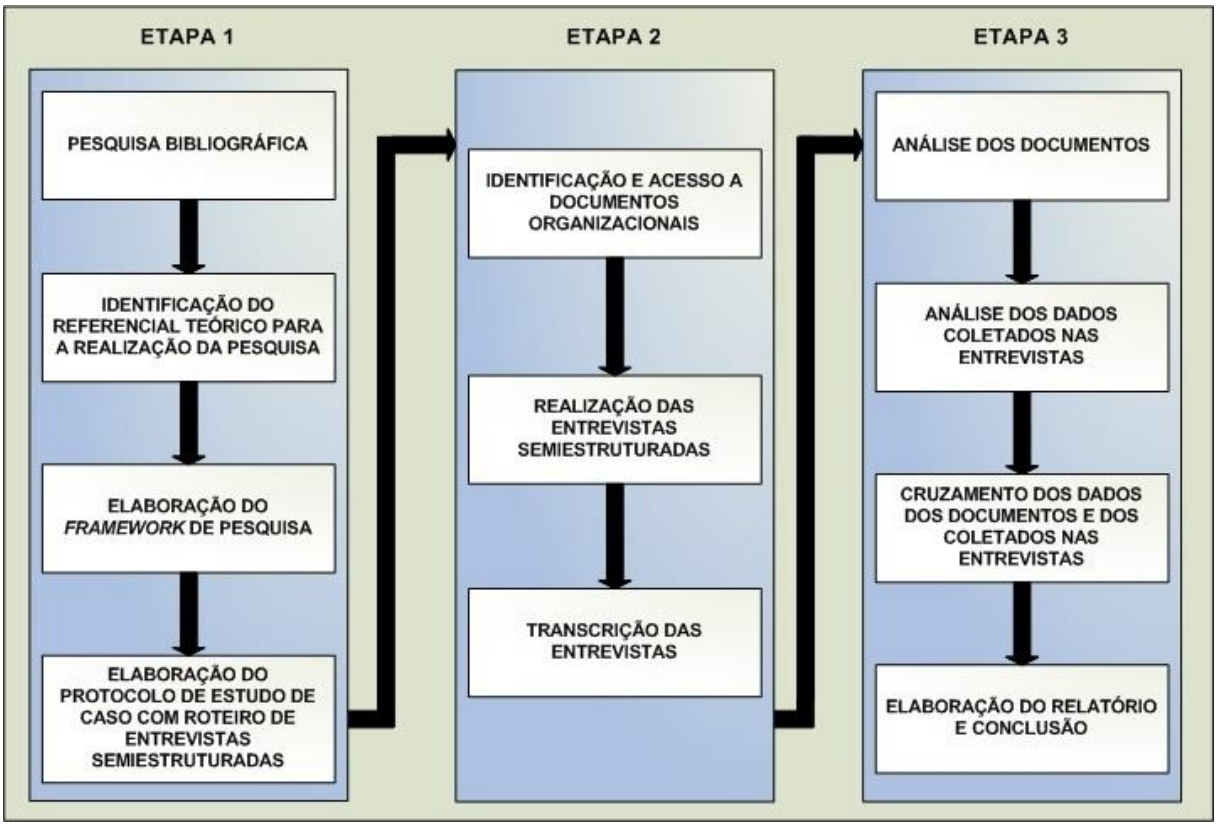


Figura 5 – Desenho da pesquisa.
Fonte: elaborado pelo autor.

4.2 PESQUISA BIBLIOGRÁFICA

Além dos artigos identificados em três pesquisas que analisaram a produção científica nacional sobre Segurança da Informação em eventos e periódicos (ALBUQUERQUE JUNIOR; SANTOS, 2013, 2014a, 2014b), a pesquisa bibliográfica envolveu ainda buscas por teses e dissertações produzidas a partir de 2009 sobre o tema em bases de dados de 25 universidades brasileiras que oferecem cursos de pós-graduação *stricto sensu* em Administração, Ciência da Informação e Engenharia de Produção, áreas de conhecimento nas quais é comum encontrar estudos da área temática de Sistemas de Informação.

Foram realizadas buscas também na Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), na base de Teses e Dissertações do Portal Domínio Público e no Banco de Teses da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Com isso, foram identificados trabalhos produzidos em cursos que têm uma aproximação teórica ou metodológica com a Administração (Regulação e Gestão de Negócios, Gestão do Conhecimento e da Tecnologia da Informação, Gestão do Desenvolvimento de Tecnologias da Informação Aplicadas, Gestão e Desenvolvimento Regional, e Ciência, Gestão e Tecnologia da Informação) e produzidos também em cursos de pós-graduação de outras áreas de conhecimento além das já citadas (Ciências Contábeis, Direito, Engenharia Biomédica, Medicina, Odontologia, Arquivologia, Psicologia, Saúde Coletiva e Tecnologia Nuclear), além das áreas em que tradicionalmente são produzidos trabalhos sobre Segurança da Informação (Ciência da Computação, Informática, Engenharia Elétrica e Engenharia de Computação).

Para que as buscas não ficassem restritas ao cenário nacional, foram consultadas as bases de dados *Open Access Theses and Dissertations* (OATD) e *Networked Digital Library of Theses and Dissertations* (NDLTD), *Scopus* e o *Google Scholar* a fim de localizar teses, dissertações e artigos publicados a partir de 2009.

As buscas nas bases de dados utilizaram as ferramentas disponibilizadas pelas próprias bases. As palavras-chave e termos utilizados nas bases nacionais foram “integridade”, “confidencialidade”, “disponibilidade”, “informação+riscos”, “segurança da informação”, “segurança+informação”, “informação+incidentes”. Já as buscas nas bases internacionais utilizaram as palavras e termos “*information security*”, “*information+security*”, “*confidentiality*”, “*integrity*”, “*availability*”, “*information+risks*”, “*information+incidents*”.

Na pesquisa bibliográfica, foram identificados 171 artigos, teses e dissertações que abordam Segurança da Informação com um enfoque organizacional ou social. Desses, 91 (53,22%) tratam do comportamento individual, principalmente da conformidade das pessoas com relação a políticas e regulamentos de Segurança da Informação, enquanto 45 trabalhos (26,32%) tratam do comportamento organizacional. A Teoria Institucional, abordagem teórica utilizada neste trabalho, foi utilizada em 21 trabalhos sobre o tema (vide Quadro 3), mas nenhum deles utilizou a tipologia de respostas estratégicas de Oliver (1991).

4.3 ESCOLHA DO CASO

O caso estudado foi escolhido dentre as 38 organizações que participaram de duas pesquisas anteriores (ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016). Essas pesquisas permitiram identificar as organizações que adotaram medidas de Segurança da Informação devido às pressões do ambiente institucional e que contam com uma estrutura de tomada de decisões e um conjunto de documentos que formalizam essa estrutura e o funcionamento da Segurança da Informação: Comitê de Segurança da Informação instituído, Política de Segurança da Informação formalizada, Escritório de Segurança da Informação presente na estrutura organizacional, regulamentos de Segurança da Informação formalizados e equipe de tratamento de incidentes de Segurança da Informação presente na estrutura organizacional.

Dentre as 11 organizações que atendem a esses critérios, a pesquisa foi realizada naquela mais acessível ao pesquisador. O fato de o pesquisador ser servidor público de uma dessas organizações facilitou o contato com os gestores de TI e Segurança da Informação da organização, que foram favoráveis à pesquisa.

4.4 PROCEDIMENTOS DE COLETA DE DADOS

A depender dos indicadores da pesquisa, as fontes de dados utilizadas foram as entrevistas realizadas ou documentos da organização, que garantem a multiplicidade de fontes de evidência. O Quadro 8 mostra a relação entre indicadores, procedimentos de coleta e fontes de dados da pesquisa.

Quadro 8 – Indicadores da pesquisa, procedimentos e meios para coleta dos dados.

INDICADORES	PROCEDIMENTOS	FONTES DE DADOS
Programas de conscientização, regulamentos e Política de Segurança da Informação formalizados na organização	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias

INDICADORES (cont.)	PROCEDIMENTOS (cont.)	FONTES DE DADOS (cont.)
Adoção inconsciente de medidas tidas como certas pelas subunidades, independentemente de terem sido adotadas por outras organizações ou subunidades	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Cópia inconsciente ou consciente pelas subunidades das medidas adotadas por outras organizações ou subunidades	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias
Adoção consciente pelas subunidades das medidas exigidas visando à obtenção benefícios decorrentes da conformidade	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Adoção pelas subunidades de medidas conflitantes com outras medidas ou com seus objetivos e atividades realizando ajustes na implementação para que não haja descumprimento	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Adoção pelas subunidades de parte das medidas exigidas e rejeição de outras consideradas conflitantes entre si ou com seus objetivos e atividades	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias
Negociações entre as subunidades e as fontes de pressão visando à alteração do quando ou o quanto as medidas devem ser adotadas	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Implantação de tecnologias pelas subunidades sem realizar as configurações e ações necessárias ou previstas nos regulamentos e na Política de Segurança da Informação da organização	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Criação de programas e regulamentos nas subunidades sem que haja cobrança quanto ao seu cumprimento	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ações da subunidade com o objetivo de esconder das fontes de pressão o nível real de conformidade e a ocorrência de incidentes	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias

INDICADORES (cont.)	PROCEDIMENTOS (cont.)	FONTES DE DADOS (cont.)
Ações da subunidade para não participar de iniciativas que exijam a adoção de medidas de Segurança da Informação	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias
Rejeição das medidas exigidas ou tidas como certas pela administração central e outras organizações	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ações da subunidade para desafiar as pressões para adoção de medidas através de críticas à sua eficiência ou rigor	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ataques deferidos pela subunidade às fontes de pressão ou às próprias pressões por considerá-las ineficientes ou rigorosas demais	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Tentativas de fazer com que membros do Comitê ou do Escritório de Segurança da Informação da administração central ou membros de outras fontes de pressão participem das decisões sobre Segurança da Informação da subunidade para neutralizar as pressões sofridas	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Sistema de Gestão de Segurança da Informação e portarias
Utilização pela subunidade de prestígio para influenciar a administração central ou outras fontes de pressão para mudarem requisitos de Segurança da Informação	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias
Utilização pela subunidade de poder sobre a administração central ou outras fontes de pressão para que exijam a adoção de medidas que a beneficiem	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, leis, relatórios, recomendações e portarias
Tratamentos distintos às pressões para adoção de medidas formais, informais e técnicas nas subunidades	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
	Pesquisa documental	Sistema de Gestão de Segurança da Informação e portarias organizacionais

INDICADORES (cont.)	PROCEDIMENTOS (cont.)	FONTES DE DADOS (cont.)
Adoção pelas subunidades de medidas formais, informais e técnicas contrárias aos objetivos e interesses da administração central	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ocorrência de respostas de conformidade e não conformidade pelas diferentes subunidades	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ocorrência de alterações em regulamentos e na Política de Segurança da Informação devido a ações promovidas pelas subunidades para atender aos seus interesses	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, relatórios, recomendações, portarias e mensagens eletrônicas
	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Ocorrência de respostas de conformidade pelas subunidades	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, relatórios, recomendações e portarias
	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades e membros do Comitê de Segurança da Informação da organização
Medidas técnicas, formais e informais adotadas pelas subunidades	Pesquisa documental	Política de Segurança da Informação, Sistema de Gestão de Segurança da Informação, regulamentos, relatórios, recomendações e portarias
	Entrevistas semiestruturadas	Responsáveis pela Segurança da Informação nas subunidades
Discurso de conformidade da administração central	Entrevistas semiestruturadas	Membros do Comitê de Segurança da Informação da organização

Fonte: elaborado pelo autor.

A pesquisa documental envolveu consulta a diferentes documentos oficiais da organização e suas subunidades, como a Política de Segurança da Informação, o Sistema de Gestão de Segurança da Informação, portarias, mensagens de correio eletrônico, relatórios e regulamentos internos. As mensagens eletrônicas citadas pelos entrevistados foram solicitadas pelo pesquisador e, quando fornecidas, foram também analisadas como documentos pessoais. No total, foram analisados 36 documentos: a Política de Segurança da Informação; nove regulamentos internos (chamados de normas institucionais); oito portarias que definem a organização e a estrutura da Segurança da Informação na FIOCRUZ; cinco relatórios de auditorias externas e internas realizadas pelo TCU em 2010, 2012 e 2014, e pelo setor de

auditoria em 2014 e 2015; dois relatórios de atividades desenvolvidas pelo setor de auditoria em 2013 e 2014; quatro relatórios de gestão publicados pela organização em 2012, 2013 e 2014; oito relatos dos assuntos discutidos e das decisões tomadas nas reuniões do Comitê de Segurança da Informação e Comunicações; e uma mensagem de correio eletrônico. O Quadro 9 mostra todos os documentos sobre Segurança da Informação disponibilizados.

Quadro 9 – Documentos analisados.

NÚM.	DATA	IDENTIFICAÇÃO	ASSUNTOS
01	13/10/2010	Levantamento de Governança de TI 2010	Relatório do levantamento sobre Governança de TI realizado pelo TCU em 2010
02	21/02/2011	Portaria 069/2011-PR	Política de Segurança da Informação
03	25/02/2011	Portaria 070/2011-PR	Modelo de Gestão do Sistema de Segurança da Informação
04	07/04/2011	Portaria 116/2011-PR	Gestor de Segurança da Informação
05	28/04/2011	Portaria 143/2011-PR	Comitê de Segurança da Informação
06	17/04/2012	Portaria 347/2012-PR	Altera o Comitê de Segurança da Informação
07	17/04/2012	Norma Institucional SIC-001/CGTI/VPGDI	Responsabilidades dos usuários, senhas, equipamentos, mesa limpa e tela limpa
08	11/05/2012	Norma Institucional SIC-002/CGTI/VPGDI	Utilização do serviço de Internet
09	14/05/2012	Norma Institucional SIC-003/CGTI/VPGDI	Utilização do serviço de correio eletrônico
10	11/11/2012	Levantamento de Governança de TI 2012	Relatório do levantamento sobre Governança de TI realizado pelo TCU em 2012
11	15/02/2013	Norma Institucional SIC-004/CGTI/VPGDI	Controle de acesso e proteção física em *datacenters*
12	15/02/2013	Norma Institucional SIC-005/CGTI/VPGDI	Geração e recuperação de cópias de segurança (*backup*)
13	15/02/2013	Norma Institucional SIC-006/CGTI/VPGDI	Aquisição, desenvolvimento e manutenção de sistemas de informação
14	01/03/2013	Portaria 002/2013-VPGDI	Equipe de tratamento e resposta a incidentes
15	11/03/2013	Portaria 003/2013-VPGDI	Modelo de Gestão de Incidentes de Segurança da Informação
16	12/04/2013	Portaria 007/2013-VPGDI	Continuidade de Negócios de TI
17	31/05/2013	Relatório de Gestão do Exercício de 2012	Apresenta ações e projetos de Segurança da Informação da FIOCRUZ e resultados de auditorias realizadas pelo TCU
18	13/09/2013	Relato da 2ª Reunião de 2013 do CSIC	2ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2013
19	23/09/2013	Norma Institucional SIC-007/CGTI/VPGDI	Acesso remoto a rede de computadores
20	23/09/2013	Norma Institucional SIC-008/CGTI/VPGDI	Acesso a redes sociais
21	07/11/2013	Norma Institucional SIC-009/CGTI/VPGDI	Utilização de dispositivos móveis

NÚM.	DATA (cont.)	IDENTIFICAÇÃO (cont.)	ASSUNTOS (cont.)
22	12/11/2013	Relato da 3ª Reunião de 2013 do CSIC	3ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2013
23	11/04/2014	Relato da 1ª Reunião de 2014 do CSIC	1ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2014
24	06/05/2014	Análise da conformidade das unidades da FIOCRUZ à Política de Segurança da Informação e Comunicações	Resultado de auditoria interna realizada em 2014 nas subunidades organizacionais da FIOCRUZ
25	13/05/2014	Relato da 2ª Reunião de 2014 do CSIC	2ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2014
26	26/05/2014	Relatório de Gestão do Exercício de 2013	Apresenta ações e projetos de Segurança da Informação da FIOCRUZ e resultados de auditorias realizadas pelo TCU
27	10/07/2014	Revisão das Normas Complementares de Segurança da Informação 1, 2 e 3	Compilação das alterações a serem feitas em três regulamentos internos de Segurança da Informação da FIOCRUZ
28	10/07/2014	Relato da 3ª Reunião de 2014 do CSIC	3ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2014
29	09/09/2014	Relato da 4ª Reunião de 2014 do CSIC	4ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2014
30	10/10/2014	Relato da 5ª Reunião de 2014 do CSIC	5ª reunião do Comitê de Segurança da Informação e Comunicações da FIOCRUZ realizada em 2014
31	16/12/2014	Levantamento de Governança de TI 2014	Relatório do levantamento sobre Governança de TI realizado pelo TCU em 2014
32	ND	Relatório de auditoria de conformidade institucional com foco em TI	Resultado de auditorias realizadas em 2014 na CGTI e em sete subunidades organizacionais da FIOCRUZ
33	ND	Análise da conformidade das unidades da FIOCRUZ à POSIC – 2015	Resultado de auditoria interna realizada em 2015 nas subunidades organizacionais da FIOCRUZ
34	30/01/2015	Relatório Anual de Atividades de Auditoria Interna	Contém informações sobre as auditorias internas realizadas na FIOCRUZ, inclusive de Segurança da Informação
35	14/05/2015	Relatório de Gestão do Exercício de 2014	Apresenta ações da FIOCRUZ realizadas em 2014, inclusive sobre Segurança da Informação
36	24/08/2015	Email sobre alteração em regulamento da FIOCRUZ	Documento com o histórico de mensagens pedindo alteração em regulamentos internos

Nota: ND – não datado.
Fonte: elaborado pelo autor.

O roteiro utilizado nas entrevistas com os responsáveis pela Segurança da Informação nas subunidades (Apêndice A) tem três perguntas para identificar as medidas formais, informais e técnicas, antecedidas de uma explicação sobre os conceitos dessas três categorias a fim de situar os entrevistados, mais as 36 perguntas associadas aos construtos da pesquisa. O Quadro 10 apresenta as perguntas feitas aos entrevistados das subunidades.

Quadro 10 – Perguntas feitas aos informantes das subunidades.

PERGUNTAS DO ROTEIRO	CONSTRUTOS
P1 – Como sua subunidade é pressionada a adotar medidas de Segurança da Informação? P2 – Que mudanças ocorreram na sua subunidade depois da publicação dos regulamentos e da Política de Segurança da Informação da organização?	Pressões Institucionais
A1 – Como a adoção de medidas de Segurança da Informação realizada por outras organizações ou subunidades influencia as decisões de sua subunidade? A2 – Como você descreve a relação da sua subunidade com outras organizações, com sua sede ou com outras subunidades em termos de uso de sistemas e compartilhamento de dados? A3 – Como a relação da sua subunidade com outras organizações, com a sede ou outras subunidades influencia na adoção de medidas de Segurança da Informação? A4 – Em quais momentos sua subunidade adotou medidas de Segurança da Informação com relação à publicação de regulamentos ou da Política de Segurança da Informação? A5 – Foram consultadas Políticas de outras organizações ou subunidades durante a elaboração da Política da sua subunidade? A6 – O que levou sua subunidade a fazer essas consultas? A7 – Quais benefícios a adoção de medidas de Segurança da Informação trouxe para sua subunidade? A8 – De onde vêm esses benefícios? A9 – Por quais motivos medidas de Segurança da Informação foram adotadas por sua subunidade?	Resposta Estratégica de Aquiescência
C1 – Como você avalia a coerência das medidas de Segurança da Informação exigidas pela sede ou por outras organizações com as atividades de sua subunidade? C2 – Como as medidas adotadas pela administração central da organização influenciam o desenvolvimento das atividades ou o alcance dos objetivos da sua subunidade? C3 – Como a adoção de medidas de Segurança da Informação limita ou restringe as atividades desenvolvidas em sua subunidade? C4 – Quais atividades sua subunidade deixa de executar por ter adotado medidas de Segurança da Informação? C5 – Como você percebe a relação entre as medidas de Segurança da Informação exigidas e a disponibilidade dos recursos necessários para sua subunidade adotá-las? Considere recursos humanos, capital, infraestrutura e quaisquer outros recursos. C6 – Como sua subunidade se comporta quando sofre pressões para adotar medidas que são contrárias às suas atividades ou contraditórias com outras medidas também exigidas?	Resposta Estratégica de Compromisso
E1 – Quais medidas de Segurança da Informação foram adotadas na sua subunidade conforme os requisitos ou exigências externas ou da organização? E2 – A adoção dessas medidas ocorreu em que momento com relação à existência desses requisitos e exigências? E3 – O que acontece na subunidade quando há uma auditoria de Segurança da Informação? E4 – Há algum movimento para melhorar a conformidade em função ou em decorrência da auditoria? E5 – Como agem os envolvidos com a Segurança da Informação quando ocorre um incidente? E6 – O que acontece quando sua subunidade é convidada a participar de um novo programa, projeto ou ação da administração central que exige a adoção de medidas de Segurança da Informação?	Resposta Estratégica de Esquiva

PERGUNTAS DO ROTEIRO (cont.)	CONSTRUTOS (cont.)
D1 – Como sua subunidade se posiciona perante a administração central ou outras organizações quando é pressionada a adotar medidas de Segurança da Informação ineficientes ou prejudiciais às suas atividades?	Resposta Estratégica de Desafio
M1 – Comente sobre a participação do Comitê de Segurança da Informação ou do Escritório de Segurança da Informação da organização nas decisões de Segurança da Informação da sua subunidade. M2 – Quais vantagens a subunidade tem ou teria com a participação de pessoas da área de Segurança da Informação da sede em suas decisões? M3 – Comente agora sobre a participação da subunidade nas decisões de Segurança da Informação da administração central, do governo ou de outras organizações que regulam a Segurança da Informação. M4 – Como os membros da sua subunidade são orientados para participarem dessas decisões? M5 – Você considera que a subunidade tem algum poder ou influência sobre sua sede, o governo ou outras organizações que regulamentam a Segurança da Informação? M6 – Comente sobre a utilização pela sua subunidade do poder ou da influência que tem sobre a sede ou outras organizações quanto à criação, alteração ou extinção de regulamentos de Segurança da Informação.	Resposta Estratégica de Manipulação
S1 – Quando há uma obrigação ou necessidade de adotar tecnologias de Segurança da Informação, como são tomadas as decisões em sua subunidade? S2 – Quando há uma obrigação ou necessidade de adotar medidas formais de Segurança da Informação, como são tomadas as decisões em sua subunidade? S3 – Quando há uma obrigação ou necessidade de adotar medidas informais de Segurança da Informação, como são tomadas as decisões em sua subunidade?	Adoção de Medidas de Segurança da Informação
O1 – Houve mudanças em regulamentos e na Política de Segurança da Informação da organização decorrentes da adoção de medidas pela sua subunidade? O2 – Quais foram as medidas adotadas que provocaram essas mudanças? O3 – Quais foram as mudanças ocorridas nos regulamentos e na Política de Segurança da Informação?	Níveis de Conformidade Organizacional

Fonte: Elaborado pelo autor.

O Gestor de Segurança da Informação da organização e um membro do Comitê de Segurança da Informação que atua no setor de auditoria interna foram também entrevistados para confrontar as respostas dadas pelos membros das subunidades e colher informações sobre a administração central da FIOCRUZ. Para isso, foi utilizado um roteiro de entrevista distinto, contendo três perguntas referentes às medidas formais, informais e técnicas de Segurança da Informação adotadas pela administração central – idênticas às perguntas feitas aos demais entrevistados – e 13 perguntas sobre a percepção deles quanto aos benefícios da adoção, a coerência das medidas com os objetivos e estratégias da organização e seus efeitos negativos, os motivos para a adoção, o processo de adoção e o comportamento das subunidades diante das medidas adotadas pela administração central (Quadro 11).

Quadro 11 – Perguntas feitas aos membros do Comitê de Segurança da Informação.

PERGUNTAS DO ROTEIRO
P1: Quais são os benefícios que a adoção de medidas de Segurança da Informação traz para a FIOCRUZ?
P2: O governo publica regulamentos que obrigam a FIOCRUZ a adotar medidas de Segurança da Informação. Por favor, fale sobre a coerência entre os objetivos e estratégias da FIOCRUZ e essas medidas que ela é obrigada a adotar.
P3: Quais são as limitações ou prejuízos que a FIOCRUZ tem ao adotar certas medidas de Segurança da Informação?
P4: Porque medidas de Segurança da Informação são adotadas pela FIOCRUZ?
P5: A FIOCRUZ consulta outras organizações sobre as medidas de Segurança da Informação que elas adotam? Como é feita a consulta?
P6: Como a interconectividade da FIOCRUZ com outras organizações ou suas subunidades influencia na adoção de medidas de Segurança da Informação?
P7: Como foi o processo de elaboração da Política de Segurança da Informação da FIOCRUZ?
P8: Como foi a criação do Comitê de Segurança da Informação da FIOCRUZ?
P9: Como foi a criação dos regulamentos de Segurança da Informação da FIOCRUZ?
P10: Fale sobre o comportamento das subunidades diante da política e dos regulamentos de Segurança da Informação da FIOCRUZ.
P11: Por quais motivos as subunidades adotam ou deixam de adotar medidas de Segurança da Informação?
P12: Quais são os interesses das subunidades ao adotarem medidas de Segurança da Informação?
P13: Como você descreve a situação da FIOCRUZ quanto à conformidade com os requisitos externos de Segurança da Informação?

Fonte: Elaborado pelo autor.

O convite para participar da pesquisa foi enviado para 27 pessoas, incluindo o Gestor de Segurança da Informação e os 10 outros membros do Comitê de Segurança da Informação, mais os responsáveis pela Segurança da Informação e os responsáveis pela TI nas suas respectivas subunidades. Do total, 21 responderam ao convite, sendo que dois declararam não ter interesse em participar da pesquisa. Como resultado, foram entrevistadas 19 pessoas que participam das decisões de Segurança da Informação na administração central da organização ou em suas subunidades organizacionais, a saber: o Gestor de Segurança da Informação da FIOCRUZ; os responsáveis pela Segurança da Informação das suas respectivas subunidades organizacionais; membros do Comitê de Segurança da Informação da FIOCRUZ nas reuniões que tratam de políticas, orientações e regulamentos de Segurança da Informação para toda a organização; gestores de TI das subunidades organizacionais. As entrevistas duraram no mínimo 25 e no máximo 59 minutos, com uma duração média de 42 minutos.

Devido ao fato de a FIOCRUZ estar presente em diferentes estados brasileiros, 17 entrevistas foram realizadas remotamente utilizando o *software* Skype e duas foram presenciais. Todas as entrevistas foram gravadas e posteriormente transcritas pelo pesquisador responsável para documentos eletrônicos, conforme proposto por Flick (2009), visando à

garantia dos significados e das mensagens passadas pelos entrevistados, bem como à anonimidade dos dados.

4.5 PROCEDIMENTOS DE ANÁLISE DOS DADOS

A codificação dos dados coletados foi realizada com base no modelo teórico da pesquisa, o que é coerente com estudos de caso qualitativos, segundo Gil (2009). A análise qualitativa de conteúdo tem a utilização de categorias obtidas de modelos teóricos como característica essencial, complementa Flick (2009). Ainda segundo este autor, as categorias "são levadas para o material empírico e não necessariamente desenvolvidas a partir deste, embora sejam reiteradamente avaliadas em contraposição a esse material e, se necessário, modificadas." (FLICK, 2009, p.291). Assim, para proceder com a análise qualitativa fundamentada na teoria, as categorias presentes no *framework* da pesquisa foram organizadas utilizando o *software* NVivo 10 em nós relacionados aos construtos da pesquisa e em subnós relacionados aos seus indicadores, os quais serviram para analisar os dados obtidos nos documentos e transcrições das entrevistas.

Inicialmente, foi feita uma organização preliminar dos documentos e foi realizada uma leitura completa para obter uma percepção geral dos dados, como recomendado por Creswell (2010). Depois, como orientado por Flick (2009), foi feita uma seleção dos trechos das entrevistas relevantes para a pesquisa; em um segundo momento, foi feita a análise da situação de coleta do material, indicando se foi presencial ou à distância, e uma caracterização do material, indicando se houve alguma influência ou interferência durante a realização da entrevista ou na transcrição para documentos digitais; por fim, foram analisados os documentos diante das categorias previamente criadas no NVivo.

Os arquivos digitais contendo os trechos relevantes das transcrições das entrevistas e os documentos organizacionais obtidos foram importados para o NVivo como fontes de dados internas, o que permitiu categorizar trechos relevantes nos subnós previamente criados no *software*, conforme os construtos da pesquisa. A categorização dos trechos relevantes das respostas às três perguntas iniciais da entrevista consistiu em uma análise e comparação com uma lista de medidas de Segurança da Informação identificadas previamente na literatura (Apêndice B) e categorizadas nos subnós "Medidas técnicas adotadas", "Medidas formais adotadas" e "Medidas informais adotadas". As demais respostas

foram analisadas a fim de identificar os indicadores da pesquisa para categorização nos subnós correspondentes. O Quadro 12 apresenta a hierarquia de nós e subnós criada no software NVivo para categorização dos dados da pesquisa.

Quadro 12 – Hierarquia de nós e subnós criada no *software* NVivo.

NÓS	SUBNÓS
Pressões institucionais	Programas de conscientização
	Regulamentos de Segurança da Informação
	Política de Segurança da Informação
Aquiescência	Hábito
	Imitação
	Conformidade
Compromisso	Equilíbrio
	Pacificação
	Barganha
Esquiva	Ocultação
	Amortecimento
	Fuga
Desafio	Rejeição
	Contestação
	Ataque
Manipulação	Cooptação
	Influência
	Controle
Adoção de medidas de Segurança da Informação	Medidas técnicas adotadas
	Medidas formais adotadas
	Medidas informais adotadas
Níveis de conformidade	Ocorrência de respostas distintas
	Tratamentos distintos às pressões para medidas técnicas, formais e informais
	Adoção de medidas contrárias aos objetivos e interesses da sede
	Ocorrência de alterações em regulamentos e na Política de Segurança
	Ocorrência de respostas de conformidade

Fonte: Elaborado pelo autor.

4.6 PROCEDIMENTOS PARA GARANTIA DA QUALIDADE DA PESQUISA

Creswell (2010) ressalta a relevância de incluir em um estudo qualitativo uma seção específica para tratar da qualidade da pesquisa. Segundo Flick (2009), a qualidade da pesquisa qualitativa é avaliada com base nos critérios de confiabilidade e validade, considerados clássicos pelo autor.

De acordo com Creswell (2010), a confiabilidade da pesquisa qualitativa indica que a abordagem do pesquisador está coerente com a utilizada em trabalhos de outros autores. Já Flick (2009) esclarece que a confiabilidade pode ser obtida por diferentes procedimentos. Nas pesquisas que envolvem entrevistas, o autor sugere que seja feita uma verificação do roteiro de entrevista e suas perguntas após a realização da primeira entrevista. Não foram realizadas mudanças após a primeira entrevista desta pesquisa, de forma que os roteiros foram mantidos até a conclusão. No entanto, o protocolo foi validado por pesquisadores e especialistas antes da realização das entrevistas, como descrito adiante.

Já durante a interpretação dos dados qualitativos, Flick (2009) sugere que os trechos sejam comparados com outros a fim de avaliar sua adequação às categorias elaboradas na codificação. O autor complementa que a origem dos dados deve estar clara de forma que seja possível separar as palavras do entrevistado da interpretação do pesquisador, e que os procedimentos adotados sejam documentados a fim de possibilitar a checagem da consistência de ambos (dados e procedimentos). Creswell (2010) cita Gibbs (2007) sugerindo que, nas pesquisas qualitativas que não envolvem mais de um pesquisador, sejam realizados os seguintes procedimentos a fim de aumentar a confiabilidade: a) uma verificação das transcrições para evitar erros cometidos no processo; e b) a realização de comparações constantes entre os dados e as categorias de análise a fim de evitar desvios de categorização. Como toda a pesquisa foi realizada por apenas um pesquisador, foi feita uma comparação entre as transcrições das entrevistas com o conteúdo das gravações: as transcrições foram lidas ao mesmo tempo em que as gravações das entrevistas eram ouvidas a fim de evitar erros de transcrição. Todo o processo de análise das transcrições das entrevistas e dos documentos obtidos durante a pesquisa foi feito através de comparações com outros trechos do mesmo ou de outros documentos, o que facilitou a organização dos dados nas categorias de análise. A interpretação dos trechos analisados foi anotada em um documento separado, não importado para a base de dados do NVivo, a fim de evitar sobreposição dos dados com a interpretação feita pelo pesquisador.

A validade da pesquisa qualitativa, segundo Flick (2009), recebe mais atenção do que a confiabilidade. Para o autor, essa questão se resume à certeza de que a interpretação daquilo que o pesquisador viu corresponde àquilo que ele de fato viu. Os três tipos de erros que podem ocorrer em uma pesquisa qualitativa, ainda segundo o autor, são: a) ver uma relação ou princípio que não existe; b) não ver (ou rejeitar) uma relação ou princípio que existe; e c) fazer as perguntas erradas nas entrevistas. Flick (2009) conclui que a validade da

pesquisa qualitativa diz respeito ao quanto as construções que o pesquisador faz dos dados têm por base as construções dos entrevistados, e ao quanto isso é transparente para as outras pessoas.

Para fins de validação, o protocolo de estudo de caso (Apêndice A), contendo o objetivo, os construtos e indicadores, o *framework*, as questões de pesquisa e o roteiro de entrevista, foi avaliado por 17 pesquisadores e autores de trabalhos da área temática de Sistemas de Informação em duas etapas. Inicialmente, o protocolo foi avaliado por nove pesquisadores do Grupo de Pesquisa de Adoção de TI da Escola de Administração da Universidade Federal da Bahia (UFBA) em diferentes reuniões. Depois de realizadas as alterações consideradas pertinentes, o documento foi enviado para 19 especialistas e pesquisadores externos com experiência em Segurança da Informação, Sistemas de Informação, metodologia de pesquisa e na abordagem teórica utilizada na pesquisa. Desses, sete enviaram comentários por correio eletrônico e um fez seus comentários através de reunião utilizando o *software* Skype. Dos que participaram da avaliação, um é especialista em Segurança da Informação com atuação no mercado e professor de pós-graduação, quatro são professores doutores que desenvolvem pesquisas na área de Sistemas de Informação – dentre os quais dois têm trabalhos publicados sobre Segurança da Informação –, e três são estudantes de doutorado de outro programa de pós-graduação. Ao final deste segundo momento do processo de validação, foram realizados diversos ajustes no protocolo, principalmente no roteiro de entrevista, o que ajudou a minimizar a possibilidade da ocorrência dos erros cuja possibilidade foi apontada por Flick (2009).

Para Creswell (2010), a validade é um dos pontos fortes das pesquisas qualitativas e se apresenta através da verificação da precisão dos resultados sob os pontos de vista do pesquisador, do participante e de terceiros. Essa precisão pode ser avaliada por diferentes estratégias apresentadas pelo autor, dentre as quais estão: a) triangulação de diferentes fontes de informações; b) verificação pelos participantes, que consiste em retornar aos participantes da pesquisa as análises realizadas com base nos dados brutos; c) riqueza e densidade da descrição, apresentando múltiplas perspectivas sobre os assuntos tratados; e d) revisão por pares, que consiste em encaminhar a pesquisa para ser revisada por uma ou mais pessoas do grupo de pesquisa, além do próprio pesquisador.

Este estudo envolveu a análise de dados obtidos através de entrevistas e documentos produzidos e disponibilizados pela organização e pelo Tribunal de Contas da União (TCU), garantindo a utilização de diferentes fontes de informações. Depois de

verificados e corrigidos eventuais erros de transcrição, os documentos eletrônicos das entrevistas foram enviados por correio eletrônico para os 19 entrevistados a fim de que os resultados fossem confirmados ou corrigidos, caso necessário, garantindo que as ideias dos entrevistados estivessem presentes nas transcrições. Do total de entrevistados, sete responderam validando as transcrições das entrevistas, um solicitou a retirada de trechos e um fez alterações no documento. As demais transcrições foram consideradas tacitamente validadas. Pelo fato de as entrevistas terem sido realizadas com gestores e responsáveis pela Segurança da Informação e TI de diferentes subunidades e membros do Comitê de Segurança da Informação da organização, fica garantido que foram analisadas múltiplas perspectivas sobre o fenômeno.

Tratando especificamente do método de estudo de caso, Yin (2010) propõe como critérios de julgamento da qualidade a realização de quatro diferentes testes:

a) Validade do construto: trata da identificação das medidas operacionais adequadas aos conceitos estudados. Isso pode ser feito durante a coleta de dados através do uso de múltiplas fontes de evidência e da manutenção de um encadeamento de evidências de forma que a questão da pesquisa leve às conclusões e vice-versa, ou através da identificação de medidas operacionais (indicadores) na literatura e da revisão do estudo de caso por informantes-chave.

b) Validade interna: busca evitar conclusões incorretas. Trata do quanto as deduções feitas pelo pesquisador estão corretas, combinadas com um padrão baseado na teoria. Trata também da construção das explicações e de explicações alternativas, que podem ser consideradas pelo pesquisador durante a análise de dados, e se foi utilizado um modelo lógico para análise dos dados. Yin (2010) esclarece ser esta uma preocupação de estudos de caso explanatórios.

c) Validade externa: teste que busca saber se é possível generalizar para além do caso estudado, o que não deve ser feito com base em preceitos estatísticos, mas a partir da ideia de generalização analítica, quando o pesquisador generaliza os resultados a uma teoria mais ampla através da realização de outros estudos de caso. Em se tratando de estudo de caso único, a validade externa limita-se à possibilidade de aplicar o mesmo procedimento em outros casos, que podem ser estudados posteriormente.

d) Confiabilidade: tem o objetivo de garantir que o mesmo procedimento, se seguido em um mesmo estudo de caso, traga os mesmos resultados. Isso pode ser feito através da documentação dos procedimentos adotados em um protocolo de estudo de caso e do desenvolvimento e manutenção de uma base de dados.

Além de terem sido utilizadas múltiplas fontes de evidência, os construtos e indicadores da pesquisa foram identificados na literatura e apresentados a pesquisadores do Grupo de Pesquisa de Adoção de TI da UFBA e a diferentes pesquisadores e especialistas externos ao grupo, o que garante a validade dos construtos. A validade interna é garantida pelo fato de os resultados terem sido apresentados a pesquisadores da área de Sistemas de Informação, que entenderam que as conclusões e as explicações apresentadas pelo autor estão corretas. Além disso, o fato de ter sido utilizado um *framework* como modelo para análise dos dados reforça sua validade interna. O estudo pode ser replicado em qualquer organização que conte com uma estrutura de Governança da Segurança da Informação, como a existência de um Comitê de Segurança da Informação e de um Escritório de Segurança da Informação, e com uma Política de Segurança da Informação e regulamentos internos complementares a essa política, e que tenha uma estrutura organizacional descentralizada, com subunidades que gozem de autonomia administrativa. Essa possibilidade de replicação em outros casos garante que seja verificada sua validade externa. Todo o processo de validação do protocolo de estudo de caso está documentado, a base de dados criada com as transcrições das entrevistas e com os documentos organizacionais e os arquivos de áudio gerados nas entrevistas estão preservados, e todos os demais procedimentos utilizados estão documentados. Com isso, fica garantida a confiabilidade da pesquisa.

Gil (2009) apresenta cinco critérios que visam assegurar rigor científico aos estudos de caso:

a) Objetividade: tem a ver com a padronização e estruturação de instrumentos de forma a tornar mais objetiva a mensuração de fenômenos sociais, ajudando o pesquisador a conseguir que seu trabalho possa ser replicado e averiguado. Gil (2009) considera que a busca pela objetividade refere-se aos métodos e técnicas utilizados para coletar os dados e analisar os resultados da pesquisa.

b) Precisão: em estudos de caso, é difícil garantir precisão, pois esses trabalhos, de modo geral, são qualitativos e não tratam de variáveis mensuráveis numericamente, mas de atributos ou conceitos. No entanto, esses atributos e conceitos devem estar claros o suficiente para que permitam a categorização dos dados.

c) Operacionalidade: os conceitos utilizados nos estudos de caso devem ser operacionais, o que Gil (2009) relaciona à validade de construto. O autor entende construto como uma construção mental que representa o significado teórico de um conceito ou proposição. A verificação da validade do construto pode ser feita contrastando os resultados com a teoria e essa validade pode aumentar em um estudo de caso único utilizando múltiplas técnicas de coleta de dados que permitam a comparação dos resultados.

d) Credibilidade: semelhante à validade interna das pesquisas quantitativas, está mais relacionada aos estudos de caso explicativos (ou explanatórios). Não se refere à relação de causa e efeito entre variáveis, mas com o quanto os resultados da pesquisa reproduzem os fenômenos pesquisados ou os pontos de vista dos participantes. Tem a ver, portanto, com a coerência entre as proposições iniciais, o desenvolvimento e os resultados da pesquisa – a correspondência entre os resultados e a realidade reconhecida pelos participantes. Entre os procedimentos para verificar a confiabilidade da pesquisa, Gil (2009) recomenda a triangulação dos dados obtidos e a revisão pelos próprios entrevistados.

e) Transferibilidade: possibilidade de os dados obtidos na pesquisa qualitativa serem aplicados a outro contexto, ou a possibilidade de generalização das descobertas, o que Gil (2009) demonstra ser possível mesmo com estudos de caso únicos, pois a generalização em estudos de caso não é estatística, mas analítica. Isso acontece através da reunião de dados de um fenômeno, comparação desses dados, identificação de regularidades e, finalmente, generalização para a uma teoria mais abrangente.

Como foi utilizado o mesmo roteiro em todas as entrevistas realizadas com informantes que atuam nas subunidades organizacionais – as exceções foram o Gestor de Segurança da Informação da organização e um membro do Comitê de Segurança da

Informação, que responderam a perguntas específicas sobre o comportamento da sede e das subunidades – e como a análise foi feita utilizando a mesma estrutura de construtos, o estudo de caso atende ao critério de objetividade. A precisão do estudo de caso é reforçada pela utilização construtos e indicadores claros, identificados na literatura. Como os construtos utilizados na pesquisa foram validados tanto com membros do grupo de pesquisa quanto com pesquisadores externos, fica demonstrada sua operacionalidade. O que dá credibilidade ao estudo é o fato de as transcrições das entrevistas terem sido validadas pelos participantes. Além disso, foram utilizadas múltiplas fontes de dados na pesquisa, reforçando sua credibilidade. Por fim, o fato de o *framework* da pesquisa poder ser utilizado para investigar o mesmo fenômeno em outras organizações permite a generalização analítica do estudo, dando a ela transferibilidade.

5 APRESENTAÇÃO DO CASO

A pesquisa foi realizada na Fundação Oswaldo Cruz (FIOCRUZ), uma fundação pública de direito público sediada no Rio de Janeiro. A FIOCRUZ é a organização vinculada ao Ministério da Saúde que tem a responsabilidade de desenvolver pesquisas e tecnologia em saúde pública. Para isto, atua em projetos de pesquisa e desenvolvimento tecnológico em diversas doenças infectocontagiosas e negligenciadas, bem como na formação e qualificação de pesquisadores e profissionais de saúde (FIOCRUZ, 2010).

A organização tem subunidades descentralizadas com atuação técnico-científica, além de diretorias, coordenações, subunidades técnico-administrativas e escritórios distribuídos em 11 estados brasileiros: Amazonas, Bahia, Ceará, Distrito Federal, Mato Grosso, Minas Gerais, Paraná, Pernambuco, Piauí, Rio de Janeiro e Rondônia, além de um escritório em Maputo, capital do Moçambique (FIOCRUZ, 2016d) (ver Figura 6).

As subunidades são, em sua maioria, institutos de pesquisa, que realizam principalmente atividades de pesquisa e ensino, mas há também fábricas de fármacos e vacinas e subunidades que prestam serviços diretamente para a sociedade. As subunidades técnico-científicas da FIOCRUZ são as seguintes (FIOCRUZ, 2016d):

a) Instituto de Tecnologia em Imunobiológicos (BIO-Manguinhos);
b) Instituto de Comunicação e Informação Científica e Tecnológica (ICICT);
c) Casa de Oswaldo Cruz (COC);
d) Escola Nacional de Saúde Pública Sérgio Arouca (ENSP);
e) Escola Politécnica de Saúde Joaquim Venâncio (EPSJV);
f) Instituto de Tecnologia em Fármacos (FARManguinhos);
g) Instituto Fernandes Figueira (IFF);
h) Instituto Nacional de Infectologia Evandro Chagas (INI);
i) Instituto Nacional de Controle e Qualidade em Saúde (INCQS);
j) Instituto Oswaldo Cruz (IOC);
k) Instituto Aggeu Magalhães (IAM), em Recife, Pernambuco;
l) Instituto René Rachou (IRR), em Belo Horizonte, Minas Gerais;
m) Instituto Leônidas e Maria Deane (ILMD), em Manaus, Amazonas;
n) Instituto Carlos Chagas (ICC), em Curitiba, Paraná;
o) Instituto Gonçalo Moniz (IGM), em Salvador, Bahia.

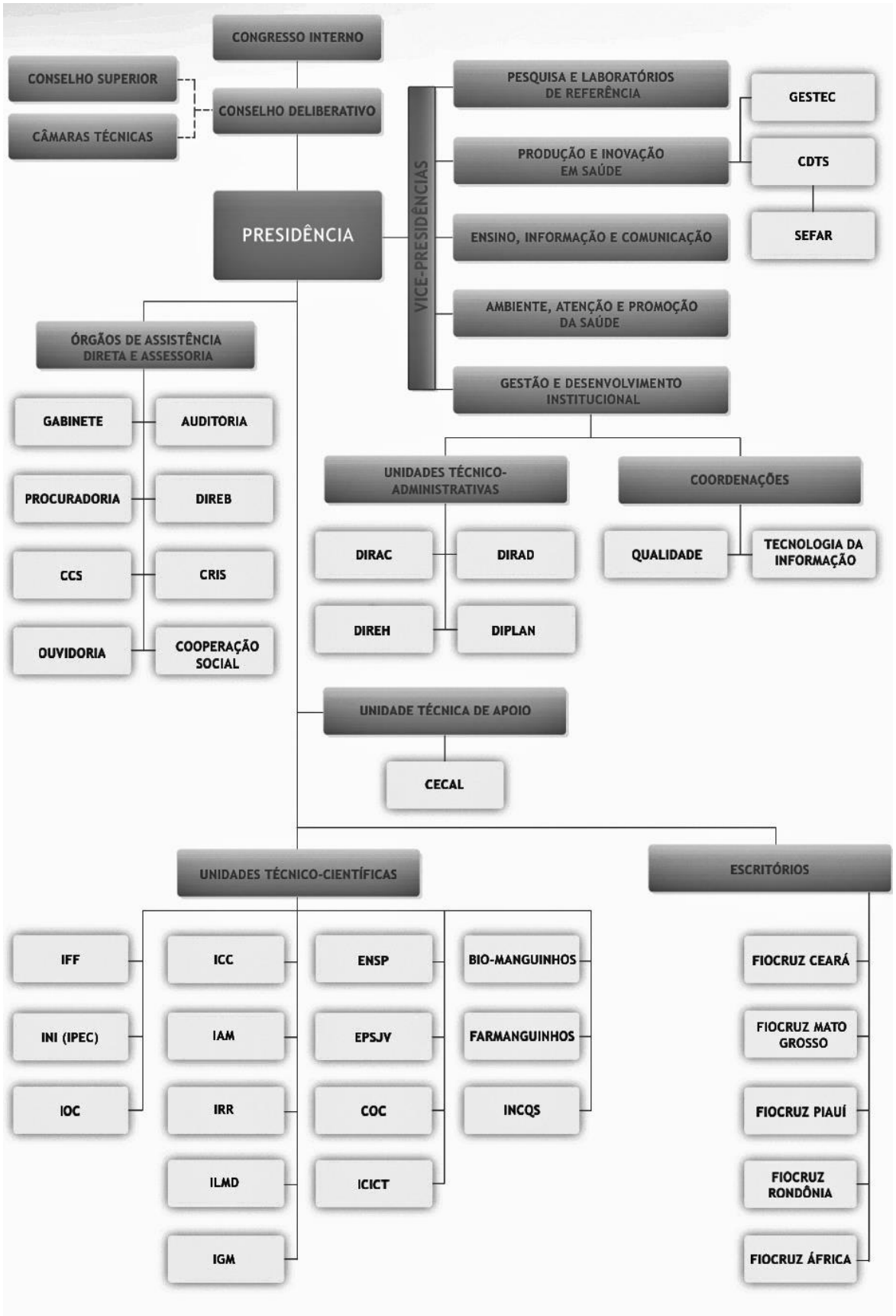


Figura 6 – Organograma da FIOCRUZ.
Fonte: FIOCRUZ (2016c).

O *website* da organização (FIOCRUZ, 2016d) mostra que, além daquelas com atuação técnico-científica, existem ainda subunidades vinculadas diretamente à Presidência da FIOCRUZ ou a uma das suas Vice-Presidências, atuando como subunidades de assessoria e apoio e tendo, portanto, menos autonomia administrativa do que as demais. Entre essas estão as subunidades técnico-administrativas: Diretoria de Administração do *Campus* (DIRAC), Diretoria de Administração (DIRAD), Diretoria de Recursos Humanos (DIREH) e Diretoria de Planejamento Estratégico (DIPLAN). As subunidades de assistência direta e assessoria e as coordenações são: o Gabinete da Presidência; Procuradoria; Ouvidoria; Auditoria Interna (AUDIN); Coordenadoria de Comunicação Social (CCS); Centro de Operações Internacionais em Saúde (CRIS); Coordenadoria de Cooperação Social; Diretoria Regional de Brasília (DIREB); Coordenação de Qualidade; Coordenação de Gestão de Tecnologia da Informação (CGTI); Coordenação de Gestão Tecnológica (GESTEC); e Centro de Desenvolvimento Tecnológico em Saúde (CDTS). Os escritórios regionais são a FIOCRUZ Ceará, FIOCRUZ Mato Grosso, FIOCRUZ Piauí, FIOCRUZ Rondônia e FIOCRUZ África. Por fim, a única subunidade técnica de apoio é o Centro de Criação de Animais de Laboratório (CECAL). Cada uma dessas subunidades é chefiada por um Diretor ou Coordenador, que responde diretamente ao Presidente ou a um dos cinco Vice-Presidentes.

Por ser uma fundação pública vinculada ao Poder Executivo Federal, a FIOCRUZ integra o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Governo Federal e está subordinada aos regulamentos emitidos pela Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MPOG) (CEPIK; CANABARRO; POSSAMAI, 2014). Está sujeita também aos regulamentos do Departamento de Segurança da Informação e Comunicações (DSIC) e Núcleo de Segurança e Credenciamento (NSC) do Gabinete de Segurança Institucional (GSI) da Presidência da República. Devido ao fato de atuar no desenvolvimento de pesquisas científicas, a FIOCRUZ está subordinada às leis, instruções normativas e outros regulamentos aplicáveis aos institutos de pesquisa públicos. A organização desenvolve pesquisas científicas na área de saúde, e por este motivo está subordinada a regulamentos e normas éticas relacionadas à privacidade dos pacientes e proteção de informações sobre o sujeito da pesquisa.

Embora parte das suas subunidades goze de autonomia administrativa, a CGTI é responsável por ações centralizadas de TI que alcançam toda a organização e é vinculada à

Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação (FIOCRUZ, 2016a). A CGTI é composta por cinco serviços (FIOCRUZ, 2011c):

a) Serviço de Suporte ao Usuário;
b) Serviço de Sistemas de Informação;
c) Serviço de Infraestrutura Tecnológica;
d) Serviço de Garantia da Qualidade em Tecnologia da Informação;
e) Serviço de Segurança da Informação e Comunicações.

A Segurança da Informação na FIOCRUZ é responsabilidade do Serviço de Segurança da Informação e Comunicações, chefiada pelo Gestor de Segurança da Informação e Comunicações, que também preside o Comitê de Segurança da Informação e Comunicações, colegiado responsável por ações de Segurança da Informação, como implantação de soluções tecnológicas, elaboração e proposição de normas e procedimentos internos de Segurança da Informação para a organização. A FIOCRUZ dispõe ainda de uma Política de Segurança da Informação e Comunicações (POSIC) e nove regulamentos já elaborados, discutidos e aprovados pelo Comitê (FIOCRUZ, 2016b).

O Comitê de Segurança da Informação da FIOCRUZ é composto por 11 membros, sendo que quatro são fixos e sete são eletivos. Os quatro membros fixos são o Gestor de Segurança da Informação e Comunicações, um membro da AUDIN, um da CCS e um da DIREH. Os sete membros eletivos compõem o Comitê por dois anos e são escolhidos entre os responsáveis pela Segurança da Informação nas suas respectivas subunidades organizacionais em reuniões da Câmara Técnica de Gestão e Desenvolvimento Institucional da FIOCRUZ – um colegiado composto pelos Vice-Diretores de Gestão das subunidades e membros da Vice-Presidência de Gestão e Desenvolvimento Institucional e da DIREH (FIOCRUZ, 2016b).

A seguir, serão apresentados os resultados da pesquisa, coletados em entrevistas com membros do Comitê de Segurança da Informação e Comunicações, gestores de TI e responsáveis pela Segurança da Informação nas subunidades, e também na análise dos documentos disponibilizados pela organização.

6 APRESENTAÇÃO E ANÁLISE DOS DADOS

A análise das transcrições das entrevistas e dos documentos foi realizada com base no *framework* da pesquisa. Inicialmente, são apresentados dados sobre os entrevistados, sobre a Segurança da Informação na FIOCRUZ e em nas subunidades organizacionais que participaram da pesquisa. Por fim, os dados são analisados de acordo com os construtos da pesquisa, como categorizados no *software* NVivo. Cabe registrar que os nomes das subunidades organizacionais e dos entrevistados foram substituídos a fim de evitar sua identificação.

6.1 OS ENTREVISTADOS

Dos 19 entrevistados, um é lotado na CGTI, dois trabalham em subunidades de assessoria e assistência direta à Presidência da FIOCRUZ, três são lotados em escritórios regionais e 13 trabalham em subunidades técnico-científicas, oito delas localizadas no Rio de Janeiro e cinco em outros estados. As subunidades técnico-científicas desenvolvem atividades principalmente de pesquisa científica, mas também de ensino, prestação de serviços e produção de insumos para a saúde, enquanto as demais atuam em questões relacionadas à gestão da organização, como planejamento estratégico, auditoria e recursos humanos. Dentre as 11 subunidades localizadas no Rio de Janeiro, nove são técnico-científicas e uma delas não fica no *campus* onde está a sede administrativa da FIOCRUZ. Todas as subunidades técnico-científicas, escritórios regionais e demais subunidades localizadas fora do *campus* da sede da FIOCRUZ têm pelo menos uma pessoa responsável pelas ações de TI no âmbito local.

Os entrevistados são, em maioria, servidores efetivos da FIOCRUZ (16), mas também foram entrevistados dois funcionários terceirizados que exercem atividades de Segurança da Informação nas suas subunidades, além de um servidor de outra organização que ocupa um cargo de chefia. O entrevistado com menos tempo na FIOCRUZ trabalha há dois anos, e o que tem mais tempo trabalha há 30 anos na organização. Oito entrevistados exercem função de chefia, enquanto os demais atuam principalmente em atividades técnicas. Três entrevistados trabalham exclusivamente com Segurança da Informação e 14 conciliam essas atividades com outras de TI, enquanto dois atuam exclusivamente em atividades de

gestão de TI. Sobre a formação dos entrevistados, 17 fizeram graduação na área de TI. Dos 19 participantes, 15 fizeram especialização e quatro cursaram mestrado. Apenas uma mulher foi entrevistada.

A seção seguinte mostra como a Segurança da Informação foi organizada na FIOCRUZ, apresentando as leis e regulamentos do Governo que pressionaram a adoção de medidas de Segurança da Informação, os documentos que definem a estrutura organizacional de Segurança da Informação e os regulamentos publicados pela organização.

6.2 SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO

A Segurança da Informação na FIOCRUZ é uma das responsabilidades da CGTI, que tem em sua estrutura o Serviço de Segurança da Informação e Comunicações. Este departamento é responsável por promover a cultura de Segurança da Informação, acompanhar investigações e avaliações dos incidentes ocorridos, propor os recursos necessários para a execução das ações de Segurança da Informação, estudar os impactos de novas tecnologias sobre a Segurança da Informação e implantar a Política de Segurança da Informação e acompanhar a conformidade da organização (FIOCRUZ, 2016b), atribuições de um Escritório de Segurança da Informação, segundo Casey (2005), Sêmola (2014) e Manoel (2014). Seu coordenador também preside o Comitê de Segurança da Informação da organização.

Os documentos analisados mostram que o Comitê de Segurança da Informação da FIOCRUZ é responsável por assessorar o Serviço de Segurança da Informação e Comunicações na implementação de ações de Segurança da Informação. Através de grupos de trabalho, o Comitê trata também de assuntos específicos relacionados ao tema e propõe soluções, procedimentos e regulamentos internos de Segurança da Informação para a organização (FIOCRUZ, 2011e). Criado em 2011 com nove membros, o Comitê foi reformulado em 2012, quando houve a inclusão de dois novos membros e a substituição de parte dos membros da composição anterior (FIOCRUZ, 2012b).

A partir dos documentos analisados, e corroborando com os dados colhidos nas entrevistas com membros do Comitê de Segurança da Informação da FIOCRUZ, ficou claro que a organização adotou diversas medidas formais de Segurança da Informação. Com políticas e regulamentos aprovados e publicados, processos formais documentados, procedimentos operacionais, profissionais especialistas com dedicação exclusiva às atividades

de Segurança da Informação e estruturas organizacionais de Segurança da Informação instituídas, a FIOCRUZ demonstra ter adotado diversas medidas formais que impõem requisitos tanto para a administração central quanto para as subunidades organizacionais.

Além de um Escritório e de um Comitê de Segurança da Informação, foi instituída através da Portaria 069/2011-PR da Presidência da organização (FIOCRUZ, 2011a) a sua Política de Segurança da Informação. Embora a literatura deixe claro que a elaboração e revisão da Política de Segurança da Informação é uma responsabilidade do Comitê de Segurança da Informação da organização (SÊMOLA, 2014; MANOEL, 2014), cabe registrar que a POSIC da FIOCRUZ foi publicada antes de seu Comitê ter sido formalizado. Além disso, o documento foi formalizado anos depois da publicação da Instrução Normativa GSI/PR nº 1 (BRASIL, 2008a) pelo GSI, que determina que os órgãos e entidades da Administração Pública federal devem instituir um Comitê e aprovar uma Política de Segurança da Informação.

A demora em ter uma Política e um Comitê de Segurança da Informação formalizados – o que só aconteceu em 2011 (FIOCRUZ, 2011a, 2011e) – foi notada em uma auditoria realizada pelo TCU em 2010, que constatou também que a organização não tinha adotado outras medidas formais, como processos de classificação de informações, análise e avaliação de riscos e gestão de incidentes, ou ter um responsável pela Segurança da Informação formalmente designado (TCU, 2010). Entretanto, no relatório de uma auditoria posterior, o TCU registrou que, embora ainda não tivesse processos de gestão de riscos nem feito inventário de ativos de informação, classificação de informações e análise de riscos, e de não ter uma política de controle de acesso ou uma equipe de tratamento de incidentes formalmente instituída, a FIOCRUZ já tinha diretrizes para gestão de Segurança da Informação, um gestor de Segurança da Informação designado e uma Política de Segurança da Informação formalizada (TCU, 2012).

O último relatório de auditoria do TCU divulgado pela FIOCRUZ (TCU, 2014) mostra que a conformidade da organização com os requisitos externos de Segurança da Informação aumentou em comparação com os resultados de auditorias anteriores (TCU, 2010, 2012), mas mostra também que a organização não realizava revisão periódica da Política de Segurança da Informação e não tinha uma Política de Controle de Acesso, processos de tratamento e classificação de informações nem de gestão de vulnerabilidades, além de não realizar monitoramento do uso dos recursos tecnológicos, embora houvesse previsão para isso

em regulamentos da organização e na literatura (HÖNE; ELOFF, 2002; MARTINS; SANTOS, 2005; ABNT, 2013; SÊMOLA, 2014).

Por outro lado, a auditoria identificou política de *backup* de dados documentada, processo de inventário de ativos de informação, responsabilidades definidas pelos ativos de informação, equipe de tratamento de incidentes, ações periódicas de conscientização, educação e treinamento, recursos criptográficos e processos de gestão de riscos, vulnerabilidades técnicas de TI e incidentes de Segurança da Informação. O relatório do TCU (2014) mostra também que, apesar de reconhecer que não tem uma rotina da classificação de informações, a FIOCRUZ considera ter adotado meios para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação – sobre isso, há um entendimento de que é necessário classificar as informações quanto à garantia de confidencialidade, o que permite definir as medidas necessárias para protegê-las, e há também uma compreensão de que a classificação é uma premissa para elaborar praticamente todos os regulamentos de Segurança da Informação (MARTINS; SANTOS, 2005; SÊMOLA, 2014).

A pesquisa documental mostrou que os regulamentos da FIOCRUZ foram criados depois da publicação de diferentes leis e regulamentos de Segurança da Informação pelo Governo Federal. Após a publicação do Decreto nº 3.505, de 13 de junho de 2000 (BRASIL, 2000), foi instituída a Política de Segurança da Informação da Administração Pública Federal, que tem o objetivo de estabelecer normas jurídicas para implantação e manutenção da Segurança da Informação nos órgãos e entidades públicos federais. A partir deste decreto, diferentes portarias, instruções normativas e normas complementares foram publicadas pelos órgãos que definem os processos de TI e Segurança da Informação na Administração Pública Federal.

Dentre os regulamentos publicados depois do Decreto nº 3.505/2000, é possível destacar a Instrução Normativa GSI/PR nº 2 (BRASIL, 2013a), a Instrução Normativa GSI/PR nº 3 (BRASIL, 2013b) e já citada Instrução Normativa GSI/PR nº 1 (BRASIL, 2008a), pois deram vez à publicação pelo DSIC e NSC de diversos outros regulamentos que criam obrigações relacionadas à adoção de medidas de Segurança da Informação. Nesse sentido, a publicação da Norma Complementar nº 2/IN01/DSIC/GSIPR (BRASIL, 2008b), que define uma metodologia de gestão de Segurança da Informação para os órgãos e entidades públicos federais, determina que as organizações devem identificar e analisar os riscos, formalizar uma Política e implementar uma infraestrutura de Segurança da Informação. A Norma Complementar nº 3/IN01/DSIC/GSIPR (BRASIL, 2009a) traz recomendações para

a elaboração, institucionalização, divulgação e atualização das políticas de Segurança da Informação dos órgãos e entidades públicos federais. Somente depois da publicação destes regulamentos, a FIOCRUZ formalizou uma Política de Segurança da Informação (FIOCRUZ, 2011a), instituiu um modelo de gestão de Segurança da Informação (FIOCRUZ, 2011b), designou um gestor de Segurança da Informação (FIOCRUZ, 2011d) e instituiu um Comitê de Segurança da Informação (FIOCRUZ, 2011e).

De forma semelhante, depois de publicada a Norma Complementar nº 5/IN01/DSIC/GSIPR (BRASIL, 2009b), que disciplina a criação de equipes de tratamento e resposta a incidentes de Segurança da Informação na Administração Pública Federal, a FIOCRUZ instituiu em 2013, através da Portaria 02/2013-VPGDI (FIOCRUZ, 2013b), sua Equipe de Tratamento de Incidentes. Com a responsabilidade de responder aos incidentes ocorridos nas redes de computadores de toda a organização, a Equipe tem profissionais dedicados exclusivamente a essas atividades. Devido ao fato de a organização ter algumas subunidades descentralizadas geograficamente, localizadas em cidades e estados distantes da administração central, supõe-se que a estrutura mais adequada da Equipe de Tratamento de Incidentes na FIOCRUZ seja a combinada (ou mista), conforme um dos modelos propostos pela Norma Complementar nº 5/IN01/DSIC/GSIPR (BRASIL, 2009b, p.9), que prevê a existência de uma "Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais central e equipes distribuídas pela organização." Entretanto, embora detalhe parte das atividades da Equipe, a Portaria não deixa claro como deve ser seu funcionamento nas subunidades geograficamente descentralizadas.

A Portaria 007/2013-VPGDI (FIOCRUZ, 2013d), publicada em 12 de abril de 2013, institui um modelo de gestão de continuidade do negócio na FIOCRUZ, que aborda apenas a área de TI da organização, ignorando outras áreas da organização. A continuidade das operações organizacionais é também o objeto da Norma Complementar nº 6/IN01/DSIC/GSIPR (BRASIL, 2009c, p.20) do Governo Federal, que determina que a gestão da continuidade do negócio pode “envolver ações mais abrangentes do que as definidas no âmbito da gestão da Segurança da Informação e Comunicações”, e apresenta o seguinte conceito para a continuidade do negócio:

> Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. (BRASIL, 2009c, p.20).

Com isso, fica claro que a gestão da continuidade do negócio, no entendimento do Governo Federal, não está restrita às atividades de TI, mas a FIOCRUZ criou um modelo de gestão que alcança apenas as atividades dessa área.

Em 2013, a FIOCRUZ formalizou a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), que trata de questões de Segurança da Informação relativas ao uso de redes sociais por quem desenvolve atividades administrativas, de ensino ou pesquisa na organização, seja como servidor, estudante, terceirizado ou bolsista. Este regulamento segue claramente as determinações da Norma Complementar nº 15/IN01/DSIC/GSIPR, de 11 de junho de 2012, que trata justamente do uso de redes sociais na Administração Pública Federal (BRASIL, 2012b). A FIOCRUZ ainda regulamentou em 2013 o uso de dispositivos móveis através da Norma Institucional SIC-009/CGTI/VPGDI (FIOCRUZ, 2013g), cuja elaboração foi depois da publicação da Norma Complementar nº 12/IN01/DSIC/GSIPR (BRASIL, 2012a), de 30 de janeiro de 2012, cujo tema é a Segurança da Informação na utilização de dispositivos móveis nos órgãos e entidades públicos federais.

Outros regulamentos foram formalizados pela FIOCRUZ entre os anos de 2012 e 2013: Norma Institucional SIC-001/CGTI/VPGDI, de 17 de abril de 2012, que trata das responsabilidades dos usuários de TI (FIOCRUZ, 2012a); Norma Institucional SIC-002/CGTI/VPGDI, de 11 de maio de 2012, que trata do uso do serviço de Internet (FIOCRUZ, 2012c); Norma Institucional SIC-003/CGTI/VPGDI, de 14 de maio de 2012, que trata do uso do serviço de correio eletrônico (FIOCRUZ, 2012d); Norma Institucional SIC-004/CGTI/VPGDI, de 15 de fevereiro de 2013, que estabelece regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em *datacenters* (FIOCRUZ, 2013a); Norma Institucional SIC-005/CGTI/VPGDI, de 15 de fevereiro de 2013, que trata da realização de cópias de segurança e da recuperação das informações (FIOCRUZ, 2013a); Norma Institucional SIC-006/CGTI/VPGDI, de 15 de fevereiro de 2013, que estabelece diretrizes para aquisição, desenvolvimento e manutenção de sistemas de informação de forma segura (FIOCRUZ, 2013a); e Norma Institucional SIC-007/CGTI/VPGDI, de 23 de setembro de 2013, que trata da concessão de acesso remoto a usuários de TI que atuam em locais geograficamente distantes da rede de computadores e dos sistemas computacionais da organização (FIOCRUZ, 2013e). O Quadro 13 apresenta os requisitos de Segurança da Informação existentes nos regulamentos da organização.

Quadro 13 – Requisitos de Segurança da Informação presentes nos regulamentos.

REGULAMENTO	REQUISITOS
Portaria 002/2013-VPGDI	Equipe de tratamento de incidentes de Segurança da Informação Processos e procedimentos de Segurança da Informação
Portaria 003/2013-VPGDI	Processos e procedimentos de Segurança da Informação Equipe de tratamento de incidentes de Segurança da Informação Divulgação de regulamentos e da Política de Segurança da Informação
Portaria 007/2013-VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Equipe de tratamento de incidentes de Segurança da Informação Processo de Análise e Avaliação de Riscos Divulgação de regulamentos e da Política de Segurança da Informação
Portaria 069/2011-PR	Política de Segurança da Informação Comitê de Segurança da Informação Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Equipe de tratamento de incidentes de Segurança da Informação Revisão periódica da Política de Segurança da Informação Divulgação de regulamentos e da Política de Segurança da Informação Ações de conscientização
Portaria 070/2011-PR	Política de Segurança da Informação Comitê de Segurança da Informação Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Processo de Análise e Avaliação de Riscos Sistema de Gestão de Segurança da Informação
SIC-001/CGTI/VPGDI	Processos e procedimentos de Segurança da Informação Classificação de informações Redundância de dados Controle de acesso lógico Controle de acesso físico Proteção ambiental Divulgação de regulamentos e da Política de Segurança da Informação Ações de conscientização
SIC-002/CGTI/VPGDI	Processos e procedimentos de Segurança da Informação Prevenção contra códigos maliciosos Controle de acesso lógico Segregação de redes de computadores Controle de acesso físico Ações de conscientização
SIC-003/CGTI/VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Prevenção contra códigos maliciosos Controle de acesso lógico Ações de conscientização
SIC-003/CGTI/VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Controle de acesso físico Proteção ambiental Treinamento de profissionais de TI Treinamento de usuários de TI Ações de conscientização
SIC-005/CGTI/VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Redundância de dados Transmissão e armazenamento seguros de dados Controle de acesso lógico Proteção ambiental Controle de acesso físico

REGULAMENTO (cont.)	REQUISITOS (cont.)
SIC-006/CGTI/VPGDI	Processos e procedimentos de Segurança da Informação Processo de Análise e Avaliação de Riscos Classificação de informações Controle de acesso lógico Transmissão e armazenamento seguros de dados Treinamento de profissionais de TI Treinamento de usuários de TI
SIC-007/CGTI/VPGDI	Processos e procedimentos de Segurança da Informação Segregação de redes de computadores Prevenção contra códigos maliciosos Controle de acesso lógico Transmissão e armazenamento seguros de dados Divulgação de regulamentos e da Política de Segurança da Informação
SIC-008/CGTI/VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Prevenção contra códigos maliciosos Controle de acesso lógico Controle de acesso físico
SIC-009/CGTI/VPGDI	Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Redundância de dados Segregação de redes de computadores Prevenção contra códigos maliciosos Controle de acesso lógico Transmissão e armazenamento seguros de dados Controle de acesso físico Ações de conscientização

Fonte: Elaborado pelo autor.
Nota: Inclui tanto portarias que criam estruturas organizacionais quanto normas institucionais.

A análise desses regulamentos e os dados colhidos nas entrevistas mostram que a administração central da FIOCRUZ adotou diferentes medidas formais de Segurança da Informação: “Política de Segurança da Informação”; “Comitê de Segurança da Informação”; “Regulamentos internos de Segurança da Informação”; “Processos e procedimentos de Segurança da Informação”; “Equipe 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”; e “Revisão periódica da Política de Segurança da Informação”. Em comparação com os dados do último relatório de auditoria externa divulgado (TCU, 2014), nota-se algumas contradições, como o fato de que a FIOCRUZ não realizava revisão periódica da Política de Segurança da Informação e não fazia classificação de informações. Cabe registrar que a inconsistência entre as respostas colhidas nas entrevistas e os dados do relatório do TCU pode ser resultado de uma diferença de pelo menos dois anos entre a realização da auditoria e o momento em que as entrevistas desta pesquisa foram realizadas, embora não tenham sido

identificados documentos que comprovassem a realização de revisões da Política de Segurança da Informação nem um regulamento ou processo documentado de classificação das informações.

Segundo o Entrevistado 18 e o Entrevistado 19, as alterações realizadas na Política de Segurança da Informação são discutidas e aprovadas inicialmente no Comitê de Segurança da Informação, como previsto na literatura (HÖNE; ELOFF, 2002; MARTINS; SANTOS, 2005; SÊMOLA, 2014). Os regulamentos vêm sendo elaborados em grupos de trabalho formados no Comitê e discutidos nas suas reuniões. Posteriormente, tanto as alterações da Política quanto os regulamentos são discutidos em reuniões da Câmara Técnica de Gestão e Desenvolvimento Institucional da FIOCRUZ, que pode aprovar os regulamentos e as alterações ou sugerir mudanças para serem discutidas novamente no Comitê. Depois de aprovadas na Câmara de Gestão, o regulamento com as alterações é enviado para a Presidência da Fundação para publicação por meio de portaria.

Embora alguns dos regulamentos de Segurança da Informação da FIOCRUZ tenham sido aparentemente formalizados para atender a necessidades específicas da organização, nota-se que a formalização aconteceu depois da publicação da Norma Complementar nº 7/IN01/DSIC/GSIPR (BRASIL, 2010), que estabeleceu diretrizes para implantação de controles de acesso lógico e físico. Este regulamento estabelece que é necessário credenciar e atribuir responsabilidades às pessoas pelo uso dos serviços TI disponibilizados pelos órgãos e entidades públicos, além de garantir a autenticação e o comprometimento dos usuários e a realização de ações de sensibilização e conscientização em Segurança da Informação. O regulamento prevê ainda a necessidade de que sejam estabelecidas regras para o uso da Internet, correio eletrônico e serviços de mensagens instantâneas. Dentre estas, a FIOCRUZ normatizou em 2012 a utilização de serviços de Internet (FIOCRUZ, 2012c) e correio eletrônico (FIOCRUZ, 2012d).

O fato de a FIOCRUZ ter adotado medidas formais de Segurança da Informação para atender a pressões coercitivas do Governo Federal foi confirmado pelo Entrevistado 18:

> Acabou que isso [pressões externas do Governo] ajudou a gente a definir aquela estrutura básica: Comitê, Gestor, Política de Segurança, modelo de segurança, modelo de gestão de incidente... São cobranças, são mudanças que o DSIC [Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional do Governo Federal] recomendava e o TCU cobrava, e que acabaram colocando a gente contra a parede e que, nesse momento, acabaram ajudando. (ENTREVISTADO 18).

O Entrevistado 18 deixa claro que, apesar de entender que a adoção de medidas formais de Segurança da Informação tem como benefícios a proteção dos ativos de informação e a segurança nas atividades desenvolvidas pelos usuários de TI, há também o benefício de estar em conformidade com os requisitos externos, o que melhora a imagem da organização perante o Governo e outras organizações e garante apoio das fontes de pressão institucional:

> Existe também a parte de *compliance* com as boas práticas, para fins de auditoria. *Compliance* com o Governo, porque nós somos auditados pelo Governo. A gente tem a obrigação de demonstrar o que está sendo feito. A gente não tem um investidor, mas o Governo não deixa de ser o nosso investidor, porque é de lá que vem o dinheiro. Então a gente tem que demonstrar também o que está sendo feito. [...] A gente lida muito com o DSIC, lá de Brasília [...]. Eles nos apoiam na implantação de alguns serviços específicos. Por exemplo, a equipe de tratamento de incidentes, a parte de riscos e a implantação da própria Política. Em contrapartida, nós também fomos convidados a ir lá falar. [...] Inclusive, no ano passado eles reconheceram que a FIOCRUZ tinha evoluído para um determinado nível e que valia a pena isso ser compartilhado com outros órgãos. Então existe uma troca, principalmente com relação aos incidentes de segurança. Quando a gente tem algum problema um pouco mais sério, um pouco mais grave, a gente reporta e pede ajuda a eles. (ENTREVISTADO 18).

No entendimento de Maynard e Ruighaver (2006), a conformidade trata do quanto padrões organizacionais e exigências legais são seguidos. A formalização da Política e a criação do Comitê de Segurança da Informação são evidências de que a adoção de medidas formais tem como objetivo a conformidade com requisitos externos de Segurança da Informação, visto que essas medidas foram adotadas após a publicação de dois regulamentos do Governo Federal que estabelecem essa obrigação (BRASIL, 2008b, 2009a). Além do Entrevistado 18, outros participantes concordaram que estar em conformidade é um dos benefícios que a adoção de medidas formais de Segurança da Informação traz para a organização. Para o Entrevistado 03, medidas formais fazem com que a organização esteja em conformidade e amparada legalmente, enquanto medidas técnicas protegem contra incidentes e demonstram que a organização buscou a Segurança da Informação, mesmo no caso de ocorrerem incidentes. O Entrevistado 06 também destaca a preservação da disponibilidade, confidencialidade e integridade como benefícios da adoção de medidas técnicas, mas acrescenta a conformidade como benefício da adoção de medidas formais.

Sem distinguir medidas formais, informais e técnicas, o Entrevistado 11 entende que a conformidade melhora a imagem da organização perante os órgãos de fiscalização, além de trazer benefícios relacionados à eficiência na Segurança da Informação. Para o Entrevistado 01, além de resguardar os dados e ter um ambiente confiável, servir de exemplo

para outras organizações é um benefício que a adoção de medidas técnicas traz para a organização. A conformidade com regulamentos governamentais através da adoção de medidas formais é destacada pelo Entrevistado 19, que associa a adoção de medidas técnicas à eficiência na proteção da informação a adoção de medidas formais à melhoria na imagem que a conformidade confere à organização, o que a insere em ações e políticas governamentais.

O Entrevistado 10, por sua vez, destaca:

> A FIOCRUZ tem relações com outras organizações e a adoção é fundamental. Existem relações em que é necessário para a FIOCRUZ adotar [medidas formais]. Sofremos auditorias e se determinados controles não existirem, acordos podem não ser fechados, ou podem ser fechados, mas ficar com pendências de melhoria. (ENTREVISTADO 10).

Já o Entrevistado 15 vê como principal vantagem da adoção de medidas formais a padronização de regras e procedimentos, uma característica da conformidade que define o comportamento desejável para os usuários e profissionais de TI e Segurança da Informação:

> A primeira vantagem é que começam a ser definidas regras e padrões, que uma vez compartilhados e homologados pela instituição, determinam como cada assunto precisa ser tratado e quais as responsabilidades atribuídas aos envolvidos, sejam profissionais técnicos ou usuários de quaisquer recursos de Informação. Muito além de vantagens técnicas de proteção a dados, a principal vantagem é o envolvimento responsável das pessoas. (ENTREVISTADO 15).

Os demais entrevistados percebem como benefícios da adoção de medidas técnicas questões mais ligadas à eficiência na Segurança da Informação, como a garantia de que os dados estão protegidos, a preservação da privacidade, a possibilidade de recuperar as atividades ou os dados, ou mesmo a isenção de responsabilização da área de TI no caso de ocorrência de incidentes, como apontado por dois entrevistados. O Entrevistado 12, por exemplo, entende que o principal benefício das medidas técnicas é a segurança dos dados armazenados e processados na organização, apresentando como justificativa o fato de já terem ocorrido incidentes na sua subunidade. O Entrevistado 16 reconhece a conformidade como um dos benefícios da adoção de medidas formais, mas entende que o principal é a proteção da informação através da adoção de medidas técnicas, demonstrando, inclusive, uma visão crítica quanto à forma como medidas formais podem ser adotadas sem que resulte em mudanças no comportamento:

> Se a gente estiver em conformidade, acho que até recursos para comprar as coisas padronizadas pela FIOCRUZ dá para a gente conseguir mais fácil. [...] Mas acho que

> isso é uma questão menor. O importante mesmo é proteger a informação. Até porque essas coisas [medidas formais] às vezes podem ser mais para constar. Por exemplo, a gente pode criar regulamentos só para ter, sem implicação prática nenhuma. (ENTREVISTADO 16).

Já na visão do Entrevistado 09, o benefício da adoção de medidas formais é viabilizar a adoção de medidas técnicas para que elas possam ser recebidas pelos usuários com menos resistência:

> Quando a gente quer fazer uma coisa, a gente mostra que está na Política, que está na norma, aí fica mais fácil de fazer uma coisa, de implantar algo técnico, ou até de dizer não para o usuário. Mas também é importante quando tem uma auditoria e a gente vê que não está tão ruim em comparação com as outras ou com o que a gente já foi, mostrar que estamos bem para a CGTI. (ENTREVISTADO 09).

O benefício percebido pelo Entrevistado 09 corrobora com a literatura, que explica que as medidas formais são úteis porque mostram para os membros da organização a importância da Segurança da Informação (HÖNE; ELOFF, 2002) e por contribuírem para que as pessoas se comportem de maneira coerente com o que a organização espera (LEE, 2001), e que medidas formais devem orientar a adoção de outras medidas (BARMAN, 2001; KING; DALTON; OSMANOGLU, 2001; ELLWANGER, 2009).

As medidas formais foram adotadas pela organização visando principalmente à conformidade com pressões coercitivas do ambiente institucional. A adoção de medidas técnicas e informais, por sua vez, foi feita antes de haver pressões coercitivas – embora a organização já estivesse sofrendo pressões normativas e miméticas – e com o intuito de garantir a segurança das informações organizacionais. Estes resultados estão de acordo com o de pesquisa anterior (ALBUQUERQUE JUNIOR *et al*., 2016), que mostrou que a adoção de medidas formais está relacionada a pressões coercitivas, enquanto medidas informais e técnicas estão mais relacionadas a pressões normativas.

Segundo o Entrevistado 18, houve iniciativas da CGTI voltadas para a conscientização dos gestores das subunidades e usuários de TI depois da publicação da Política de Segurança da Informação e dos regulamentos elaborados pelo Comitê de Segurança da Informação da FIOCRUZ. De acordo com o entrevistado, foram realizadas ações de divulgação da Política de Segurança da Informação que envolveu a distribuição de panfletos e cartazes e o envio de mensagens eletrônicas para os usuários de TI, além de palestras realizadas tanto na sede quanto nas subunidades. Essas ações de conscientização

foram confirmadas por outros participantes da pesquisa, como o Entrevistado 10, que afirmou que “No início teve uma série de palestras para explicar como seria o planejamento, inicialmente para gestores e depois aberto para todos os funcionários”, e Entrevistado 01, Entrevistado 03 e Entrevistado 08, que declararam que o Gestor de Segurança da Informação da FIOCRUZ tem ainda realizado palestras atendendo a demandas dos responsáveis pela Segurança da Informação nas subunidades.

A importância dessas medidas informais é vista em declarações como a do Entrevistado 16, segundo o qual “O ganho que se tem com isso [ações de conscientização] é na melhoria do comportamento dos usuários quanto à segurança.” O Entrevistado 07, por sua vez, declarou: “Acho a questão da conscientização muito interessante porque isso afeta o dia a dia das pessoas. Acho interessante que o aprendizado que você tem dentro da organização pode levar para o dia a dia, você não cai em fraudes eletrônicas, por exemplo.” Segundo Sveen, Torres e Sarriegi (2009), medidas informais são importantes porque visam à mudança do comportamento das pessoas, reforçando o respeito às medidas formais, e AlKalbani, Deng e Kam (2015) entendem que essas medidas promovem a cultura de Segurança da Informação, o que pode aumentar a conformidade com os requisitos externos.

Durante a realização da pesquisa, alguns entrevistados informaram que esse tipo de iniciativa já havia ocorrido em suas subunidades. O Entrevistado 01 infirmou que uma campanha de conscientização estava programada para acontecer em breve na sua subunidade, e o Entrevistado 15 informou que ações desse tipo ocorrem sempre que há novos regulamentos de Segurança da Informação. Ações de conscientização são realizadas na subunidade do Entrevistado 17 sempre que são adotadas medidas técnicas que impliquem em mudanças maiores na rotina de trabalho dos usuários, enquanto Entrevistado 02 e Entrevistado 04 informaram que pretendem tornar essas ações uma rotina nas suas respectivas subunidades. O Entrevistado 09 declarou que, embora não tenha uma programação, pelo menos uma vez por ano são feitas apresentações sobre Segurança da Informação na sua subunidade. O Entrevistado 11, por sua vez que sempre faz palestras de conscientização e apresentações para as pessoas que ingressam na subunidade.

Ocorreram ações de conscientização e divulgação, mas os entrevistados relataram poucas as iniciativas de treinamento e capacitação, o que contradiz os resultados de pesquisa anterior (ALBUQUERQUE JUNIOR *et al.*, 2016) que mostrou que os treinamentos de profissionais de TI são as medidas informais mais comuns. Os treinamentos oferecidos pela CGTI, quando ocorreram, foram relativos à implantação de soluções de Segurança da

Informação específicas, como esclarecido pelo Entrevistado 18. Como exemplo de treinamento oferecido pela CGTI, o Entrevistado 03 citou o antivírus adotado pela FIOCRUZ, cujo processo de aquisição e implantação envolveu cursos voltados para os profissionais de TI das subunidades que iriam utilizar a solução. Não houve relatos de outras ações de treinamento e capacitação em Segurança da Informação de iniciativa da CGTI, apesar de sua importância reconhecida na literatura (BJÖRCK, 2005).

Entrevistados de sete subunidades que ficam no *campus* da administração central da FIOCRUZ informaram que a organização utiliza diversos serviços e recursos tecnológicos de Segurança da Informação, como antivírus, *firewall*, *proxy*, anti-spam, equipamentos redundantes, peças redundantes, realização de *backups*, criptografia de dados, sistemas de detecção e prevenção de intrusão, autenticação com senhas complexas, controle de acesso para sistemas e rede de computadores, restrições de acesso a salas de equipamentos, além de soluções de segurança ambiental com o *datacenter*. Essas são medidas técnicas de redundância de dados, segregação de redes de computadores, redundância de peças de equipamentos, prevenção contra códigos maliciosos, controle de acesso lógico, transmissão e armazenamento seguros de dados, autenticação forte, redundância de equipamentos, controle de acesso físico e proteção ambiental. Esses entrevistados entendem ainda que essas medidas são eficientes para garantir a confidencialidade, integridade de disponibilidade, mas têm pouca relevância para a conformidade da FIOCRUZ com os requisitos externos de Segurança da Informação.

Embora as medidas técnicas adotadas pela sede sejam percebidas como eficientes, não têm efeito sobre todas as subunidades da organização: o *firewall* implantado pela CGTI protege os sistemas e informações armazenadas na sede da organização, mas não os que estão nas redes de computadores das subunidades de outros *campi*; os sistemas de detecção e prevenção de intrusos também só funcionam na rede de computadores da sede da FIOCRUZ; o controle de acesso à Internet realizado através do *proxy* instalado pela CGTI também não atende às subunidades geograficamente distantes; os *backups* realizados pela CGTI só geram cópias de segurança dos dados armazenados nos servidores que estão hospedados no *datacenter* da organização; o mesmo pode ser dito sobre os mecanismos de controle de acesso físico ao *datacenter*; a criptografia utilizada só garante a confidencialidade de informações acessadas através dos sistemas de informação disponibilizados pela CGTI, embora chaves de criptografia sejam disponibilizadas pela sede para as subunidades utilizarem em seus sistemas.

A percepção de que medidas técnicas são eficientes para a Segurança da Informação enquanto medidas formais são eficientes para garantir a conformidade da organização com os requisitos coercitivos externos soma-se ao fato de a adoção de muitas medidas técnicas ser feita pelos profissionais de TI sem que haja discussões sobre sua necessidade ou previsão em regulamentos, enquanto a adoção de medidas formais é discutida e negociada entre técnicos e gestores. Com isso, explica-se em parte o porquê de haver mais medidas técnicas do que formais adotadas, e de a adoção de medidas técnicas ter acontecido antes mesmo da publicação dos regulamentos e da Política de Segurança da Informação. Embora as medidas informais sejam percebidas como importantes, são menos adotadas do que as técnicas. Essa desarmonia entre a adoção das três categorias de medidas de Segurança da Informação é contrária ao entendimento de Sveen, Torres e Sarriegi (2009), que ressaltam as diferentes medidas são interdependentes.

O Quadro 14 compila os tipos de medidas formais, informais e técnicas adotadas pela administração central da organização.

Quadro 14 – Tipos de medidas adotadas pela administração central da organização.

CATEGORIA	MEDIDAS ADOTADAS
Formais	Política de Segurança da Informação Comitê de Segurança da Informação Regulamentos internos de Segurança da Informação Processos e procedimentos de Segurança da Informação Equipe de tratamento de incidentes de Segurança da Informação Escritório de Segurança da Informação Processo de Análise e Avaliação de Riscos Sistema de Gestão de Segurança da Informação
Técnicas	Redundância de dados Segregação e monitoramento de redes de computadores Redundância de peças de equipamentos Prevenção contra códigos maliciosos Controle de acesso lógico Transmissão e armazenamento seguros de dados Autenticação forte Redundância de equipamentos Controle de acesso físico Proteção ambiental
Informais	Treinamento de profissionais de TI Divulgação de regulamentos e da Política de Segurança da Informação Ações de conscientização

Fonte: Dados coletados na pesquisa com base nas categorias propostas por Dhillon (1999).

A seção seguinte apresenta as subunidades da organização, mostrando como cada uma organizou a Segurança da Informação e apresentando dados relacionados à conformidade

delas com os requisitos de Segurança da Informação da administração central e do ambiente institucional, bem como as medidas de Segurança da Informação adotadas.

6.3 SEGURANÇA DA INFORMAÇÃO NAS SUBUNIDADES

Apesar de a FIOCRUZ ter em sua estrutura a CGTI, que é responsável pelas ações de TI que abrangem toda a organização, todas as subunidades técnico-científicas e a subunidade técnica de apoio têm seus próprios responsáveis por questões locais relacionadas a TI. O mesmo se aplica à única subunidade de assessoria que não está localizada no *campus* da administração central. Os escritórios regionais têm equipes ou profissionais de TI, necessários por estarem localizados longe da administração central. Já as quatro subunidades técnico-administrativas e todas as coordenações e demais subunidades de assistência direta e assessoria não contam com equipe própria de TI, sendo, portanto, responsabilidade da CGTI.

Os serviços de TI das subunidades técnico-científicas e da subunidade técnica de apoio não têm relação hierárquica com a CGTI, mas os escritórios regionais respondem hierarquicamente. Da mesma forma, embora exista um Comitê e um setor responsável pela Segurança da Informação da organização, cada subunidade autônoma pode ter seu próprio Escritório de Segurança da Informação e tem entre suas responsabilidades a criação de seu subcomitê de Segurança da Informação para tratar de questões locais relativas ao tema, como previsto na Portaria 070/2011-PR (FIOCRUZ, 2011b) e descrito por Sêmola (2014) e Manoel (2014).

Apesar de não existir uma relação de hierarquia entre a CGTI e algumas subunidades, os regulamentos da organização definem responsabilidades para as subunidades, como a própria Portaria 070/2011-PR, que prevê a criação de subcomitês e a aplicação de ações corretivas e disciplinares no caso que quebra de segurança, a Portaria 003/2013-VPGDI (FIOCRUZ, 2013c), que define que a TI da subunidade tem a obrigação de informar a ocorrência de incidentes à Equipe de Tratamento de Incidentes da CGTI, e a Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), que define que as subunidades devem definir os *softwares* que podem ser utilizados para acesso à Internet por seus usuários, além de homologar recursos computacionais para serem utilizados em suas redes de computadores.

Há uma compreensão na literatura de que a administração central é uma importante fonte de pressão coercitiva sobre as subunidades (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 1994). Ao atribuírem responsabilidades para as subunidades, esses regulamentos reforçam o entendimento de que a Segurança da Informação é uma obrigação, e que não pode ser tratada de maneira isolada, como definido na Política de Segurança da Informação ao prever a aplicação de sanções para o caso de violação das suas regras (FIOCRUZ, 2011a). Mas o relatório de auditoria interna publicado em 2014 pela CGTI (FIOCRUZ, 2014) mostra que, naquele momento, as subunidades não estavam em conformidade com mais da metade dos regulamentos de Segurança da Informação publicados pela organização.

Já na auditoria interna seguinte (FIOCRUZ, 2015), a análise envolveu os nove regulamentos publicados pela FIOCRUZ. Nesta auditoria, houve a preocupação em distinguir medidas previstas nos regulamentos que não se aplicam à realidade das subunidades, além da identificação das situações em que a conformidade é parcial – quando as medidas previstas não estão totalmente implementadas. O relatório mostra que nenhum dos regulamentos formalizados pela administração central da organização tem adesão plena das subunidades. A Figura 7 apresenta o percentual de conformidade das subunidades com os nove regulamentos.

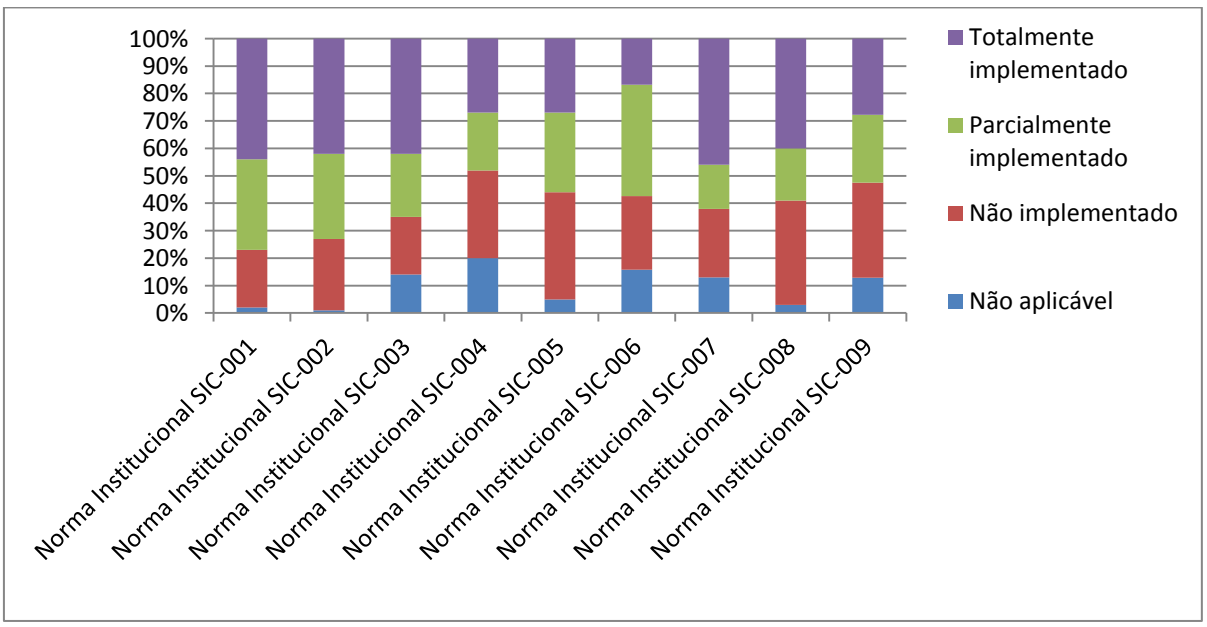


Figura 7 – Conformidade das subunidades com os regulamentos da organização.
Fonte: Adaptado de FIOCRUZ (2015).

De acordo com este último relatório de auditoria (FIOCRUZ, 2015), a Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e) é a que tem mais adesão das subunidades, enquanto a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a) é a que tem menos adesão. Apesar de a maior parte das medidas previstas nos regulamentos ser de natureza técnica, algumas são formais, como o processo de credenciamento de usuários envolvendo autorização da chefia imediata e anuência da área responsável pelos vínculos dos usuários com a organização antes da concessão do acesso aos recursos computacionais, e a divulgação permanente da Política de Segurança da Informação – ambas previstas na Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a).

O relatório aponta que as subunidades apresentam grandes diferenças quanto à adoção das medidas de Segurança da Informação previstas nos regulamentos da FIOCRUZ. Da mesma forma que há medidas que não foram adotadas, algumas medidas foram adotadas integralmente, algumas parcialmente e há também medidas que não se aplicam à realidade das subunidades. A seguir são apresentados os dados sobre as 17 subunidades cujos responsáveis pelo setor de TI ou pela Segurança da Informação foram entrevistados.

6.3.1 Subunidade 01

A Subunidade 01 não está localizada no *campus* da administração central da FIOCRUZ. Esta subunidade não tem profissionais dedicados exclusivamente às atividades de Segurança da Informação e todas as ações referentes a este assunto são realizadas por dois profissionais do quadro permanente da FIOCRUZ, que cuidam também de outras questões relacionadas a TI. A subunidade tem autonomia administrativa, com uma diretoria própria e sua área de TI não tem nenhum vínculo com a CGTI. A entrevista, que teve duração de 32 minutos, foi realizada através do *software* Skype com o coordenador de TI da subunidade que é também membro do Comitê de Segurança da Informação da FIOCRUZ. O entrevistado tem graduação e especialização na área de TI.

Quanto às medidas formais de Segurança da Informação, a subunidade não tem Política, subcomitê ou regulamentos próprios de Segurança da Informação. Não tem também uma equipe técnica para tratar de incidentes, processos de classificação das informações nem de análise e avaliação de riscos na subunidade, segundo o Entrevistado 01. Apesar disso, o entrevistado relatou que tem procedimentos de Segurança da Informação documentados que

orientam atividades operacionais da equipe de TI local. Com isso, os dados evidenciaram que a subunidade adota apenas um tipo de medida formal: “Processos e procedimentos de Segurança da Informação”.

Dentre as medidas técnicas, o entrevistado informou que a subunidade tem servidores de rede redundantes, utiliza equipamentos com peças e discos redundantes e utiliza *storage* para armazenamento de dados, embora não tenha uma solução de *backup* dos dados. A subunidade utiliza *firewall* e *virtual local area networks* (VLANs) para segregar redes de computadores com diferentes requisitos de Segurança da Informação, utiliza a solução corporativa de antivírus adotada pela FIOCRUZ e faz controle de acesso lógico aos dados armazenados em seu servidor de arquivos. O acesso à rede de computadores e aos dados armazenados nos servidores depende de *login* e senha complexa, composta por letras maiúsculas, minúsculas, números e caracteres especiais. Segundo o entrevistado, a subunidade não tem sistemas de informação próprios. Assim, seus usuários utilizam basicamente os sistemas de informação corporativos da FIOCRUZ e do Governo Federal, cujo acesso é feito após identificação também através de *login* e senha complexa. O acesso à sala onde estão armazenados os servidores é restrito ao pessoal de TI e a sala conta com proteção contra incêndio e aparelhos de ar condicionado. Dessa forma, pode-se dizer que a subunidade adota todos os tipos de medidas técnicas de Segurança da Informação.

Segundo o entrevistado, foi realizado um evento de conscientização voltado para todas as pessoas que trabalham ou estudam nos setores e laboratórios da subunidade, que contou com a presença do gestor de Segurança da Informação da FIOCRUZ, mas não há medidas informais de capacitação. O Entrevistado 01 relatou que houve o envio de mensagens informando sobre a proibição do uso de serviços de armazenamento virtual na Internet, mas as mensagens não surtiram efeito e os regulamentos foram sistematicamente desrespeitados pelos usuários, o que motivou outras ações de conscientização na subunidade. Com isto, é possível afirmar que a Subunidade 01 adotou medidas de “Divulgação de regulamentos e da Política de Segurança da Informação” e “Ações de conscientização”.

Quanto à conformidade com os regulamentos publicados pela CGTI, cabe destacar que a Subunidade 01 adotou 100% das medidas previstas na Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e), que dispõe sobre acesso remoto na FIOCRUZ. A subunidade adotou também 89% das medidas da Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a) e 88% das medidas da Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c) – a primeira sobre credenciamento dos usuários de TI e a segunda sobre o

uso da Internet. Dentre as medidas que tiveram menos aderência da subunidade, destacam-se a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a), sobre aquisição, desenvolvimento e manutenção seguros de sistemas, que teve 3% das suas medidas adotadas, a Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a), que trata de *backup* de dados, que teve 10% das medidas adotadas, e a Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d), que trata do uso do serviço de correio eletrônico e que a subunidade adotou 20% das medidas.

Para o Entrevistado 01, o benefício da adoção de medidas de Segurança da Informação, de forma geral, é a eficiência na garantia da confidencialidade, integridade e disponibilidade. Mas o entrevistado vê a adoção de medidas de Segurança da Informação também como uma forma de prover novos serviços, pois o fato de a subunidade não ter adotado algumas medidas impede que esses serviços sejam disponibilizados para seus usuários com segurança. Como exemplo, explica que não pode oferecer um serviço de acesso remoto de acordo com a Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e) porque a subunidade não tem como implantar um serviço de *Virtual Private Network* (VPN), que ele entende como um requisito da norma para que um serviço como este seja implantado. De forma semelhante, não oferece um serviço de acesso à rede sem fio seguro porque a subunidade não tem a infraestrutura necessária para implantá-lo.

A adoção de medidas formais é limitada a procedimentos documentados de Segurança da Informação, que são mais úteis para os profissionais de TI do que para os usuários, embora sejam vistos também como eficientes para garantir a proteção da informação. Apesar de não ter políticas ou regulamentos, o Entrevistado 01 entende que estas medidas são importantes para que os usuários entendam os motivos para a adoção de medidas técnicas, uma questão de eficiência também. No entanto, não houve nenhum indício de que a subunidade pretende adotar este tipo de medida de Segurança da Informação. As medidas técnicas, por sua vez, são também percebidas como eficientes para garantir a proteção da informação. O Entrevistado 01 afirmou: “Acho que é uma necessidade. Ainda mais que a gente tem vários processos de pesquisa cujos dados podem gerar uma patente. É mais para proteger os dados das pesquisas.” Embora o entrevistado declare compreender que a adoção dessas medidas visa à proteção da informação, reconhece que elas são úteis também para que a subunidade sirva de exemplo para as outras, o que demonstra uma percepção de que a subunidade tem com a adoção vantagens que estão além da garantia da integridade, disponibilidade e confidencialidade. Já a adoção de medidas informais visa à mudança do

comportamento dos seus usuários – portanto, uma questão de eficiência quanto à Segurança da Informação.

Na visão do Entrevistado 01, a subunidade recebe pressões principalmente da administração central da FIOCRUZ. Em nenhum momento o entrevistado relatou que a subunidade recebe pressões de outros constituintes do ambiente institucional. As pressões da administração central se apresentam na forma da Política de Segurança da Informação e de regulamentos publicados pela Presidência da organização através de portarias, mas esses documentos são percebidos muito mais como recomendações do que imposições da administração central: "[...] o Comitê [de Segurança da Informação da organização] gera as normas, que seriam como recomendações, mas uma pressão efetiva eu não vejo." Em outro momento, o entrevistado deixou claro que a adoção acontece se a subunidade quiser adotar, pois "[...] a Política não tem uma obrigação, não é taxativa, mas é mais uma recomendação." Não sendo percebidas como pressões coercitivas, não há, portanto, a necessidade de a subunidade estar em conformidade.

A pesquisa mostrou que o comportamento característico da Subunidade 01 quanto às pressões para adoção de medidas formais é o compromisso através da pacificação, pois a maior parte das medidas não é adotada, a despeito de essas medidas serem percebidas como importantes para justificar a adoção de medidas técnicas. Quanto às medidas técnicas, o comportamento característico é a aquiescência, pois todos os tipos de medidas técnicas são adotados, e a tática característica é o hábito, pois a adoção visa à garantia da confidencialidade, integridade e disponibilidade. Diante de comportamentos de desrespeito à Política e aos regulamentos por parte dos usuários, a subunidade realizou eventos de conscientização e divulgação. Como não houve eventos de capacitação, fica claro um comportamento característico de compromisso, e como outras medidas informais não foram adotadas, fica caracterizada a pacificação. O relatório de auditoria (FIOCRUZ, 2015) mostra que, embora esteja em conformidade parcial ou total com os regulamentos, parte das medidas foi rejeitada.

A subunidade adotou as tecnologias de Segurança da Informação padronizadas pela administração central da FIOCRUZ, como antivírus e anti-spam, e adotou diversas outras soluções tecnológicas em resposta a outras pressões institucionais, como relatou o Entrevistado 01. Estas e outras medidas são adotadas devido à percepção de que são eficientes, mas também porque a conformidade com os requisitos externos é vantajosa para a subunidade, o que caracteriza a tática de conformidade. Mas o entrevistado relatou que houve

também uma tentativa da administração central de obrigar a utilização do *datacenter* da FIOCRUZ, o que gerou uma resposta de desafio, através da contestação dessa exigência perante os dirigentes de TI da organização. Embora tenha recursos para impedir que usuários utilizem serviços privados de armazenamento na nuvem, a subunidade não toma nenhuma atitude por entender que os regulamentos são meras recomendações e que, por este motivo, as medidas técnicas previstas não são obrigatórias, o que configura também uma resposta de desafio. Estas respostas de desafio não minimizam o fato de que a subunidade adota todos os tipos de medidas técnicas que é pressionada a adotar.

A aquiescência é o comportamento característico da Subunidade 01 quanto à forma como responde às pressões da administração central feitas através dos regulamentos de Segurança da Informação, pois a maioria das medidas previstas nos regulamentos é adotada, segundo o relatório de auditoria (FIOCRUZ, 2015), mas nem todas as medidas formais e informais são adotadas, como mostrou a pesquisa. Apesar de ser esta a resposta que caracteriza o comportamento da subunidade, os dados categorizados no NVivo mostram que a resposta estratégica que tem maior cobertura de percentual é o desafio, com 14,71%, e a tática de contestação teve 7,80% de cobertura de percentual. Quanto às referências de codificação, a resposta de aquiescência foi a que apresentou mais referências codificadas, corroborando com o resultado da auditoria: oito referências foram identificadas, das quais cinco foram codificadas na tática de conformidade. Este resultado mostra que a resposta estratégica mais identificada nos dados analisados para esta subunidade é a aquiescência, embora trechos maiores evidenciem a resposta estratégica de desafio.

6.3.2 Subunidade 02

A Subunidade 02 fica localizada no mesmo *campus* da administração central da FIOCRUZ e conta com três profissionais dedicados às atividades de Segurança da Informação. A direção da subunidade tem autonomia administrativa e a área de TI não tem vínculo hierárquico com a CGTI. Apesar de não haver nenhuma formalização quanto à chefia do setor, o Entrevistado 02 é o responsável pela TI na subunidade. Ele é graduado na área de TI e fez especialização também nesta área. A entrevista foi através de Skype e teve 33 minutos de duração.

A subunidade não tem formalmente uma Equipe de Tratamento de Incidentes de Segurança da Informação, mas tem dois profissionais dedicados a essas atividades. Com isso, aumenta a possibilidade de haver priorização e tratamento adequados aos incidentes de Segurança da Informação. A Subunidade 02 tem também um processo de análise e avaliação de riscos, regulamentos e procedimentos documentados, formalização exigida pelos órgãos que fiscalizam suas atividades, segundo o Entrevistado 02. Foram identificados na subunidade documentos que formalizam procedimentos e regulamentos internos voltados para armazenamento de arquivos digitais na rede de computadores, restauração de *backups* e arquivamento de dados. A subunidade tem um subcomitê de Segurança da Informação formal designado para essa finalidade e as decisões relacionadas ao tema são discutidas neste grupo, que tem uma composição heterogênea, com servidores públicos efetivos da organização com conhecimentos não só em TI, mas também em privacidade de dados e qualidade em saúde, o que é desejável diante do tipo de dados com os quais a subunidade lida. De acordo com os dados colhidos na entrevista, a subunidade adota seis tipos diferentes de medidas formais de Segurança da Informação: "Política de Segurança da Informação", "Comitê de Segurança da Informação", "Regulamentos internos de Segurança da Informação", "Processos e procedimentos de Segurança da Informação", "Equipe de tratamento de incidentes de Segurança da Informação" e "Processo de Análise e Avaliação de Riscos". A subunidade tem sua própria Política de Segurança da Informação, mas o entrevistado afirmou que segue também a Política da organização para elaborar seus processos, procedimentos e regulamentos locais.

O Entrevistado 02 relatou que a subunidade tem rotinas de *backup* documentadas, servidores redundantes e equipamentos com peças redundantes, *firewall* e rede com zona desmilitarizada (DMZ), antivírus, anti-spam e *antimalware*. Há mecanismos de controle sobre o que é acessado pelos usuários na Internet. O acesso aos sistemas e à rede de computadores é através de *login* e senha e os privilégios de acesso dos usuários são também controlados. Recursos de criptografia são utilizados para acessar sistemas através da Internet, como o *webmail* da subunidade. O entrevistado relatou também que a subunidade conta com *no-break* e gerador para proteger os equipamentos contra eventuais falhas no fornecimento de energia elétrica e que o acesso às salas onde estão os equipamentos é restrito. Com isso, os dados mostram que a subunidade adota medidas técnicas dos dez tipos: "Redundância de dados", "Segregação e monitoramento de redes de computadores", "Redundância de peças de equipamentos", "Prevenção contra códigos maliciosos", "Controle de acesso lógico",

“Transmissão e armazenamento seguros de dados”, “Autenticação forte”, “Redundância de equipamentos”, “Controle de acesso físico” e “Proteção ambiental”.

De acordo com o entrevistado, os profissionais de TI da subunidade tiveram treinamentos em Segurança da Informação. Além disso, foram realizadas ações de conscientização voltadas para os usuários, mas essas ações não são realizadas de forma sistemática. Quanto a isso, o Entrevistado 02 informou que pretende realizar eventos de conscientização de forma rotineira. Parte dos regulamentos de Segurança da Informação é divulgada internamente, após uma avaliação quanto à necessidade de fazer a divulgação. Assim, são adotados “Programas de treinamento para profissionais de TI”, “Divulgação de regulamentos e da Política de Segurança da Informação” e “Ações de conscientização” entre as medidas informais.

O relatório de auditoria interna (FIOCRUZ, 2015) mostra que a subunidade adotou 100% das medidas presentes nas Normas Institucionais SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), sobre o uso do serviço de Internet, SIC-003/CGTI/VPGDI, sobre correio eletrônico (FIOCRUZ, 2012d), e SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e), que trata de acesso remoto. A subunidade está em conformidade também com pelo menos metade das medidas previstas nos demais regulamentos da organização, tendo como única exceção a Normas Institucionais SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), sobre o uso de mídias sociais, cujas medidas adotadas correspondem a 33% do previsto.

O Entrevistado 02 reconhece que a subunidade está sob pressão não só da sua administração central, mas também de outras organizações. No seu entendimento, a adoção de medidas técnicas de Segurança da Informação visa à garantia da disponibilidade das informações, um dos pilares clássicos da Segurança da Informação. Apesar da ênfase na disponibilidade, o entrevistado destaca a necessidade de atender às exigências externas, principalmente de organizações que fiscalizam as atividades da subunidade. A adoção de medidas formais, na visão do entrevistado, visa à conformidade com os constituintes do ambiente institucional. Medidas informais, por sua vez, são associadas à mudança de comportamento dos usuários e, portanto, à eficiência da Segurança da Informação.

Quanto à conformidade com pressões externas, a Subunidade 02 segue principalmente a Política e os regulamentos da FIOCRUZ, de acordo com o Entrevistado 02. A Segurança da Informação na subunidade tem como base “[...] os documentos da CGTI, as recomendações da FIOCRUZ, que a gente segue. [...] A gente tem basicamente usado quase

100% do que a POSIC da FIOCRUZ recomenda. Quase tudo a gente aplica. E o que tem de boa prática fora, a gente procura aplicar, pensando no impacto interno.” (ENTREVISTADO 02). Esse comportamento organizacional de aderência aos regulamentos da organização foi observado na auditoria interna (FIOCRUZ, 2015).

O comportamento característico da subunidade em resposta aos regulamentos de Segurança da Informação da organização é a aquiescência, pois todos os tipos de medidas técnicas são adotados e essas medidas são associadas pelo entrevistado à eficiência na garantia da disponibilidade das informações. No caso das medidas formais, a subunidade busca estar em conformidade com as exigências externas adotando a maioria das medidas desta categoria, tendo adotado inclusive algumas que são pouco comuns em subunidades da organização, como um Comitê próprio e uma Política de Segurança da Informação. Algumas medidas informais também são adotadas por haver um entendimento por parte do entrevistado de que são importantes para adequar o comportamento dos usuários aos regulamentos de Segurança da Informação. A estratégia de aquiescência é percebida no relatório de auditoria (FIOCRUZ, 2015), que mostra que poucas medidas previstas nos regulamentos da organização foram rejeitadas e poucas foram adotadas parcialmente.

No entanto, o compromisso foi a resposta estratégica mais associada aos trechos da entrevista e aos documentos analisados referentes à Subunidade 02, com 16,71% de cobertura de percentual e três referências de codificação, e a tática foi a pacificação, com 9,48% de cobertura e duas referências identificadas, contrariando o comportamento característico da subunidade identificado no relatório de auditoria.

6.3.3 Subunidade 03

Localizada em uma cidade distante da sede administrativa da FIOCRUZ, a Subunidade 03 não tem uma equipe dedicada à Segurança da Informação. A subunidade tem autonomia administrativa, de forma que atuação da área de TI é também autônoma com relação à CGTI. A entrevista foi por Skype, teve duração de 40 minutos e o entrevistado é o chefe do Serviço de TI da subunidade, que tem graduação e especialização na área de TI e é membro do Comitê de Segurança da Informação da organização.

No entendimento do Entrevistado 03, a Subunidade 03 não sofre pressões para que adote medidas de Segurança da Informação. Os regulamentos criados tanto pela CGTI

quanto pelo Governo Federal são percebidos como recomendações. Ainda segundo o Entrevistado 03, a subunidade não tem uma equipe dedicada aos incidentes de Segurança da Informação, embora isso venha sendo discutido com sua direção. A subunidade não tem também subcomitê, processos, regulamentos ou Política de Segurança da Informação. De acordo com o entrevistado, as medidas formais que a subunidade segue são as da CGTI da FIOCRUZ. Por não ter uma equipe de profissionais dedicados à Segurança da Informação, a atuação no caso da ocorrência de incidentes concorre com o atendimento de outras demandas de TI, podendo levar a priorização e tratamento inadequados.

Já houve na subunidade uma tentativa de elaboração de uma Política de Segurança da Informação própria, mas o entrevistado acrescentou que esta iniciativa foi abortada quando a FIOCRUZ iniciou a elaboração da Política corporativa. Sobre a conformidade com os regulamentos externos, o Entrevistado 03 entende que a adoção dá à subunidade amparo legal por estar fazendo o que se espera que ela faça, evitando consequências mais graves mesmo na ocorrência de incidente de Segurança da Informação. Assim, no entendimento do entrevistado, medidas formais têm como benefícios principais vantagens associadas à conformidade legal. A entrevista deixou claro que a subunidade não adota medidas formais, mas que a adoção é considerada importante para a conformidade com os requisitos externos. No entanto, não foi identificado nenhum indício de que a subunidade busca adotar medidas formais de Segurança da Informação.

A despeito de não ter medidas formais próprias, a Subunidade 03 adota diferentes medidas técnicas de Segurança da Informação. De acordo com o coordenador de TI, a subunidade tem antivírus, utiliza equipamentos com peças redundantes, faz controle de acesso dos seus usuários à Internet através de *proxy*, tem uma rotina de *backup*, tem um *firewall* para proteger sua rede interna de acessos indevidos oriundos da Internet, utiliza senhas complexas e tem uma rotina de trocas periódicas de senha, tem *no-break* e aparelhos de ar-condicionado nas salas dos servidores de rede, faz controle de acesso lógico aos serviços disponibilizados para seus usuários e utiliza criptografia para prover serviços *web*, como o *webmail*. Com isso, as únicas medidas técnicas que não foram identificadas nas respostas do Entrevistado 03 foram a “Redundância de equipamentos” e o “Controle de acesso físico”. A adoção de medidas técnicas, no entendimento do entrevistado, está relacionada à eficiência, pois as medidas visam à garantia da confidencialidade, integridade e disponibilidade da informação na sua subunidade.

O Entrevistado 03 afirmou que a única iniciativa de capacitar os profissionais de TI da subunidade em Segurança da Informação foi um treinamento promovido pela CGTI na ocasião da implantação do antivírus corporativo. O único treinamento que não estava relacionado com a implantação de uma tecnologia foi um curso que ele fez por conta própria em uma empresa especializada em Segurança da Informação, mas que foi anterior às iniciativas recentes da FIOCRUZ, como a criação do Comitê e da Política de Segurança da Informação. Em contrapartida, foram organizados na subunidade eventos de divulgação e conscientização com palestras sobre Segurança da Informação com a presença do Gestor de Segurança da Informação da FIOCRUZ, em que foram apresentadas também as diversas iniciativas da organização. O Entrevistado 03 entende que a realização desses eventos é fundamental para fomentar a Segurança da Informação, pois além de conscientizar, faz com que as pessoas saibam o porquê de certas medidas técnicas e formais estarem sendo adotadas. Assim, as medidas informais de "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização" são adotadas, também visando à eficiência na Segurança da Informação.

Apesar de ter adotado diversas medidas técnicas e dois tipos de medidas informais, a auditoria de conformidade das subunidades (FIOCRUZ, 2015) mostra que poucas medidas adotadas estão de acordo com os regulamentos da organização. O regulamento que tem mais adesão da Subunidade 03 é o de uso do serviço de Internet, a Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), que tem 100% das medidas parcialmente implementadas. Em seguida, destaca-se o regulamento que trata de responsabilidades dos usuários, a Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a), que tem 89% das medidas previstas parcialmente implementadas na subunidade. Cabe registrar que a subunidade não adota nenhuma das medidas previstas na Norma Institucional SIC-006/CGTI/VPGDI, que trata da aquisição, desenvolvimento e manutenção de sistemas (FIOCRUZ, 2013a).

O fato de parte das medidas técnicas não ter sido adotada, no entendimento do entrevistado, é a "Falta de profissionais voltados para a área, infraestrutura básica para aplicar completamente as recomendações, e principalmente, fundamental: a conscientização dos usuários." (ENTREVISTADO 03).

Pressões para adoção de medidas formais, por sua vez, não são percebidas como obrigatórias pela subunidade, embora previstas nos regulamentos organizacionais. Apesar disso, o Entrevistado 03 reconhece que há uma necessidade de criar regulamentos de

Segurança da Informação na subunidade. O entrevistado relaciona esta necessidade à coerência entre o que a sociedade espera da FIOCRUZ e o que ela de fato está fazendo: “Há necessidade de uma regulamentação, sim, para manter o mínimo necessário de coerência com isso.” Os requisitos externos são também percebidos como pressões institucionais, e o entrevistado deixou claro que a intenção ao adotar medidas formais é a conformidade com estes requisitos externos. Apesar do reconhecimento da necessidade, a entrevista não trouxe elementos que mostrassem que há a intenção de adotar medidas formais de Segurança da Informação.

As medidas informais de Segurança da Informação, por outro lado, foram associadas pelo entrevistado a pressões normativas do ambiente institucional, pois vêm da percepção de que elas são necessárias, não havendo um julgamento quanto aos benefícios que a adoção pode trazer junto ao ambiente institucional. No entanto, nem todas as medidas informais requisitadas pelo ambiente institucional foram adotadas pela subunidade. Essa compreensão a respeito das medidas informais pode ser notada na entrevista: “Estamos buscando uma conscientização da melhor usabilidade de todos os recursos computacionais, sejam eles lógicos ou físicos.” (ENTREVISTADO 03). Em outro trecho, o Entrevistado 03 complementa: “[...] tenho certeza que a conscientização através de palestras e cursos [...] são fundamentais para fomentar isso [a Segurança da Informação].”

O relatório de auditoria interna da organização (FIOCRUZ, 2015) mostra que muitas medidas presentes nos regulamentos não foram adotadas, mas que a concentração é maior nas medidas cuja adoção foi parcial. Este resultado mostra que a resposta estratégica que caracteriza a subunidade ao ser pressionada pela sua administração central é o compromisso.

A análise a partir do *software* NVivo permitiu constatar que a resposta estratégica que teve maior cobertura de percentual foi a aquiescência, cujo nó teve 16,29% de cobertura, e a tática foi a conformidade, com 15,14% de cobertura de percentual. A aquiescência teve também seis referências de codificação, sendo que a tática de conformidade teve cinco referências, o que aponta que a maioria das medidas adotadas foram motivadas por uma compreensão de que a Subunidade 03 teria vantagens junto aos constituintes do ambiente institucional. Este resultado contradiz a resposta característica da subunidade identificada no relatório de auditoria.

6.3.4 Subunidade 04

A Subunidade 04 está localizada no *campus* da sede administrativa da FIOCRUZ. Além de ter uma equipe própria de TI, conta com profissionais que se dedicam exclusivamente às atividades de Segurança da Informação. Por ter uma diretoria própria, a subunidade tem autonomia administrativa e organiza sua TI de forma independente da CGTI. O Entrevistado 04 é o coordenador de TI da subunidade e tem formação na área de TI, com especialização em Segurança da Informação. A entrevista teve 44 minutos e foi realizada remotamente, através do *software* Skype.

As medidas formais que a Subunidade 04 adota são as seguintes: "Escritório de Segurança da Informação", "Processos e procedimentos de Segurança da Informação" e "Regulamentos internos de Segurança da Informação". O Entrevistado 04 informou que a subunidade não tem uma Política de Segurança da Informação própria, mas que ela está sendo elaborada. Por não ter uma Política, a subunidade não pode fazer uma revisão periódica deste documento. O entrevistado informou também que a subunidade não tem subcomitê de Segurança da Informação, nem faz análise e avaliação de riscos ou classificação de informações, além de não ter um Sistema de Gestão de Segurança da Informação.

Segundo o coordenador de TI, a subunidade realiza *backups* dos dados armazenados em seus servidores de rede e alguns desses servidores são redundantes e têm também peças e discos redundantes. Com isso, os dados mostram que a subunidade adota medidas de "Redundância de dados", "Redundância de equipamentos" e "Redundância de peças de equipamentos". A subunidade utiliza antivírus e anti-spam, que são tecnologias de "Prevenção contra códigos maliciosos". O *firewall* é a única tecnologia de "Segregação e monitoramento de redes de computadores" que o entrevistado informou que sua subunidade utiliza. As tecnologias e soluções adotadas como medidas de "Autenticação forte" são as senhas complexas e a biometria. O *login* único para os usuários de TI e a definição de níveis de permissão de acesso a recursos computacionais e sistemas de informação são as formas de garantir "Controle de acesso lógico". Para ter medidas de "Controle de acesso físico" e "Proteção ambiental", a subunidade mantém a sala de equipamentos de TI fechada e com acesso restrito, com ar condicionado para evitar o aumento de temperatura e umidade no ambiente e *no-breaks* para garantir o fornecimento ininterrupto de energia elétrica. A subunidade utiliza criptografia para garantir acesso seguro a suas aplicações *web*, uma medida

“Transmissão e armazenamento seguros de dados”. Os dados mostram, portanto, que todos os tipos de medidas técnicas foram adotados pela subunidade.

Segundo o Entrevistado 04, não houve qualquer ação de treinamento, conscientização ou divulgação em Segurança da Informação na Subunidade 04. Assim, esta subunidade não adotou medidas informais de Segurança da Informação.

No último relatório de auditoria interna disponibilizado pela organização (FIOCRUZ, 2015), é possível notar que o regulamento interno com o qual a subunidade está com maior percentual de conformidade é a Norma Institucional SIC-007/CGTI/VPGDI, que trata de acesso remoto (FIOCRUZ, 2013e): 64% das medidas previstas neste regulamento foram adotados pela subunidade. O regulamento que trata de *backup* – Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a) foi o segundo regulamento com maior aderência desta subunidade: 57% das medidas previstas foram adotadas. Dentre os regulamentos com menor nível de conformidade estão a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), que não teve nenhuma medida plenamente adotada (apesar de 33% delas terem sido adotadas parcialmente), e a Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), que teve apenas 13% das medidas previstas adotadas – a primeira sobre redes sociais e a segunda sobre acesso à Internet.

A adoção de medidas de Segurança da Informação é percebida pelo Entrevistado 04 como uma questão de eficiência, pois visam à proteção das informações. No entanto, o entrevistado admitiu também que a adoção traz ainda benefícios para além da eficiência técnicas das medidas: “É tanto uma questão de necessidade quanto de conformidade. Um pouco dos dois. Tem necessidades técnicas e precisa ter conformidade.”

A entrevista mostrou que as medidas técnicas são adotadas com a intenção de garantir a confidencialidade através de controles de acesso físico e digital, o que reduz a possibilidade de ocorrência de incidentes com as informações sensíveis que são armazenadas e processadas na subunidade: “A gente trabalha com dados sensíveis. Precisa ter esse tipo de controle. São dados de pesquisas, dados de pacientes.” (ENTREVISTADO 04).

Segundo o Entrevistado 04, há a compreensão na subunidade de que a adoção de medidas informais tem a intenção de conscientizar os usuários de TI quanto à Segurança da Informação. “Na verdade, é que precisamos informar ao usuário o que é responsabilidade do [nome da subunidade] e o que não é” (ENTREVISTADO 04). Este trecho demonstra que, no entendimento do entrevistado, o viés da adoção é a eficiência na Segurança da Informação

através da mudança do comportamento das pessoas. Cabe registrar que, mesmo com o entendimento de que as medidas informais são importantes, a subunidade não adotou medidas desta categoria. Embora o entrevistado tenha deixado claro que nada impede a adoção e que há na subunidade a clareza de que as medidas são necessárias, nenhuma ação foi tomada neste sentido e não há planos para adoção destas medidas.

Já sobre as medidas formais, o Entrevistado 04 declarou que a adoção acontece "por necessidade. Para ter acesso a informação, é preciso identificar que tipo de dado cada pessoa vai ter acesso, que tipo de dispositivo cada um pode utilizar, cada serviço prestado pelo [nome da subunidade] e quais são os direitos [do usuário], o que ele pode utilizar e o que não pode, o que pode fazer ou não pode." Sendo uma questão de necessidade técnica, a adoção de medidas formais está relacionada também a uma percepção de que são eficientes para a garantia da Segurança da Informação.

Quanto às pressões que a subunidade sofre, o Entrevistado 04 apontou as auditorias realizadas pela administração central, a Política de Segurança da Informação e os regulamentos da organização. Os programas de treinamento, divulgação e conscientização não foram citados na entrevista. O entrevistado relaciona diretamente as auditorias à adoção de medidas de Segurança da Informação: "São feitas algumas auditorias, e por isso devem existir esses controles. [...] São realizadas algumas auditorias que exigem esse tipo de controle de acesso. [...] Tem que seguir e é auditado. Todos os anos, passamos por auditoria para ver se tem esse controle. Quando não tem, o auditor reclama, diz que não está funcionando." Sobre os regulamentos e a Política, o Entrevistado 04 deixou claro que foram criados pela FIOCRUZ para fazer com que as subunidades adotem as medidas de Segurança da Informação necessárias. Além disso, as tecnologias adotadas pela administração central também pressionam a Subunidade 04 a adotar medidas de Segurança da Informação, a exemplo do antivírus: como a subunidade adotou a solução corporativa da FIOCRUZ, fica dependente da CGTI para realizar atualizações e para renovar o contrato de uso.

A resposta estratégica que caracteriza a Subunidade 04 quanto à adoção de medidas de Segurança da Informação previstas nos regulamentos da organização é o compromisso, o que está de acordo com a percepção de que a adoção está associada à eficiência, mas que ainda assim nem tudo é adotado. O relatório de auditoria (FIOCRUZ, 2015) mostra que houve uma tendência a adotar as medidas de Segurança da Informação na subunidade, com uma leve inclinação para a adoção parcial. Muitas medidas foram adotadas por serem tidas como certas, sem que tenha havido uma análise dos benefícios que a

subunidade teria diante dos constituintes do ambiente institucional. Apesar disso, respostas estratégicas diferentes foram identificadas para situações específicas relacionadas à adoção de medidas técnicas: esquiva, quando as pressões eram para adoção de medidas de controle de acesso físico a salas cujo acesso deve ser restrito; desafio, ao desrespeitar regulamentos que determinam a adoção de medidas de controle de acesso lógico à Internet; e manipulação, ao buscar incluir membros da subunidade em grupos de trabalho que tomam decisões relacionadas à Segurança da Informação. Nenhuma medida informal foi adotada. O relatório de auditoria (FIOCRUZ, 2015) revela que todos os regulamentos da organização têm medidas rejeitadas e adotadas parcialmente pela subunidade, o que reforça a caracterização do seu comportamento como compromisso.

O desafio figura como resposta estratégica com maior cobertura de percentual identificada na subunidade (22,09%), cuja tática que aparece com maior cobertura é a rejeição, com 17,01%. O fato de a subunidade rejeitar todas as medidas informais as quais é pressionada a adotar pode ter influenciado a quantidade de indicadores de desafio identificados nas respostas do Entrevistado 04, o que pode explicar este alto índice de cobertura de percentual. O desafio é também a resposta com maior número de referências de codificação: 14 referências foram identificadas para esta resposta estratégica. A tática com maior quantidade de referências codificadas é também a rejeição, com nove referências.

A incapacidade de adotar as medidas exigidas pelo ambiente institucional pode explicar o desafio como a resposta estratégica que tem maior cobertura de percentual e maior quantidade de referências codificadas. A falta de recursos financeiros e de pessoas capacitadas na subunidade foi apontada pelo Entrevistado 04 como uma causa para a não adoção de medidas de Segurança da Informação. A entrevista com o informante da Subunidade 04 mostrou uma resposta de desafio que não pode ser caracterizada como nenhuma das táticas propostas por Oliver (1991). O comportamento da subunidade de não adotar as medidas de Segurança da Informação por falta de recursos ao mesmo tempo em que reconhece a necessidade de adotá-las difere da tática de rejeição porque nesta tática, as regras e valores institucionais são ignorados como uma opção estratégica (OLIVER, 1991; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009), mas esta opção por rejeitar as medidas não foi identificada na entrevista. A tática adotada pela Subunidade 04 também não pode ser caracterizada como contestação ou ataque, pois não houve qualquer negociação com as fontes de pressão institucional nem houve qualquer tipo de ataque às medidas, pressões ou fontes de pressão institucional, como previsto na teoria (OLIVER, 1991; ARMÊNIO NETO;

MACHADO-DA-SILVA, 2009). Ao mesmo tempo, a tática adotada não pode ser enquadrada como qualquer uma das táticas de esquiva, pois a subunidade não esconde a não conformidade nem tenta parecer estar em conformidade, mito menos contorna a obrigação de adotar essas medidas, como a teoria descreve o amortecimento, a ocultação e a fuga (OLIVER, 1991; ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). A tática adotada pela subunidade é um meio-termo entre a fuga (da resposta estratégica de esquiva) e a rejeição (da resposta estratégica de desafio), pois a subunidade reconhece que não está aderente e reconhece também que a adoção é necessária.

É possível argumentar que a falta de capacidade de adotar pode levar a subunidade a optar pela não adoção, mas o Entrevistado 04 deixou claro que a subunidade não escolheu pelo caminho da não adoção, não há uma rejeição consciente. Ao contrário disso, a subunidade pretendia adotar, mas a adoção não foi possível, um comportamento que demonstra o reconhecimento da necessidade de adotar a medida. Por não haver previsão desta tática na tipologia de Oliver (1991), justifica-se a inclusão do reconhecimento no *framework* de pesquisa.

6.3.5 Subunidade 05

A entrevista com o responsável pela TI na Subunidade 05 foi realizada remotamente através de Skype e teve duração de 47 minutos. A Subunidade 05 não se localiza na mesma cidade da sede da organização e a área de TI tem apenas duas pessoas, sendo que nenhuma trabalha exclusivamente com Segurança da Informação. Por ser um escritório regional, a subunidade não tem autonomia administrativa e está subordinada às determinações da CGTI da FIOCRUZ. O entrevistado é terceirizado e tem graduação e especialização na área de TI.

Segundo o Entrevistado 05, a subunidade tem regras documentadas para utilização da rede de computadores e uma portaria estava sendo preparada para regulamentar o credenciamento dos usuários de TI na subunidade. A subunidade tem também um processo documentado de autorização para acessar dados documentados. O entrevistado relatou que a subunidade não tem Política, subcomitê, equipe de tratamento de incidentes, escritório de Segurança da Informação, processo de análise e avaliação de riscos, classificação de informações, Sistema de Gestão de Segurança da Informação e, evidentemente, revisão

periódica da Política. Dessa forma, dentre as medidas formais de Segurança da Informação, a subunidade adota apenas "Regulamentos internos de Segurança da Informação" e "Processos e procedimentos de Segurança da Informação".

A Subunidade 05 adotou medidas de "Segregação e monitoramento de redes de computadores" e "Controle de acesso lógico", segundo o Entrevistado 05: "Temos três redes distintas: uma para computadores da FIOCRUZ, outra para os dispositivos móveis particulares e outra para visitantes. [...] Então são redes separadas, que não se enxergam". O entrevistado complementa que "Todas [as redes de computadores] possuem regras e o usuário se identifica para poder usar a rede [...] eles [os usuários] só podem ter acesso às pastas que eles podem ver, com *login* e senha. [...] Para os usuários administrativos, os usuários de cada departamento têm acesso às pastas dos seus departamentos." Ainda segundo o entrevistado, configurações de *firewall* foram realizadas para controlar o acesso à *web* a fim de garantir a disponibilidade de serviços e *websites* acessados na Internet e foi implantada uma solução de autenticação para usuários da rede sem fio. A subunidade tem também servidores de rede redundantes e realiza *backups* diários dos dados armazenados em seus servidores de rede, medidas técnicas de "Redundância de dados" e de "Redundância de equipamentos". As senhas dos usuários são trocadas periodicamente e é exigida certa complexidade para evitar a utilização de senhas fáceis, medidas de "Autenticação forte". Como medidas de "Proteção ambiental", *no-break* e ar condicionado garantem alguma proteção contra falta de energia e problemas relacionados à variação de temperatura e umidade na sala em que ficam os equipamentos da rede de computadores. Entre as medidas de "Prevenção contra códigos maliciosos", a subunidade utiliza o antivírus corporativo da FIOCRUZ, e como utiliza o *webmail* da FIOCRUZ, a subunidade utiliza também a solução de anti-spam adotada pela organização. Para fazer "Controle de acesso físico", a Subunidade 05 tem uma sala com acesso restrito. Assim, oito dos dez tipos de medidas técnicas são adotados pela subunidade.

O responsável pela TI da Subunidade 05 relatou que já fez divulgação da Política e dos regulamentos de Segurança da Informação e que a divulga sempre que há um novo usuário de serviços de TI e sempre que há alguma divergência quanto às proibições, permissões e responsabilidades, para fins de conscientização. Novos regulamentos são também divulgados quando aprovados e publicados pela Presidência da FIOCRUZ. O entrevistado não relatou ter havido qualquer ação de treinamento para profissionais da área de TI ou usuários da subunidade, tendo citado inclusive a implantação do antivírus corporativo, momento em que poderia ter havido um treinamento, mas não houve: "Não tive treinamento.

Eles só mandaram. Mandaram a gente instalar e não teve treinamento e eu não fico sabendo de nada. Só recebo um email dizendo que equipamento tal está infectado, e diz o que o antivírus fez. Eu fico cego. Não tenho acompanhado, não sei como funciona." (ENTREVISTADO 05). Com isso, os dados mostram que as medidas informais adotadas foram de "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização".

Poucas medidas previstas nos regulamentos da FIOCRUZ são adotadas pela Subunidade 05. O regulamento com o qual a subunidade está em maior conformidade é a Norma Institucional SIC-009/CGTI/VPGDI (FIOCRUZ, 2013g), sobre a utilização de dispositivos móveis, pois 50% das medidas previstas neste regulamento são adotadas. Das medidas existentes nos demais regulamentos, a subunidade não adota mais do que 10%, havendo casos em que nenhuma medida prevista é adotada. No entanto, destaca-se que a subunidade adota parcialmente diversas medidas existentes em cinco regulamentos organizacionais: Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a), Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d), Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a) e Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f).

A adoção de medidas de Segurança da Informação na subunidade é uma questão de disponibilidade, segundo o Entrevistado 05. Para ele, é uma necessidade ampla, pois envolve regulamentos, conscientização e medidas técnicas, mas a adoção garante o acesso das pessoas às informações, sistemas e demais recursos computacionais. O entrevistado complementa que há também uma preocupação com a confidencialidade: "De um tempo para cá, teve aquele vazamento de informações da Presidente [ex-Presidente Dilma] [...]. O governo se preocupa bastante, mas com medo de vazamento de informações. Acho também que aqui existe muita patente, descobertas, e tem muita gente de olho."

Na entrevista ficou claro o viés técnico das medidas adotadas, o que pode ser explicado pelo fato de a subunidade ter sido incorporada pela organização há poucos anos, não tendo havido tempo para a elaboração de medidas formais. Diferentemente de medidas técnicas e formais, que são associadas à garantia da disponibilidade, medidas informais são percebidas como importantes para a mudança do comportamento dos usuários, o que explica a realização constante de ações de conscientização e divulgação. A entrevista deixou claro também que, para o Entrevistado 05, o desconhecimento é a causa da resistência dos usuários às medidas técnicas e formais adotadas, o que é minimizado pelas medidas informais. Assim,

a preocupação com a adoção de medidas técnicas é garantir que as informações estejam disponíveis para seus usuários e protegidas contra acessos indevidos, enquanto as medidas formais visam justificar as medidas técnicas, enquanto a adoção de medidas informais tem a intenção de conscientizar e educar os usuários. Com isso, fica claro que a adoção das medidas de Segurança da Informação é uma questão de eficiência (principalmente garantia da disponibilidade e da integridade), e não de conformidade, no entendimento do Entrevistado 05.

As pressões da administração central da organização são exercidas por meio das tecnologias adotadas, como o antivírus, o *datacenter* e a solução corporativa de correio eletrônico, que obrigam a subunidade a adotar medidas de Segurança da Informação para se adequar e poder utilizá-los. Mas o Entrevistado 05 informou que a subunidade sofre pressões também de outras organizações, com destaque para órgãos e entidades que tratam de TI na administração pública federal, como a maior empresa estatal de TI e o próprio Governo Federal, que produzem regulamentos e também conhecimentos sobre Segurança da Informação. Algumas dessas organizações são consultadas pelo entrevistado para saber como determinadas necessidades estão sendo tratadas, o que facilita a tomada de decisões na sua subunidade. Essas pressões mostram que, no entendimento do entrevistado, a subunidade está sujeita a pressões internas (da administração central) e externas, que são de natureza coercitiva, normativa e mimética.

O entrevistado informou que já realizou viagens ao Rio de Janeiro para conversar com o gestor de Segurança da Informação da organização a fim de se informar sobre como agir quando houver ocorrências na subunidade. Os regulamentos criados pelo Comitê de Segurança da Informação são vistos pelo entrevistado como coerentes com os objetivos e atividades da subunidade e, por este motivo, são respeitados:

> Eu acho que, com tudo isso aí que a FIOCRUZ cria [os regulamentos], a gente tem alta disponibilidade, pois tem gente que vem trabalhar à noite, no fim de semana. Acho que é muito bom ter o recurso [computacional] na hora que a gente quer, na hora que precisa. Essas regras fazem com que a estrutura fique disponível. Se deixar muito solto, acho que prejudica (ENTREVISTADO 05).

No entanto, a pesquisa mostrou que nenhuma das categorias de medidas de Segurança da Informação teve todos os tipos de medidas adotadas. O entrevistado deixou claro que tem consciência de que não adota todas as medidas que precisam ser adotadas, mas esclareceu que a causa da não adoção é a falta de recursos. A auditoria mostrou que apenas

dois regulamentos tiveram algumas das medidas previstas adotadas integralmente. Todos os regulamentos tiveram pelo menos a metade das medidas previstas rejeitadas e dois deles foram integralmente rejeitados pela subunidade. No entanto, a subunidade pretende adotar as medidas e negocia recursos para esta finalidade: "Do jeito que está hoje, se ela [um equipamento da rede de computadores da subunidade] queimar agora, a gente fica sem nada. Fica sem Internet, sem absolutamente nada. Nossa rede praticamente para. Eu já mandei *emails* para a diretoria, já documentei isso informando que eu preciso de uma redundância física." (ENTREVISTADO 05). A quantidade de medidas previstas nos regulamentos e que não são adotadas é muito maior do que a das medidas adotadas integralmente ou parcialmente. Com isto, o relatório de auditoria interna (FIOCRUZ, 2015) mostra que o comportamento característico da subunidade em resposta aos regulamentos da organização é o desafio.

A resposta estratégica desta subunidade que figura no NVivo como a que tem maior cobertura de percentual é a aquiescência, com 13,05%, e a tática que aparece com maior percentual é a conformidade, com 9,60% de cobertura, o que parece ser uma contradição, pois a subunidade adota poucas medidas previstas nos regulamentos da organização e não adota todas as medidas de nenhuma das três categorias propostas por Dhillon (1999). No entanto, muitas medidas técnicas e algumas medidas formais e informais são adotadas, demonstrando que a subunidade responde com aquiescência a pressões institucionais. Foram identificadas sete referências à resposta de aquiescência, sendo quatro foram codificadas no subnó da tática de compromisso, sendo estas a resposta e a tática que tiveram maior quantidade de referências de codificação.

6.3.6 Subunidade 06

A entrevista com o responsável pela TI da Subunidade 06 foi realizada remotamente (utilizando Skype) e teve duração de 38 minutos. A subunidade fica na cidade do Rio de Janeiro, mas não está no mesmo *campus* da administração central da FIOCRUZ. O entrevistado é o coordenador de TI da subunidade. A Subunidade 06 tem uma equipe própria de TI, mas somente uma pessoa trabalha com foco em Segurança da Informação. A subunidade tem autonomia administrativa e não há nenhum vínculo hierárquico entre sua área de TI e a CGTI da FIOCRUZ. O Entrevistado 06 não tem graduação na área de TI, mas tem

duas especializações e mestrado, sempre nas áreas de gestão e de TI, e é membro do Comitê de Segurança da Informação da organização.

O entrevistado afirmou que sua subunidade tem regulamentos de Segurança da Informação e uma Política, mas que esta não foi ainda formalizada. A subunidade já realizou treinamentos para profissionais de TI e usuários sobre Segurança da Informação e já houve ações de divulgação da Política e dos regulamentos de Segurança da Informação, bem como ações de conscientização sobre o assunto. São utilizados os serviços de comunicação interna e a lista de distribuição de mensagens de correio eletrônico para divulgar textos e regulamentos de Segurança da Informação. Assim, apesar da falta de formalização da Política de Segurança da Informação da subunidade, a entrevista mostrou que a subunidade adota como medidas formais "Regulamentos internos de Segurança da Informação" e "Processos e procedimentos de Segurança da Informação", e entre as medidas informais, a entrevista mostrou que a subunidade realiza "Treinamento de profissionais de TI", "Treinamento de usuários de TI", "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização".

As tecnologias de Segurança da Informação identificadas na entrevista são antivírus e anti-spam como medidas técnicas de "Prevenção contra códigos maliciosos". Como medidas de "Segregação e monitoramento de redes de computadores", a subunidade utiliza *firewall* e *proxy*, sendo que este último é também uma solução de "Controle de acesso lógico" à Internet. Ainda como solução de controle de acesso lógico, os usuários de TI da Subunidade 06 tem *login* único para identificá-los nos sistemas e na rede de computadores, onde também são definidos níveis de permissão. Ainda sobre senhas, o entrevistado relatou que são utilizadas senhas complexas, que são trocadas periodicamente, o que configura a adoção de medidas técnicas de "Autenticação forte". Para ter "Redundância de dados", "Redundância de equipamentos" e "Redundância de peças de equipamentos", a subunidade tem tecnologias como equipamentos redundantes e com peças redundantes e espelhamento de disco, além de realizar *backups* rotineiros e de armazenar dados em sistemas de *storage*. A utilização de criptografia para prover acesso aos sistemas disponibilizados na Internet garante que a subunidade adota medidas técnicas de "Transmissão e armazenamento seguros de dados". As medidas de "Proteção ambiental" adotadas pela subunidade são a proteção contra falhas no fornecimento de energia elétrica através da utilização de *no-break* e a proteção contra variação de temperatura e umidade por meio de ar condicionado. O Entrevistado 06 afirmou que a subunidade não adota medidas de controle de acesso físico, sendo esta uma das

maiores demandas dele como responsável pela TI da subunidade e a única categoria de medidas de Segurança da Informação que não é adotada.

A Subunidade 06 adota 63% das medidas previstas no regulamento da FIOCRUZ que trata de acesso à Internet (Norma Institucional SIC-002/CGTI/VPGDI) (FIOCRUZ, 2012c), sendo este o maior percentual de conformidade identificado no relatório de auditoria interna analisado (FIOCRUZ, 2015). O regulamento que trata de Segurança da Informação na aquisição, desenvolvimento e manutenção de sistemas de informação também merece destaque, pois todas as medidas previstas foram adotadas pela subunidade, sendo que 57% foram totalmente e 43% foram de maneira parcial. Todos os regulamentos tiveram pelo menos 13% das medidas previstas adotadas, sendo as piores situações o que trata de segurança em *datacenter* (Norma Institucional SIC-004/CGTI/VPGDI) (FIOCRUZ, 2013a) e o que trata de mídias sociais (Norma Institucional SIC-008/CGTI/VPGDI) (FIOCRUZ, 2013f) – este último com destaque para o fato de 67% das medidas não terem sido adotadas.

O Entrevistado 06 acha importante a preocupação crescente com a Segurança da Informação na organização, pois a subunidade lida com dados sensíveis:

> [Segurança da Informação] É uma área muito perigosa, que guarda dados de pacientes, que são informações sigilosas. E quando estou falando de Segurança da Informação, não estou falando somente de Segurança da Informação nos equipamentos de informática. Estou falando de Segurança da Informação na questão física mesmo, nos prontuários de pacientes, que são deixados em cima da mesa. [...] É uma questão muito complexa para ser tratada, mas ao mesmo tempo necessária e não tem como fugir disso. A gente tem que estar preocupado com essa questão. A vantagem [de adotar medidas de Segurança da Informação] é que você minimiza os riscos de perda e de que esses dados possam ser acessados por quem não deveria. Quando eu falo perda, não é só perda do dado em si, mas perda da possibilidade de estar acessando, perda do acesso à Internet. (ENTREVISTADO 06).

Com isso, a entrevista mostrou que a adoção de medidas de Segurança da Informação tem um viés para a garantia da confidencialidade e da disponibilidade das informações, sendo, portanto, uma questão de eficiência. Mas o Entrevistado 06 também percebe como vantagem a conformidade da subunidade com os regulamentos e a Política de Segurança da Informação da FIOCRUZ: “Estar em conformidade com a FIOCRUZ e com outros órgãos governamentais é uma vantagem também. Você segue uma política única. Acho isso uma vantagem [de adotar medidas de Segurança da Informação].”

Apesar de a conformidade ser também um objetivo da subunidade ao adotar medidas de Segurança da Informação, a adoção de medidas formais, técnicas e informais foi

associada pelo entrevistado à eficiência: medidas técnicas garantem principalmente a disponibilidade das informações e sistemas, medidas informais garantem a conscientização e a mudança do comportamento dos usuários de TI, e medidas formais permitem a adoção das outras medidas sem que haja questionamentos.

Para o Entrevistado 06, a subunidade sofre pressões coercitivas de órgãos do Governo Federal, através das leis e dos regulamentos publicados, e da FIOCRUZ, que tem seus próprios regulamentos e que também adota tecnologias que forçam as subunidades a se submeterem às medidas adotadas. Como exemplo da pressão exercida através de tecnologias, o entrevistado citou a imposição de regras de *firewall* e controle de acesso à Internet que limitam a realização de pesquisas sobre temas bloqueados nos equipamentos que controlam o acesso. Segundo o entrevistado, essas questões deveriam ser tratadas nas subunidades, que têm conhecimento sobre o trabalho dos seus pesquisadores e demais usuários de TI.

Foi citada também como exemplo a tentativa de imposição de uma tecnologia de comunicação pelo Governo para todos os órgãos e entidades da administração pública federal. O Entrevistado 06 entende que sua subunidade está sujeita também a pressões miméticas, pois acredita que o fato de outras subunidades estarem adotando influencia a adoção em sua subunidade. Apesar disso, fez a ressalva de que as subunidades que não estão no *campus* da administração central da FIOCRUZ estão menos sujeitas a essas pressões. Por fim, a ocorrência de pressões normativas foi observada quando o Entrevistado 06 afirmou que utiliza boas práticas de mercado como base para adotar medidas técnicas, formais e informais de Segurança da Informação: “Tem pessoas aqui que estão antenadas com essas questões e a gente vai aplicando determinadas práticas que são consideradas as melhores práticas do mercado.”

Embora o Entrevistado 06 perceba a adoção das medidas de Segurança da Informação como uma questão de eficiência, o comportamento característico da subunidade frente às pressões que recebe é o compromisso. Este comportamento é observado principalmente quanto às pressões para adoção de medidas técnicas e formais, e a tática utilizada em ambos os casos é a pacificação, pois uma parte das medidas é adotada, e outra parte é rejeitada. Já as pressões para adoção de medidas informais resultam em um comportamento característico de aquiescência, sendo o hábito a tática característica.

É possível identificar a resposta de desafio quando o entrevistado relata o bloqueio realizado pela CGTI através do *firewall* da rede do *campus* e a reação da

subunidade. Medidas de “Controle de acesso físico”, cuja adoção é obrigatória, de acordo com a Norma Institucional SIC-004/CGTI/VPGDI (FIOCRUZ, 2013a), não são adotadas porque a subunidade não tem recursos para isso, como informou o Entrevistado 06. A falta de recursos financeiros, humanos e de tempo são os principais motivos relatados para a não adoção de parte das medidas de Segurança da Informação, mas o responsável pela TI da subunidade percebe essas medidas como importantes. Todos os regulamentos da organização tiveram medidas rejeitadas ou adotadas parcialmente, conforme o relatório de auditoria (FIOCRUZ, 2015), mas cinco regulamentos tiveram mais da metade das medidas previstas adotadas pela subunidade. O comportamento característico da subunidade diante dos regulamentos da organização é a aquiescência, pois a maioria das medidas previstas é adotada pela subunidade e há mais medidas adotadas parcialmente do que rejeitadas.

Para o entrevistado, as particularidades das subunidades devem ser consideradas pela organização ao regulamentar a adoção de medidas de Segurança da Informação, pois regras que limitem as atividades ou mesmo a autonomia tendem a ser rejeitadas, mas ele complementa que a subunidade está buscando a conformidade, que é facilitada pelo fato de ele compor o Comitê de Segurança da Informação da FIOCRUZ.

A busca pela conformidade é condizente com a percepção do Entrevistado 06 de que as medidas de Segurança da Informação são necessárias para proteger a informação e garantir a conformidade com os regulamentos, e explica o fato de a aquiescência ter sido a resposta com mais destaque, com 15,58% de cobertura percentual calculada pelo NVivo, e cuja tática que teve maior cobertura foi a conformidade, com 8,31%. A resposta de aquiescência teve também cinco referências de codificação identificadas no NVivo, e as táticas de conformidade e hábito tiveram duas referências cada, confirmando os resultados da cobertura de percentual e contradizendo o comportamento característico da subunidade.

6.3.7 Subunidade 07

O entrevistado da Subunidade 07 é o responsável pelo setor de TI. Com duas pessoas, o setor está subordinado à CGTI da FIOCRUZ, pois a subunidade não tem autonomia administrativa, e não há nenhuma formalização do entrevistado como coordenador ou responsável pelo setor nem existe uma pessoa que esteja dedicada às atividades de Segurança da Informação na subunidade. O Entrevistado 07 tem formação na área de TI e

duas especializações. A entrevista foi através de Skype e demorou 34 minutos. A subunidade fica distante da administração central da FIOCRUZ.

O Entrevistado 07 afirmou que houve a divulgação da Política de Segurança da Informação e que há divulgação dos regulamentos e recomendações da organização. No entanto, a divulgação é feita depois de analisar se o regulamento ou recomendação é voltado para os usuários ou para profissionais de TI. O Entrevistado 07 informou que já teve oportunidade de participar de um treinamento, mas não pôde devido ao fato de estar trabalhando no período em que aconteceram as aulas, e fez a ressalva de que isso não é uma rotina da subunidade. Treinamentos para usuários de TI e ações de conscientização não foram relatados pelo informante. A publicação de regulamentos pela CGTI tem pouco impacto sobre a subunidade, acrescenta o entrevistado. Ele justifica que a subunidade tem recursos limitados e que a implantação de certas restrições não acontece, o que resulta em um pequeno impacto sobre a subunidade. Com isso, a entrevista mostrou que a única medida informal de Segurança da Informação adotada pela subunidade foi do tipo "Divulgação de regulamentos e da Política de Segurança da Informação", por iniciativa do próprio entrevistado. Não foram identificadas medidas formais adotadas pela subunidade na entrevista realizada.

Entre as medidas técnicas, a entrevista mostrou que realiza *backup* diário dos dados armazenados no computador que funciona como servidor de arquivos, o que é uma medida de "Redundância de dados". Os equipamentos de rede não são redundantes nem têm peças redundantes. Como medidas de "Segregação e monitoramento de redes de computadores", a subunidade tem *firewall* e utiliza VLANs para fazer segmentação da rede de computadores, isolando equipamentos e usuários de setores distintos e também com finalidades distintas, como rede de pesquisa, rede administrativa e rede sem fio. Como medida de "Proteção ambiental", o entrevistado relatou apenas a utilização de *no-break* para um dos equipamentos de rede (os outros não têm este tipo de proteção). A subunidade utiliza o antivírus e o anti-spam da FIOCRUZ, que são soluções de "Prevenção contra códigos maliciosos". O acesso dos usuários aos recursos de rede depende de autenticação com *login* e senha em seus computadores e não conseguem acessar dados de outros usuários, medidas de "Controle de acesso lógico" que existem também nos sistemas de informação corporativos da FIOCRUZ. "Controle de acesso físico" existe para equipamentos específicos da área de pesquisa, mas não para todos os equipamentos da rede de computadores. Como medida de "Transmissão e armazenamento seguros de dados", o Entrevistado 07 relatou que a subunidade utiliza recursos de criptografia em sistemas e serviços disponibilizados para

acesso através da Internet, informando que é uma exigência da administração central da organização: “A gente usa [criptografia] no acesso ao *email* e nos sistemas. Mas, no caso, é a política da FIOCRUZ. [...] Mas é interessante citar: existe um acesso externo de um pessoal a um *cluster* e máquinas usadas na pesquisa, e aí houve o cuidado de colocar acesso seguro, utilizando [nome de protocolo de rede seguro].” (ENTREVISTADO 07). Medidas de redundância de peças de equipamentos, autenticação forte e redundância de equipamentos não foram identificadas a partir dos dados colhidos na entrevista.

A análise do último relatório de auditoria disponibilizado (FIOCRUZ, 2015) mostra que a Subunidade 07 adota apenas 27% das medidas relacionadas a acesso remoto previstas na Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e) e 25% das medidas relativas ao uso da Internet previstas na Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c). Ainda sobre estes dois regulamentos, 36% das medidas presentes no primeiro e 50% das medidas do segundo são adotadas parcialmente. O regulamento de trata de dispositivos móveis (Norma Institucional SIC-009/CGTI/VPGDI) (FIOCRUZ, 2013g) tem apenas 7% das medidas adotadas pela subunidade. Nenhum outro regulamento teve medidas adotadas plenamente, e a Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a), que regulamenta a realização de *backups*, não tem nenhuma das medidas previstas adotada plenamente ou parcialmente pela subunidade.

O principal benefício que a Subunidade 07 tem ao adotar medidas de Segurança da Informação é a tranquilidade dos usuários na realização das atividades da subunidade devido à garantia de um ambiente de TI seguro, na visão do Entrevistado 07, pois os usuários costumam trabalhar em colaboração com pessoas de outras organizações, trocando informações e provendo acesso a sistemas locais, além de lidar com dados de pesquisa que podem ser importantes e cuja perda pode provocar prejuízos para a organização. O entrevistado acrescentou ainda que é “fundamental a proteção da imagem da instituição” que a adoção de medidas de Segurança da Informação traz, pois a ocorrência de um incidente extrapola a fronteira da organização, mostrando para o ambiente externo descaso da organização com seus dados sensíveis. A entrevista mostrou que, na opinião do participante, a subunidade adota medidas de Segurança da Informação para ter eficiência na garantia da confidencialidade, integridade e disponibilidade da informação.

Pressão coercitiva da administração central, exercida através da Política de Segurança da Informação da organização, é relatada pelo entrevistado, mas ao mesmo tempo ele entende que a cobrança para que haja conformidade nas subunidades é muito pequena:

“Eu acho que ela é um pouco relaxada com relação a isso. Então não vejo uma cobrança efetiva interna, e isso é muito ruim. Se é para funcionar, eu acho que tem que haver algum rigor nessa cobrança.” O Entrevistado 07 complementa que as subunidades têm muita autonomia quanto à Segurança da Informação, de forma que a Política, que deveria ser seguida em todas elas, termina por não ser seguida ou cada subunidade elabora sua própria Política, fazendo com que a Segurança da Informação fique descentralizada e com que haja pouca cobrança. O fato de outras subunidades ou organizações adotarem certas medidas de Segurança da Informação é visto pelo entrevistado como uma influência para a sua subunidade, pois servem como exemplos. No entanto, ele acrescenta que é necessário ainda convencer a direção da subunidade, correndo o risco de a adoção não acontecer devido à autonomia da subunidade. Com isso, pressões miméticas têm menos influência sobre a subunidade. Não foram identificados elementos que mostrassem que o entrevistado percebe que a subunidade sofre pressões normativas, o que é uma contradição frente à percepção de que a adoção de medidas de Segurança da Informação é uma questão de eficiência.

O desafio é uma resposta estratégica que aparece na entrevista associada às pressões para adoção de medidas formais, que resulta no fato de nenhuma medida desta categoria ter sido adotada. A tática utilizada é a rejeição, visto que a justificativa pela não adoção é a limitação de recursos, que faz com que a subunidade não tenha capacidade de adotar. A pequena quantidade de medidas informais caracteriza uma resposta de compromisso, sendo que, neste caso, a tática é a pacificação, pois apenas parte das medidas é adotada. O resultado da auditoria confirma este comportamento, pois mostra que poucas medidas previstas nos regulamentos são adotadas pela subunidade.

Apesar de o compromisso ser o comportamento da subunidade frente às pressões para adotar medidas técnicas, a barganha é uma resposta identificada nos dados, pois o entrevistado relata que o regulamento da FIOCRUZ que obriga a restrição do acesso à sala de equipamentos de rede (FIOCRUZ, 2013a), mas a subunidade ainda não adota, o que será feito em um futuro próximo, quando a subunidade estiver em um novo prédio, com salas preparadas para essa finalidade.

A resposta de desafio foi também associada a medidas técnicas. Utilizando a tática de rejeição, a subunidade permite que serviços gratuitos de armazenamento de dados na nuvem sejam utilizados pelos usuários de TI, apesar de ser expressamente proibido pela CGTI. O entrevistado justifica a resposta estratégica com o argumento de que os usuários

precisam desse serviço e que a FIOCRUZ tem nuvem privada, mas não disponibiliza seu serviço para a subunidade. Sobre essa situação, o Entrevistado 07 diz:

> Eu penso dessa forma: a Política de Segurança [da Informação] não pode limitar a atuação das áreas fins. [...] Se por algum motivo você não puder usar algum serviço por causa de medidas de segurança, é obrigação da instituição oferecer esse ou outro serviço de forma segura. A segurança não pode estar acima dos interesses da área fim. [...] Entre negar o serviço e obedecer à Política de Segurança, eu sou da filosofia de que se deve oferecer o serviço e ignorar a Política de Segurança. Obviamente, vai depender de o quão crítico o serviço é. (ENTREVISTADO 07).

A resposta de compromisso foi identificada em diferentes trechos da entrevista, principalmente através da tática de pacificação, o que pode ser notado na quantidade de regulamentos que são parcialmente cumpridos pela subunidade, como, por exemplo, a ausência de *no-break* para garantir o funcionamento ininterrupto de todos os equipamentos da rede de computadores, mas apenas de um deles. A adoção de medidas técnicas de controle de acesso lógico, o que só deve acontecer quando a subunidade tiver sido instalada em um novo *campus*, também é uma resposta de compromisso, mas pela tática de barganha. Foi também identificada uma resposta de esquiva por ocultação quando o entrevistado relatou que implantou um *firewall* sem realizar as configurações para impedir o acesso a *websites* potencialmente perigosos.

O relatório de auditoria interna (FIOCRUZ, 2015) mostra que há muito mais medidas presentes nos regulamentos da organização que foram rejeitadas do que a quantidade de medidas que foi adotada parcialmente e integralmente, o que faz com que o desafio seja a resposta característica da organização.

Apesar da variedade de respostas estratégicas identificadas na pesquisa, o desafio teve 18,07% de cobertura de percentual e nove referências de codificação, e a rejeição teve 15,20% de cobertura de percentual e sete referências, sendo estas a resposta estratégica e a tática mais relevantes para a subunidade.

6.3.8 Subunidade 08

A Subunidade 08 tem um setor de TI com uma divisão interna específica para infraestrutura e suporte ao usuário e outra para desenvolvimento de sistemas, mas não tem uma equipe dedicada à Segurança da Informação. A subunidade está localizada no *campus* da

sede da FIOCRUZ, tem um coordenador de TI formalmente designado e não tem nenhum vínculo hierárquico com a CGTI, pois goza de autonomia administrativa. A entrevista foi por Skype, teve duração de 42 minutos e o entrevistado foi o responsável pela Segurança da Informação da subunidade, que também é membro do Comitê de Segurança da Informação da FIOCRUZ. O entrevistado tem graduação na área de TI e especialização.

Conforme afirmou o Entrevistado 08, a implantação de novas tecnologias, serviços e sistemas de informação passa por uma homologação que inclui um "Processo de análise e avaliação de riscos". Procedimentos de *backup* e restauração de dados são documentados, o que indica que há "Processos e procedimentos de Segurança da Informação" adotados. A subunidade tem também um processo definido de "Classificação de informações", que avalia a necessidade de confidencialidade das informações e, caso necessário, implica na adoção de outras medidas como criptografia das informações. No entanto, o entrevistado admitiu que nem sempre esse processo é executado e nem sempre o regulamento é seguido integralmente: "Assim, a gente faz a classificação, mas nem todos os documentos nossos estão 100% classificados." (ENTREVISTADO 08). A subunidade não adotou outras medidas formais de Segurança da Informação.

Entre as medidas informais, a subunidade realizou "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização" voltadas tanto para os usuários de TI quanto para gestores da subunidade. Segundo o entrevistado, o Gestor de Segurança da Informação da FIOCRUZ realizou palestras de conscientização e divulgação voltada para os gestores da subunidade e participou de eventos voltados para os usuários. O entrevistado informou que medidas internas de conscientização e divulgação foram adotadas e são realizadas periodicamente. O Entrevistado 08 informou também que, apesar de não ter programas de treinamento para profissionais de TI, a subunidade realizou "Treinamentos de usuários de TI".

As medidas técnicas de Segurança da Informação adotadas pela subunidade incluem a realização rotineira de atualizações nos servidores e sistemas de informação, dos computadores dos usuários e do antivírus da subunidade. A subunidade também utiliza o antivírus e o anti-spam da FIOCRUZ, o que são caracterizadas como medidas de "Prevenção contra códigos maliciosos". A subunidade utiliza virtualização de servidores de rede como forma de ter medidas de "Redundância de equipamentos" adotadas. Os servidores de rede têm recursos de "Redundância de peças de equipamentos". As medidas de "Redundância de dados" incluem a utilização de *storages* para armazenamento e replicação de dados e a

realização de *backups* dos dados armazenados em seus servidores de rede. Para "Segregação e monitoramento de redes de computadores", a subunidade tem *firewall* segmentando a rede de computadores em uma DMZ e uma rede interna. Todos os sistemas têm "Controle de acesso lógico", bem como a rede de computadores, para controlar as permissões de acesso dos usuários, e o acesso é garantido através de "Autenticação forte" com *login* e senha complexa, que é trocada periodicamente.

As medidas de "Proteção ambiental" são o uso de *no-break* e gerador para evitar danos e indisponibilidades provocadas por falta de energia, além de ar condicionado nas salas de equipamentos. Apesar de não ter outras medidas de proteção ambiental na sala onde estão armazenados seus equipamentos, o entrevistado informou que tem também servidores de rede hospedados no *datacenter* da organização, que oferece outras medidas, como proteção contra incêndio, inundação e fumaça, além de acesso restrito, medida de "Controle de acesso físico". O acesso a sistemas pela Internet é seguro, o que caracteriza a adoção de medida de "Transmissão e armazenamento seguros de dados". Com isso, é possível afirmar que a subunidade adotou todas as categorias de medidas técnicas.

A despeito de ter adotado todas as categorias de medidas técnicas e ainda três categorias de medidas informais, o relatório da última auditoria mostra que a subunidade não está em conformidade plena com nenhum dos regulamentos da organização. A Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e), que regulamenta o acesso remoto na FIOCRUZ, tem 73% das suas medidas adotadas pela subunidade e 27% adotadas parcialmente, sendo o regulamento interno da organização com o qual a subunidade apresenta maior conformidade. Os outros dois regulamentos que têm destaque são a Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a) e a Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c) – a primeira sobre responsabilidades dos usuários de TI e a segunda sobre acesso à Internet – ambas com 50% das medidas adotadas. Os demais regulamentos não têm mais do que 22% das medidas adotadas pela subunidade, mas cabe destacar que poucas medidas são rejeitadas pela subunidade. À exceção da Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), que regulamenta o acesso a redes sociais e que tem 100% de rejeição por parte da subunidade, os demais regulamentos têm pelo menos 57% das medidas previstas adotadas parcialmente ou integralmente.

O Entrevistado 08 entende que a adoção de medidas de Segurança da Informação traz para a subunidade benefícios ligados à eficiência, como a possibilidade de recuperar

dados e de rastrear o uso dos sistemas, que estão relacionadas à disponibilidade e integridade da informação.

O viés técnico e a ideia de ganho em eficiência que o entrevistado associa à Segurança da Informação é notado quando ele relata que antes mesmo de haver uma Política de Segurança da Informação na organização, a subunidade já tinha diversas medidas adotadas, seguindo recomendações e boas práticas do mercado e imitando outras organizações, como a implantação de medidas técnicas, como *firewall*, soluções de segurança de redes, como *Intrusion Prevention System* (IPS), medidas de controle de acesso. A adoção dessas medidas foi associada pelo entrevistado à atuação dos profissionais técnicos, orientados por recomendações e boas práticas do mercado. No entanto, o entrevistado admite que os técnicos também se espelharam no que é feito em outras organizações, o que evidencia que a adoção de medidas técnicas foi influenciada por pressões institucionais normativas e miméticas.

Mas o entrevistado relata que a Subunidade 08 adotou medidas também devido a pressões coercitivas da administração central da FIOCRUZ. Na entrevista, relatou que a pressão da CGTI levou a sua subunidade a migrar seus recursos de TI para o *datacenter* da FIOCRUZ, além de realizar ações de conscientização para os usuários e a classificar informações organizacionais. Neste caso, a adoção de medidas formais e informais pode ser relacionada à conformidade com requisitos de Segurança da Informação impostos pela administração central da organização.

Não foram encontradas evidências de adoção de medidas informais e formais de todos os tipos previstos, mas foram encontradas evidências para todos os tipos de medidas técnicas. O comportamento característico da subunidade ao ser pressionada pela administração central através de regulamentos de Segurança da Informação é o compromisso, pois há uma grande quantidade de medidas previstas nos regulamentos que são adotadas parcialmente, como mostra o relatório de auditoria (FIOCRUZ, 2015), enquanto há um equilíbrio entre as quantidades de medidas adotas e rejeitadas.

A Subunidade 08 respondeu às pressões institucionais com desafio quando o Entrevistado 08 relatou que, ao responder a uma auditoria, informou que não adotou medidas que a subunidade é obrigada a adotar, mas que não houve qualquer implicação prática por não estar em conformidade, o que motivou não ter se esforçado para adotá-las, uma tática de rejeição. No entanto, o compromisso foi a resposta estratégica com maior cobertura de percentual: 15,54%. As evidências identificadas na entrevista apontam que a tática mais

utilizada é o equilíbrio, que é a adoção de medidas conflitantes entre si ou com os objetivos e atividades da subunidade, cuja implementação é ajustada para que não se configure o descumprimento. Esta tática teve 11,47% de cobertura de percentual, segundo o *software* NVivo. No entanto, a aquiescência, que teve 10,42% de cobertura de percentual, apresentou seis referências de codificação, enquanto o compromisso teve cinco referências identificadas. As táticas com maior quantidade de referências de codificação foram o equilíbrio e a conformidade, com três referências identificadas, sendo que a primeira tática é da estratégia de compromisso e a segunda é da aquiescência.

Diferentes respostas podem ser identificadas, mas a resposta de compromisso através da tática de equilíbrio foi identificada quando o entrevistado explicou o processo de análise e avaliação de riscos da subunidade, mas deixou claro que nem sempre esse processo é seguido. Quando afirmou que a subunidade faz a classificação das informações quanto à confidencialidade, mas admitiu que nem todas as informações com as quais a subunidade lida são classificadas, fica clara a resposta de compromisso. Quando informou que a subunidade faz monitoramento e atualização dos equipamentos da rede de computadores, mas que esses procedimentos não são feitos em todos eles, a resposta de compromisso fica evidenciada também. A tática, em ambos os casos, é o equilíbrio, uma vez que as medidas de Segurança da Informação são adotadas parcialmente.

A Subunidade 08 não adota as medidas que limitam o acesso dos usuários a repositórios virtuais na Internet, mas há um entendimento de que elas são importantes e necessárias, embora nenhuma atitude tenha sido tomada nem haja planos para a adoção: “A gente deixa claro que não está aderente e o motivo de não estar aderente: ‘A gente não cumpre essa norma aqui por causa disso’. Mas, por enquanto, ainda não teve uma tentativa de mudar porque a gente não está aderente.” (ENTREVISTADO 08).

Tal qual s Subunidade 04, a Subunidade 08 também utiliza a tática de reconhecimento, cujas características são o reconhecimento da necessidade, benefícios e importância, sem qualquer ação no sentido de rejeitar ou adotar.

6.3.9 Subunidade 09

A Subunidade 09 não está localizada na mesma cidade da sede da FIOCRUZ e tem autonomia administrativa, com uma diretoria própria. A subunidade tem um setor de TI

estruturado, sem qualquer ligação hierárquica com a CGTI da FIOCRUZ. A entrevista foi realizada por Skype com o responsável pela Segurança da Informação na subunidade e teve duração de 50 minutos. O Entrevistado 09 tem graduação na área de TI, não tem nenhum cargo comissionado ou função gratificada e é o único profissional que trabalha com Segurança da Informação na subunidade, embora admita que outras pessoas da área de TI também realizam atividades relacionadas ao tema.

De acordo com o Entrevistado 09, a subunidade não tem processos ou procedimentos de Segurança da Informação definidos e documentados. O entrevistado informou que também não tem equipe de tratamento de incidentes, subcomitê, regulamentos, escritório nem Política de Segurança da Informação na Subunidade 09, não faz classificação de informações, não tem um sistema de gestão definido nem faz análise e avaliação de riscos de Segurança da Informação, não havendo, portanto, nenhuma medida formal adotada.

Embora não tenha medidas formais adotadas, são realizadas ações de conscientização pelo menos uma vez a cada ano. O entrevistado não relatou haver programas de capacitação de funcionários e profissionais da área de TI nem ações de divulgação dos regulamentos e da Política de Segurança da Informação. Dessa forma, a única medida informal adotada pela Subunidade 09 é a realização de "Ações de conscientização".

Com relação às medidas técnicas, o entrevistado afirmou que a Subunidade 09 implantou *firewall* para proteger acessos indevidos à rede de computadores separando a rede interna da rede pública e para controlar os acessos externos aos sistemas de informação da subunidade. Para controlar o acesso dos usuários à Internet, a subunidade tem também um *proxy*, que filtra os conteúdos na Internet acessíveis internamente. Os computadores dos usuários de TI da subunidade são bloqueados automaticamente quando não são utilizados. Essas características mostram que a subunidade adotou medidas de "Controle de acesso lógico" e "Segregação e monitoramento de redes de computadores". A subunidade tem também medidas de "Prevenção contra códigos maliciosos", que são um antivírus e um anti-spam. O acesso à rede de computadores e aos sistemas de informação é controlado por *login* único e senha, que precisa atender a critérios de complexidade e ser alterada periodicamente. Assim, os dados mostram que a subunidade adotou medidas técnicas de "Autenticação forte". O entrevistado afirma que os equipamentos da rede de computadores ficam em uma sala com acesso restrito, o que mostram que a subunidade adota medidas de "Controle de acesso físico". Além disso, os equipamentos são protegidos contra falta de energia elétrica por *no-breaks* e gerador, a sala tem aparelhos de ar-condicionado, tem extintor de incêndio e detector

de fumaça com alarme, que são medidas de “Proteção ambiental”. Os sistemas e *websites* da subunidade que são acessados a partir da Internet têm acesso seguro, protegido por criptografia, o que garante a transmissão segura de dados, uma medida de “Transmissão e armazenamento seguros de dados”. Os equipamentos da rede de computadores têm peças redundantes que podem ser substituídas sem que seja necessário seu desligamento, uma medida de “Redundância de peças de equipamentos”. Por fim, o entrevistado afirmou que a subunidade utiliza um *storage* e que realiza *backups* diariamente utilizando uma solução de *tape library*, além de armazenar as fitas contendo os dados de *backup* em um cofre, o que garante “Redundância de dados”.

A partir da entrevista, fica claro que o único tipo de medidas técnicas de Segurança da Informação que a subunidade não adota é a de redundância de equipamentos. A entrevista mostrou também que a subunidade adota principalmente medidas técnicas, dando pouca atenção para medidas formais e informais de Segurança da Informação, visto que não adotou medida formal e apenas uma medida informal foi adotada. Apesar desse viés técnico, no relatório de auditoria (FIOCRUZ, 2015) é possível notar que a Subunidade 09 adota, ainda que parcialmente, não menos do que 75% das medidas de Segurança da Informação previstas em cada um dos regulamentos da FIOCRUZ, o que mostra que há uma preocupação em manter a conformidade com os requisitos de Segurança da Informação da organização. Dentre os nove regulamentos, aquele que tem menos medidas previstas adotadas pela subunidade é a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a), e isso pode ser explicado pelo fato de a subunidade não ter uma área de desenvolvimento de sistemas, um dos temas tratados pelo regulamento.

A Subunidade 09 adota apenas uma medida informal e nenhuma medida formal, mas a adoção de medidas técnicas é percebida pelo entrevistado como importante para dar amparo legal para as ações de Segurança da Informação, uma visão que não está relacionada à eficiência quanto à garantia da integridade, disponibilidade e confidencialidade, mas com a conformidade com os requisitos externos. Mas o Entrevistado 09 acrescenta que as medidas técnicas foram adotadas também por haver um entendimento de que são importantes para proteger a informação e os equipamentos da organização, o que, na sua visão, é uma questão de os profissionais de TI entenderem essas medidas como certas e necessárias. Isso condiz com o fato de essas medidas terem sido adotadas antes da publicação da Política de Segurança da Informação e dos regulamentos organizacionais, embora modelos internacionais de Segurança da Informação sejam mais antigos e possam ter influenciado a adoção. Ainda que

tenha pouca medidas formais e informais, ambas as categorias foram associadas à conformidade com requisitos externos.

De acordo com as respostas do Entrevistado 09, as pressões que incidem sobre a subunidade para adotar medidas de Segurança da Informação são principalmente de natureza coercitiva. Na sua percepção, a subunidade é pressionada pelo Governo Federal através de regulamentos e leis, mas a pressão externa vem principalmente da administração central da FIOCRUZ:

> O governo faz suas normas, que obriga a fazer algumas coisas. Tem as instruções normativas também. Mas a pressão vem mesmo da FIOCRUZ, da CGTI. Tem o Comitê de Segurança da Informação lá, que discute os temas e faz as normas internas. Essas normas passam a compor a Política de Segurança da Informação da FIOCRUZ. Então é uma pressão que a gente sofre para seguir essas normas e a Política. Tem ainda as auditorias, que vez em quando verifica se a gente está em conformidade. Já aconteceram pelo menos duas. (ENTREVISTADO 09).

A adoção de tecnologias pela sede, como padrões de ativos de rede, antivírus corporativo, sistemas de informação corporativos, recursos de criptografia contratados pela CGTI e a construção do *datacenter*, também fazem com que a subunidade adote medidas de Segurança da Informação, o que o Entrevistado 09 entende como pressões da administração central da organização. O informante complementa que as auditorias não geram obrigação para as subunidades, mesmo que não conformidades sejam identificadas: "Se é uma política institucional, é obrigatório. Tem portaria da Presidência [da FIOCRUZ], então é obrigatório. A gente sabe, mas como não acontece nada, como não dá nada se não cumprir, a gente, todas as unidades, eu acho, não se sentem obrigadas a cumprir." Segundo o entrevistado, há ainda uma pressão da sociedade com relação à privacidade dos dados e pressões internas da própria subunidade:

> A gente sempre se preocupa com privacidade dos dados dos pacientes, porque tem a questão ética, então é uma pressão também. E tem a pressão da direção e dos usuários, que querem que tudo esteja funcionando, então tem que adotar uma série de mecanismos de Segurança da Informação. (ENTREVISTADO 09).

Apesar disso, as respostas apontam também que a subunidade sofre pressões miméticas de outras subunidades:

> Quando alguém já utiliza alguma coisa ou já fez uma coisa interessante, é bom a gente saber para ver se é possível fazer aqui, se usa determinada solução, se faz de um jeito diferente. Isso acaba influenciando. Já viajei para outro estado para ver como eles fazem

> lá o monitoramento de servidores e da rede, como lidam com virtualização e redundância. Então, o que a gente achou viável, a gente implementou aqui. (ENTREVISTADO 09).

A Subunidade 09 responde às pressões institucionais com desfio, sendo que a tática utilizada é a de rejeição, pois a subunidade não age ativamente contra as pressões ou as fontes de pressão institucional, mas simplesmente ignora as pressões sofridas sempre que não há cobrança quando à conformidade. Esse comportamento pode ser notado nas respostas do entrevistado, ao afirmar que as medidas não são adotadas mesmo após a realização de auditorias devido ao fato de não haver punição pela não conformidade. O Entrevistado 09 também se referiu a regulamentos da FIOCRUZ que não tiveram adesão da subunidade pelo fato de as medidas previstas serem consideradas inadequadas à sua realidade:

> Se a gente for seguir a norma do *datacenter* [Norma Institucional SIC-004/CGTI/VPGDI] como está escrito lá, a unidade não vai ter dinheiro para isso. A norma do acesso remoto [Norma Institucional SIC-007/CGTI/VPGDI] dificulta [a implementação de serviço de acesso remoto], pois não dá para colocar um serviço desse garantindo a segurança do computador da casa do usuário, cadastrando os equipamentos particulares dos usuários. Então, não dá para colocar um serviço desse na unidade, porque a gente não vai na casa do usuário ver o computador dele. (ENTREVISTADO 09).

Além desses regulamentos da administração central, o Entrevistado 09 deu exemplos de respostas de desafio a outros regulamentos e normas, como normas técnicas da ABNT, cuja implementação é cara, e a criação de uma equipe de tratamento de incidentes na subunidade, que não é possível por não ter profissionais que possam ficar dedicados às atividades inerentes a essa estrutura organizacional e a contratação é difícil devido à necessidade de realizar concurso público para contratação.

O entrevistado também afirmou que a diretoria da subunidade já se posicionou ativamente contra regulamentos adotados pela CGTI, o que configura o uso da tática de contestação:

> Minha diretoria já se posicionou contra algumas coisas. [...] Já aconteceu de [nome do Vice-Diretor de Gestão da subunidade] ser contra, participar de reunião e dizer que era contra para todo mundo. Claro, sempre justificando seu posicionamento. Se a coisa não é boa para nós, ele pode até chegar a fazer isso, porque as coisas nem sempre são discutidas amplamente com as unidades. Então às vezes a coisa chega para nós quase decidida, quase do tipo 'vai ser assim'. Teve o caso de tentar proibir de comprar servidor, equipamento de rede, essas coisas, e nosso Vice [Vice-Diretor de Gestão da subunidade] não aceitou. Discutiu na reunião, se posicionou contra, e desistiram disso. Tinha até uma portaria que ia ser publicada, mas desistiram. (ENTREVISTADO 09).

Quando o Entrevistado 09 afirma que a subunidade adota medidas consideradas importantes ou vantajosas, que medidas adotadas por outras subunidades podem ser imitadas se forem consideradas também úteis ou importantes, e que outras subunidades ou organizações são consultadas durante os processos de aquisição e contratação, a aquiescência é a resposta que parece se desenhar. Segundo o relatório de auditoria (FIOCRUZ, 2015), nem todas as medidas técnicas que a subunidade é pressionada a adotar são de fato adotadas, mas a quantidade de medidas adotadas é maior do que as quantidades de medidas adotadas parcialmente e rejeitadas, o que faz com que o comportamento característico da subunidade seja a aquiescência. Medidas informais e formais foram pouco adotadas, mas três regulamentos da organização tiveram mais da metade das medidas previstas adotadas parcialmente, e um regulamento teve todas as medidas adotadas, o que reforçou a aquiescência como resposta característica da subunidade ao ser pressionada pela administração central através dos regulamentos de Segurança da Informação.

No entanto, o desafio tem 22,43% de cobertura de percentual, sendo a resposta com maior percentual, e a rejeição, com 20,04%, é a tática com maior cobertura de percentual, resultado que acontece devido ao fato de muitas medidas formais e informais serem rejeitadas pela subunidade. Mas os dados mostram também que a resposta estratégica de aquiescência tem 19,91% de cobertura de percentual, e que a tática de hábito tem 13,79%, o que é explicado pela tendência de a Subunidade 09 adotar medidas técnicas e pelo fato de o entrevistado entender que essas medidas são importantes para proteger a informação, ainda que ressalte sua importância para manter a subunidade em conformidade com os requisitos institucionais. Já quanto às referências codificadas, a aquiescência aparece com 11 referências identificadas, e a tática de conformidade aparece com cinco referências de codificação. O desafio, por outro lado, apresentou 10 referências identificadas, sendo a rejeição, com sete referências, a tática que apresentou mais referências de codificação.

6.3.10 Subunidade 10

O Entrevistado 10 tem graduação e especialização na área de TI, é membro do Comitê de Segurança da Informação da FIOCRUZ e é o responsável pela Segurança da Informação na sua subunidade, embora seja funcionário terceirizado. A Subunidade 10 fica

localizada no *campus* da administração central da organização e tem uma equipe de Segurança da Informação com dois profissionais dedicados às atividades técnicas. Conta ainda com um Comitê de Segurança da Informação local para decisões estratégicas sobre o tema no âmbito da subunidade. Por ter autonomia administrativa, a área de TI da subunidade não tem vínculo hierárquico com a CGTI. A entrevista teve duração de 35 minutos e foi realizada remotamente utilizando o *software* Skype.

De acordo com o Entrevistado 10, o "Comitê de Segurança da Informação" da subunidade é composto por nove pessoas, incluindo representantes das diretorias da subunidade e dos departamentos de TI, recursos humanos e outras áreas relevantes para a Segurança da Informação. A subunidade tem uma "Política de Segurança da Informação" formal, criada para atender ao Decreto nº 3.505/2000 (BRASIL, 2000) antes mesmo de a FIOCRUZ ter elaborado a sua Política. A entrevista mostra que a subunidade adota ainda medidas formais de outros tipos: "Regulamentos internos de Segurança da Informação", que, segundo o entrevistado, são nove e são anteriores aos regulamentos da FIOCRUZ; "Processos e procedimentos de Segurança da Informação", como um processo de revisão e adequação dos regulamentos existentes aos regulamentos da organização; "Equipe de tratamento de incidentes de Segurança da Informação", que é composta por dois funcionários do setor de TI da subunidade; e um processo de "Revisão periódica da Política de Segurança da Informação". A subunidade tem também um Escritório de Segurança da Informação cujo responsável é o próprio entrevistado, mas faz a ressalva de que o Escritório não está formalmente instituído, assim como o papel dele como gestor de Segurança da Informação não é formalizado. Neste caso, o entrevistado esclarece que devido ao fato de ele ser terceirizado, o responsável formal pela Segurança da Informação na subunidade é o coordenador de TI. Não foram identificados na pesquisa elementos que indiquem que a subunidade tem um Sistema de Gestão de Segurança da Informação documentado nem que realiza análise e avaliação de riscos e classificação de informações. Apesar de não ter adotado todos os tipos de medidas formais, a existência de um subcomitê e de uma Política de Segurança da Informação na subunidade facilita a adoção de outras medidas de Segurança da Informação.

A Subunidade 10 realizou "Treinamentos de profissionais de TI" ministrados por outros profissionais de TI da subunidade. "Treinamentos de usuários de TI" são realizados sempre que novos funcionários ingressam na subunidade. Ações de conscientização e divulgação da Política e dos regulamentos de Segurança da Informação da subunidade e da

FIOCRUZ foram realizadas, o que mostra que "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização" foram também medidas informais adotadas. Com isso, a subunidade adotou as quatro categorias de medidas informais.

Entre as medidas técnicas de Segurança da Informação, a entrevista mostrou que a Subunidade 10 utiliza antivírus e anti-spam como medidas de "Prevenção contra códigos maliciosos". Utiliza também equipamentos de rede redundantes para evitar indisponibilidade de serviços como medida de "Redundância de equipamentos", faz espelhamento de discos e realiza *backup* em *tape library*, que são medidas de "Redundância de dados". Utiliza ainda equipamentos com peças redundantes, que é uma medida de "Redundância de peças de equipamentos". A subunidade faz "Segregação e monitoramento de redes de computadores" através de *firewall* e controla o acesso à Internet e aos seus sistemas de informações e recursos da rede de computadores através de *login* único de identificação dos usuários e com permissões diferenciadas, medidas de "Controle de acesso lógico". As senhas de acesso aos sistemas de informação e à rede de computadores atendem a requisitos de complexidade e são trocadas periodicamente, medidas de "Autenticação forte". A sala em que ficam os equipamentos da rede de computadores tem acesso controlado, uma medida de "Controle de acesso físico", tem aparelho de ar-condicionado e os equipamentos são protegidos por *no-break* e gerador, medidas de "Proteção ambiental". Os sistemas utilizam recursos de criptografia, medida de "Transmissão e armazenamento seguros de dados". Com isso, os dados mostram que a subunidade adota medidas técnicas de Segurança da Informação de todos os tipos, segundo as categorias propostas por Dhillon (1999).

A Subunidade 10 adota integralmente pelo menos metade das medidas previstas em sete dos nove regulamentos de Segurança da Informação da FIOCRUZ. Os dois regulamentos que não tem pelo menos metade das medidas adotadas integralmente são a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f) e a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a): a subunidade adota integralmente 33% e parcialmente 67% das medidas previstas no primeiro regulamento, e adota integralmente 45% e parcialmente 45% das medidas do segundo regulamento. Portanto, apesar de adotar menos da metade das medidas desses dois regulamentos, há ainda a adoção parcial de quase a totalidade das medidas previstas neles. Destaca-se o fato de a subunidade adotar integralmente 84% e parcialmente 16% das medidas previstas na Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a), que trata de *backup*.

O Entrevistado 10 admite que órgãos externos exigem a adoção de medidas formais e técnicas de Segurança da Informação: "O TCU, legislações específicas, também normas do DSIC fazem exigências de implantação de recursos ou o uso de ferramentas, ou adoção de processos e procedimentos. São determinações relacionadas a Segurança da Informação sim. Às vezes nem é tecnologia, às vezes é um processo ou procedimento." Auditorias também foram lembradas pelo entrevistado como forma de outras organizações e a administração central da FIOCRUZ exercerem pressão sobre a subunidade. Pressões normativas foram notadas quando o entrevistado afirmou que a Política e os primeiros regulamentos da subunidade foram elaborados por uma empresa de consultoria contratada para esta finalidade.

Em outro momento, porém, ele ressalta as pressões coercitivas da administração central da FIOCRUZ ao afirmar que a publicação da Política e de regulamentos de Segurança da Informação da organização obriga as subunidades a adotarem medidas no âmbito local:

> [A publicação da POSIC e de regulamentos] Faz com que as pessoas [nas subunidades] se mexam, tendo um foco, olhando para a mesma coisa, com o mesmo foco, e isso é bom. Desde que as pessoas não fiquem acomodadas, isso é importante sim. A ideia é essa. [...] Acho que obrigam sim, mas tem de continuar desse modo. A CGTI tem que ditar as regras, de uma forma abrangente, óbvio, porque a FIOCRUZ tem vários focos, cada unidade tem sua infraestrutura, seus recursos, mas tem que ditar sim a forma como as unidades devem agir sim. Mas de forma abrangente, para todas as unidades. (ENTREVISTADO 10).

As pressões coercitivas citadas são consideradas coerentes com os objetivos e atividades da subunidade, e o principal benefício que a adoção das medidas de Segurança da Informação traz, na visão do entrevistado, é a conformidade com os requisitos externos. A entrevista mostrou que essa percepção está associada à adoção de medidas formais e técnicas, que, mesmo tendo sido adotadas antes de haver obrigações internas, seguiam requisitos do Governo e de outras organizações com quem firmou contratos e acordos. Medidas informais estão mais associadas à educação, conscientização e mudança do comportamento dos usuários, sendo, portanto, uma questão de eficiência. Mas o Entrevistado 10 esclarece que há benefícios além da conformidade: "Você tem que cumprir uma regulamentação, uma determinação, uma obrigação, entendendo que aquela demanda é para proteger, não só para cumprir."

Cabe registrar que foram identificadas todas as outras respostas estratégicas na subunidade. O desafio foi identificado quando o entrevistado relata que analisa a adequação

da medida à subunidade antes da adoção: “O que a gente procura fazer sempre aqui em [nome da subunidade] é entender a demanda do negócio. O negócio está em primeiro lugar. [...] Então existem regras, mas algumas exceções existem sim, desde que haja uma justificativa plausível, para não impactar no negócio.” Neste caso, a tática é a de rejeição, pois essas medidas não são adotadas por não serem coerentes com as atividades da subunidade ou a subunidade não dispõe de recursos para a aquisição ou implantação, como pode ser visto no trecho a seguir: “O problema é que algumas áreas ignoram ou não têm recursos para realizar aquelas atividades ou processos.” O trecho a seguir reforça esta percepção do Entrevistado 10 de que a falta de recursos atrapalha a adoção: “Em alguns casos, precisa de orçamento mesmo. Pior agora que estamos em uma fase de crise, uma época de crise. E às vezes, não está de acordo com a visão de negócio mesmo. Nesse momento, pode não ser estrategicamente viável.” A esquiva através da tática de ocultação também foi identificada: “Você precisa entender aquela demanda e implementar corretamente. Às vezes, a depender da área, do setor de atividade, você [a subunidade] implementa mascarando, implementa só para cobrir uma auditoria. [...] A gente vê certos casos em que se quer só tapar um buraco para não ser pego em não conformidades em uma auditoria.”(ENTREVISTADO 10).

O comportamento característico da subunidade frente às pressões da administração central através dos regulamentos de Segurança da Informação é a aquiescência. Conforme o relatório de auditoria interna (FIOCRUZ, 2015), a Subunidade 10 adota muito mais do que adota parcialmente ou rejeita as medidas previstas nos regulamentos da FIOCRUZ, e a entrevista mostrou também que adota grande parte das medidas exigidas pelo ambiente institucional.

Independentemente da variedade de respostas da Subunidade 10, a que teve mais cobertura de percentual foi a aquiescência, com 17,14%, e a tática foi a conformidade, com 9,53%. Essa estratégia teve também dez referências codificadas, e a tática de conformidade teve cinco. Todos os tipos de medidas técnicas e diferentes medidas informais são adotados. Como a adoção tem a conformidade com os requisitos externos de Segurança da Informação como motivação principal, caracterizando uma adoção consciente, visando à obtenção de benefícios dos constituintes do ambiente institucional (OLIVER, 1991), fica reforçada a identificação da conformidade como tática principal da organização. Com relação às pressões para adoção de medidas informais, a resposta estratégica mais identificada também foi a aquiescência, reforçando sua identificação como resposta mais identificada na entrevista.

6.3.11 Subunidade 11

A entrevista com o responsável pela Segurança da Informação na Subunidade 11 teve 52 minutos de duração e foi realizada através de Skype. O Entrevistado 11 tem graduação e especialização na área de TI e está cursando mestrado. Embora seja o responsável na sua subunidade, o entrevistado esclareceu que a estrutura organizacional da subunidade não tem uma área específica e apenas uma pessoa trabalha com Segurança da Informação, sendo que conciliando esta atividade com outras de TI. A Subunidade 11 fica no *campus* da sede administrativa da FIOCRUZ e tem uma área de TI sem vínculo hierárquico com a CGTI da organização.

De acordo com os dados colhidos na entrevista, a Subunidade 11 tem processos de Segurança da Informação documentados e um procedimento de responsabilidade do usuário, medidas que podem ser classificadas como "Processos e procedimentos de Segurança da Informação". Não foram identificados na entrevista elementos que indiquem que a subunidade adote outras medidas, como Política de Segurança da Informação, Comitê de Segurança da Informação e regulamentos internos, ou que tenha uma Equipe de Tratamento de Incidentes de Segurança da Informação.

O responsável pela Segurança da Informação da Subunidade 11 informou ter realizado palestras e apresentações para gestores e usuários das áreas de pesquisa e gestão, e relatou enviar regulamente mensagens de correio eletrônico para divulgação da Política de Segurança da Informação e dos regulamentos organizacionais, que são "Divulgação de regulamentos e da Política de Segurança da Informação" e "Ações de conscientização". De acordo com o informante, sempre que alguma medida vai ser implantada, os usuários são informados antecipadamente, mas não houve ações de treinamento de profissionais de TI ou de usuários da subunidade em Segurança da Informação.

Diferentes medidas técnicas foram citadas pelo Entrevistado 11. A subunidade utiliza *firewall*, antivírus, anti-spam, *login* único com senha complexa para todos os usuários de TI, troca periódica de senha para todos os sistemas, acesso restrito à sala de equipamentos de rede, ar condicionado e *no-break* para todos os equipamentos e servidores de rede, criptografia para acesso externo a sistemas de informação e *webmail*, discos redundantes e peças redundantes nos servidores de rede e rotina de *backup* dos dados armazenados. Os dados mostram que a Subunidade 11 adota medidas técnicas de "Redundância de dados",

“Segregação e monitoramento de redes de computadores”, “Redundância de peças de equipamentos”, “Prevenção contra códigos maliciosos”, “Controle de acesso lógico”, “Transmissão e armazenamento seguros de dados”, “Autenticação forte”, “Controle de acesso físico” e “Proteção ambiental”. Com isso, o único tipo de medidas técnicas que não foi identificado na entrevista foi a redundância de equipamentos. Segundo o Entrevistado 11, as medidas foram adotadas, em maioria, antes da Política de Segurança da Informação e dos regulamentos terem sido publicados pela FIOCRUZ.

Dos nove regulamentos publicados pela organização, apenas dois tem mais da metade das suas medidas adotadas pela Subunidade 11: o regulamento de acesso remoto (FIOCRUZ, 2013e) e o regulamento de acesso a redes sociais (FIOCRUZ, 2013f), cujas medidas adotadas pela subunidade correspondem respectivamente a 73% e a 67% do que está previsto. Dentre os demais, a conformidade é pior no que trata do uso de dispositivos móveis (FIOCRUZ, 2013g), cujas medidas previstas são rejeitadas em quase sua totalidade, e o de acesso à Internet (FIOCRUZ, 2012c), que tem mais da metade delas rejeitadas. Apesar de não adotar uma parte significativa das medidas previstas nesses regulamentos, o Entrevistado 11 entende alguns deles como coerentes com suas atividades e necessidades:

> O que está na norma de *email* parece coerente. O que está na norma de mídias sociais parece coerente. A ideia do antivírus para toda a FIOCRUZ também é coerente. Se muitas unidades são interligadas com a FIOCRUZ, todas têm que ter um antivírus, e o melhor é que seja o mesmo, uma mesma linguagem. Acho coerente também a previsão de ter um subcomitê de segurança em cada unidade. Acho que não funciona, mas acho coerente. (ENTREVISTADO 11).

Seguindo a ideia de que as medidas previstas nos regulamentos são coerentes com as atividades e objetivos da subunidade, o entrevistado entende que a adoção de medidas de Segurança da Informação traz como benefício a garantia de que as informações da organização e dos indivíduos estão seguras, um benefício relacionado à eficiência das medidas adotadas. O Entrevistado 11 percebe também a conformidade como benefício, pois “Se algum órgão de fiscalização vier aqui e auditar e descobrir que a gente tem controles para muitas coisas, se vier o TCU ou mesmo a AUDIN, acho que fica bem para a direção da unidade. Se vier uma fiscalização [...] e se tudo estiver dentro do esperado, ainda que não esteja perfeito, acho que a direção fica bem.” (ENTREVISTADO 11). Segundo o informante, uma imagem positiva da subunidade na organização pode ser também uma vantagem: “Então ela fica bem perante as outras unidades e para a CGTI.” (ENTREVISTADO 11). No entanto, o maior benefício percebido pelo Entrevistado 11 não tem relação com a eficiência ou a

imagem externa da subunidade: “O principal benefício [...] é dar para a gente a garantia de que a gente não vai ser responsabilizado se tiver algum problema. Se tiver um incidente e a gente estiver bem, acho que a gente vai poder dizer ‘olha, fizemos tudo, nos preparamos, mas isso aconteceu porque não tinha jeito’”. Este benefício principal está relacionado mais à conformidade e aplica-se a medidas técnicas, formais e informais, segundo os dados da entrevista.

A não conformidade da subunidade com grande parte das medidas de Segurança da Informação previstas nos regulamentos da FIOCRUZ pode ser explicada pelo fato de essas pressões coercitivas não serem percebidas como tal. Sobre isto, o Entrevistado 11 declarou: “As coisas que a CGTI faz, que publica, a gente encara mais como recomendação. Não é aquela coisa obrigatória. Eu sei que a gente tem que proteger dados de pesquisa, porque muitas vezes envolve dado de paciente, então tem de proteger, mas isso não tem muito a ver com o que a CGTI faz.”

Mas o entrevistado admite que a subunidade foi pressionada pela administração central quando houve a tentativa fazer com que utilizasse os serviços do *datacenter*: “A gente teve uma pressão forte aqui da CGTI para migrar as coisas lá para o *datacenter*. Eles fizeram o *datacenter* [...] e queriam que a gente, e não só a gente, mas todas as unidades, colocassem as coisas, os servidores lá. Então fizeram umas coisas, tentaram impedir que a gente comprasse equipamentos de rede, como servidores novos” (ENTREVISTADO 11). Assim, embora a Política e os regulamentos de Segurança da Informação não sejam percebidos como obrigatórios, outras pressões coercitivas foram citadas pelo entrevistado.

Apesar de ter havido pressão coercitiva para migração dos serviços de TI para o *datacenter*, a adoção de medidas técnicas está relacionada a um entendimento por parte dos profissionais de TI de que são necessárias, segundo o Entrevistado 11. Esta ideia é coerente com o isomorfismo normativo de DiMaggio e Powell (1983) e com a adoção de medidas técnicas devido a pressões normativas, segundo Albuquerque Junior *et al*. (2016). O trecho abaixo mostra claramente como medidas técnicas estão relacionadas a pressões normativas e são adotadas por serem consideradas eficientes:

> Os mecanismos de Segurança [da Informação], como *firewall*, antivírus, essas coisas mais técnicas, eu acho que são adotados porque precisa. Não vejo como uma empresa, um órgão público ou uma unidade grande da FIOCRUZ pode existir sem ter um *firewall*, antivírus, *no-breaks* para servidores, controle de acesso lógico. Essas coisas são adotadas pelo pessoal de TI, que tem uma consciência sobre Segurança da Informação. Então ele vê o que está acontecendo, o que é oferecido no mercado, e adota, implementa. Pode ser que nem tudo seja implementado como o pessoal de TI

> quer, mas a decisão de implementar essas coisas é técnica. [...] Então as decisões técnicas imperam na implementação de mecanismos técnicos. (ENTREVISTADO 11).

O Entrevistado 11 percebe também os regulamentos e a Política de Segurança da Informação como meios para pressionar as subunidades, ainda que não sejam encarados como obrigações: "As normas de Segurança que a CGTI tem publicado [...], isso é uma forma de pressionar a unidade a andar na linha. [...] A POSIC, por exemplo, diz um monte de coisa, que acaba sendo uma forma de pressão." Neste mesmo sentido, medidas informais são consideradas eficientes e foram adotadas por serem tidas como certas pelo entrevistado: "As outras coisas que foram feitas, como apresentações de conscientização, foi por iniciativa minha. Eu acho que precisa fazer isso para que as pessoas passem a conhecer e respeitar."

Apesar de a Subunidade 11 ter poucas medidas formais adotadas e de haver uma compreensão de que os regulamentos da FIOCRUZ não são obrigatórios, o entrevistado entende que a organização formaliza regulamentos internos devido à obrigação criada por leis e regulamentos externos e por ser uma questão de conformidade:

> Mas se você quer saber o motivo pelo qual a FIOCRUZ fez uma POSIC, criou um Comitê, colocou o [nome do gestor de Segurança da Informação da FIOCRUZ] lá para cuidar da Segurança [da Informação], eu acho que foi porque teve uma diretiva, uma obrigação maior, que veio do Governo Federal, do Ministério do Planejamento, da SLTI, do pessoal de Segurança Institucional da Presidência da República. Eu acho que foi por isso que toda essa conversa de Segurança [da Informação] começou aqui na FIOCRUZ. (ENTREVISTADO 11).

Diferentes respostas estratégicas foram identificadas na entrevista, como o compromisso através da tática de equilíbrio apresentada no trecho a seguir: "Normalmente, se a medida vai prejudicar ou provocar um impacto muito grande, a gente não adota de imediato. Nesse caso, a gente procura alternativas para não ficar totalmente descoberto, e depois vê o que faz." (ENTREVISTADO 11).

A tentativa da matriz de centralizar os recursos da rede de computadores no *datacenter* resultou em uma resposta de manipulação, tendo a influência como tática:

> Quando a CGTI veio com a ideia como aquela de colocar os servidores de todas as unidades no *datacenter*, a gente teve argumento. Eu falei para a diretoria o que a gente tinha, como a gente fazia, e que isso iria prejudicar a gente. Eu soube que conversaram lá na Presidência, que houve umas discussões na Câmara de Gestão [Câmara Técnica de Gestão e Desenvolvimento Institucional da FIOCRUZ], mas o caso é que parece que as diretorias da maioria das unidades não concordaram e fizeram com que o [nome do

> Vice-Presidente de Gestão e Desenvolvimento Institucional] recuasse da ideia. (ENTREVISTADO 11).

Em outro momento, a mesma resposta foi identificada, desta vez com relação à tentativa da administração central de impedir as subunidades de adquirir equipamentos de TI e Segurança da Informação:

> A unidade se posicionou contra isso [a proibição de adquirir equipamentos de rede de computadores] lá na Vice-Presidência [de Gestão e Desenvolvimento Institucional da FIOCRUZ] e também na Câmara de Gestão. Foi no sentido de fazer pressão para que a exigência não fosse adiante. Não sei se conversar com a Vice-Presidência não surtiu o efeito desejado, mas na Câmara de Gestão a coisa ganhou corpo, com certeza. Os gestores conversaram com os de outras unidades, e aí a coisa funcionou. (ENTREVISTADO 11).

A diversidade de respostas da subunidade explica o fato de não ter havido adoção de todos os tipos de medidas de nenhuma das três categorias. Além disso, boa parte das medidas que interferem no trabalho das pessoas foi recebida com resistência, como a mudança periódica de senha e o bloqueio de uso de memória portátil nos computadores. Nesses casos, embora tenha havido a intenção inicial de adotar, a subunidade rejeitou as medidas. Para o Entrevistado 11, "O importante é permitir que a unidade funcione. Se prejudica a unidade, a ideia é não adotar. Se a questão for objeto de auditoria, por exemplo, a gente justifica porque não adotou."

Apesar de diferentes medidas técnicas, formais e informais terem sido adotadas, o entrevistado afirmou que não existe uma preocupação constante em seguir os regulamentos e a Política de Segurança da Informação. O relatório de auditoria (FIOCRUZ, 2015) mostra que, dentre as medidas previstas nos nove regulamentos da organização, há um equilíbrio nas quantidades de medidas adotadas integralmente e as rejeitadas pela subunidade, sendo que as rejeitadas têm uma pequena vantagem. O relatório mostra que também há mais medidas adotadas parcialmente do que adotadas integralmente e não adotadas, o que caracteriza uma resposta de compromisso da subunidade diante dos regulamentos de Segurança da Informação da organização. Assim, medidas consideradas incoerentes com as atividades da subunidade ou cuja implantação é inviável, como parte das medidas presentes na Norma Institucional SIC-007/CGTI/VPGDI, regulamento da FIOCRUZ que trata de acesso remoto, ou a maioria das medidas da Norma Institucional SIC-009/CGTI/VPGDI, que regulamenta o uso de dispositivos móveis, não são adotadas, mas a grande maioria das medidas presentes na Norma

Institucional SIC-005/CGTI/VPGDI, que trata de *backup*, foi parcialmente adotada, e quase a metade das medidas presentes na Norma Institucional SIC-006/CGTI/VPGDI, que trata de aquisição e desenvolvimento de sistemas, foi parcialmente adotada também.

No entanto, a resposta estratégica de desafio é a que tem maior cobertura de percentual: 10,53%. A tática de rejeição, com 8,96% de cobertura de percentual, é a que teve maior destaque no NVivo. As quantidades de referências de codificação identificadas também apontam para o desafio (nove referências) e a rejeição (oito referências) como resposta e tática mais utilizadas pela Subunidade 11.

6.3.12 Subunidade 12

Localizada longe da sede administrativa da organização, a Subunidade 12 tem uma equipe de TI própria, que tem duas pessoas trabalhando com Segurança da Informação em dedicação exclusiva. No entanto, a subunidade não tem autonomia administrativa, o que torna sua equipe de TI subordinada à CGTI da FIOCRUZ. Não existe uma designação formal, com atribuição de cargo ou gratificação para o responsável pela Segurança da Informação nem para o coordenador de TI da subunidade. A entrevista com o responsável pela Segurança da Informação durou 52 minutos e foi realizada através de Skype. O Entrevistado 12 tem graduação e especialização na área de TI e é membro do Comitê de Segurança da Informação da FIOCRUZ.

A entrevista mostrou que a Subunidade 12 tem processos de identificação e análise de vulnerabilidades, monitoramento da rede de computadores e elaboração de relatórios de ocorrência de incidentes. Assim, é possível afirmar que a subunidade tem "Processos e procedimentos de Segurança da Informação" e uma "Equipe de tratamento de incidentes de Segurança da Informação". Nenhuma outra medida formal foi identificada nos dados.

Não foram identificadas medidas informais que tenham sido adotadas na subunidade. Sobre isto, o Entrevistado 12 entende que precisa oferecer serviços de Segurança da Informação melhores antes de investir em ações de conscientização e cobrar comportamentos mais adequados dos usuários de TI. Sobre treinamentos em Segurança da Informação, o entrevistado afirmou que, embora tenha feito pedidos, o único que aconteceu foi oferecido gratuitamente por outro órgão do Governo Federal, e que a subunidade não

autorizou nem aprovou a participação em nenhum dos treinamentos solicitados. Assim, nenhuma medida informal de Segurança da Informação foi adotada pela subunidade.

O serviço de diretórios utilizado para autenticar os usuários da rede de computadores da Subunidade 12 é integrado ao utilizado pela CGTI da FIOCRUZ. Com isso, o entrevistado entende que melhorou a Segurança da Informação quanto a autenticação e autorização de usuários. A integração dos serviços de diretórios fez com que senhas complexas fosse exigidas dos usuários, o que gerou certa resistência. Independentemente da reação dos usuários, foram adotadas medidas de "Controle de acesso lógico" e "Autenticação forte" pela subunidade.

No momento da entrevista, as caixas postais de correio eletrônico estavam sendo migradas do sistema próprio da subunidade para o sistema da FIOCRUZ, que tem uma solução de anti-spam implantada. Além disso, uma solução de antivírus e um *firewall* haviam sido implantados na subunidade, o que evidencia a adoção de medidas de "Prevenção contra códigos maliciosos" e "Segregação e monitoramento de redes de computadores". A subunidade realiza *backup* de dados e tem equipamentos com peças redundantes, que são medidas de "Redundância de dados" e "Redundância de peças de equipamentos". Para prover acesso seguro aos seus sistemas de informação, utiliza protocolo de rede criptografado, uma medida de "Transmissão e armazenamento seguros de dados". Não foram identificadas outras medidas técnicas adotadas.

Dentre os regulamentos da FIOCRUZ, o que apresenta maior rejeição da subunidade é a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a), sobre aquisição, desenvolvimento e manutenção de sistemas de informação, que tem 83% das medidas previstas rejeitadas. Em segundo lugar está a Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a), que trata da realização de *backups*, que tem 67% das medidas previstas rejeitadas pela subunidade. Por outro lado, o regulamento que tem maior adesão da subunidade é a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), que regulamenta a utilização e o acesso a redes sociais na organização. Neste caso, a subunidade adota 67% das medidas previstas, mas não adota os outros 33%. Nenhum outro regulamento de Segurança da Informação tem mais da metade das medidas adotadas pela subunidade. Esse resultado reforça o fato de que poucas medidas formais, informais e técnicas são adotadas, como visto nas respostas do entrevistado.

O Entrevistado 12 vê a segurança dos dados armazenados e processados na subunidade como o maior benefício da adoção de medidas de Segurança da Informação: "[o maior benefício] é a questão da segurança de dados. Eu sou um profissional contratado, através de concurso, especificamente para Segurança da Informação, por conta de incidentes que já ocorreram aqui. Então, a instituição viu a possibilidade de ter um profissional dessa linha aqui." Assim, a adoção é realizada por haver uma compreensão de que é importante para garantia da Segurança da Informação, sendo, portanto, uma questão de eficiência, e não de conformidade. O entrevistado reforça este entendimento ao demonstrar que as pressões coercitivas sobre a subunidade não têm efeito prático:

> A questão de adotar padrões e procedimentos de Segurança [da Informação] ainda é muito no convencimento. Até quando a gente mostra a importância de desenvolver ou implementar determinados procedimentos, temos muita dificuldade para convencer. Então, infelizmente, é no convencimento ainda. Nada externo, dizendo que tem que adotar. Olha que têm leis, decretos, normas complementares estabelecendo a questão de Segurança [da Informação], acesso à informação e uma série de coisas que obrigam, mas isso não tem impacto. (ENTREVISTADO 12).

Apesar de a Subunidade 12 não ter adotado medidas informais, o informante admite que o convencimento dos usuários e gestores quanto à necessidade de adotar medidas e respeitar regulamentos podem ter um efeito positivo sobre o comportamento das pessoas: "O que eu tenho observado que tem impacto mesmo é o convencimento, de mostrar que tem que ser assim por conta disso, se não adotar tais procedimentos".

As pressões coercitivas foram associadas pelo entrevistado à adoção de regulamentos internos de Segurança da Informação, ou seja, medidas formais. Já a adoção de medidas técnicas e informais foi associada a pressões normativas, uma vez que são tidas como certas pelo responsável pela Segurança da Informação da subunidade. Pela análise da entrevista, nota-se que a subunidade sofre pressões miméticas, pois o entrevistado relatou que a adoção de certas medidas por outras organizações ou subunidades influencia a adoção na Subunidade 12: "Quando ela [a direção da subunidade] observa que alguma unidade ou outra instituição está à frente de algo que pode beneficiar ela, algo que possa agregar, de certa forma, isso faz uma pressão." A entrevista mostrou ainda que a implantação de uma tecnologia pela FIOCRUZ pode resultar na adoção de medidas de Segurança da Informação pela subunidade:

> Uma das coisas que fortaleceram a gente se integrar ao [serviço de diretórios] da CGTI é porque é integrado ao CAFE [Comunidade Acadêmica Federada]. [...] A questão de

> trazer o [serviço de diretórios] da CGTI para cá, com *email* e tudo, teve como impacto o CAFE, que outras unidades também estão implementando e a FIOCRUZ aqui de [local onde está a unidade] achou que também poderia ser importante para ela. Então essas ações que são feitas em outras unidades, que eles veem que tem um retorno, com certeza tem uma influência sim. (ENTREVISTADO 12).

Ainda segundo o entrevistado, as pressões coercitivas não resultam em punições, o que pode explicar a baixa conformidade com os regulamentos da organização. Para ele, as punições podem alcançar a administração central, mas não têm impacto sobre a subunidade: "Eu nunca percebi nenhum tipo de restrição, ou por parte do Governo ou por qualquer órgão, com relação a isso. Se chega alguma coisa, fica lá [na CGTI]." Outra passagem da entrevista que reforça esta percepção do entrevistado é a seguinte: "Esses padrões [...], isso não é tão levado a sério, mesmo a gente mostrando que é uma norma do Ministério do Planejamento afirmando que aquilo tem que ser assim. É difícil implementar esses padrões." Em outro momento, complementa: "Enquanto não acontecer problema, fica do jeito que está. Se acontece, aí tem uma postura de adotar algum controle ou dar uma atenção àquilo que a gente propõe melhorar."

Nasution (2012) destaca que incidentes, embora sejam indesejáveis, possibilitam o acréscimo ou a adequação de medidas de Segurança da Informação existentes. Neste sentido, a adoção na Subunidade 12 é feita de forma gradual e lenta, pois é principalmente uma reação à ocorrência de incidentes. Além disso, as medidas são adotadas devido a necessidades que surgem com o tempo, como parcerias estabelecidas com outras organizações e a adoção de tecnologias pela administração central. Isso configura a tática de barganha, em que a adoção é negociada com as fontes de pressão institucional, de acordo com as possibilidades e necessidades da organização, como explica Oliver (1991).

A adoção de medidas técnicas, na visão do entrevistado, é resultado de uma compreensão de que são necessárias. A análise do relatório de auditoria (FIOCRUZ, 2015) mostra que o comportamento característico da subunidade diante dos regulamentos de Segurança da Informação é o desafio, pois metade das medidas previstas é rejeitada. A pesquisa mostrou que a adoção na subunidade, de forma geral, é feita após a ocorrência de incidentes. Além disso, nem todos os tipos de medidas técnicas foram identificados na entrevista. Medidas informais, também percebidas como necessárias, não são adotadas, pois, segundo o Entrevistado 12, a subunidade não tem condições de adotá-las. O mesmo ocorre com as medidas formais, que estão associadas a pressões coercitivas e relacionadas pelo entrevistado à conformidade.

A análise dos dados da entrevista utilizando o *software* NVivo mostrou que na Subunidade 12 a resposta estratégica com maior cobertura de percentual foi o desafio, que teve 14,01%, e a tática é a rejeição, com 11,22% de cobertura de percentual. O desafio teve 14 referências de codificação, sendo também a resposta com maior número de referências identificadas, e a tática que teve maior quantidade foi a rejeição, com 12 referências codificadas. O desafio tem destaque na subunidade porque a Subunidade 12 não adota todas as medidas técnicas, não adota todas as formais e não adota qualquer medida informal que é pressionada a adotar. O que pode explicar esta resposta ser a mais identificada são os seguintes fatos: as pressões coercitivas não são percebidas como tal pelo entrevistado, pois não há nenhuma punição quando há o descumprimento; a adoção das medidas de Segurança da Informação é muito mais uma reação à ocorrência de incidentes do que uma questão de prevenção.

6.3.13 Subunidade 13

A área de TI da Subunidade 13 está subordinada à CGTI pelo fato de a subunidade não ter autonomia administrativa. Com três funcionários, sendo dois servidores públicos efetivos e um estagiário, a área de TI não tem uma pessoa dedicada à Segurança da Informação. A subunidade fica em outro estado, distante, portanto, da administração central da FIOCRUZ. O responsável pela TI da subunidade foi o entrevistado, que tem graduação e está cursando mestrado na área de TI. Não existe uma designação formal do responsável pela TI como coordenador do setor. A entrevista foi através do *software* Skype e demorou 25 minutos.

Não foram identificadas medidas formais de Segurança da Informação adotadas pela subunidade na entrevista. Segundo o Entrevistado 13, o único procedimento de Segurança da Informação adotado pela subunidade é a realização de *backups*, mas este não é documentado.

Sobre as medidas informais, o entrevistado declarou que sempre que adota alguma medida técnica, os usuários são informados e há uma preocupação em mostrar para eles a relação dessas medidas aos regulamentos da FIOCRUZ. Não foram realizados treinamentos para usuários ou profissionais de TI nem houve ações de conscientização. Assim, os dados

mostram que a subunidade adota medidas informais de “Divulgação de regulamentos e da Política de Segurança da Informação”.

Segundo o entrevistado, a subunidade tem um *firewall*, realiza *backup* semanal dos dados, utiliza o antivírus corporativo da FIOCRUZ, tem controles de acesso lógico dos usuários aos dados armazenados na rede e aos sistemas de informação, controla o acesso dos computadores à rede e à Internet, tem *no-breaks* para os equipamentos da rede de computadores, controla atualizações dos sistemas operacionais dos computadores e faz detecção e prevenção de intrusos na rede de computadores. Assim, a análise dos dados coletados na entrevista mostra que a subunidade adota medidas técnicas de “Segregação e monitoramento de redes de computadores”, “Redundância de dados”, “Prevenção contra códigos maliciosos”, “Controle de acesso lógico” e “Proteção ambiental”. Outras medidas não foram identificadas.

A pequena quantidade de medidas formais, informais e até mesmo técnicas pode ser explicada pelo fato de a adoção ser relativamente recente na Subunidade 13. A subunidade não tinha sequer profissionais de TI, até quando o entrevistado foi contratado para trabalhar. “Quando eu cheguei aqui, não tinha nem um *firewall*”, declarou o entrevistado, e a implantação de controles de acesso lógico ainda não estava concluída no momento em que foi realizada a entrevista. Essa adoção se reflete em uma conformidade muito baixa com as medidas previstas nos regulamentos da FIOCRUZ. O único regulamento com o qual a subunidade está em conformidade com mais da metade das medidas previstas é a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), sobre utilização de mídias sociais: 67% das medidas previstas são plenamente adotadas pela subunidade, segundo o último relatório de auditoria interna divulgado (FIOCRUZ, 2015). Quatro dos regulamentos não têm nem uma medida prevista adotada pela Subunidade 13, nem totalmente nem parcialmente. Dentre os outros regulamentos, o maior percentual de conformidade é a Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), que trata do acesso à Internet na organização.

A subunidade não adota muitas medidas de Segurança da Informação, mas o Entrevistado 13 acredita que a adoção melhora o ambiente computacional, reduzindo a quantidade de incidentes e dando tranquilidade para os usuários. Segundo ele, “[Segurança da Informação] é uma questão de bom senso. A Segurança em primeiro lugar, mas se ter Segurança prejudicar o trabalho de alguém, não justifica adotar.” Assim, o entrevistado entende que a adoção de medidas de Segurança da Informação é uma questão de eficiência, e reforça o entendimento admitindo que a não adoção pode trazer prejuízos para a organização.

Não foi possível identificar diferenças na percepção do entrevistado quanto aos benefícios da adoção de medidas técnicas, formais e informais.

A partir da entrevista com o Entrevistado 13, foi possível identificar que a subunidade sofre pressões coercitivas, miméticas e normativas para adoção de medidas de Segurança da Informação. As pressões miméticas aparecem em consultas a outras organizações realizadas pelos profissionais de TI antes de adotarem medidas de Segurança da Informação: "Sempre que a gente vai fazer uma coisa, vai primeiro pesquisar. Pelo menos eu, quando vou implantar alguma coisa, sempre pesquiso no serviço público, vou ver o que já fizeram, os casos de sucesso, esse tipo de coisa." As pressões coercitivas vêm através de regulamentos externos que atingem toda a FIOCRUZ, e não especificamente a subunidade: "Eu acho que existem regulamentos que ameaçam a FIOCRUZ quanto a isso [adoção de medidas de Segurança da Informação]." O Entrevistado 13 declarou ter a percepção de que as medidas de Segurança da Informação são necessárias para a organização, sendo uma questão de bom senso adotá-las, mas não foram identificadas pressões normativas na entrevista.

A resposta que caracteriza o comportamento da subunidade quanto à adoção de medidas de Segurança da Informação previstas nos regulamentos da organização é o desafio, pois o relatório de auditoria (FIOCRUZ, 2015) mostra que a grande maioria das medidas exigidas pela FIOCRUZ não é adotada. Embora a entrevista tenha mostrado que medidas informais são tidas como importantes para a conscientização das pessoas, algumas medidas são consideradas prejudiciais às atividades desenvolvidas na subunidade, o que pode explicar a grande rejeição na subunidade.

A subunidade respondeu às diferentes pressões institucionais que sofre com aquiescência, compromisso, esquiva e desafio. A resposta estratégica de compromisso através de barganha foi identificada na entrevista quando o informante relatou que a subunidade pretende documentar os procedimentos internos de Segurança da informação, mas que isto será feito futuramente. A aquiescência vem através da imitação, quando o entrevistado admite que realiza consultas a outras organizações, casos de sucesso e experiências anteriores antes de adotar medidas de Segurança da Informação. O entrevistado citou que algumas medidas de Segurança da Informação foram adotadas inicialmente, mas que elas provocaram prejuízos ao trabalho das pessoas na subunidade e que, por este motivo, foram rejeitadas, o que caracteriza a resposta de desafio através da tática de rejeição.

A resposta de esquiva foi a que teve maior cobertura de percentual, com 6,24%, e a tática utilizada foi a ocultação, também com cobertura de percentual de 6,24%. A resposta de esquiva e a tática de ocultação tiveram duas referências de codificação cada, o que reforça o resultado para cobertura de percentual, mas não corrobora com os resultados identificados na auditoria. A esquiva foi identificada quando o Entrevistado 13 relata a adoção de medidas de Segurança da Informação sem que as configurações necessárias tenham sido realizadas, como pode ser visto no trecho a seguir: "Não tinha nem *firewall* na rede. Então eu coloquei um [nome do fabricante do *firewall*], mas sem muita regra, porque tinha muitas outras coisas para fazer. Então só coloquei o *firewall* com o básico." Essa resposta aparece também na adoção de controles de acesso lógico, quando, segundo o entrevistado, houve a implantação de uma tecnologia para essa finalidade, mas ela não está funcionando como deveria: "O universo de usuários ainda é pequeno e a gente ainda vai decidir o que fazer quanto a isso aí. Essa parte não está completa ainda."

Destaca-se ainda para esta subunidade a aquiescência, que teve 5,78% de cobertura de percentual e duas referências de codificação, e a tática de imitação, com 3,58% de cobertura e uma referência de codificação. A imitação é identificada quando o entrevistado admite que outras organizações e subunidades foram consultadas antes de adotar medidas de Segurança da Informação.

6.3.14 Subunidade 14

A Subunidade 14 fica localizada em outro estado, distante da sede administrativa da organização. Foi entrevistado o responsável pela Segurança da Informação, servidor público efetivo da subunidade e componente do Comitê de Segurança da Informação da FIOCRUZ. A entrevista foi remota, através de Skype, e teve 38 minutos. O Entrevistado 14 é graduado na área de TI, tem especialização em Gestão de TI e está cursando mestrado. O setor de TI da subunidade tem subdivisões internas com profissionais de desenvolvimento de sistemas, infraestrutura e suporte ao usuário. Não existe uma subdivisão específica para Segurança da Informação dentro da área de TI e apenas o entrevistado lida diretamente com Segurança da Informação na subunidade.

A Subunidade 14 não tem um Comitê de Segurança da Informação próprio. O entrevistado afirmou que houve a intenção de criar um, mas não foi criado devido ao fato de a

equipe de TI ser pequena e com muitas atribuições, o que limitaria a disponibilidade das pessoas para as atividades inerentes a um Comitê. Apesar de não ter um Comitê, a subunidade tem um documento que é seu único regulamento de Segurança da Informação. Segundo o entrevistado, o documento já existia antes de ter sido formalizada a Política de Segurança da Informação e os regulamentos da FIOCRUZ, mas ele foi atualizado e aprovado pela direção da subunidade. O entrevistado complementa que o regulamento trata de temas como acesso a redes sociais e vídeos na Internet, uso do serviço de correio eletrônico, impressão de documentos, pirataria e uso de recursos computacionais, assuntos que são tratados por regulamentos específicos da FIOCRUZ. "Apesar de a FIOCRUZ ter essas normas gerais, a gente também tem as nossas normas. Agora, são baseadas nelas, não fugindo muito do que são as normas da FIOCRUZ. A gente não pode ter uma Política na FIOCRUZ e a gente ter outra totalmente diferente na unidade", afirmou o entrevistado. Com isto, a entrevista mostrou que a Subunidade 14 tem "Regulamentos internos de Segurança da Informação". O participante referiu-se a "normas" de Segurança da Informação da subunidade, mas no decorrer da análise da entrevista, percebeu-se que se trata de um regulamento apenas. Assim, além do regulamento citado, não foram identificadas outras medidas formais de Segurança da Informação na entrevista.

Da mesma forma que não foi criado um Comitê de Segurança da Informação local por falta de pessoal, não foram realizadas ações de conscientização e educação, segundo o Entrevistado 14. No entanto, ele deixou claro que há intenção de realizar eventos com esta finalidade: "Existe interesse de trazer uma pessoa para fazer uma palestra bem didática com relação a segurança na Internet, o que pode fazer, o que não pode, essa coisa do *email*, que às vezes o pessoal responde, mas que não pode responder. Uma coisa mais educativa [...], uma coisa para os usuários." Apesar do interesse declarado pelo entrevistado, não foi adotada nenhuma medida informal de Segurança da Informação na Subunidade 14.

Quanto às medidas técnicas, a entrevista mostrou que a Subunidade 14 tem um *firewall* para "Segregação e monitoramento de redes de computadores", faz "Controle de acesso lógico" para evitar acessos indevidos à rede de computadores, aos seus recursos e informações e à Internet, faz "Redundância de equipamentos" ao ter servidores com funções redundantes, tem antivírus e anti-spam como medidas de "Prevenção contra códigos maliciosos", provê acesso seguro ao serviço de *webmail*, uma medida de "Transmissão e armazenamento seguros de dados", e realiza *backup* dos dados armazenados em seus servidores de rede como medida de "Redundância de dados".

Apesar da identificação de poucas medidas, a Subunidade 14 adota grande parte das medidas previstas nos regulamentos da CGTI. O último relatório de auditoria interna disponibilizado (FIOCRUZ, 2015) mostra que somente três regulamentos não tiveram pelo menos 66% das medidas previstas adotadas: Norma Institucional SIC-004/CGTI/VPGDI (FIOCRUZ, 2013a), sobre *datacenters*; Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a), sobre de backups; e Norma Institucional SIC-009/CGTI/VPGDI (FIOCRUZ, 2013g), sobre dispositivos móveis, sendo que este último é o destaque negativo, pois 73% das medidas deste regulamento não foram adotadas.

O Entrevistado 14 entende que a maioria das medidas adotadas pela sede é coerente com as necessidades da subunidade, mas cita a tentativa de centralização dos serviços de TI no *datacenter* da organização como um exemplo de medida incoerente, pois a infraestrutura de rede de computadores não permite que os serviços de subunidades remotas sejam centralizados. Ainda sobre isto, citou que o custo da centralização dos serviços no *datacenter* seria muito alto, o que pode inviabilizar a ideia.

Segundo o Entrevistado 14, há perdas para as subunidades com a adoção das medidas previstas nos regulamentos da FIOCRUZ, mas os ganhos são maiores do que as perdas. No seu entendimento, a adoção de medidas de Segurança da Informação é importante, pois a interconexão da organização com a Internet expõe suas informações a riscos. Embora reconheça que a ocorrência de incidentes pode prejudicar a imagem da organização, o entrevistado minimiza este prejuízo. Sem distinguir medidas técnicas, formais e informais, ele deixa claro que entende que a motivação para adoção das medidas de Segurança da Informação é mais a eficiência na proteção dos dados do que a conformidade com requisitos de Segurança da Informação, como pode ser visto no trecho abaixo:

> Acho que isso [Segurança da Informação] é uma tendência, os dados estão cada vez mais expostos, cada vez mais críticos. E além de ser uma tendência, é uma necessidade. Imagine se vaza alguma informação de uma patente que a FIOCRUZ está tentando aprovar e que vai trazer benefícios para a instituição. Se isso vaza e cai nas mãos da iniciativa privada, então o prejuízo é muito grande. Você tem que estar preocupado em garantir a segurança desses dados. (ENTREVISTADO 14).

No entendimento do Entrevistado 14, sua subunidade não é pressionada por outras organizações, mas apenas pela sua administração central, mas ele faz a ressalva de que uma subunidade pode receber pressões que, devido à autonomia, não atingem as outras. As pressões exercidas através de regulamentos e da Política de Segurança da Informação são

percebidas como recomendações, e não como obrigações na subunidade. Pressões normativas foram identificadas em evidências de que o regulamento da subunidade teve por base a norma ABNT NBR 27002 (ABNT, 2013) e que costuma consultar o grupo de profissionais com quem mantém contato antes de adotar medidas de Segurança da Informação. A entrevista mostrou ainda que outras formas de exercer pressão coercitiva ou mimética, como auditorias ou o fato de outras organizações estarem adotando algumas medidas, não necessariamente influenciam ou resultam na adoção de medidas de Segurança da Informação pela subunidade.

A entrevista mostrou que o participante entende que medidas técnicas são adotadas pela Subunidade 14 por serem percebidas como necessárias para garantir a proteção dos dados, pois não adotá-las pode pôr em risco os dados organizacionais e a própria organização. Pela análise das respostas do entrevistado, a adoção de medidas técnicas é resultado principalmente de pressões normativas sofridas pela subunidade. Ainda que essas medidas tenham sido adotadas com base nos regulamentos da organização, estes regulamentos não são

Apenas uma medida formal foi identificada na entrevista, mas o responsável pela Segurança da Informação na subunidade entende que essas medidas são importantes para que se tenha conformidade com requisitos legais de Segurança da Informação: “Hoje em dia a gente sabe que tudo está muito na *web*, então você tem que ter realmente uma diretriz [...], até porque existe uma responsabilidade legal da instituição.” Assim, no entendimento do entrevistado, medidas formais são tidas como certas, necessárias para a garantia da Segurança da Informação. Não houve elementos identificados na entrevista que associassem a adoção de medidas informais de Segurança da Informação a pressões institucionais normativas, coercitivas ou miméticas.

A estratégia que caracteriza o comportamento da Subunidade 14 frente aos regulamentos da administração central é a aquiescência, pois mais da metade das medidas previstas foi adotada, sendo que poucas foram adotadas parcialmente e ainda menos foram rejeitadas, segundo o relatório de auditoria (FIOCRUZ, 2015). Apesar de não terem sido identificadas medidas informais e de apenas uma medida formal ter sido adotada pela subunidade, a adoção de medidas técnicas é vista como uma necessidade pelo Entrevistado 14, o que explica a aquiescência como estratégia característica.

Aquiescência é também a estratégia com maior cobertura de percentual (11,72%), sendo a conformidade a tática com maior cobertura (9,64%), indicando a adoção consciente e

estratégica das medidas de Segurança da Informação. Quatro referências de codificação foram identificadas para a resposta de aquiescência e duas para a tática de conformidade, corroborando com a cobertura de percentual de ambas. Ao adotar somente seis dos dez tipos de medidas técnicas, somente um tipo de medida informal e nenhuma medida formal, a primeira impressão que sem tem sobre a subunidade é que ela rejeita requisitos de Segurança da Informação do ambiente externo e da sua administração central, mas a conformidade com os regulamentos da FIOCRUZ e a percepção de que a motivação para adotar medidas técnicas é a proteção dos dados explicam como a aquiescência é a resposta que teve maior destaque na análise dos dados utilizando o *software* NVivo.

6.3.15 Subunidade 15

A Subunidade 15 está localizada no *campus* da administração central da FIOCRUZ, tem autonomia administrativa e conta com um departamento de TI com cinco funcionários, dentro os quais um trabalha dedicado à Segurança da Informação, embora não tenha um setor para esta finalidade no organograma da subunidade. O entrevistado, que não tem graduação na área de TI, é o coordenador de TI da subunidade. A entrevista foi realizada presencialmente e teve duração de 33 minutos.

O Entrevistado 15 informou que a subunidade faz adaptações da Política e dos regulamentos de Segurança da Informação para as necessidades da subunidade: “Buscamos seguir as recomendações da CGTI, fazendo adaptações para assuntos específicos, às vezes não abordados numa Política mais ampla.” A subunidade não tem ainda sua Política de Segurança da Informação própria, mas o entrevistado explica que “A Política de Segurança da Informação da [nome da subunidade] está em desenvolvimento e baseia-se principalmente na Política de Segurança da CGTI. [...] A Política completa ainda não foi publicada. Estamos redigindo e formulando normas.” Com isso, o informante esclareceu que a Subunidade 15 adotou “Regulamentos internos de Segurança da Informação”, mas não adotou outras medidas formais, embora a subunidade esteja elaborando uma Política própria.

O Entrevistado 15 informou que medidas informais também estavam sendo planejadas para a subunidade, de acordo com os regulamentos de Segurança da Informação da subunidade e da organização. No entanto, não foram identificadas evidências de que a

subunidade tivesse adotado qualquer medida informal no momento em que a pesquisa estava sendo realizada.

Apesar de não ter medidas informais e de ter apenas uma medida formal, a Subunidade 15 adotou diferentes medidas técnicas de Segurança da Informação. Como exemplo, o entrevistado citou a elaboração de um projeto para limitar a utilização dos computadores pelos usuários, impedindo a instalação de *softwares* e outras ações potencialmente perigosas. De acordo com o entrevistado, a subunidade tem ainda antivírus, anti-spam, equipamentos com peças redundantes, rotina de *backup*, *firewall*, *login* único para os usuários, *no-break* e ar condicionado na sala de equipamentos de rede. Assim, os dados mostram que a subunidade adotou medidas técnicas de "Redundância de dados", "Segregação e monitoramento de redes de computadores", "Redundância de peças de equipamentos", "Prevenção contra códigos maliciosos", "Controle de acesso lógico" e "Proteção ambiental". Não foram identificadas outras medidas técnicas, como uso de tecnologias para transmissão e armazenamento seguro de dados, redundância de equipamentos ou controle de acesso físico.

A Subunidade 15 adotou várias medidas técnicas, mas poucas formais e poucas informais foram adotadas. Na auditoria (FIOCRUZ, 2015), foi identificado que dois regulamentos da FIOCRUZ têm menos da metade das medidas adotadas: a Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a), sobre segurança na aquisição, desenvolvimento e manutenção de sistemas de informação, e a Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), sobre o acesso a redes sociais. Os demais regulamentos têm mais da metade das medidas previstas adotadas, e dois deles tiveram todas as medidas de Segurança da Informação previstas adotadas pela subunidade.

A adoção de medidas de Segurança da Informação é percebida pelo entrevistado como importante para a Subunidade 15 porque padroniza o tratamento de questões relacionadas ao assunto e resulta em uma mudança no comportamento dos usuários de TI. De acordo com o Entrevistado 15, "Muito além de vantagens técnicas de proteção a dados, a principal vantagem é o envolvimento responsável das pessoas." O entrevistado complementa ainda que "Quando não temos política de senha forte e outros aspectos, aumentamos o risco de envio de spam e, consequentemente, podemos ficar sem comunicação com vários usuários de alguns domínios." (ENTREVISTADO 15). Com isso, pesquisa mostrou que a adoção de medidas técnicas é uma questão de eficiência, na visão do informante. A partir das sua respostas, não foi possível identificar diferenças entre os objetivos da subunidade ao adotar medidas técnicas, formais ou informais de Segurança da Informação. Em todos os casos, a

intenção com a adoção é adequar o comportamento do usuário às necessidades da organização, enquanto a conformidade com regulamentos externos não foi citada.

Na visão do entrevistado, as pressões que a Subunidade 15 sofre através dos regulamentos da FIOCRUZ são recomendações, cuja adoção não é obrigatória. Para ele, as pressões coercitivas alcançam somente a CGTI, que recomenda a adoção de medidas de Segurança da Informação nas subunidades através da Política organizacional: "A Política de Segurança criada pela CGTI é fruto de indicações de órgãos externos" (ENTREVISTADO 15).

Os dados da pesquisa mostram que a subunidade se baseia também em experiências de outras organizações ao adotar medidas de Segurança da Informação, o que mostra que ela sofre pressões miméticas do ambiente institucional, mas a autonomia e a falta de conexão entre as subunidades dificultam a disseminação de experiências positivas dentro da organização, segundo o entrevistado. Não foram identificadas evidências nas respostas do entrevistado de que a subunidade sofra pressões coercitivas, tanto da administração central da organização quanto de outras organizações do ambiente institucional.

O comportamento característico da subunidade para com os regulamentos da organização é a aquiescência, pois muito mais medidas previstas nos regulamentos foram adotadas pela subunidade do que foram rejeitadas ou adotadas parcialmente, segundo o relatório de auditoria interna (FIOCRUZ, 2015).

Apesar de a subunidade ter adotado diversas medidas previstas nos regulamentos da organização, foram identificadas respostas de desafio e manipulação. Uma das respostas de desafio identificada teve como tática a rejeição e a causa foi a falta de recursos para adotá-las: "Normalmente conseguimos adotar controles de acordo com necessidades técnicas mais latentes, porém priorizá-los depende também da estrutura de pessoal da área e dos custos envolvidos" (ENTREVISTADO 15). Outra causa de rejeição identificada foi a limitação que as medidas provocam no trabalho dos usuários de TI da subunidade.

Já a resposta de manipulação foi identificada quando o Entrevistado 15 declarou que a participação de pessoas de TI nas discussões estratégicas da organização estimula os debates sobre os regulamentos e a adoção de medidas importantes, o que caracteriza a tática de influência.

Apesar de terem sido identificadas respostas de desafio e manipulação, a resposta estratégica que tem maior cobertura de percentual é a aquiescência, com 8,78%, cuja tática

com maior cobertura é a conformidade, com 8,28%. A aquiescência teve cinco referências de codificação identificada nos dados, e a tática de conformidade teve quatro referências, corroborando com os resultados para cobertura de percentual e de comportamento característico da subunidade identificado na auditoria interna. O Entrevistado 15 afirma que adota medidas técnicas de acordo com as necessidades mais importantes, acrescentando que a adoção é benéfica por questões técnicas, mas principalmente para garantir o comportamento adequado dos usuários de TI e seu envolvimento em assuntos relacionados à Segurança da Informação. A entrevista também mostrou que a Subunidade 15 responde com aquiescência através da imitação, uma vez que o entrevistado afirmou que experiências de outras organizações podem ser usadas para adoção na subunidade.

Nas respostas desta subunidade também foi identificada a tática de reconhecimento, como ocorreu na Subunidade 08, quando o entrevistado admitiu que o fato de não adotar uma medida de Segurança da Informação pode claramente causar um prejuízo à subunidade, mas a medida não é adotada nem rejeitada, embora haja uma intenção de adotá-la:

> Perdemos muito na qualidade quando alguns controles não são adotados. Um exemplo é no controle mais rígido de *emails*. Quando não temos política de senha forte e outros aspectos, aumentamos o risco de envio de spam e consequentemente podemos ficar sem comunicação com vários usuários de alguns domínios. (ENTREVISTADO 15).

6.3.16 Subunidade 16

A Subunidade 16 fica no *campus* da FIOCRUZ, tem um setor de TI estruturado que, devido à sua autonomia, não tem ligação hierárquica com a CGTI. No entanto, o setor de TI da subunidade não tem uma área específica para tratar de Segurança da Informação – apenas o entrevistado trabalha exclusivamente com isso na subunidade, embora outros profissionais de TI também realizem atividades relacionadas ao tema. A entrevista teve 59 minutos e foi realizada por Skype. O entrevistado tem graduação e especialização na área de TI.

As respostas do Entrevistado 16 mostram que a única medida formal de Segurança da Informação que subunidade adotou é a formalização de um procedimento para credenciamento e autorização de criação de contas de acesso para seus usuários, o que mostra

que pelo menos uma medida do tipo “Processos e procedimentos de Segurança da Informação” foi adotada. Além desta medida formal, a subunidade adota apenas duas medidas informais: acontecem ações voltadas para os usuários orientando a não divulgarem senhas e a bloquearem os computadores ao se afastarem, que podem ser consideradas como medidas de “Ações de conscientização”, e também são enviadas mensagens de correio eletrônico divulgando a Política de Segurança da Informação para seus usuários de TI:

> A gente mandou *email* para todos informando, dizendo o que era, para que serve [a Política de Segurança da Informação]. Isso para não pegar o pessoal de surpresa. [...] Aqui a gente divulgou, teve um trabalho de divulgação da Política, logo quando ela foi aprovada pela Presidência [da FIOCRUZ]. A gente decidiu... foi uma decisão minha, de mandar *email* para todos os usuários da rede informando, comunicando a existência dela. (ENTREVISTADO 16).

Dessa forma, a entrevista mostrou que a subunidade adota apenas “Divulgação de regulamentos e da Política de Segurança da Informação” e “Ações de conscientização” como medidas informais de Segurança da Informação. Medidas importantes para a adoção de outras medidas não são adotadas, como a criação de um subcomitê de Segurança da Informação e a existência de um Escritório de Segurança da Informação, e não houve iniciativas de treinamento de usuários e profissionais de TI na subunidade.

A Subunidade 16 tem poucas medidas informais e adota apenas uma medida formal, mas diferentes medidas técnicas de Segurança da Informação foram adotadas desde antes da elaboração da Política de Segurança da Informação da organização. Segundo o entrevistado, a subunidade tem sistema de detecção de incêndio, medida de “Proteção ambiental”. Ainda como medidas de proteção ambiental, a subunidade tem *no-breaks* redundantes, gerador e redes elétricas redundantes, que indicam que a subunidade adotou medidas de “Redundância de equipamentos”. As senhas utilizadas pelos usuários da rede de computadores e dos sistemas de informação da subunidade precisam atender a requisitos de complexidade e precisam ser trocadas periodicamente para garantir “Autenticação forte”. A subunidade controla o acesso a *websites* na Internet para evitar acessos a endereços potencialmente perigosos e indevidos, controla a instalação de *softwares* nos computadores dos usuários e controla o acesso dos usuários da rede de computadores a recursos específicos, o que são medidas de “Controle de acesso lógico”. O acesso dos usuários de TI aos servidores da rede da subunidade também é uma medida de controle de acesso lógico. A subunidade tem um *firewall*, tecnologia utilizada para fazer “Segregação e monitoramento de redes de computadores”. A possibilidade de restauração de *backups* de dados em outro servidor da

rede de computadores é uma medida de "Redundância de dados". Por fim, a subunidade utiliza antivírus como medida de "Prevenção contra códigos maliciosos". Parte das medidas foi adotada antes de a FIOCRUZ ter publicado sua Política de Segurança da Informação, como *no-break* e *firewall*, como citou o entrevistado:

> Algumas coisas foram feitas bem antes de se falar em política da FIOCRUZ. Por exemplo, isso do *no-break*, de gerador, a gente tem bem antes dela, da política. A gente tem *firewall* desde [...] antes da FIOCRUZ ter qualquer coisa nesse sentido. [...] Não temos política documentada, nem regras, mas a gente já fazia muita coisa antes de ter a política da FIOCRUZ. Exigia senha complexa, com troca periódica, orientava os usuários a não emprestarem senha, a bloquear computador, controlava o acesso a sites para não deixar acessar pornografia e pirataria, vídeos, rádio, essas coisas. Isso bem antes da POSIC. (ENTREVISTADO 16).

A pesquisa mostrou que a subunidade não adota muitas das medidas previstas nos regulamentos de Segurança da Informação da FIOCRUZ. A auditoria interna cujo relatório foi divulgado em 2015 (FIOCRUZ, 2015) revelou que a Subunidade 16 não adota integralmente nenhuma medida do regulamento que define as responsabilidades dos usuários de TI – a Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a) – e não adota integralmente sequer metade das medidas de cada um dos demais regulamentos, além de rejeitar mais da metade das medidas previstas em cinco regulamentos.

A tendência a desafiar os regulamentos da FIOCRUZ por serem consideradas ineficientes ou inadequadas à sua realidade faz com que a Subunidade 16 tenha como comportamento característico o desafio, pois a maior parte das medidas previstas nos regulamentos da organização foi rejeitada, como mostra o relatório da auditoria interna (FICORUZ, 2015).

Para o Entrevistado 16, as medidas de Segurança da Informação que a subunidade é pressionada a adotar são coerentes com as atividades desenvolvidas na subunidade: "Se elas têm o objetivo de proteger as informações e a gente tem informações que precisam ser protegidas, então acho que tem tudo a ver." O entrevistado complementa que não concorda com pressões que obriguem a subunidade a adotar medidas técnicas que não estejam de acordo com as necessidades da subunidade ou que prejudiquem suas atividades, citando um exemplo:

> A FIOCRUZ colocou uma regra lá que exigia que as caixas postais fossem apagadas logo depois do afastamento, quando o usuário fosse demitido [...] um terceirizado saiu, ou o contrato acabou, a bolsa acabou, o aluno defendeu [...]. Mas isso se aplica a terceirizados. Não se aplica a bolsista, que na maioria das vezes vai voltar como aluno

> de mestrado ou doutorado. Nem a ex-aluno, que vai passar na seleção para doutorado ou pós-doutorado, ou vai passar no concurso e vai virar pesquisador ou professor da FIOCRUZ. Então, o usuário fez a pesquisa, defendeu, fez o artigo e quando vai ter uma resposta do periódico, não tem mais *email* para receber essa resposta, porque defendeu e não tem mais *email*. (ENTREVISTADO 16).

O responsável pela Segurança da Informação da Subunidade 16 cita ainda outros exemplos de medidas que não considera coerentes, como bloqueio e exclusão de caixas postais de servidores públicos aposentados há mais de dois anos, o que pode prejudicar atividades de orientação e pesquisa em andamento, ou a limitação do tamanho para envio de mensagens de correio eletrônico, que, segundo ele, limita as possibilidades de troca de arquivos necessários para as atividades de pesquisa e ainda leva o usuário a utilizar serviços de armazenamento de dados em nuvem, o que também é proibido pelos regulamentos da organização.

O entrevistado percebeu incoerências também entre as pressões para adotar medidas formais de Segurança da Informação:

> Quando veio aquela regra de criar um grupo [...], um subcomitê de Segurança nas unidades, não criamos. Isso só iria atrapalhar, burocratizar as decisões, e esse pessoal está mais preocupado com seus laboratórios e seus setores do que com a [nome da unidade]. Então suas decisões são para as necessidades dos laboratórios. [...] Se eles são do Comitê daqui [subcomitê de Segurança da Informação da subunidade], não aprova uma regra sequer. (ENTREVISTADO 16).

A adoção de medidas de Segurança da Informação pela subunidade, segundo o entrevistado, tem como benefício a proteção da informação:

> [O benefício] É a proteção da informação mesmo. A gente previne a ocorrência de várias coisas. Não dá para prevenir tudo, mas dá para ter alguma garantia. Hoje não temos risco de queimar servidor por falta de energia, nem de perder dados por isso [...]. Hoje nossa rede não vai ser acessada indevidamente tão facilmente, porque tem um *firewall* aqui. Hoje não é qualquer site que vai ser acessado pelos nossos usuários, porque a gente tem aqui um controle de acesso. Se tiver um problema grande, se perder um servidor, a gente tem *backup* e dá para restaurar em outro servidor [...]. É aquela coisa de integridade, disponibilidade e confidencialidade mesmo. (ENTREVISTADO 16).

Essa visão está de acordo com a eficiência na garantia da integridade, confidencialidade e disponibilidade, como o entrevistado frisou. Apesar de perceber a adoção como positiva para proteger a informação, ele nota também que ficar em conformidade com os requisitos externos é importante para a Subunidade 16. Segundo ele, o fato de não ter

apontamento em auditorias internas ou externas pode facilitar a obtenção de recursos para fazer aquisições e contratações, mas ele ressalta que a conformidade é uma questão menor, reiterando que "O importante mesmo é proteger a informação. Até porque essas coisas às vezes podem ser mais para constar. [...] Por exemplo, a gente pode criar regulamentos só para ter, sem implicação prática nenhuma." A partir disso, o Entrevistado 16 explica que entende que medidas técnicas visam à proteção dos recursos tecnológicos: "Eles são para proteger a parte técnica, os equipamentos, os dados, as informações. Então acho que os controles técnicos são mais voltados para proteger as informações". Assim, enquanto medidas técnicas são mais relacionadas à eficiência na Segurança da Informação, medidas formais são associadas à conformidade com requisitos externos. As medidas informais, por sua vez, visam a mudança do comportamento dos usuários de TI e, consequentemente, têm um viés de eficiência: "Acho que [medidas informais] são para isso mesmo... para conscientizar os usuários, para que eles aceitem melhor as políticas, as normas. O ganho que se tem com isso é na melhoria do comportamento dos usuários quanto à Segurança." (ENTREVISTADO 16).

As pressões institucionais que a Subunidade 16 sofre vêm da própria FIOCRUZ, através da Política de Segurança da Informação, e da AUDIN, que realiza auditorias sobre o assunto, bem como do Governo Federal, através de regulamentos sobre Segurança da Informação que vêm sendo publicados. Sofre pressões também de outras organizações e órgãos estatais, como o TCU e a Controladoria Geral da União (CGU) (atual Ministério da Transparência, Fiscalização e Controladoria-Geral da União). O Entrevistado 16 acrescenta ainda pressões da sociedade, preocupada com a privacidade dos dados pessoais que estão de posse da organização.

As pressões identificadas são principalmente coercitivas, pois vêm da administração central da organização e de órgãos que regulamentam e fiscalizam suas atividades, mas foram identificadas também pressões miméticas, pois as medidas adotadas foram baseadas em políticas, regulamentos e experiências de outras organizações e subunidades e de recomendações do TCU: "Foram baseadas em políticas de outras organizações, principalmente de universidades. A gente viu também como o Ministério do Planejamento faz, como o TCU faz, quais são as recomendações do TCU. Perguntei para o [nome de outra subunidade da FIOCRUZ] como eles estavam tratando de bloqueio de usuários." (ENTREVISTADO 16). Tecnologias adotadas pela administração central também pressionam a subunidade: "Se a FIOCRUZ tem um sistema novo ou implanta uma tecnologia nova, é normal ela forçar a gente a ficar em conformidade." (ENTREVISTADO 16).

Pressões normativas também foram identificadas: “Eu vi também as normas, a ISO, algumas recomendações de outros modelos, como o COBIT [o modelo *Control Objectives for Information and Related Technology* de governança de TI]. Não fiz tudo o que tem lá, mas, vamos dizer, me inspirei nelas.” (ENTREVISTADO 16). Como a subunidade adota poucas medidas formais e informais, é possível afirmar que essas pressões estão relacionadas à adoção de medidas técnicas de Segurança da Informação.

Apesar de reconhecer que a adoção de medidas de Segurança da Informação foi uma decorrência das pressões sobre a Subunidade 16, o entrevistado admite que as pressões coercitivas não necessariamente farão com que a subunidade deixe de utilizar as tecnologias e demais medidas adotadas para se adequar às exigências da administração central:

> Daí o desconforto em ter que se adequar aos padrões que eles querem. A gente tem nossa tecnologia, confia nela, [...] não quer sair disso, porque a gente conhece o que tem e não quer deixar de lado simplesmente porque a FIOCRUZ adotou outra coisa. Antes não tinha nada. Compramos e implantamos porque não tinha nada. Não pode dizer “deixe de usar isso e use aquilo”. (ENTREVISTADO 16).

Neste caso, fica clara a resposta estratégica de desafio através da rejeição das medidas que a subunidade é pressionada a adotar, visto que não são consideradas adequadas às necessidades da subunidade em comparação com as tecnologias que já estão implantadas. O desafio é a resposta estratégica mais recorrente da subunidade, de acordo com os resultados apresentados pelo *software* NVivo: teve 12 referências de codificação. A tática de contestação, com sete referências identificadas, foi a mais identificada. Quanto à cobertura de percentual, o desafio teve 17,60% e a tática de contestação apresentou 9,55%.

Como exemplo retirado da entrevista com o responsável pela Segurança da Informação, é possível citar a pressão que a Subunidade 16 recebeu para mudar o *firewall* para uma solução de outro fabricante, padronizada pela organização para prover acesso à Internet para a subunidade, mas a subunidade não adotou o padrão requisitado. Com relação à exigência da administração central da organização para que as caixas postais de correio eletrônico de ex-usuários fossem bloqueadas e excluídas, a subunidade respondeu da mesma forma ao manter as caixas postais ativas por mais tempo do que o regulamentado a fim de não prejudicar atividades que ainda estejam em andamento. A subunidade respondeu com desafio também contra a proibição da utilização de serviços de armazenamento de dados em nuvem, visto que há uma limitação para envio de arquivos anexos no sistema de correio eletrônico e o usuário precisa enviar arquivos grandes para outras pessoas. O regulamento que trata de

datacenters – a Norma Institucional SIC-004/CGTI/VPGDI (FIOCRUZ, 2013a) – também é contestado pela subunidade: "Não faz sentido para a gente. Não dá para a gente construir um *datacenter* com aqueles requisitos, a gente não tem dinheiro nem pessoal. E a regra não dá abertura para fazer algo menor, um CPD [Centro de Processamento de Dados] com o mínimo necessário." O relatório de auditoria mostra que 36% das medidas previstas no regulamento não são adotadas e 23% são adotadas parcialmente pela subunidade (FIOCRUZ, 2015).

A pesquisa mostrou ainda outras situações em que a subunidade respondeu com desafio utilizando a tática de contestação contra medidas previstas na Norma Institucional SIC-007/CGTI/VPGDI (FIOCRUZ, 2013e), que regulamenta o acesso remoto às redes de computadores da FIOCRUZ e que teve 82% de rejeição da subunidade. Contra a tentativa da CGTI de impedir a aquisição de equipamentos de rede pelas subunidades para concentrar a infraestrutura no *datacenter* da organização, a Subunidade 16 respondeu também com desafio utilizando a contestação como tática: "Nesse caso, o nosso Vice-Diretor se posicionou contra e disse que a gente iria comprar os equipamentos que fossem necessários. [...] Acho que outras unidades fizeram o mesmo. Então eles recuaram. Construíram o *datacenter*, mas não estão mais com essa política [de obrigar as subunidades a hospedarem seus equipamentos de TI lá]."

A incoerência das medidas exigidas pela CGTI pode ser o motivo das respostas de desafio por parte da Subunidade 16. De acordo com o Entrevistado 16, o Comitê de Segurança da Informação da FIOCRUZ toma decisões que não consideram a realidade das subunidades:

> Cada unidade tem uma realidade. Tem coisas que eles fazem lá, tem normas e recomendações que são específicas para o *campus* de Manguinhos. *Datacenter*? Qual unidade tem condições de construir um *datacenter*? Não seria melhor pensar em como organizar os CPDs [Centros de Processamento de Dados] das unidades? Aí põe uma série de requisitos que impedem as unidades de melhorar os CPDs. Não tem recurso, não tem espaço, não tem gente. (ENTREVISTADO 16).

Como mostrou a entrevista com o Entrevistado 16, o fato de o Comitê e a CGTI não considerarem as necessidades das subunidades leva à rejeição de certas medidas de Segurança da Informação. O entrevistado deixou claro que "Se atrapalhar, a gente [a subunidade] não faz. A gente não implementa, não adota, não elabora o documento, a regra."

Além da rejeição inequívoca através do desafio, a subunidade também responde às pressões institucionais com esquiva. Através da tática de ocultação, a subunidade permite o

uso de recursos de armazenamento de arquivos em nuvem, uma prática proibida pelos regulamentos da organização, para não atrapalhar o trabalho dos usuários de TI. A ocultação é a tática mais adequada para este comportamento porque a medida não é adotada, mas a subunidade tem condições de fazer o bloqueio, inclusive a tecnologia necessária. A esquiva por ocultação aparece também quando o entrevistado admitiu que incidentes de Segurança da Informação não são informados à administração central da FIOCRUZ e aos órgãos de controle da Internet. As táticas de amortecimento e fuga também foram utilizadas pela subunidade quando o entrevistado declarou que esconde de auditorias internas o nível real de conformidade com os regulamentos da organização e quando admitiu que a subunidade não participa de iniciativas da administração central que exijam a adoção de medidas de Segurança da Informação que não são do seu interesse, ainda que sejam do interesse da sede da organização.

Enfim, a despeito de o desafio ter sido a resposta estratégica mais identificada na entrevista, a Subunidade 16 respondeu também com aquiescência, compromisso, esquiva e manipulação, a depender da percepção quanto à coerência das medidas com suas atividades e objetivos.

6.3.17 Subunidade 17

A Subunidade 17 tem autonomia administrativa e está localizada em outro estado, distante da administração central da FIOCRUZ. Apesar de ter um setor de TI estruturado (com áreas internas de desenvolvimento, infraestrutura e suporte ao usuário), a subunidade não tem uma pessoa que se dedique exclusivamente às atividades de Segurança da Informação, embora seja apontado como a pessoa responsável na subunidade. Segundo o entrevistado, a subunidade não tem um Escritório de Segurança da Informação nem uma Equipe de Tratamento de Incidentes, mas tem um subcomitê de Segurança da Informação formalmente instituído. A entrevista foi realizada com coordenador de TI da subunidade, que foi formalmente designado para a função, teve duração de 48 minutos e foi presencial. O entrevistado tem graduação e especialização na área de TI, mestrado em outra área e está cursando doutorado.

Além de um Comitê próprio para tratar de Segurança da Informação próprio, a Subunidade 17 tem também um regulamento formalizado antes de a FIOCRUZ elaborar sua

Política de Segurança da Informação e seus regulamentos. A subunidade tem ainda diversos procedimentos de Segurança da Informação documentados e um processo formal de credenciamento e autorização de usuários de TI, que define critérios para conceder acesso à rede e aos sistemas de informação, o acesso a crachá para destravar as fechaduras eletrônicas existentes nas portas dos prédios do *campus* e a vigência do cadastro (e consequentemente do *login* criado para acessar a rede e os sistemas de informação da subunidade):

> Todas as pessoas que fazem algum tipo de serviço [na subunidade] estão cadastradas e precisam ter algum tipo de vínculo. [...] Então, quando o prazo do vínculo acaba, automaticamente a TI aqui é avisada e o acesso a todos os serviços de TI são cancelados automaticamente. Se a pessoa não comprovar a renovação do vínculo de forma documental, ou eventualmente a Diretoria autorizar a renovação do vínculo, o acesso não é liberado de forma alguma. (ENTREVISTADO 17).

Assim, a subunidade adota as seguintes medidas formais: "Comitê de Segurança da Informação", "Regulamentos internos de Segurança da Informação" e "Processos e procedimentos de Segurança da Informação". Outras medidas formais não foram identificadas na entrevista.

Dentre as medidas informais, a Subunidade 17 realizou ações de divulgação de medidas adotadas e de conscientização para evitar comportamentos inadequados dos usuários após a adoção dessas medidas.

> Quando a gente integrou o [serviço de diretórios utilizado para autenticação de usuários na rede de computadores] com nossos sistemas, com a Intranet. A gente fez um processo de conscientização para que as pessoas entendessem que agora havia um perigo ao passar o usuário e a senha para outras pessoas, já que agora a senha é a mesma, era uma única senha. (ENTREVISTADO 17).

O entrevistado relatou também que foi realizada na subunidade uma campanha sobre a utilização de crachás para controle de acesso físico: "Teve também o controle de acesso, a segurança no acesso, teve um trabalho aqui forte para utilização de crachás por todas as pessoas. Hoje a pessoa é obrigada a utilizar crachá, mesmo que seja estudante, que venha eventualmente aqui." (ENTREVISTADO 17). Por fim, ações de conscientização quanto ao uso da rede sem fio da organização e palestras regulares de conscientização em Segurança da Informação e de divulgação dos regulamentos da organização e da subunidade foram realizadas. Houve ainda treinamentos para profissionais de TI em gestão de Segurança da Informação e em tecnologias específicas, como antivírus e *firewall*. Com isso, a entrevista

mostrou que a subunidade adota as seguintes medidas informais: “Treinamento de profissionais de TI”, “Divulgação de regulamentos e da Política de Segurança da Informação” e “Ações de conscientização”.

Como medidas técnicas de Segurança da Informação, a Subunidade 17 utiliza um sistema integrado de autenticação dos usuários para acesso à rede de computadores, sistema de correio eletrônico e demais sistemas de informação da própria subunidade, implantou uma solução de controle de acesso físico com fechadura eletrônica e identificação por crachás e biometria, controle de acesso lógico à rede de computadores e à rede sem fio, controle de acesso à Internet com bloqueio de endereços eletrônicos potencialmente perigosos através de palavras-chave, o acesso ao Centro de Processamento de Dados (CPD) da subunidade é feito através de crachá ou biometria e é restrito aos servidores públicos do setor de TI, o acesso à rede de computadores e aos sistemas de informação é através de *login* e senha complexa, e as senhas são alteradas periodicamente. O acesso a funcionalidades dos sistemas de informação e aos recursos da rede de computadores é autorizado apenas às pessoas que precisam.

A subunidade utiliza o antivírus da FIOCRUZ e tem uma solução própria de anti-spam. O acesso ao *webmail* e demais sistemas de informação é feito utilizando criptografia. Alguns servidores da rede de computadores têm discos, fontes e placas redundantes, a subunidade tem um *storage* e faz regularmente *backup* dos dados. A subunidade utiliza *firewalls* separando redes de computadores com finalidades distintas e tem ainda *no-breaks*, aparelhos de ar-condicionado, gerador e redes elétricas redundantes, detector de fumaça e extintor de incêndio na sala do CPD. Os servidores da rede têm peças redundantes e alguns deles são também redundantes. Com isso, é possível afirmar que a subunidade adotou todas as categorias de medidas técnicas, segundo a classificação de Dhillon (1999).

Apesar de adotar diversas medidas técnicas e algumas informais e formais, o relatório de auditoria (FIOCRUZ, 2015) mostra que a Subunidade 17 não está em conformidade com todos os regulamentos de Segurança da Informação da FIOCRUZ. Quatro regulamentos tiveram menos de 50% das medidas previstas adotadas pela subunidade: Norma Institucional SIC-004/CGTI/VPGDI (FIOCRUZ, 2013a), sobre *datacenters*; Norma Institucional SIC-006/CGTI/VPGDI (FIOCRUZ, 2013a), sobre aquisição, desenvolvimento e manutenção de sistemas de informação; Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f), sobre redes sociais; e Norma Institucional SIC-009/CGTI/VPGDI (FIOCRUZ, 2013g), sobre a utilização de dispositivos móveis. Dentre estas, a Norma Institucional SIC-006/CGTI/VPGDI é a que tem menos adesão da subunidade e é também a

que tem mais medidas adotadas parcialmente. Mesmo não tendo adotado muitas das medidas de Segurança da Informação dos regulamentos, o relatório mostra que a Subunidade 17 rejeita poucas das medidas previstas, pois apenas a Norma Institucional SIC-008/CGTI/VPGDI teve um alto percentual de medidas não adotadas.

Como o Entrevistado 17 afirmou, o regulamento interno sobre utilização de correio eletrônico tem diferenças em comparação com o regulamento da FIOCRUZ que trata do assunto, a Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d). Neste caso, a subunidade busca ficar em conformidade com o regulamento local, embora o entrevistado tenha afirmado que ele foi discutido e revisado pelo subcomitê de Segurança da Informação da subunidade para ficar adequado ao regulamento da organização, mas que ainda não foi aprovado pela direção. Cabe registrar que a subunidade adota integralmente 78% das medidas previstas pelo regulamento de utilização de correio eletrônico da organização.

O Entrevistado 17 declarou que percebe as medidas que a subunidade é pressionada a adotar como coerentes com as necessidades e atividades que realiza. Além disso, a entrevista mostrou que o coordenador de TI da subunidade entende que a adoção de medidas de Segurança da Informação traz para a subunidade garantias de que "as informações sejam acessadas pelas pessoas que deveriam ter acesso àquelas informações, e no momento que elas precisam." (ENTREVISTADO 17). Trata-se da garantia da disponibilidade e da confidencialidade das informações, que é percebida pelo entrevistado como benefício da adoção de medidas de Segurança da Informação. O entrevistado acrescenta que a adoção das medidas previne a responsabilização dos profissionais de TI e da direção da subunidade caso ocorra algum incidente, pois mostra que a subunidade buscou evitar a ocorrência. Em outras palavras, a adoção de medidas de Segurança da Informação é percebida como uma questão de eficiência. Não foi identificada na entrevista diferenças na percepção quanto aos benefícios da adoção de medidas técnicas, formais e informais.

Pressões institucionais normativas foram identificadas no trecho em que o Entrevistado 17 declara que há "uma consciência do pessoal de infraestrutura da TI local de que medidas de segurança precisam ser adotadas". Isso pode ser o motivo pelo qual grande parte das medidas foi adotada antes de existirem os regulamentos e da Política de Segurança da Informação da organização – portanto, antes de haver qualquer pressão por parte da administração central da organização.

O coordenador de TI da subunidade reconhece que a conformidade com os regulamentos da organização vem sendo questionada em auditorias, mas ressalta que não há cobranças, inclusive quanto à implantação de uma infraestrutura mínima de Segurança da Informação, à formalização de regulamentos internas ou à existência de uma equipe local de Segurança da Informação. Além disso, os regulamentos da FIOCRUZ são percebidos pelo entrevistado como recomendações: "CGTI faz recomendações. Então tem uma série de recomendações que um bom *datacenter* precisa adotar. Isso é feito aqui, na medida do possível." O Entrevistado 17 complementa que "As unidades têm autonomia para seguir a norma que mais convier." Sobre outras fontes de pressão institucional, o entrevistado reconhece que a subunidade sofre pressões de outras organizações, como MPOG e Presidência da República, mas não como obrigações, e sim como sugestões que podem ser seguidas ou não. Assim, as pressões coercitivas sofridas pela subunidade não são assim percebidas.

Pressões miméticas foram também identificadas na entrevista: "Em conversas com outras unidades, a gente tem notícias de itens, de medidas de Segurança da Informação, e outras coisas também que são seguidas." (ENTREVISTADO 17). Mas o fato de outra subunidade não adotar determinada medida é também percebido como uma pressão para que a sua subunidade não adote, ou mesmo deixe de adotar: "E o contrário também acontece. 'Aqui a gente segue, e vocês lá não estão fazendo?' [...] Não é que desobrigue, mas você fica achando que é só você que está atendendo às normas." (ENTREVISTADO 17).

O comportamento característico da Subunidade 17 frente às pressões institucionais é a aquiescência. Os dados revelaram que a subunidade adotou medidas técnicas de todos os tipos e algumas medidas formais e informais. Mas, apesar de a maioria das medidas previstas nos regulamentos da organização ter sido adotada pela subunidade, eles são constantemente alvo de questionamentos dos membros da diretoria ou do colegiado que toma decisões estratégicas na subunidade, o que dificulta a adoção principalmente de medidas formais, mas também técnicas.

Devido ao julgamento que a direção da subunidade faz das medidas de Segurança da Informação, respostas estratégicas dos cinco tipos apresentados por Oliver (1991) foram identificadas. A resposta de esquiva foi identificada no trecho da entrevista em que o coordenador de TI da subunidade admite que o Comitê de Segurança da Informação da subunidade não tem mais se reunido e que a última demanda analisada, que resultou em uma revisão do regulamento de correio eletrônico da subunidade em 2014, não foi ainda aprovada

pela direção. Os fatos de o subcomitê ainda existir, mas não receber mais nenhuma demanda, e de o resultado de seu último trabalho não ter sequer sido apreciado pela direção da subunidade caracterizam uma resposta estratégica de esquiva e a utilização da tática de ocultação.

O responsável pela TI da Subunidade 17 relatou também uma resposta estratégica de manipulação por parte da subunidade. Segundo ele, por não concordar com uma medida prevista na Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d), regulamento que trata do uso de correio eletrônico na FIOCRUZ, a direção da subunidade entrou em contato diretamente com a Presidência da organização solicitando a suspensão da medida sob a alegação de que prejudica as atividades de pesquisa. A medida em questão é o bloqueio de caixas postais de ex-usuários dos sistemas de correio eletrônico da organização. Neste caso, a resposta de manipulação se deu através da tática de influência. A possibilidade de influenciar a administração central da organização como fonte de pressão institucional é admitida pelo entrevistado: "Existe agora um fórum das unidades regionais, e um dos itens que eles vêm discutindo é Segurança [da Informação]. [...] E nossa unidade tem um representante, que é o Vice-Diretor de Gestão [e Desenvolvimento Institucional]. De alguma forma, o que esse fórum define tem força para ser adotado para a FIOCRUZ como um todo." Cabe registrar que não existe qualquer referência ao fórum citado pelo entrevistado nos documentos analisados.

Embora tenham sido identificadas diferentes estratégias, a resposta predominante da organização às pressões para adotar medidas de Segurança da Informação é a aquiescência, que teve oito referências de codificação identificadas, sendo o hábito, com quatro referências identificadas uma das táticas mais recorrentes. A resposta de desafio, no entanto, foi a que apresentou maior cobertura de percentual, com 8,92%, cuja tática que apresentou maior cobertura foi a contestação, com 3,54%. A título de comparação, a aquiescência apresentou 8,11% de cobertura de percentual, e sua tática com maior cobertura foi o hábito, com 3,94%.

A resposta estratégica de contestação foi identificada mesmo para medidas técnicas já implantadas. Segundo o Entrevistado 17, a direção contestou o controle de acesso de dispositivos móveis particulares à rede sem fio e o impedimento do acesso aos dados armazenados nos servidores da rede de computadores através desses mesmos dispositivos particulares, medidas previstas na Norma Institucional SIC-009/CGTI/VPGDI (FIOCRUZ, 2013g), alegando que prejudicam o trabalho na subunidade, o que levou o coordenador de TI da subunidade a realizar apresentações para os membros da direção e do colegiado que toma

decisões estratégicas para explicar as motivações técnicas e regulamentares para a adoção dessas medidas.

O entrevistado esclarece também que houve questionamentos da Subunidade 17 também quanto à padronização dos endereços e das caixas postais de correio eletrônico, medida prevista na Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d) e no regulamento local que trata do assunto, sob o argumento de que prejudicam as atividades de pesquisa. Este comportamento também configura uma resposta estratégica de desafio através da tática de contestação.

O Entrevistado 17 relatou mais uma resposta estratégica de desafio utilizando a tática de contestação: "Já tentaram colocar os servidores das unidades no *datacenter* da FIOCRUZ, mas [nome do Vice-Diretor de Gestão] foi contra isso e esse posicionamento da Presidência [da FIOCRUZ] não foi adiante."

Apesar de a contestação ser a tática de desafio mais comum nas respostas do Entrevistado 17, uma resposta clara de desafio através de rejeição identificada na entrevista foi a utilização de sistemas de correio eletrônico particulares para fins de trabalho. Esta medida, prevista na Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d), não foi adotada porque, segundo o entrevistado, diversos usuários, inclusive membros da direção da subunidade, não respeitam o regulamento: "Já tentamos proibir o uso de sistemas de *email* privados para armazenar mensagens daqui, mas isso sempre foi motivo de críticas. Não conseguimos. Aqui, isso não é respeitado." (ENTREVISTADO 17). Com isso, a pesquisa evidenciou que houve uma resposta de desafio através da rejeição a uma pressão coercitiva da administração central da organização – no caso, rejeição a um regulamento organizacional cujo cumprimento é obrigatório.

A análise dos dados de cada subunidade como parte de um caso maior permitiu a codificação de trechos das entrevistas e documentos no *software* NVivo de forma que fosse possível identificar as pressões institucionais que a administração central da organização e suas subunidades sofrem, as medidas de Segurança da Informação adotadas por cada uma das subunidades em decorrência dessas pressões institucionais, como elas respondem a essas pressões institucionais e como as respostas influenciam a conformidade da organização com os requisitos externos de Segurança da Informação. A seção seguinte apresenta o resultado da codificação dos trechos na estrutura de nós e subnós criada no *software* NVivo.

6.4 RESULTADO DA CODIFICAÇÃO DOS DADOS NO NVIVO

A partir dos construtos e indicadores da pesquisa, foi criada a hierarquia de nós e subnós no *software* NVivo. Os indicadores permitiram identificar os trechos nos documentos e transcrições das entrevistas, as quais foram codificadas nos subnós.

No nó “Pressões institucionais”, a análise dos dados permitiu identificar os subnós “Adoção de tecnologias pela administração central”, “Realização de auditorias”, “Recomendações de Segurança da Informação”, “Treinamentos”, “Modelos e normas técnicas”, “Notificação de incidentes” e o “Mimetismo”. Assim, somando estes com os subnós já existentes “Programas de conscientização”, “Regulamentos de Segurança da Informação” e “Política de Segurança da Informação”, ficaram dez subnós dentro de “Pressões institucionais”, no qual foram identificadas 161 referências no total. Os destaques foram “Regulamentos de Segurança da Informação”, com 35 referências de codificação, e “Adoção de tecnologias pela administração central”, com 31.

A maioria dos nós referentes às respostas estratégicas manteve os mesmos subnós criados inicialmente: “Aquiescência”, com “Hábito”, “Imitação” e “Conformidade”; “Compromisso”, com “Equilíbrio”, “Pacificação” e “Barganha”; o nó “Esquiva” permaneceu com “Ocultação”, “Amortecimento” e “Fuga”; o nó “Manipulação” ficou com “Cooptação”, “Influência e “Controle”. O nó “Desafio”, que tinha originalmente “Rejeição”, “Contestação” e “Ataque”, teve o acréscimo de “Reconhecimento”. O nó “Aquiescência” teve 106 referências de codificação, “Compromisso” teve 67 referências, “Esquiva” teve 34, “Desafio” apresentou 108 referências identificadas, e “Manipulação” teve 27 referências.

O nó “Adoção de medidas de Segurança da Informação” ficou com 167 referências de codificação identificadas nos seus subnós originais: “Medidas técnicas adotadas”, “Medidas formais adotadas” e “Medidas informais adotadas”.

O nó “Níveis de conformidade”, com 355 referências, também manteve os cinco subnós originalmente criados: “Ocorrência de respostas distintas”, “Tratamentos distintos às pressões para medidas técnicas, formais e informais”, “Adoção de medidas contrárias aos objetivos e interesses da sede”, “Ocorrência de alterações em regulamentos e na Política de Segurança da Informação”, e “Ocorrência de respostas de conformidade” (Tabela 1).

Tabela 1 – Quantidade de referências codificadas nos subnós do NVivo.

NÓS	SUBNÓS	REFER.
Pressões institucionais	Programas de conscientização	11
	Regulamentos de Segurança da Informação	35
	Política de Segurança da Informação	27
	Adoção de tecnologias pela administração central	31
	Realização de auditorias	26
	Recomendações de Segurança da Informação	15
	Treinamentos	7
	Modelos e normas técnicas	3
	Notificação de incidentes	3
	Mimetismo	2
Aquiescência	Hábito	25
	Imitação	22
	Conformidade	59
Compromisso	Equilíbrio	13
	Pacificação	22
	Barganha	32
Esquiva	Ocultação	19
	Amortecimento	12
	Fuga	3
Desafio	**Reconhecimento**	5
	Rejeição	69
	Contestação	29
	Ataque	5
Manipulação	Cooptação	0
	Influência	9
	Controle	0
Adoção de medidas de Segurança da Informação	Medidas técnicas adotadas	90
	Medidas formais adotadas	44
	Medidas informais adotadas	36
Níveis de conformidade	Ocorrência de respostas distintas	141
	Tratamentos distintos às pressões para medidas técnicas, formais e informais	106
	Adoção de medidas contrárias aos objetivos e interesses da sede	71
	Ocorrência de alterações em regulamentos e na Política de Segurança	7
	Ocorrência de respostas de conformidade	30

Notas: Os nós em negrito emergiram na pesquisa. A tática de reconhecimento não consta na tipologia original de Oliver (1991).
Fonte: Elaborado pelo autor a partir do *software* NVivo 10.

A codificação dos dados foi a forma utilizada para identificar as pressões institucionais para adoção de medidas de Segurança da Informação, que serão tratadas a seguir.

6.5 PRESSÕES PARA ADOÇÃO DE MEDIDAS DE SEGURANÇA

A análise dos documentos e entrevistas evidenciou que a Política, as estruturas organizacionais e uma grande parte dos regulamentos da FIOCRUZ foram criadas porque a organização foi pressionada por órgãos governamentais que fiscalizam suas atividades. O Entrevistado 15, por exemplo, esclarece que "A Política de Segurança criada pela CGTI é fruto de indicações de órgãos externos". O Entrevistado 18 deixou claro que não só a formalização da Política, mas também a criação do Comitê e a designação do Gestor de Segurança da Informação da FIOCRUZ aconteceram em decorrência de cobranças dos órgãos de fiscalização do Governo.

O Entrevistado 16 concorda que a administração central adota medidas para atender a pressões externas, mas acrescenta que a Política de Segurança da Informação da organização é também uma forma de pressionar as subunidades: "A POSIC [...] diz um monte de coisas, o que acaba sendo uma forma de pressão. O governo, que tem publicado uma porção de normas, também faz pressão sobre a gente [as subunidades] [...]. Aí a CGTI corre para atender, faz suas normas e publica." (ENTREVISTADO 16). Esta percepção está de acordo com o entendimento de Boschman (2006), segundo o qual tanto a administração central quanto as subunidades são pressionadas pelo ambiente. Está de acordo também com o entendimento de Holland *et al*. (1994), Teo, Wei e Benbasat (2003) e Osmundsen (2005), segundo os quais as subunidades são pressionadas pela administração central da organização através de políticas e regulamentos para que se comportem conforme seus interesses.

Alguns entrevistados entendem que suas subunidades são pressionadas pela administração central da FIOCRUZ e também por outras organizações. No entanto, a maioria percebe somente as pressões da própria organização, como o Entrevistado 09, que admite que "[...] a pressão vem mesmo da FIOCRUZ, da CGTI. Tem o Comitê de Segurança da Informação lá, que discute os temas e faz as normas internas." As subunidades são pressionadas pela administração central através de diferentes mecanismos. A Política de Segurança da Informação (FIOCRUZ, 2011a), os regulamentos e as portarias que definem como a organização deve formalizar e organizar a Segurança da Informação são instrumentos através dos quais a administração central exerce pressão coercitiva sobre as subunidades, conforme a literatura (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003).

A Política e os regulamentos de Segurança da Informação foram apontados como fontes de pressão da administração central por 14 informantes. O Entrevistado 09 exemplifica esse entendimento: "Essas normas [regulamentos de Segurança da Informação] passam a compor a Política de Segurança da Informação da FIOCRUZ. Então é uma pressão que a gente sofre para seguir essas normas e a Política." Já o Entrevistado 10 entende que "A CGTI tem que ditar as regras, de uma forma abrangente [...] porque a FIOCRUZ tem vários focos, cada unidade tem sua infraestrutura, seus recursos, mas tem que ditar, sim, a forma como as unidades devem agir. Mas de forma abrangente, para todas as unidades." Este entrevistado complementa com o seguinte: "Eu acho que se tem uma determinação, é preciso ser cumprida. Deve ser útil. Então é preciso entender o porquê daquela determinação. Então, depois tentar implementar, seja uma ferramenta, seja um sistema, seja um processo." (ENTREVISTADO 10). Sobre as pressões que a administração central exerce sobre as subunidades, o Entrevistado 08 afirmou o seguinte:

> Nos últimos dois anos, o pessoal da presidência da FIOCRUZ pressionou bastante a gente. O pessoal da CGTI que está dedicado à Segurança [da Informação] foi o que pressionou bastante a gente para aderir pelo menos às normas que estavam padronizadas pelo Comitê de Segurança [da Informação]. Então, nos últimos dois anos a gente sofreu uma pressão deles para se adequar a essas normas, até porque eles entenderam que a gente faz algumas coisas que são importantes para toda a FIOCRUZ, então a gente teria que estar mais adequado, tinha que seguir essas normas por causa disso. Então a gente teve uma pressão sim nos últimos dois anos por causa disso. Nessa pressão deles [da CGTI], a gente acabou tomando algumas atitudes, como a migração para a sala cofre [o *datacenter* da FIOCRUZ], campanhas de conscientização voltada para os usuários, classificação de informações nossas. Algumas coisas que a gente teve que fazer por pressão deles. (ENTREVISTADO 08).

Entre as medidas informais, foram relatados eventos de conscientização e divulgação, tanto por iniciativa do Escritório de Segurança da Informação para divulgar a Política da organização, como também demandas dos responsáveis pela Segurança da Informação das subunidades, como deixou claro o Entrevistado 03: "Chamei o [Gestor de Segurança da Informação da FIOCRUZ] para ministrar algumas palestras. Tivemos dois dias de palestras focadas, voltadas para Segurança da Informação." O Entrevistado 08 explicou que as ações de conscientização aconteceram em virtude de um processo incremental, que começa com ações voltadas para os profissionais e gestores de TI das subunidades e, em um segundo momento, voltadas para os usuários:

> O pessoal do [Gestor de Segurança da Informação da FIOCRUZ] conscientizou a gente que a gente teria que treinar nossos usuários. Foi por isso que a gente acabou fazendo. Os primeiros foram em parceria com eles. Eles vieram no [nome da subunidade] para

> fazer essa divulgação, fazer essa conscientização, e depois a gente começou a fazer por conta própria. (ENTREVISTADO 08).

Informar às pessoas as razões pelas quais medidas de Segurança da Informação são adotadas é um aspecto importante para que elas sejam compreendidas e respeitadas, segundo Björck (2005) e Ellwanger (2009). O fato de o foco inicial dessas ações ter sido gestores e profissionais de TI pode explicar o porquê de as medidas informais serem adotadas sob demanda, uma vez que os entrevistados afirmaram que elas vêm sendo mais voltadas para os usuários de TI das subunidades atualmente. O Entrevistado 01 também relatou a ocorrência desses eventos com a participação do Gestor de Segurança da Informação da FIOCRUZ na sua subunidade.

A implantação do antivírus corporativo foi motivo para um treinamento oferecido pela CGTI para os profissionais de TI das subunidades. O Entrevistado 03, o Entrevistado 06, o Entrevistado 08 e o Entrevistado 10 afirmaram ter participado desses cursos e o Entrevistado 12 afirmou que participou de cursos promovidos por outras organizações. Segundo o Entrevistado 07 e o Entrevistado 05, houve treinamentos, mas eles não puderam participar. Segundo Cavusoglu *et al*. (2015), ações de capacitação de profissionais de TI, como o treinamento promovido pela CGTI, estão associadas a pressões normativas do ambiente institucional, e de acordo com Albuquerque Junior *et al*. (2016), são as medidas informais mais comuns. No entanto, apenas sete entrevistados relataram a ocorrência de treinamentos nas suas subunidades.

As entrevistas mostraram que, além das ações de treinamento e conscientização e da divulgação da Política e dos regulamentos de Segurança da Informação, as subunidades sofrem pressões também por meio de recomendações de Segurança da Informação, que têm caráter informativo e são voltadas para gestores e profissionais de TI. As recomendações têm cunho técnico, são baseadas no conhecimento dos profissionais de TI e foram citadas por seis entrevistados como mecanismos de pressão, mas não geram obrigações para as subunidades.

As pressões normativas que se apresentam como modelos de boas práticas adotados por diversas organizações foram observadas em três entrevistas. O Entrevistado 03 afirmou que a adoção de medidas de Segurança da Informação em sua subunidade se baseia também nas normas de Segurança da Informação da ISO, no modelo *Control Objectives for Information and Related Technology* (COBIT) e na biblioteca *Information Technology Infrastructure Library* (ITIL). As medidas da Subunidade 16 foram também baseadas nas

normas ISO e no COBIT. Já o Entrevistado 14 afirmou que as medidas adotadas na sua subunidade são baseadas na norma NBR ISO/IEC 27001.

Outro elemento que emergiu das entrevistas como meio de pressão por parte da administração central foi a realização de auditorias internas. As auditorias são apontadas como fontes de pressão coercitiva por Hu, Hart e Cooke (2007) e Spears, Barki e Barton (2013) e a pesquisa documental permitiu analisar dois relatórios publicados em 2014 e 2015, cujos questionamentos abordavam também a adoção de medidas de Segurança da Informação pelas subunidades..

Nesse sentido, além dos regulamentos do Governo e da FIOCRUZ, o Entrevistado 16 citou as auditorias como pressões sofridas por sua subunidade. Da mesma forma, o Entrevistado 04 afirmou em duas oportunidades que medidas de controle de acesso são objeto de auditorias e que, por isso, precisam ser adotadas. Já o Entrevistado 05 admite que as auditorias trazem oportunidades para realizar ajustes na subunidade no sentido de adotar medidas que ainda não haviam sido adotadas ou realizar alterações naquelas já adotadas. O responsável pela TI da Subunidade 07 informou que ainda não passou por auditorias, mas concorda que a realização daria oportunidade para que ajustes fossem feitos.

Segundo o Entrevistado 10, sua subunidade é alvo constante de auditorias externas, e se as medidas que são auditadas não estiverem implementadas, a realização de acordos entre sua subunidade e outras organizações podem não acontecer ou podem ficar com pendências. As auditorias e a conformidade têm, portanto, um impacto direto sobre as atividades da sua subunidade, de acordo com o entrevistado.

Em sentido oposto, o Entrevistado 08 afirmou que sua subunidade sofreu auditorias e que não estava em conformidade com vários itens, mas acrescentou que “como não teve punição, acabou que ficou por isso mesmo. O fato de não ter uma punição não está forçando as unidades a adotarem.” O Entrevistado 09 afirmou também que sua subunidade já sofreu duas auditorias, mas que “não tem nenhuma punição para que não está conforme.” O Entrevistado 17, por sua vez, acrescentou que as auditorias questionam a conformidade com os regulamentos, mas que, devido à autonomia das subunidades, não há cobrança quanto à existência de uma infraestrutura mínima, o que prejudica a conformidade. As auditorias foram apontadas por 11 entrevistados como pressões institucionais, e foram identificadas 26 referências de codificação para esta pressão institucional.

Independentemente da importância das auditorias como meio de exercer pressão e dos seus efeitos sobre a adoção de medidas de Segurança da Informação pelas subunidades, um dos entrevistados, membro do Comitê de Segurança da Informação da FIOCRUZ, esclareceu que a AUDIN vem realizando auditorias internas nas subunidades, mas que o Comitê precisa ainda ter mais informações sobre a eficiência das medidas adotadas em função dos regulamentos existentes, o que está fora do escopo das auditorias realizadas.

Além de auditorias, a CGTI tem pressionado as subunidades ainda através de notificações de ocorrência de incidentes, como acrescenta o Entrevistado 18. Como membro do Comitê de Segurança da Informação, ele informou que os responsáveis pela TI nas subunidades são notificadas quando algum incidente é detectado pela CGTI e nenhuma providência é tomada. A Política e todos os regulamentos de Segurança da Informação determinam também que as subunidades precisam comunicar à CGTI a ocorrência de incidentes. Em ambos os casos, pode-se considerar que essa notificação é uma forma de a CGTI exercer pressão sobre as subunidades. Apenas o entrevistado da Subunidade 16 admitiu que a administração central pressiona através de notificações de incidentes.

Tecnologias implantadas pela administração central também pressionam as subunidades. De acordo com o Entrevistado 16, "Se a FIOCRUZ tem um sistema novo, ou implanta uma tecnologia nova, é normal ela forçar a gente [as subunidades] a ficar em conformidade." O Entrevistado 09 concorda: "Tem algumas coisas que a CGTI adota, como padrões de ativos de rede e antivírus, que acabam direcionando as unidades. [...] Se os sistemas que a gente usa têm exigências de Segurança da Informação, a gente é obrigado a cumprir." Da mesma forma entende Entrevistado 17: "Se o serviço for disponibilizado pela sede, a gente tem que seguir as normas de Segurança [da Informação] da sede."

O uso de sistemas de informações e de outras soluções tecnológicas da FIOCRUZ e do Governo Federal é obrigatório e exige a adoção de medidas como utilização de certificados digitais, o antivírus e o controle de acesso, como citam os informantes da Subunidade 16 e da Subunidade 17. A utilização do serviço de diretórios da CGTI para controle de acesso lógico também resulta em obrigações e mudanças no gerenciamento de senhas das subunidades, como relatou o Entrevistado 12.

Nesse mesmo sentido, a aquisição de uma solução de antivírus com gestão centralizada na CGTI permite o monitoramento constante das subunidades. Oito entrevistados informaram que utilizam o antivírus da FIOCRUZ, que é uma forma de implantar uma

proteção contra códigos maliciosos em toda a organização, mas o gerenciamento centralizado retira das subunidades a capacidade de gerenciamento do antivírus e a capacidade de reação no caso de ocorrência de incidentes, como observou o Entrevistado 11.

O Entrevistado 06 relatou que a administração central configurou regras de controle de acesso no *firewall* do *campus* da sede, mas as limitações de acesso a determinados serviços na Internet decorrentes dessas regras deveriam ser configuradas nos *firewalls* das subunidades, conforme suas necessidades. A inclusão das regras, no entendimento do entrevistado, é uma imposição para todas as subunidades que estão localizadas no *campus* da sede. Essa pressão também foi relatada pelo Entrevistado 08, que informou que sua subunidade sofreu restrições em decorrência das medidas adotadas pela CGTI.

Além do *firewall* e do antivírus, diversas subunidades utilizam o sistema de correio eletrônico da FIOCRUZ, o que faz com que aceitem as imposições tecnológicas da administração central, como regras e critérios de anti-spam, critérios de senhas complexas, trocas periódicas de senhas e restrições quanto ao uso de alguns sistemas para acesso ao correio eletrônico. De acordo com o Entrevistado 17, se a subunidade quiser utilizar a solução de correio eletrônico da CGTI, "tem que se adequar às regras dela."

O processo de implantação do *datacenter* fez com que a Presidência da FIOCRUZ tomasse atitudes que levaram algumas subunidades a reagirem negativamente. Alguns entrevistados relatam que houve uma tentativa de impedir que as subunidades adquirissem equipamentos de rede como forma de obrigar as subunidades a hospedar seus serviços e sistemas de informação no *datacenter*. O Entrevistado 11 afirmou: "A gente teve uma pressão forte aqui da CGTI para migrar as coisas lá para o *datacenter*. Eles fizeram o *datacenter*, gastaram uma fortuna, e queriam que a gente, e não só a gente, mas todas as unidades colocassem as coisas, os servidores [da rede de computadores] lá."

O coordenador de TI da Subunidade 16 citou o *datacenter* também como uma tecnologia da administração central que exige a adoção de diversas outras medidas pelas subunidades: "Tem a sala cofre, que ela [a FIOCRUZ] investiu [...] para construir. Então, para colocar nossos servidores lá, é preciso fazer umas coisas. Quem está distante vai ter de implantar VPN, *link* dedicado, ou algum tipo de acesso remoto mais seguro."

Apesar de a maioria das subunidades ter desafiado as pressões para hospedar equipamentos e sistemas no *datacenter*, o Entrevistado 08 afirmou que sua subunidade cedeu às pressões e hospedou seus sistemas na CGTI. De acordo com o Entrevistado 14, a CGTI

pressionou as subunidades de forma mais intensa inicialmente e as decisões eram tomadas sem consultar as subunidades, o que pode explicar a rejeição. O Entrevistado 09 entende que hospedar serviços de TI no *datacenter* não beneficiaria sua subunidade, mas admite que "Se não fosse o *datacenter*, [...] muitas unidades não teriam onde armazenar seus servidores com segurança, porque é caro manter um ambiente seguro para os servidores de rede."

A adoção de tecnologias pela administração central foi relatada por 12 entrevistados como meio pelo qual a administração central exerce pressão para adotar medidas de Segurança da Informação, totalizando 31 referências codificadas.

Em suma, a administração central da organização pressiona as subunidades através da Política de Segurança da Informação e dos regulamentos publicados, bem como por meio de ações de conscientização e divulgação desses documentos, realização de auditorias internas, publicação e divulgação de recomendações e adoção de tecnologias, como previsto na teoria (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003).

As pressões identificadas são principalmente coercitivas e normativas, embora medidas adotadas por outras subunidades também influenciem a adoção. A pesquisa mostrou ainda que pressões miméticas, normativas e coercitivas de outros constituintes do ambiente institucional também influenciam as subunidades: medidas adotadas por outras organizações, presentes em normas e modelos de boas práticas e tidas como necessárias, e medidas presentes na legislação e cobradas em auditorias realizadas por outras organizações. A Tabela 2 apresenta as pressões institucionais identificadas na pesquisa.

Tabela 2 – Pressões institucionais e quantidade de referências.

TIPO	PRESSÕES	REFERÊNCIAS
Coercitivas	Leis e regulamentos	35
	Adoção de tecnologias pela administração central	31
	Política de Segurança da Informação	27
	Realização de auditorias	26
	Notificações de incidentes de Segurança da Informação nas subunidades	3
Normativas	Publicação de recomendações de Segurança da Informação	15
	Ações de conscientização em Segurança da Informação	11
	Treinamentos em Segurança da Informação	7
	Modelos e normas técnicas de Segurança da Informação	3
	Divulgação da Política e dos regulamentos de Segurança da Informação	1
Miméticas	Medidas adotadas por outras organizações ou subunidades	3

Fonte: Elaborado pelo autor com dados analisados no *software* NVivo 10.

Esses dados mostram que os entrevistados se referiram mais a pressões coercitivas do que a normativas e miméticas, o que pode significar que as obrigações criadas pela Política de Segurança da Informação e pelas leis, regulamentos, padrões tecnológicos, auditorias e notificações de incidentes são mais constantes do que outras pressões externas. Embora parte dos entrevistados admita que as subunidades são obrigadas a adotar as medidas previstas nos regulamentos e na Política de Segurança da Informação da organização, as entrevistas mostram também que a maioria percebe essas pressões não como obrigação, mas como recomendação. O Entrevistado 16 exprime esta ambiguidade: "A gente viu o que já tinha [medidas já adotadas], o que está *ok* [em conformidade], e então começamos a ver o que era pertinente e adotar o que era possível. Mas adotamos boa parte dos controles que estavam sendo exigidos, ou recomendados."

O Entrevistado 15, por sua vez, deixa claro que percebe os regulamentos e a Política como recomendações, que podem ou não ser seguidas: "Buscamos seguir as recomendações da CGTI, fazendo adaptações para assuntos específicos". De forma semelhante, o Entrevistado 14 também vê os documentos como recomendações: "Eu acho que a Política [de Segurança da Informação] da FIOCRUZ é bem genérica, não fala assim 'você não pode isso'. Ela diz assim: 'recomendamos tal coisa', bem genérica."

No entanto, os regulamentos da organização não deveriam ser entendidos simplesmente como recomendações, visto que a CGTI divulga também Recomendações de Segurança da Informação contendo orientações como descarte de informações, armazenamento de senhas e ataques de *hackers*.

Sobre as pressões coercitivas, o Entrevistado 03 reconhece que os regulamentos de Segurança da Informação influenciam as ações da subunidade, enquanto o Entrevistado 06 admite que as medidas adotadas na sua subunidade foram baseadas nos regulamentos da organização. Além disso, apesar de parte dos entrevistados perceber esses regulamentos como recomendações que não precisam ser seguidas, alguns são percebidos como obrigações, como a hospedagem de equipamentos e sistemas de forma centralizada no *datacenter* da organização, e a tentativa controlar ou mesmo impedir a aquisição de equipamentos para as redes de computadores das subunidades, cujo intuito era trazer para o datacenter os serviços de TI providos pelas subunidades.

Essa percepção dúbia quanto às pressões exercidas pela administração central tem como resultado a pequena quantidade de medidas formais de Segurança da Informação

adotadas pelas subunidades, como pode ser visto no trecho retirado da entrevista com o Entrevistado 19: “São poucas as unidades que têm regras próprias. Isso é muito fácil de ser enxergado quando se trata de manuais e procedimentos em [nome de subunidades que têm regulamentos próprios], pelas especificidades das unidades. Mas esses procedimentos são muito vinculados às normas centrais, às regras gerais.”

Todos os 19 entrevistados declararam considerar eficientes e adequadas muitas das medidas de Segurança da Informação que as subunidades são pressionadas a adotar, mas algumas foram consideradas incoerentes, sendo mais criticadas as que estão relacionadas a *datacenters* na sede e nas subunidades, regras relativas a controle de acesso físico, controle de acesso lógico à Internet e a sistemas de informação e regras de Segurança da Informação para acesso remoto, como mostra a Tabela 3.

Das medidas consideradas incoerentes, duas são informais, sete são formais e 12 são técnicas, conforme a classificação de Dhillon (1999). As medidas são consideradas incoerentes com a realidade das subunidades principalmente por dificultarem as atividades desenvolvidas, por exigirem recursos que não dispõem e por dificultarem as atividades desenvolvidas pelos seus setores de TI.

Os dados evidenciam que sete medidas técnicas são consideradas incoerentes principalmente porque dificultam as atividades desenvolvidas pelas subunidades, cinco são consideradas incoerentes porque exigem que as subunidades tenham recursos que não dispõem e duas porque dificultam as atividades desenvolvidas nos setores de TI das subunidades.

Cinco medidas formais são consideradas incoerentes porque dificultam as atividades desenvolvidas pelas subunidades, duas exigem recursos que as subunidades não têm, enquanto uma é considerada incoerente por ser considerada insegura e também uma prejudica a imagem da subunidade.

Quanto às medidas informais, duas são consideradas incoerentes por exigirem recursos que as subunidades não têm (Figura 8). A influência da disponibilidade de recursos sobre a adoção de medidas de Segurança da Informação foi observada por Hsu, Lee e Straub (2012), enquanto a influência da percepção de que a adoção traria prejuízos para o desenvolvimento das atividades foram observados por Hu, Hart e Cooke (2007) e Kam *et al*. (2013).

Tabela 3 – Medidas consideradas inadequadas para as subunidades.

MEDIDA	MOTIVOS	ENTREVISTADOS
Datacenter centralizado	Dificulta as atividades do setor de TI	8
Controle de acesso físico	Exige recursos que a subunidade não tem	5
	Dificulta as atividades da subunidade	1
Controle de acesso lógico à Internet	Dificulta as atividades da subunidade	5
	Exige recursos que a subunidade não tem	1
Controle de acesso lógico a sistemas de informação	Dificulta as atividades da subunidade	5
Controle de acesso remoto	Dificulta as atividades da subunidade	4
Antivírus com gerenciamento centralizado	Dificulta as atividades do setor de TI	3
Proteção contra incêndio	Exige recursos que a subunidade não tem	3
Atualização de sistemas operacionais	Dificulta as atividades da subunidade	3
Padronização de sistemas operacionais	Exige recursos que a subunidade não tem	2
	Insegurança	1
Padronização de solução de segregação de redes de computadores	Dificulta as atividades da subunidade	2
Comunicação à administração central sobre a ocorrência de incidentes	Prejudica a imagem da subunidade	2
Política de Segurança da Informação da subunidade	Exige recursos que a subunidade não tem	1
	Dificulta as atividades da subunidade	1
Programa de conscientização	Exige recursos que a subunidade não tem	1
Treinamento em Segurança da Informação	Exige recursos que a subunidade não tem	1
Comitê de Segurança da Informação da subunidade	Dificulta as atividades da subunidade	1
Exigência de *login* único para os usuários	Dificulta as atividades da subunidade	1
Controle de acesso à rede sem fio	Exige recursos que a subunidade não tem	1
Proibição do uso de dispositivos móveis particulares na rede de computadores	Dificulta as atividades da subunidade	1
Instalação de antivírus nos computadores	Dificulta as atividades da subunidade	1
Armazenamento de fitas de *backup* em cofres seguros contra incêndio e água	Exige recursos que a subunidade não tem	1
Exigência de senhas complexas para vários sistemas de informação, correio eletrônico e rede de computadores	Dificulta as atividades da subunidade	1

Nota: O campo entrevistados mostra quantos informantes manifestaram que as medidas são incoerentes.
Fonte: Elaborado pelo autor com dados analisados no *software* NVivo 10.

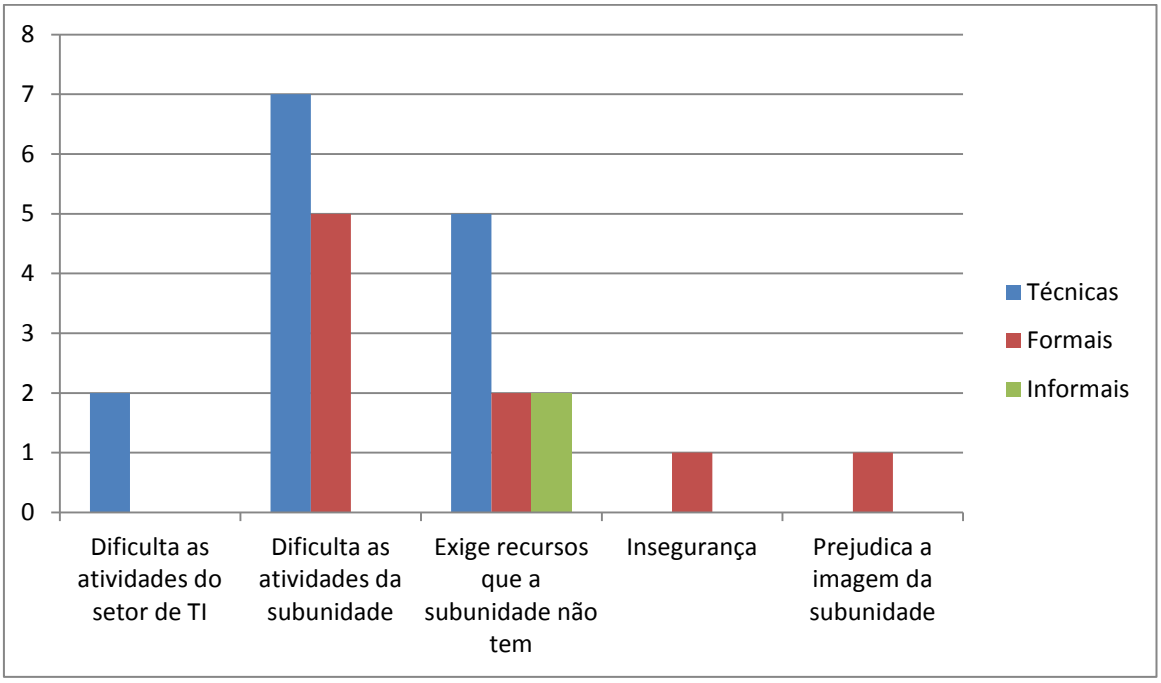


Figura 8 – Motivos pelos quais medidas são consideradas incoerentes.
Fonte: Imagem criada pelo autor a partir de dados da pesquisa.

6.6 ADOÇÃO DE MEDIDAS DE SEGURANÇA PELAS SUBUNIDADES

Os dados mostram que uma das dez categorias de medidas formais não foi identificada em nenhuma das subunidades que participaram da pesquisa: "Sistema de Gestão de Segurança da Informação". Isto significa que nenhuma das subunidades tem um documento que formalize o funcionamento, as estruturas organizacionais e os demais documentos que definem a Segurança da Informação em seu contexto. Embora esteja prevista na literatura (BJÖRCK, 2004, 2005; FARN; LIN; FUNG, 2004; MARTINS; SANTOS, 2005; PARK; JANG; PARK, 2010; SÊMOLA, 2014), essas características não foram identificadas também nas políticas de Segurança da Informação das subunidades.

Apesar de haver previsão na literatura, a existência de um Sistema de Gestão de Segurança da Informação formalizado pela administração central da organização pode justificar a não existência nas subunidades, visto que define como deve ser organizada a Segurança da Informação em toda a organização, incluindo estruturas organizacionais, mecanismos de elaboração e revisão e a formalização de políticas e regulamentos em todas as subunidades. No entanto, a formalização de sistemas de gestão de Segurança da Informação

nas subunidades, desde que alinhados ao Sistema de Gestão organizacional, permite organizar a Segurança da Informação considerando necessidades e características locais.

A maioria das medidas formais também tem pouca adesão das subunidades. O "Escritório de Segurança da Informação", a "Classificação de informações" e a "Revisão periódica da Política de Segurança da Informação" são adotadas por apenas uma subunidade cada. De forma semelhante, apenas duas subunidades declararam ter uma "Política de Segurança da Informação" e "Processo de Análise e Avaliação de Riscos", três têm "Comitê de Segurança da Informação" e "Equipe de tratamento de incidentes de Segurança da Informação".

É discutível a necessidade de cada subunidade ter uma Política de Segurança da Informação própria que precisa ser revisada periodicamente, mas a existência de um subcomitê de Segurança da Informação local, como propõem Sêmola (2014) e Manoel (2014) e como previsto na Portaria 070/2011-PR da Presidência da FIOCRUZ (FIOCRUZ, 2011b), pode fazer com que as decisões de Segurança da Informação das subunidades sejam tomadas de forma equilibrada, sem um viés técnico e considerando a diversidade de profissionais, áreas de atuação e necessidades internas. Além disso, o Comitê pode também elaborar regulamentos internos que complementam a Política local ou mesmo a corporativa, cobrindo lacunas e situações específicas das subunidades.

O Escritório de Segurança da Informação, por sua vez, tem um foco na gestão da Segurança da Informação e atua monitorando indicadores e avaliando a conformidade da subunidade com os regulamentos da organização e outros requisitos externos (CASEY, 2005; MARTIN; KHAZANCHI, 2006; MANOEL, 2014; SÊMOLA, 2014). A existência de processos de classificação da informação e de análise e avaliação de riscos são importantes para todas as subunidades, uma vez que definem quais ativos de informação precisam de proteção e quais são os riscos aos quais estão sujeitos, permitindo a adoção de medidas adequadas (MARTINS; SANTOS, 2005; SÊMOLA, 2014).

Embora o Comitê e a Política de Segurança da Informação sejam também medidas necessárias para as subunidades, ambas as medidas foram adotadas pela administração central da organização, o que pode explicar o fato de poucas subunidades as terem adotado. Sobre isso, seis entrevistados declararam que suas subunidades não têm políticas nem subcomitês porque ambos já existem na FIOCRUZ. O Escritório de Segurança da Informação é também uma estrutura organizacional prevista na literatura (CASEY, 2005;

MARTINS; SANTOS, 2005; MARTIN; KHAZANCHI, 2006; MANOEL, 2014; SÊMOLA, 2014). Devido aos fatos de as subunidades terem grande autonomia administrativa, equipes e recursos de TI próprios, armazenarem informações sensíveis e estarem, em alguns casos, distantes da administração central da organização, a criação de escritórios de Segurança da Informação pode favorecer a conformidade com os requisitos externos, motivo pelo qual sua criação nas subunidades está prevista em um regulamento organizacional (FIOCRUZ, 2011b), mas a maioria das subunidades não tem em sua estrutura organizacional. O mesmo se aplica a outras medidas formais, como "Classificação de informações", "Comitê de Segurança da Informação" e "Processos de análise e avaliação de riscos" e "Equipe de tratamento de incidentes de Segurança da Informação", algumas das quais são requisitos para a adoção de outras medidas de Segurança da Informação.

A "Equipe de Tratamento de Incidentes de Segurança da Informação" é uma medida formal prevista pela ABNT (2013) e abordada na literatura científica (KILLCRECE *et al*., 2003; MANDIA; PROSISE; PEPE, 2003; ALEXANDRIA, 2009) que permite que a organização dê o tratamento e a priorização adequados aos incidentes. De acordo o regulamento do Governo brasileiro que trata do assunto (BRASIL, 2009b), as organizações com estrutura descentralizada podem criar equipes de tratamento de incidentes também de forma descentralizada, atendendo às necessidades locais das subunidades de organizações como a FIOCRUZ, o que faz sentido quando as subunidades gozam de grande autonomia administrativa e são geograficamente descentralizadas.

Os "Regulamentos internos de Segurança da Informação" e os "Processos e procedimentos de Segurança da Informação" estão previstos na literatura (FONTES, 2006) e são medidas formais adotadas respectivamente por oito e onze subunidades. Regulamentos e processos de Segurança da Informação devem ser orientados por uma Política e um Sistema de Gestão de Segurança da Informação (FORCHT; AYERS, 2001), mas o fato de não haver políticas na maioria e sistemas de gestão em nenhuma das subunidades não impede a adoção dessas medidas por todas elas, visto que a organização tem sua Política e seu Sistema de Gestão corporativos, que definem regras e estruturas para toda a organização.

As medidas técnicas são mais difundidas pelas subunidades do que as formais. Todas as subunidades adotam medidas de "Redundância de dados", "Segregação e monitoramento de redes de computadores", "Prevenção contra códigos maliciosos" e "Controle de acesso lógico". Apesar de medidas técnicas de "Prevenção contra códigos maliciosos" serem adotadas por todas as subunidades, a única tecnologia identificada em

todas elas que caracteriza a adoção dessas medidas é o antivírus. Medidas de "Proteção ambiental" são adotadas por 15 subunidades, sendo o *no-break* a solução mais comum. Medidas de "Autenticação forte" são adotadas por 13 subunidades, que utilizam principalmente senhas complexas. O *firewall*, utilizado por todas as subunidades, é a tecnologia de "Segregação e monitoramento de redes de computadores" mais utilizada, embora VLANs e *proxies* tenham sido identificados nas respostas. As medidas de "Transmissão e armazenamento seguros de dados" são adotadas por 13 subunidades, sendo que a tecnologia mais comum é a criptografia para acesso a serviços *web*. Medidas de "Redundância de peças de equipamentos" foram identificadas nas respostas de entrevistados de 12 subunidades. Já medidas de "Redundância de equipamentos" e "Controle de acesso físico" foram adotadas por 10 subunidades. O fato de essas medidas serem mais adotadas do que as formais pode ser explicado pelo Entrevistado 09: "Aqui já tinha várias coisas, principalmente recursos tecnológicos e configurações que a gente já fazia." Outros entrevistados corroboram com essa explicação:

> Mesmo antes de a gente ter qualquer tipo de política, a gente já tinha *firewall*, a gente já tinha algumas coisas adotadas. Mas eu acredito que adotou mais seguindo recomendações de boas práticas do mercado. Não tínhamos política, mas a gente adotava *firewall*, IPS [*Intrusion Prevention System*], controle de acesso, esse tipo de coisa. Acredito que os técnicos adotaram isso aqui mais seguindo recomendações de mercado mesmo, e alguns deles pensavam assim: se todo mundo lá fora faz isso, então a gente tem que fazer também. Acredito que foi mais por esses motivos. (ENTREVISTADO 08).

> Muita coisa foi implementada antes. Muita coisa já existia, mas foi lapidada depois que esses documentos foram elaborados. Quando a gente tem no que se basear, fica mais fácil. Até quando a TI tem algo para se referenciar, fica mais fácil para falar para o usuário que tem de seguir. Tem que agir desse jeito por causa daquele documento, tem que seguir esse procedimento por causa do documento tal. Então sempre tem uma referência para seguir, tanto para quem está prestando atendimento ou implementando um recurso novo, quanto para o usuário final também. (ENTREVISTADO 10).

> Quando a POSIC foi feita, muita coisa já tinha sido adotada, muita coisa já tinha aqui. *Firewall*, *no-break*, *storage*, rotina de *backup*. Essa parte técnica, a gente já tinha muita coisa. [...] Tudo isso [medidas técnicas] está previsto em modelos de boas práticas, na [norma técnicas] ISO 27002. Está também na cabeça de qualquer profissional de TI que tem que ter *firewall*, antivírus, anti-spam, *no-break*, essas coisas. Tudo isso é para atender a requisitos externos. Mesmo não sendo obrigação, é exigência externa. (ENTREVISTADO 11).

Em outras palavras, a adoção de medidas técnicas é realizada pelos profissionais de TI e muitas delas são tidas como certas para esses profissionais. A explicação para isso pode ser o fato de estarem institucionalizadas nas organizações e entre profissionais de TI,

como argumentam Meyer e Rowan (1977) e DiMaggio e Powell (1983), e como mostraram Albuquerque Junior *et al*. (2016).

Cabe registrar que parte dessas medidas tem um impacto grande sobre as organizações, sendo importante a adoção nas suas subunidades para garantir a Segurança da Informação. Como argumenta Larson (2012), há integração e interconexão entre as subunidades, o que pode expor a organização a riscos. A interligação entre as subunidades e a sede da organização através de redes de computadores para compartilhamento de informações e sistemas pode pôr em risco tanto a matriz quanto as subunidades caso uma delas não tenha adotado as medidas de Segurança da Informação necessárias, como proteção contra códigos maliciosos e segregação de redes de computadores, cuja ausência ou funcionamento inadequado pode expor toda a organização a acessos não autorizados e vírus.

Os dados mostram que algumas medidas informais são mais adotadas do que outras, sendo que as ações de "Divulgação de regulamentos e da Política de Segurança da Informação", identificadas nas respostas dos entrevistados de 12 subunidades, e "Ações de conscientização", identificadas em 11 entrevistas, são as mais adotadas. A maioria dos entrevistados informou que não houve iniciativas de capacitação promovidas pelas suas subunidades: apenas quatro subunidades fizeram "Treinamento de profissionais de TI" e três realizaram "Treinamento de usuários de TI". Iniciativas de capacitação não são comuns, mas nove entrevistados consideram importantes as ações de divulgação e conscientização. Essa importância é ressaltada na literatura por diversos autores, uma vez que a finalidade dessas medidas é promover a Segurança da Informação através de mudanças de crenças, atitudes e da cultura organizacional (EMINAGAOGLU; UÇAR; EREN, 2009; SHAW; CHEN; HARRIS, 2009; BULGURCU; CAVUSOGLU; BENBASAT, 2010; ALKALBANI; DENG; KAM, 2015).

A Tabela 4 apresenta a quantidade de subunidades que adota cada tipo de medida de Segurança da Informação. As medidas formais mais comuns são de "Processos e procedimentos de Segurança da Informação", adotadas em 11 subunidades. As medidas técnicas mais adotadas são de "Redundância de dados", "Segregação e monitoramento de redes de computadores", "Prevenção contra códigos maliciosos" e "Controle de acesso lógico", adotadas por todas as subunidades. Já as medidas informais mais adotadas são as ações de "Divulgação de regulamentos e da Política de Segurança da Informação", que foram identificadas em 12 subunidades.

Tabela 4 – Tipos de medidas adotadas e quantidade de subunidades que as adotam.

CATEG.	TIPOS DE MEDIDAS	ADOTANTES	%
Formais	Política de Segurança da Informação	2	11,76
	Comitê de Segurança da Informação	3	17,65
	Regulamentos internos de Segurança da Informação	8	47,06
	Processos e procedimentos de Segurança da Informação	11	64,71
	Equipe de tratamento de incidentes de Segurança da Informação	3	17,65
	Escritório de Segurança da Informação	1	5,88
	Processo de Análise e Avaliação de Riscos	2	11,76
	Classificação de informações	1	5,88
	Sistema de Gestão de Segurança da Informação	0	-
	Revisão periódica da Política de Segurança da Informação	1	5,88
Técnicas	Redundância de dados	17	100,00
	Segregação e monitoramento de redes de computadores	17	100,00
	Redundância de peças de equipamentos	12	70,59
	Prevenção contra códigos maliciosos	17	100,00
	Controle de acesso lógico	17	100,00
	Transmissão e armazenamento seguros de dados	13	76,47
	Autenticação forte	13	76,47
	Redundância de equipamentos	10	58,82
	Controle de acesso físico	10	58,82
	Proteção ambiental	15	88,24
Informais	Treinamento de profissionais de TI	4	23,53
	Treinamento de usuários de TI	3	17,65
	Divulgação de regulamentos e da Política de Segurança da Inform.	12	70,59
	Ações de conscientização	11	64,71

Nota: Informações colhidas com entrevistados da CGTI, por ser a administração central de TI na organização, e a AUDIN, subunidade que não tem um departamento de TI autônomo, não foram consideradas.
Fonte: Dados coletados na pesquisa com base nas categorias propostas por Dhillon (1999).

A pesquisa revelou que houve a adoção de medidas contrárias aos interesses da administração central. O Entrevistado 11 relatou a utilização de tecnologias gratuitas ou baseadas em *software* livre quando a organização tentava padronizar tecnologias proprietárias para toda a organização. De acordo com o entrevistado, a utilização de soluções gratuitas foi motivada pela compreensão de que são mais seguras, mas esta decisão limitou o acesso da subunidade a outras soluções padronizadas pela CGTI: "Teve um contrato da FIOCRUZ com a [fabricante de sistema operacional proprietário] [...]. Se você usa [sistema operacional livre], não tem acesso às soluções de Segurança [da Informação] que são apropriadas para o [sistema operacional proprietário], como o antivírus que eles [a CGTI] adotaram." (ENTREVISTADO 11).

A padronização do uso de *softwares* proprietários pela organização também é criticada pelo Entrevistado 04, enquanto a Subunidade 16 decidiu manter o padrão de *firewall* em uso na sua rede de computadores em detrimento do produto de outro fabricante, que era exigido para ter acesso à Internet, segundo relatou o Entrevistado 16.

Além de não hospedar seus equipamentos no *datacenter* da organização porque o acesso seria lento e prejudicaria as atividades desenvolvidas na subunidade, o Entrevistado 05 relatou que considera o *software* de virtualização de servidores de rede padronizado pela sede e usado no *datacenter* menos seguro do que o que usa na subunidade e que, por este motivo, não vai adotá-lo, contrariando o interesse da administração central de padronizar este tipo de *software*.

Independentemente de haver um regulamento que trata da participação de membros da organização em redes sociais, o Entrevistado 05 relatou que houve o bloqueio desse tipo de serviço na sua subunidade sob o argumento de que pode prejudicar o acesso à Internet e o desenvolvimento de outras atividades. Esta medida de controle de acesso lógico pode ser considerada contrária aos interesses da organização, pois há um incentivo para que profissionais de comunicação utilizem redes sociais para divulgar notícias sobre a organização, ainda que de forma regulada, como previsto na Norma Institucional SIC-008/CGTI/VPGDI (FIOCRUZ, 2013f). O mesmo aconteceu na Subunidade 03 e na Subunidade 07. Estas subunidades adotaram medidas de Segurança da Informação para atender aos seus próprios interesses, em detrimento dos interesses da organização, tanto de padronizar produtos quanto de divulgar suas atividades em redes sociais.

Todos os entrevistados informaram que a maioria das medidas técnicas e todas as medidas formais de suas subunidades foram adotadas antes de os regulamentos e a Política de Segurança da Informação terem sido formalizados pela organização. As medidas informais, por sua vez, foram adotadas depois, em grande parte para divulgar os regulamentos e a Política da organização.

As pressões da administração central da organização são reconhecidas pelos entrevistados, mas a adoção de medidas pelas subunidades foi pouco relacionada às ações de conscientização e divulgação dos regulamentos e da Política de Segurança da Informação da organização. Os regulamentos e a Política também não são percebidos como pressões coercitivas, mas como recomendações. Não sendo percebidas como obrigatórias, a adesão depende do interesse e autonomia das subunidades.

Medidas formais são adotadas visando à conformidade com os requisitos externos, principalmente regulamentos da administração central da organização. Já a adoção de medidas informais acontece com o intuito de mudar o comportamento das pessoas, enquanto medidas técnicas são adotadas para garantir a confidencialidade, integridade e

disponibilidade das informações – em ambos os casos, a intenção é garantir a Segurança da Informação, seja pela conscientização das pessoas, seja por meios técnicos.

De acordo com Anthony, Appari e Johnson (2014), diferentes pressões institucionais sobre diferentes subunidades resultam em diferenças quanto à conformidade com os requisitos de Segurança da Informação. A pesquisa mostrou que pressões miméticas, normativas e coercitivas da administração central, de outras subunidades e de outras organizações incidem sobre as subunidades.

Aliada à percepção diferenciada quanto aos benefícios da adoção das três categorias de medidas, os regulamentos da administração central não são percebidos como obrigatórios, e as pressões de outros constituintes do ambiente institucional não são reconhecidas pelas subunidades. Com isso, as pressões para adoção de medidas formais, medidas informais e medidas técnicas resultam em respostas estratégicas distintas das subunidades.

A próxima seção apresenta as respostas estratégicas das subunidades às pressões institucionais identificadas na pesquisa.

6.7 RESPOSTAS ESTRATÉGICAS DAS SUBUNIDADES ORGANIZACIONAIS

A análise das respostas estratégicas das subunidades às pressões institucionais foi feita com base nas cinco respostas previstas na tipologia de Oliver (1991): aquiescência, compromisso, esquiva, desafio e manipulação.

6.7.1 Aquiescência

A aceitação passiva e consentida dos requisitos institucionais, na tipologia de Oliver (1991), é representada pela resposta estratégica de aquiescência. Como proposta pela autora, esta resposta tem três diferentes táticas: hábito, imitação e conformidade. O hábito é a forma mais inconsciente de aquiescência, de acordo com Oliver (1991), e está relacionado à aceitação de práticas institucionais tidas como certas, conforme DiMaggio e Powell (1983). Assim, entende-se que a adoção de medidas de Segurança da Informação devido a uma

resposta de hábito aconteceu sem que tenha havido uma obrigação legal ou regulatória, ou sem a consciência de que sua adoção traz benefícios outros além da confidencialidade, integridade e disponibilidade da informação.

Através do *software* NVivo, foi possível constatar que o hábito foi referido por 16 entrevistados e que 25 referências a esta tática foram identificadas nas transcrições das entrevistas, sendo a Subunidade 13 a única em que não foi constatada a utilização desta tática. A análise dos trechos das entrevistas mostrou que todas as outras responderam em algum momento a pressões institucionais com aquiescência através do hábito, principalmente em se tratando de medidas técnicas. O trecho mais ilustrativo desse comportamento foi retirado da entrevista com o responsável pela TI na Subunidade 02:

> Não sei te dizer o porquê [da subunidade adotar medidas técnicas de Segurança da Informação]. Como a gente é da área de tecnologia, a gente tenta manter os sistemas o mais seguro possível para evitar a indisponibilidade deles. Nesse sentido, a gente procura adotar tudo o que for necessário para seguir nessa linha. A gente, por exemplo, segue a POSIC, a gente segue normas e boas práticas externas, a gente segue as recomendações que a gente recebe de órgãos de auditoria que controlam [o nome da subunidade]. (ENTREVISTADO 02).

A administração central da FIOCRUZ contratou um antivírus corporativo, com gerenciamento distribuído, o que permite delegar às subunidades parte do controle do sistema, mas com centralização de comandos e relatórios na CGTI. Informantes de 11 diferentes subunidades informaram que utilizam a solução corporativa de antivírus da organização. A contratação e implantação da solução de antivírus corporativo pela CGTI foi uma pressão exercida pela administração central, que resultou em respostas de aquiescência dessas subunidades. A tática utilizada, neste caso, foi o hábito, pois o antivírus é uma medida técnica de Segurança da Informação tida como certa, cuja adoção é imprescindível. Neste sentido, o Entrevistado 09 afirmou que "Não dá para ficar sem antivírus", e o Entrevistado 05 tem a mesma percepção ao afirmar que sua subunidade tem que ter antivírus. O Entrevistado 11 explica a razão da necessidade de ter antivírus nas subunidades: "Se muitas unidades são interligadas com a FIOCRUZ, todas têm que ter um antivírus". Este entendimento está de acordo com o que argumentam Larson (2012) e Von Simson (1990) e Bowersox *et al*. (2014), segundo os quais as organizações interligam e integram suas subunidades, aumentando o risco de incidentes ocorridos em uma delas atingirem as outras. Com isso, a implantação de antivírus nas subunidades foi considerada o resultado de uma resposta de aquiescência por

hábito. A consequência é o fato de todas as subunidades terem antivírus, uma medida de "Prevenção contra códigos maliciosos".

Outras soluções tecnológicas são também percebidas como necessidades, cuja adoção é tida como certa. O Entrevistado 11 afirmou: "Não vejo como uma empresa, um órgão público ou uma unidade grande da FIOCRUZ pode existir sem ter um *firewall*, antivírus, *no-breaks* para servidores, controle de acesso lógico."

Este entendimento está de acordo com o fato de muitas das medidas técnicas terem sido adotadas pelos profissionais de TI das subunidades antes de haver um direcionamento tecnológico por parte da administração central ou mesmo os regulamentos e a Política de Segurança da Informação. A adoção de medidas técnicas, na visão do Entrevistado 01, é uma questão de proteger os dados de pesquisa: "Acho que é uma necessidade. Ainda mais que a gente tem vários processos de pesquisa cujos dados podem gerar uma patente." Já o Entrevistado 10 afirma que muitas medidas já existiam antes dos regulamentos de Segurança da Informação da organização. Em outro momento da entrevista, este participante complementou: "os controles são necessários para a sobrevivência da instituição, para garantir que as informações estarão sempre lá e a instituição vai continuar funcionando. Não dá para uma empresa ou instituição pública existir sem Segurança da Informação."

O Entrevistado 09 também tem essa visão sobre as medidas técnicas:

> As medidas mais técnicas foram adotadas porque há um entendimento de que elas são importantes, pois protegem as informações e os equipamentos da instituição. Isso é um consenso entre os profissionais de TI, então por isso elas são adotadas. Tanto que são anteriores às normas da instituição. As ações de conscientização, idem. A gente não faria se não fosse importante, se a gente não achasse que daria algum resultado. (ENTREVISTADO 09).

O trecho acima mostra que o Entrevistado 09 não percebe somente medidas técnicas desta forma, mas também medidas informais de Segurança da Informação. A aquiescência por hábito foi notada ainda na adoção de medidas informais pela Subunidade 08, cujo informante entende que ações de conscientização são necessárias, e que "Sem conscientização, não dá para ter Segurança [da Informação]." (ENTREVISTADO 08).

Não foram identificadas evidências de que a tática de hábito tenha sido utilizada para responder com aquiescência às pressões para adotar medidas formais. Isto pode ser explicado pelo fato de medidas formais terem sido associadas por diferentes entrevistados a pressões coercitivas, que estão mais relacionadas à tática de conformidade. Isto é coerente

com o fato de as medidas formais serem a categoria mais associada pelos entrevistados à conformidade com regulamentos e outros requisitos externos quanto aos benefícios da adoção – sete entrevistados veem a conformidade com esses requisitos como uma vantagem da adoção de medidas formais.

Três subunidades apresentaram quatro referências de codificação para a tática de hábito, sendo as que apresentaram mais referências identificadas: Subunidade 09, Subunidade 10 e Subunidade 17. Em seguida vem a Subunidade 06, com duas referências de codificação. Outras 11 subunidades apresentaram uma referência à tática de hábito. Ao analisar a cobertura de percentual, os dados destacam novamente a Subunidade 09, com 13,79%, seguida da Subunidade 10, com 6,39% (Figura 9). Estes resultados mostram que Subunidade 09, Subunidade 10 e Subunidade 17 foram as que mais aceitaram de forma inconsciente as pressões e adotaram medidas sem julgar sua adequação às necessidades ou os benefícios que podem obter do ambiente institucional.

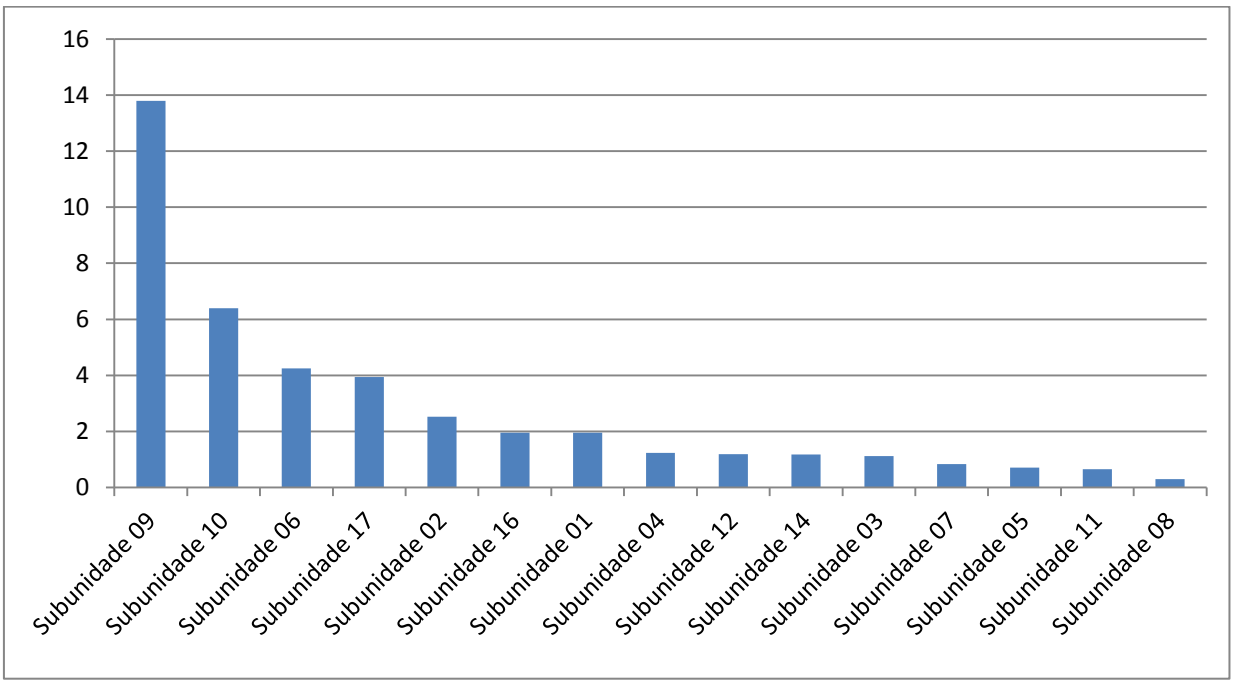


Figura 9 – Cobertura de percentual das subunidades para a tática de hábito.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

A imitação é a segunda tática de aquiescência e, ao contrário do hábito, pode ser ou não resultado de uma ação consciente (OLIVER, 1991). Independentemente de ser consciente ou inconsciente, a utilização da tática de imitação significa que a subunidade

observou medidas de Segurança da Informação em outras organizações ou subunidades consideradas bem sucedidas na sua organização ou no ambiente institucional (ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016). A imitação pode ser através de consultas a regulamentos, políticas ou outros documentos de outras subunidades ou organizações, e da adoção dos mesmos processos, procedimentos e tecnologias.

A tática de imitação foi identificada nas entrevistas com participantes de 14 subunidades, em 22 referências identificadas no NVivo. Segundo o responsável pela TI na Subunidade 01, houve uma pressão mimética sobre a subunidade, quando um membro da direção visitou outra subunidade e viu que havia controle de acesso à rede sem fio. Nas palavras do Entrevistado 01: "O pessoal da [nome de outra subunidade da FIOCRUZ], quando tem algum visitante, fazem todo um cadastro para ter acesso. O próprio Vice-Diretor [da Subunidade 01] já veio conversar com a gente para adotarmos esse tipo de atitude. Mas fui explicando que, na nossa situação atual, não é viável." Apesar de a aquiescência não ter sido a resposta da subunidade, o fato de ter um ambiente computacional estável e seguro torna a subunidade um exemplo para as outras, de acordo com o Entrevistado 01.

Consultas a empresas de TI, outras organizações públicas e subunidades da organização sobre a implantação de medidas de Segurança da Informação foram realizadas pelo Entrevistado 05. Segundo ele, a intenção foi conhecer soluções adotadas e tirar dúvidas sobre a implantação. O responsável pela TI na Subunidade 06 também realiza consultas a outras subunidades, embora esclareça que nem tudo o que é adotado em outros lugares se aplica à realidade da sua subunidade. A imitação aparece ainda na realização de licitações para aquisição de tecnologias de Segurança da Informação, como afirmou o Entrevistado 09, ou na implantação de tecnologias que já tenham sido adotadas pela CGTI, como afirmou o Entrevistado 10.

O Entrevistado 11 citou a imitação de experiências de outras organizações nas quais ele já trabalhou, além da consulta a outras subunidades:

> Eu tenho experiência com Segurança da Informação, então acabo vendo o que aconteceu, como foi feito nos outros lugares que eu trabalhei. Eu trago as boas experiências para cá. Quando a gente sabe que outra unidade está fazendo alguma coisa boa, interessante, a gente tenta entrar em contato, vê como fez, vai lá, conversa, e tenta fazer parecido, ajustando para nossa necessidade. (ENTREVISTADO 11).

A integração do serviço de diretório da Subunidade 12 com o da administração central da organização, um mecanismo utilizado para autenticação de usuários e autorização de acesso, foi motivada pela possibilidade de ter acesso a um serviço chamado Comunidade Acadêmica Federada (CAFE), que havia sido observado por usuários da subunidade em outras organizações, despertando o interesse pela adoção.

Para o Entrevistado 07, o fato de outra subunidade ter adotado determinada medida não é garantia de adoção na sua subunidade, pois vai depender de ações de sensibilização anteriores junto à direção. O Entrevistado 08 exemplifica bem a tática de imitação: "Acredito que os técnicos adotaram isso aqui mais seguindo recomendações de mercado mesmo, e alguns deles pensavam assim: 'se todo mundo lá fora faz isso, então a gente tem que fazer também'. Acredito que foi mais por esses motivos." Outro exemplo da tática de imitação é o do Entrevistado 09, que afirmou já ter viajado para outro estado para conhecer a experiência de outra subunidade, o que resultou na implantação de tecnologias consideradas viáveis para a sua subunidade. Não foram identificados relatos de imitação inconsciente. Os resultados mostram que nem tudo o que foi visto em outras subunidades ou organizações foi imitado e que houve também adaptações do que foi observado para a realidade da subunidade. Cabe registrar que as medidas que foram imitadas eram todas técnicas, segundo os relatos dos entrevistados.

Através do *software* NVivo, foi possível identificar três referências de codificação para a Subunidade 11 e para a Subunidade 16, sendo estas as que apresentaram maior quantidade de referências. Em seguida, com duas referências identificadas, vêm a Subunidade 01, a Subunidade 08, a Subunidade 09 e a Subunidade 17. A maior cobertura de percentual para a tática de imitação foi 3,62%, identificada na Subunidade 08. As outras subunidades que apresentaram maiores percentuais foram a Subunidade 13, com 3,58%, Subunidade 05, com 3,45%, e Subunidade 16, com 3,36% (Figura 10). Os resultados mostram que a imitação de tecnologias adotadas por outras organizações e subunidades é uma realidade dentro da organização.

A terceira tática de aquiescência proposta por Oliver (1991), a conformidade, significa que houve a adoção consciente visando benefícios, como apoio ou recursos obtidos com a conformidade com os requisitos externos, como entendem Pfeffer e Salancik (1978). Sendo uma tática de adoção consciente, é resultado de uma escolha feita pela organização. Há uma compreensão de que a Segurança da Informação é uma questão estratégica e de sobrevivência da organização (HONG *et al.*, 2003; POSTHUMUS; VON SOLMS, 2004;

DOHERTY; FULFORD, 2006; RYAN; RYAN, 2006; HEDSTRÖM *et al*., 2011; WU; SAUNDERS, 2011), mas esta não pode ser a justificativa para considerar que a tática de conformidade foi utilizada, pois não está relacionada à obtenção de benefícios de constituintes do ambiente institucional. Ao invés disso, a tática de conformidade está associada à legitimidade obtida com ela, que é um meio de acesso a recursos externos (POSTHUMUS; VON SOLMS, 2004).

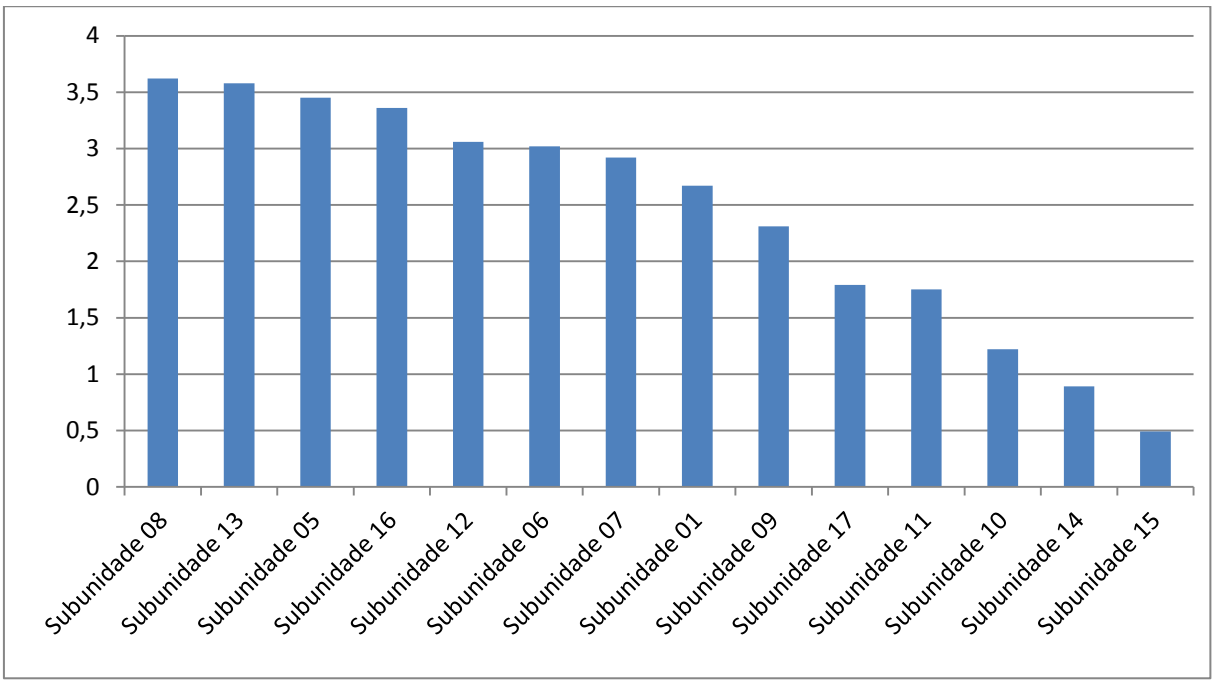


Figura 10 – Cobertura de percentual das subunidades para a tática de imitação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Todas as subunidades responderam a pressões institucionais com aquiescência utilizando a tática de conformidade, totalizando 59 referências de codificação. Na Subunidade 13, a adoção de medidas de Segurança da Informação é reativa, o que caracteriza a intenção de adotar. Segundo o Entrevistado 13, se receber algum regulamento, exigência ou recomendação da administração central, o comportamento da subunidade é de respeitar e adotar as medidas exigidas. Ele complementa que a organização pode ser prejudicada caso não cumpra seus requisitos externos de Segurança da Informação, o que deixa clara a intenção de evitar prejuízos junto ao ambiente institucional.

A adoção através da tática de conformidade foi percebida na entrevista com o Entrevistado 03: “Tem aquela questão: se não entrar em conformidade, se não buscar a

regulamentação própria, você pode ser responsabilizado. Então estou buscando isso para não ferir nenhum tipo de regra recomendada, não somente pela CGTI, mas muito acima dela, pelo DSIC, do Governo Federal." O entrevistado deixa claro que a adoção é uma questão de conformidade e acrescenta ainda a necessidade de adotar medidas formais com esta finalidade.

A adoção de medidas técnicas sem ter como objetivo a garantia da Segurança da Informação, mas a conformidade com requisitos institucionais, foi observada em trechos das entrevistas com três participantes da pesquisa. O Entrevistado 04 declarou: "[A adoção de medidas de Segurança da Informação] É tanto uma questão de necessidade quanto de conformidade. Um pouco dos dois. Tem necessidades técnicas e precisa ter conformidade." Em outro trecho da entrevista, ele complementa: "A gente trabalha com dados sensíveis. Precisa ter esse tipo de controle [medidas técnicas de Segurança da Informação]. São dados de pesquisas, dados de pacientes." (ENTREVISTADO 04).

O antivírus é visto pelos entrevistados como uma necessidade, mas a aquisição pela CGTI a um custo abaixo do praticado no mercado foi percebida como vantajosa para pelo menos uma subunidade: o Entrevistado 17 afirmou que a subunidade já tinha uma solução de antivírus, mas a renovação do contrato teria um custo alto, o que levou a aderir ao contrato capitaneado pela administração central da organização. Ou seja, a adoção do antivírus na Subunidade 17 foi resultado de uma resposta de aquiescência por conformidade, pois foi uma decisão consciente, tendo em vista benefícios para a subunidade. O Entrevistado 09, que também entende que o antivírus é uma necessidade, admitiu que aderiu à solução corporativa porque foi vantajoso para a subunidade: "Teve coisa que [...] era interessante, como o antivírus, que a gente precisava e aderimos. Então a gente analisa se é importante, se dá para a gente, e se for do interesse e se tiver recurso, a gente entra, participa da iniciativa." (ENTREVISTADO 17). Não foram identificadas evidências do uso da tática de conformidade relacionado à adoção de medidas informais de Segurança da Informação.

A Subunidade 03 apresentou maior cobertura de percentual para a tática de conformidade no NVivo: 14,69%. Em segundo lugar, figura a Subunidade 09, com 12,99% de cobertura de percentual, e em seguida estão a Subunidade 14, com 9,64% de cobertura de percentual, a Subunidade 05, com 9,60%, e a Subunidade 10, com 9,53% (Figura 11). Foram identificadas cinco referências de codificação em seis subunidades: Subunidade 01, Subunidade 03, Subunidade 05, Subunidade 09, Subunidade 10 e Subunidade 16. São estas as subunidades que mais utilizaram a tática de conformidade para responder com aquiescência.

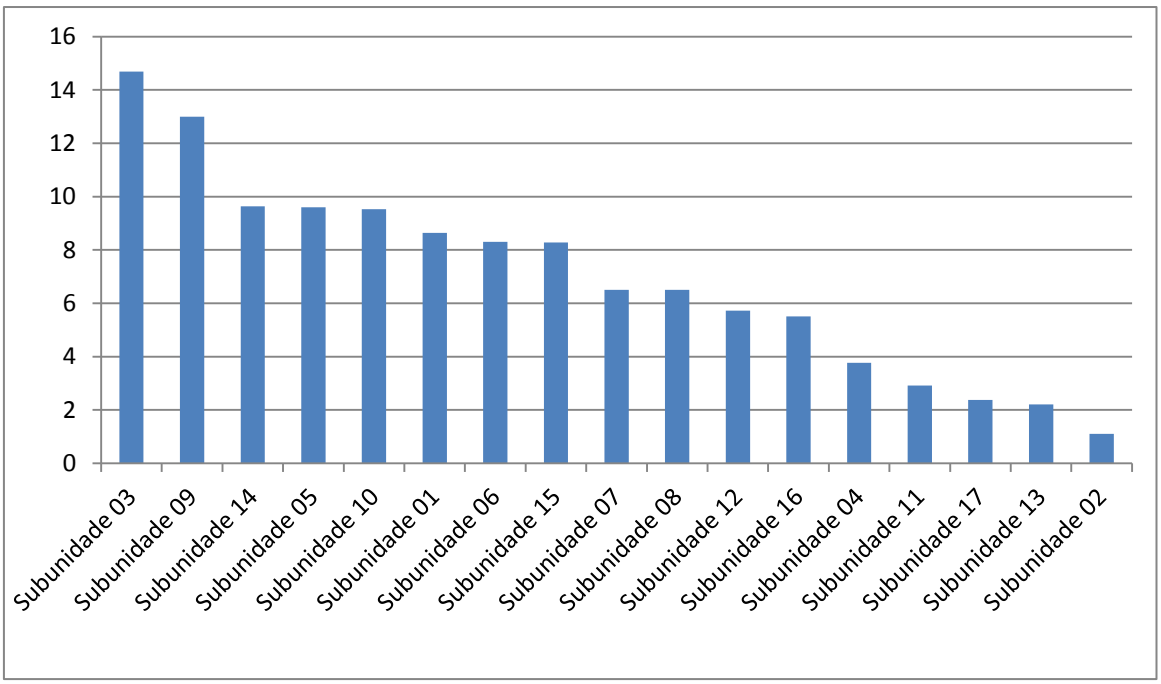


Figura 11 – Cobertura de percentual das subunidades para a tática de conformidade.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Os dados mostram mais referências à conformidade do que às outras táticas de aquiescência: hábito teve 25 referências, imitação teve 22 referências e conformidade teve 59. Isto significa que as respostas de aquiescência foram mais intencionais, com objetivos que vão além da garantia da disponibilidade, confidencialidade e integridade das informações, como a necessidade de atender às expectativas externas quanto à Segurança da Informação, de acordo com o Entrevistado 03 e o Entrevistado 09, a proteção da imagem externa da organização, segundo o Entrevistado 07, e a conformidade da subunidade com requisitos externos, segundo Entrevistado 02, Entrevistado 04, Entrevistado 06 e Entrevistado 08. A aquiescência teve 106 referências codificadas no NVivo, identificadas nas 17 subunidades. A conformidade foi identificada em 17 subunidades, o hábito em 15 e a imitação em 14.

A Figura 12 mostra que todas as subunidades que participaram da pesquisa responderam a pressões institucionais com aquiescência, sendo que as que tiveram maior cobertura de percentual para esta resposta foram: a Subunidade 09 teve 19,91% de cobertura de percentual, seguida da Subunidade 10, com 17,14%, e da Subunidade 03, com 15,80% de cobertura. A Subunidade 02 foi a que teve menor cobertura de percentual para esta estratégia, com 3,18%. Esses resultados mostram quais subunidades tiveram maior percentual dos dados analisados relacionados à aquiescência.

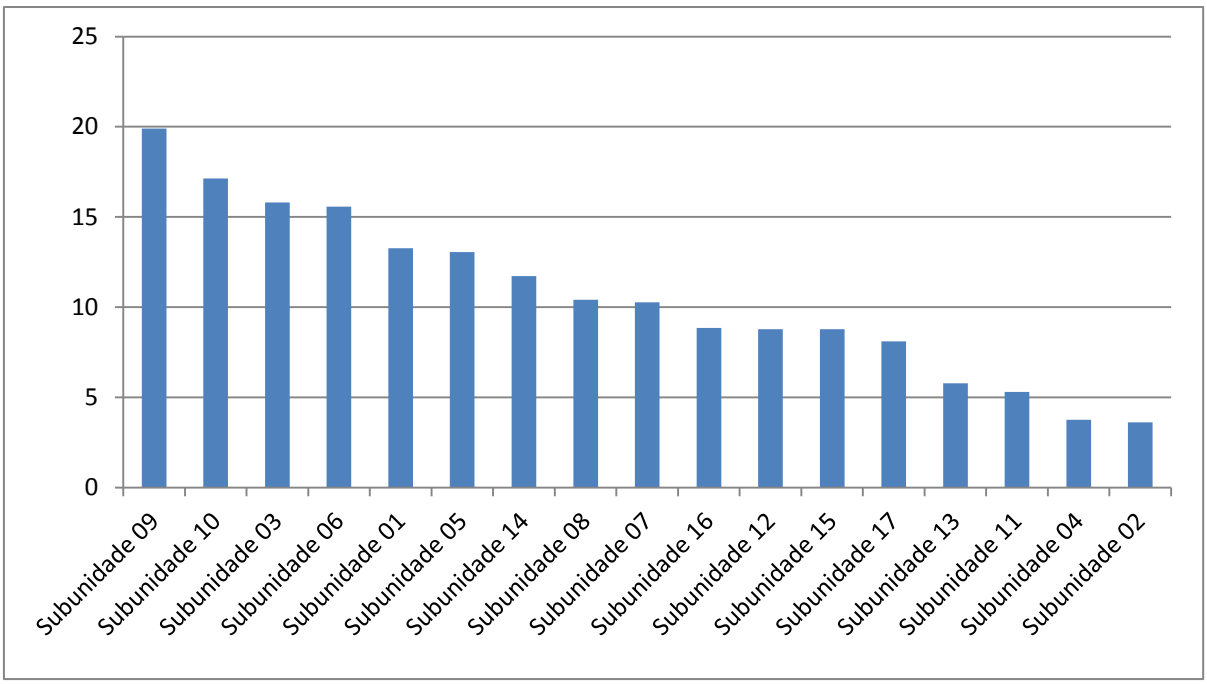


Figura 12 – Cobertura de percentual das subunidades para a resposta de aquiescência.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Já a Figura 13 apresenta quantas referências à resposta de aquiescência foram identificadas nos dados analisados, agrupados por subunidade. Como mostra o gráfico, a Subunidade 09 teve 11 referências identificadas, seguida da Subunidade 10, com dez, e da Subunidade 16, com nove referências. O gráfico mostra que todas as subunidades tiveram pelo menos duas referências a esta estratégia, sendo esses os casos da Subunidade 02 e Subunidade 13.

A partir dos dados, nota-se que a Subunidade 09 foi a que apresentou maior cobertura de percentual e também a maior quantidade de referências codificadas para aquiescência, o que é uma contradição com o resultado da auditoria (FIOCRUZ, 2015), que mostra que a subunidade adotou integralmente 39,3% e parcialmente 30,8% das medidas previstas nos regulamentos da organização. Este resultado pode ser interpretado como uma distância entre o discurso do Entrevistado 09 e a prática identificada na auditoria. A Subunidade 10, que também aparece em uma posição de destaque nos dados analisados, adotou integralmente 51,7% e parcialmente 20,9% das medidas previstas, de acordo com o mesmo relatório de auditoria, confirmando a aquiescência como sua principal resposta estratégica.

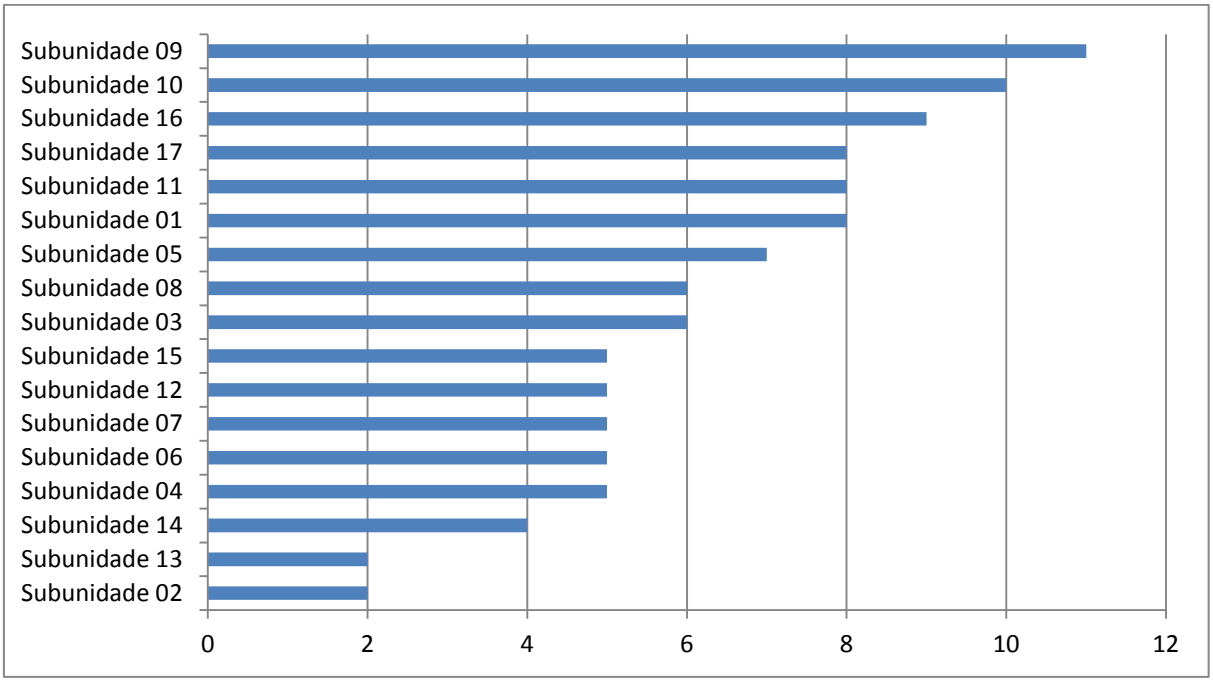


Figura 13 – Referências de codificação para a resposta de aquiescência.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

6.7.2 Compromisso

O compromisso é a resposta de aceitação parcial das normas, valores e regras institucionais, de acordo com Oliver (1991). Como explicam Meyer e Rowan (1977), essas normas, regras e valores institucionais podem ser considerados conflitantes com os objetivos da organização. Oliver (1991) complementa que podem ser impossíveis de serem incorporadas. Sendo uma resposta de aceitação parcial, o compromisso explica o comportamento das subunidades diante da rigidez ou do excesso de restrições impostos pelos regulamentos e medidas de Segurança da Informação (KARYDA; KIOUNTOUZIS; KOKOLAKIS, 2005; ELLWANGER, 2009; ABRAHAM; CHENGALU-SMITH, 2011; SUN; AHLUWALIA; KOONG, 2011) e do fato de as pressões institucionais terem diferentes origens e expectativas (TEJAY; BARTON, 2013; ALKALBANI; DENG; KAM, 2014; ANTHONY; APPARI; JOHNSON, 2014; LOPES; SÁ-SOARES, 2014; ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016). Assim, medidas podem ser interpretadas pelas subunidades como inadequadas ou conflitantes com suas atividades, ou até mesmo que a conformidade com essas expectativas é impossível. As três táticas de compromisso são o equilíbrio, a pacificação e a barganha.

A tática de equilíbrio significa que a subunidade acomodou múltiplas expectativas institucionais (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). Em Segurança da Informação, o equilíbrio significa que as medidas foram implantadas, mas não da forma prevista pelos constituintes do ambiente institucional, e sim com ajustes para que não haja o descumprimento total dos requisitos externos. A análise dos dados através do *software* NVivo mostrou que o equilíbrio é utilizado por sete subunidades e foram identificadas 13 referências a esta tática nas entrevistas e documentos analisados.

As ações de adequação das medidas conforme as necessidades das subunidades foram reconhecidas pelo Entrevistado 19, que relatou que alguns projetos são articulados com outras organizações e as subunidades precisam seguir regras dessas organizações, adequando a implementação às suas necessidades.

De acordo com o Entrevistado 08, sua subunidade tem processos e procedimentos de atualização dos sistemas a fim de evitar vulnerabilidades, mas essa atualização não alcança todos os equipamentos e sistemas. Parte das medidas técnicas adotadas é voltada para os servidores da rede de computadores: "A gente tem mais é controles para os servidores e para os sistemas que rodam nos servidores." (ENTREVISTADO 08). A Subunidade 08 tem também um processo de classificação de informações que, embora documentado, não é utilizado sempre que possível. O mesmo se aplica ao processo de análise e avaliação de riscos, que a subunidade tem documentado, mas que não é realizado para todas as situações.

A atualização dos sistemas computacionais da organização, como expressamente recomendado pela CGTI, é realizada na Subunidade 02, mas não em todos os computadores devido ao risco de prejudicar o funcionamento de sistemas específicos utilizados nas atividades de pesquisa:

> São computadores que não podem sofrer atualização do fabricante justamente porque o *software* da máquina [de pesquisa à qual o computador está acoplado] não foi atualizado. Então o *software* do computador não pode ser atualizado, e isso é um risco de segurança, então a gente mantém essas máquinas fora até que uma solução seja feita. Isso impacta até no suporte dos fabricantes dessas máquinas. (ENTREVISTADO 02).

Com isso, a pesquisa mostrou que a atualização dos computadores na Subunidade 02 é realizada, mas quando há a possibilidade de interferir no funcionamento de determinados equipamentos utilizados nas atividades da subunidade, não há atualização. Neste caso, há múltiplas expectativas institucionais em confronto, o que põe a subunidade em risco: a necessidade de atualizar os sistemas de todos os computadores para corrigir vulnerabilidades

e a necessidade manter os *softwares* utilizados nos equipamentos desatualizados devido à possibilidade de a atualização interferir em seu funcionamento.

As necessidades de realizar *backup* de dados, ter antivírus e armazenar os documentos de trabalho em um repositório da rede de computadores que ofereça controle de acesso lógico são parcialmente atendidas na Subunidade 07. Neste caso, como a subunidade não tem servidores de rede com recursos redundantes (considerados adequados para estas necessidades pelo Entrevistado 07), é utilizado um computador convencional para desempenhar as funções de servidor de antivírus e de arquivos, garantindo a existência de um servidor de antivírus, o armazenamento dos dados em um repositório central e a realização de *backup* desses dados. No entanto, esta situação tipifica a tática de equilíbrio, pois o equipamento utilizado não é adequado por não apresentar recursos que garantam seu funcionamento como servidor de rede, como redundância de peças.

O Entrevistado 17 relata que sua subunidade tem um regulamento próprio sobre correio eletrônico, que é anterior ao regulamento da FIOCRUZ. Quando houve a regulamentação pela organização, situações de conflito entre os dois regulamentos surgiram e a subunidade optou por equilibrar os dois regulamentos conflitantes tentando estar em conformidade com os dois: "Quando a FIOCRUZ publicou a norma geral, válida para todas as unidades, a nossa tinha várias coisas diferentes, o que levou a unidade a rever a norma local. Como a revisão ainda não foi aprovada, a gente está praticando o que está na nossa, complementando com o que está na norma da FIOCRUZ." (ENTREVISTADO 17). Com isto, fica caracterizada a tática de equilíbrio e a resposta de compromisso.

O último relatório de auditoria interna disponibilizado pela organização (FIOCRUZ, 2015) evidencia também um comportamento de equilíbrio ao mostrar que várias medidas são adotadas apenas parcialmente pelas subunidades. A Norma Institucional SIC-006/CGTI/VPGDI, que define requisitos de Segurança da Informação para a aquisição, desenvolvimento e manutenção de sistemas de informação (FIOCRUZ, 2013a), apresenta 41% de adoção parcial das medidas previstas, sendo a que tem maior percentual de medidas adotadas parcialmente dentre os nove regulamentos internos da organização.

O informante da Subunidade 16 aponta o motivo para a utilização desta tática de compromisso: "A gente analisa, vê como fazer, se dá para fazer tudo ou se precisa mudar alguma coisa para trazer para as nossas necessidades." (ENTREVISTADO 16). O

entrevistado da Subunidade 11 confirma: “A gente procura alternativas para não ficar totalmente descoberto, e depois vê o que faz.” (ENTREVISTADO 11).

A partir do NVivo, é possível construir o gráfico que apresenta a cobertura de percentual de cada uma das subunidades que utilizaram a tática de equilíbrio para responder com compromisso às pressões institucionais (Figura 14). Pelo gráfico, nota-se que a Subunidade 08 tem cobertura de percentual de 11,47%, a maior apresentada para esta tática entre as subunidades. A Subunidade 02 aparece em segundo lugar, com 7,23%, e em terceiro lugar está a Subunidade 07, com 4,92% de cobertura de percentual. A Subunidade 17 aparece em seguida, com 4,74% de cobertura. As demais subunidades são a Subunidade 16, a Subunidade 11 e a Subunidade 01, que têm 1,11%, 0,63% e 0,50% de cobertura de percentual, respectivamente. A Subunidade 17 e a Subunidade 08 apresentaram três referências de codificação, sendo as duas que apresentaram maior quantidade. A Subunidade 11 e a Subunidade 07 apresentaram duas referências cada, enquanto a Subunidade 01, a Subunidade 02 e a Subunidade 16 apresentaram uma referência de codificação cada.

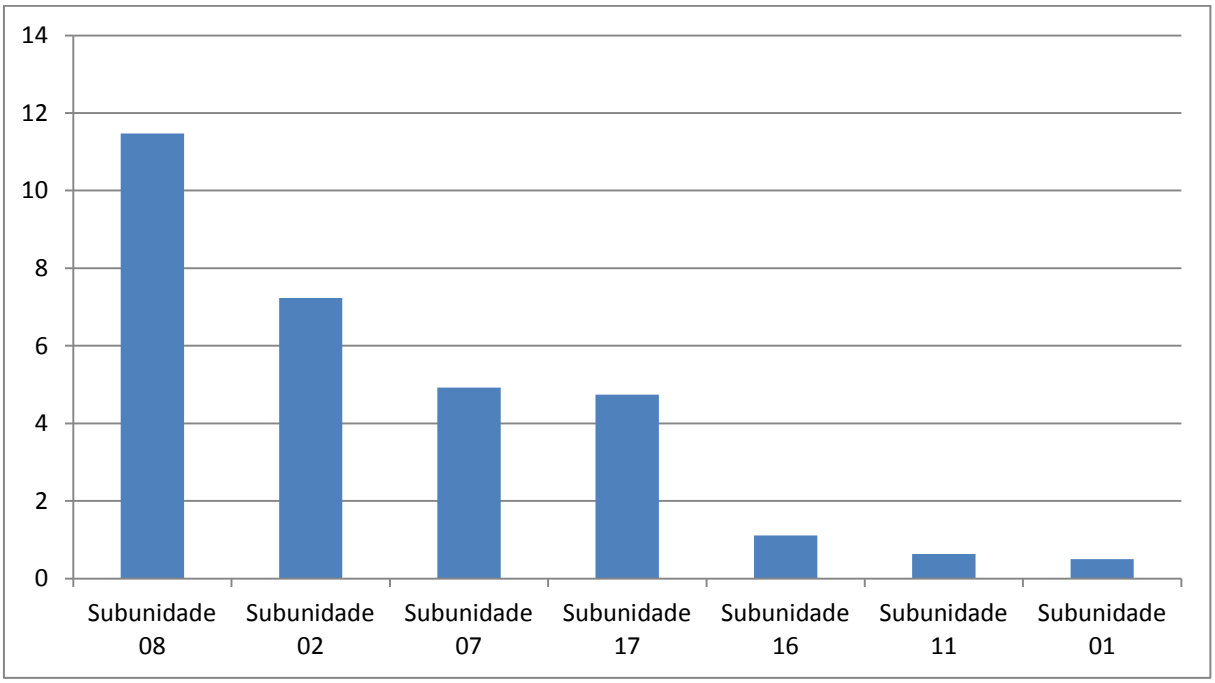


Figura 14 – Cobertura de percentual das subunidades para a tática de equilíbrio.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

A pacificação é a tática apresentada por Oliver (1991) que se caracteriza pelo esforço da organização para minimizar as pressões que sofre, mas com as quais não concorda.

No contexto da Segurança da Informação, parte das medidas exigidas pode ser adotada, enquanto outras são rejeitadas por serem consideradas conflitantes entre si ou com os objetivos e atividades da organização. Para Hu, Hart e Cooke (2007), a preocupação com eficiência pode levar à resistência organizacional às medidas de Segurança da Informação.

O último relatório de auditoria interna publicado (FIOCRUZ, 2015) evidencia a pacificação ao mostrar que nenhum dos regulamentos internos está sendo integralmente respeitado por todas as subunidades. O relatório mostra que a Subunidade 03 desrespeita a Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a): embora realize *backups*, a subunidade não armazena as cópias geradas em um local seguro – em outras palavras, adotou uma medida de redundância de dados, mas desrespeitou outra. Esta informação não foi identificada na entrevista, mas apenas no relatório de auditoria consultado, o que mostra que o discurso do entrevistado difere da realidade identificada na auditoria.

A mesma auditoria mostrou que a Subunidade 02 divulga a Política e os regulamentos de Segurança da Informação da organização, mas não monitora o cumprimento das responsabilidades dos usuários de TI, como previsto na Norma Institucional SIC-001/CGTI/VPGDI (FIOCRUZ, 2012a). Com isto, fica evidenciado que uma das duas medidas complementares não é adotada. O informante admite que, devido à falta de recursos, nem tudo que é necessário é adotado:

> A gente faz a adoção do que é capaz de adotar, pois tem a questão orçamentária também, que impacta na adoção dessas coisas [medidas de Segurança da Informação]. [...] O que a gente não está conforme é porque demanda orçamento para fazer tal projeto para chegar ao ponto necessário. [...] Por exemplo, a gente tem algumas necessidades internas, que são recomendações de órgãos, que a gente não pode fazer porque não tem orçamento, pois envolve aquisição de infraestrutura, ampliação... Por outro lado, a gente não abre para poder deixar insegurança, que vá gerar risco para as informações internas, para a casa. (ENTREVISTADO 02).

O entrevistado da Subunidade 09 cita o regulamento organizacional que trata de acesso remoto (FIOCRUZ, 2013e) para exemplificar uma situação na qual medidas consideradas incoerentes com a realidade da subunidade não são adotadas: “A de acesso remoto [Norma Institucional SIC-007/CGTI/VPGDI] é boa, mas tem umas coisas que eu não concordo. Eles dificultaram. Praticamente, eles impediram que a unidade adotasse alguma solução de acesso remoto.” (ENTREVISTADO 09). Em outro momento da entrevista, o informante complementou: “O que é coerente e não tem um custo, que a gente pode fazer, a gente faz. Se tem um custo, a direção diz se vai investir. O que não é coerente, a gente explica

para a direção e eles decidem. Em geral, eles concordam em não adotar. Respeitam nossa opinião sobre isso.” (ENTREVISTADO 09).

A conformidade parcial, típica da tática de pacificação, é identificada também na Subunidade 05, cujo entrevistado informou que nem tudo o que é previsto nos regulamentos é feito:

> Pelo que olhei na documentação, não estou fazendo nada que não possa, mas também não estou fazendo tudo que está ali. E estou fazendo algumas coisas de forma diferente, mas não acho que estou fazendo errado. Por exemplo, não estou adotando os mesmos sistemas operacionais deles, mas isso não é errado, e é uma questão de ter sucesso. Acho que [nome do sistema operacional adotado na unidade] é mais seguro, funciona, não dá problema, não trava, não tem tanto vírus. (ENTREVISTADO 05).

As medidas que restringem o trabalho na Subunidade 11 são citadas pelo entrevistado desta subunidade. Segundo ele, os regulamentos que obrigam a mudança periódica das senhas de acesso à rede de computadores e aos sistemas de informação são percebidos como prejudiciais às atividades dos usuários. Outras medidas criticadas pelo entrevistado estão presentes no regulamento que trata de acesso remoto na organização (FIOCRUZ, 2013e) e a proibição de armazenamento de documentos de trabalho na nuvem:

> Aquela norma do acesso remoto [Norma Institucional SIC-007/CGTI/VPGDI] restringe as pesquisas, porque impede o trabalho de casa ou de outro lugar. O cara tem um computador na casa dele que, pela regra, precisa estar sem vírus, protegido e tal. Mas a gente não sabe a situação do computador. Então não deixa acessar, como diz a norma, e isso causa uma limitação para o pesquisador. Mas existem outras formas de acesso remoto que não colocam a rede em risco. A gente sabe que é proibido armazenar coisa em disco virtual, na nuvem. Mas se bloquear essas coisas daqui de dentro, o pesquisador não vai trabalhar direito. A FIOCRUZ não tem um disco virtual institucional ainda. Se tivesse, seria uma alternativa. Então o cara vai e coloca na nuvem mesmo e manda para seu grupo de pesquisa, seus colaboradores. Se a gente for seguir a norma na íntegra, o pesquisador não vai conseguir pesquisar. (ENTREVISTADO 11).

Embora reconheça há uma integração entre a Subunidade 12 e a CGTI, o Entrevistado 12 afirma que as medidas requeridas pela administração central não são integralmente adotadas pela subunidade porque há conflitos e a subunidade, para atender às suas necessidades internas de Segurança da Informação, adota suas próprias medidas.

A Subunidade 16 também responde com compromisso utilizando a tática de pacificação ao não implantar o *firewall* exigido para se integrar à rede de computadores utilizada pela organização: “A gente tem *firewall* aqui. Eles não podem exigir que a gente adote a tecnologia deles porque eles consideram a melhor. Porque a nossa realidade é essa,

que pode ser diferente da deles. São necessidades diferentes.” (ENTREVISTADO 16). O entrevistado cita outras medidas não adotadas, como as previstas nos regulamentos sobre uso de correio eletrônico (FIOCRUZ, 2012d) e acesso à Internet (FIOCRUZ, 2012c), e as portarias que estabelecem a criação de um subcomitê de Segurança da Informação em cada subunidade (FIOCRUZ, 2011b, 2011e), consideradas incoerentes com as necessidades de Segurança da Informação da subunidade. O trecho a seguir trata do regulamento da FIOCRUZ sobre *datacenters* (FIOCRUZ, 2013a): “Não dá para fazer tudo como manda a regra. A gente se adapta também. Tem as exigências de *datacenter*, que a gente não tem como seguir e não vai fazer mesmo. O que é importante e possível, a gente faz, mas não dá para fazer tudo aquilo. É mais para lá para a CGTI.” (ENTREVISTADO 16).

Com 15,31%, a Subunidade 02 foi a que apresentou a maior cobertura de percentual para a tática de pacificação. Na sequência, a Subunidade 16 aparece com 7,39%, e a Subunidade 09, que tem cobertura de percentual de 5,48% (Figura 15). Quanto às referências de codificação, a Subunidade 16 apresentou seis referências, a maior quantidade dentre as subunidades que utilizaram a tática de pacificação. A Subunidade 09 apresentou quatro referências de codificação identificadas, enquanto a Subunidade 12 e a Subunidade 02 tiveram três cada uma. A Subunidade 03 teve duas referências identificadas, e as demais apresentaram uma. Este resultado mostra que a Subunidade 16 foi a que mais utilizou a tática de pacificação.

A terceira tática que Oliver (1991) apresenta para a resposta estratégica de compromisso é a barganha. Armênio Neto e Machado-da-Silva (2009) explicam que esta tática consiste em negociar para obter concessões das fontes de pressão institucional no sentido de reduzir o nível exigido de conformidade com os requisitos institucionais. Uma subunidade pode negociar com sua administração central ou outras fontes de pressão tanto o nível de conformidade quanto o momento em que precisa estar em conformidade com os requisitos de Segurança da Informação, ou porque não é capaz de adotar ou devido ao fato de as medidas serem incompatíveis com seus objetivos e atividades.

A barganha é identificada no relatório de auditoria interna (FIOCRUZ, 2015), que mostra como as subunidades negociam com os auditores a adoção das medidas exigidas pelos regulamentos organizacionais. A Subunidade 06 assumiu o compromisso de divulgar internamente a Política da FIOCRUZ e de instituir um subcomitê de Segurança da Informação. Sobre a exigência de medidas de controle de acesso físico ao CPD da subunidade, o Entrevistado 06 informou que o assunto já foi levado à Vice-Diretoria

competente, mas que a implantação foi adiada. Em diversos outros apontamentos, a Subunidade 06 negociou a mudança de condutas e a realização de procedimentos, como monitoramento dos usuários de TI e ações de conscientização e divulgação.

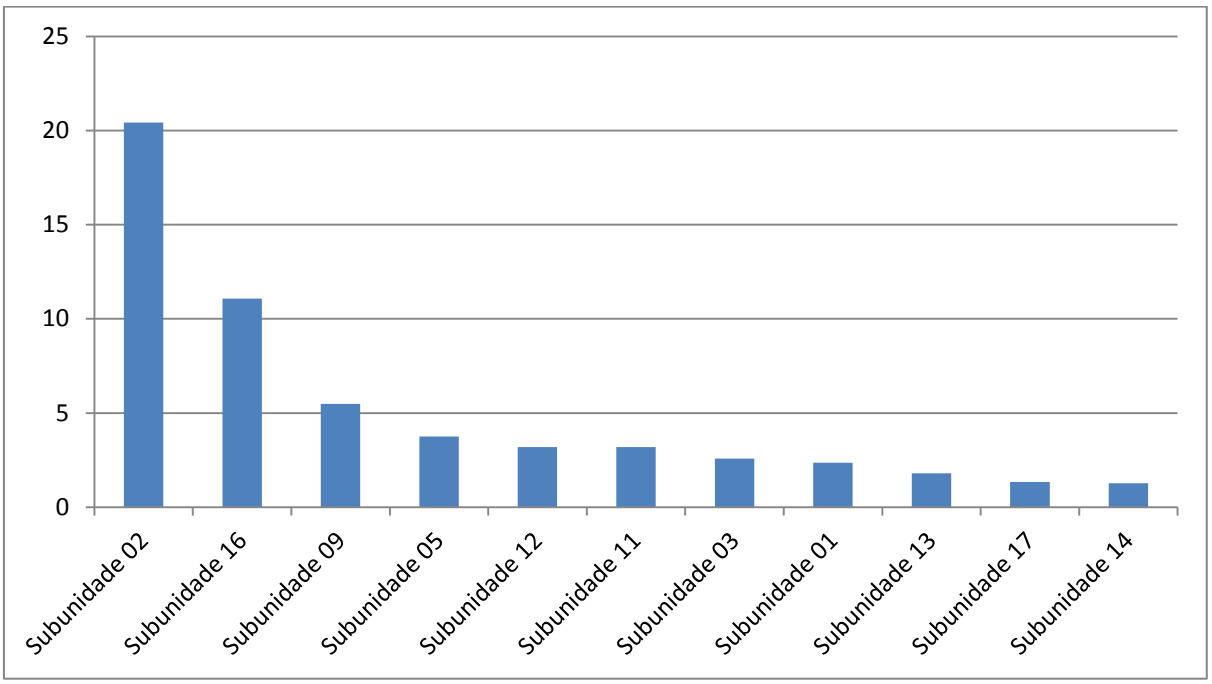


Figura 15 – Cobertura de percentual das subunidades para a tática de pacificação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Devido à ocorrência de um incidente que danificou o CPD e equipamentos da rede de computadores da Subunidade 05, a implantação de diversas medidas de Segurança da Informação teve que ser adiada. Parte das medidas depende de licitação para aquisição de novos equipamentos, o que adia a implantação indefinidamente. Na ocorrência de uma auditoria que aponte não conformidades quanto aos regulamentos de Segurança da Informação, o Entrevistado 05 admite: "O que pode acontecer é eu solicitar um tempo para ajustar alguma coisa que não estiver certa." (ENTREVISTADO 05), um exemplo do uso da tática de barganha frente a pressões institucionais. Na auditoria interna, a Subunidade 05 teve diversos apontamentos (FIOCRUZ, 2015), como a necessidade de adotar medidas de controle de acesso físico ao CPD e à própria subunidade, a criação de um subcomitê de Segurança da Informação, a realização de análise e avaliação de riscos, a adoção de medidas de controle de acesso aos computadores e de medidas relacionadas à realização de *backups*. Em todos os casos, a subunidade negociou com os auditores o momento da adoção.

As negociações para que determinadas medidas sejam adotadas na Subunidade 12 depende da melhoria da sua infraestrutura, segundo o Entrevistado 12. A adoção de diferentes medidas técnicas, formais e informais estava vinculada à realização de concurso público prevendo a contratação de um servidor público responsável pela Segurança da Informação na subunidade. Enquanto não acontecia a contratação, a adoção de diversas medidas era adiada. Durante esse impasse, houve um incidente que danificou equipamentos da rede de computadores, provocando indisponibilidade de serviços, sistemas e informações, que, segundo o Entrevistado 12, impulsionou a contratação. Quando a entrevista foi realizada, a subunidade aguardava a aquisição de equipamentos para implantar medidas exigidas pela administração central da organização e por outros constituintes do ambiente institucional.

Ocorreram negociações para adiar a implantação do antivírus corporativo da FIOCRUZ na Subunidade 04. Como relatou o Entrevistado 04, a licença de uso do antivírus expirou, fazendo com que as atualizações parassem de funcionar. Para a subunidade não deixar a subunidade tão vulnerável a códigos maliciosos, foi negociada a instalação de um antivírus diferente até que a situação do licenciamento fosse resolvida.

Na Subunidade 07, a tática de barganha foi evidenciada quando o Entrevistado 07 respondeu sobre a implantação de *no-breaks* para os equipamentos da rede de computadores. Segundo o informante, apenas o *firewall* está protegido contra falhas de fornecimento de energia elétrica. Além de não serem redundantes, os equipamentos também não têm peças redundantes. No entanto, medidas de proteção ambiental e redundância vão ser adotadas quando a subunidade for deslocada para um novo prédio, que estava em construção no momento da entrevista, o que tipifica a tática de barganha: "Fonte redundante, equipamento redundante não. Aqui, fora a questão do *firewall*, que eu tive o cuidado de colocar ligado a um *no-break* para dar proteção elétrica, não tem redundância não. Mas vamos melhorar quando formos para a sede definitiva, que deve ter uma infraestrutura mais robusta." (ENTREVISTADO 07). Em outro momento, o entrevistado reforça esta pretensão:

> Nossa expectativa é, com o *campus* novo, ter *softwares* atualizados, tecnologia mais nova, equipamentos melhores, uma rede [elétrica] dedicada. Então acho que lá vai dar para fazer uma coisa bem bacana. Quero chegar ao nível de o cara não conseguir usar um equipamento estranho na rede se ele não estiver autorizado. Acho que lá vai dar para fazer um trabalho bacana com relação a Segurança. (ENTREVISTADO 07).

Apesar de não dependerem da infraestrutura física, medidas formais também serão adotadas somente quando a Subunidade 07 estiver na nova sede: "A ideia é implementar

isso [regulamentos de Segurança da Informação] quando a gente estiver no *campus* novo. Imagino que a gente já vai ter recursos para trabalhar.” (ENTREVISTADO 07).

O Entrevistado 10 entende que os regulamentos da administração central são positivos, mas medidas consideradas incoerentes fazem com que haja negociações com a CGTI: “Nem sempre estamos de acordo com tudo o que a CGTI demanda, mas a ideia é positiva. E quando a gente não está de acordo, a gente senta e conversa com eles e tenta achar o melhor ponto para todos.” (ENTREVISTADO 10).

Outros casos de barganha foram identificados nas entrevistas com informantes da Subunidade 01 e da Subunidade 16. O Entrevistado 03 também relatou que o diretor da sua subunidade foi ao Rio de Janeiro negociar com a CGTI a implantação de medidas técnicas e solicitou apoio técnico para melhorar a infraestrutura de TI da subunidade. Também alvo de auditorias internas, o relatório (FIOCRUZ, 2015) mostrou que a Subunidade 03 negociou a adoção de diversas medidas que foram apontadas pelos auditores, como a formalização do subcomitê de Segurança da Informação, monitoramento do comportamento dos usuários de TI quanto ao uso de senhas, acesso a computadores e acesso à Internet, adoção de medidas de redundância de dados (*backup*), divulgação de regulamentos da organização e adoção de medidas de controle de acesso físico ao CPD.

Outras subunidades também utilizaram a barganha após a auditoria interna apontar não conformidades, como a Subunidade 02, que solicitou a criação do seu subcomitê de Segurança da Informação depois de identificada a não conformidade. Esta subunidade também se comprometeu a adotar procedimentos e medidas previstos nos regulamentos da organização. Outras subunidades cujas não conformidades foram apontadas na auditoria e cujas respostas indicam o uso da tática de barganha não participaram desta pesquisa.

A Subunidade 06 tem a maior cobertura de percentual para a tática de barganha (16,65%), que se mostra através da negociação da adoção de diversas medidas apontadas na auditoria interna. A Subunidade 05, que aparece em segundo lugar (7,05% de cobertura de percentual), precisou negociar a adoção de diversas medidas devido à ocorrência de um incidente. Já a Subunidade 12, com 6,73% de cobertura, ficou em terceiro lugar (Figura 16). Quanto à quantidade de referências de codificação, a Subunidade 06 apresentou sete referências, sendo a que apresentou mais ocorrências da tática de barganha. A Subunidade 12, com cinco referências, ficou em segundo lugar, e Subunidade 05, Subunidade 07, Subunidade 09 e Subunidade 10 vêm em seguida, com três referências identificadas cada uma. Esse

resultado mostra que a Subunidade 06 é mais propensa a negociar com as fontes de pressão institucional do que as outras, o que se reflete também na cobertura de percentual apresentada.

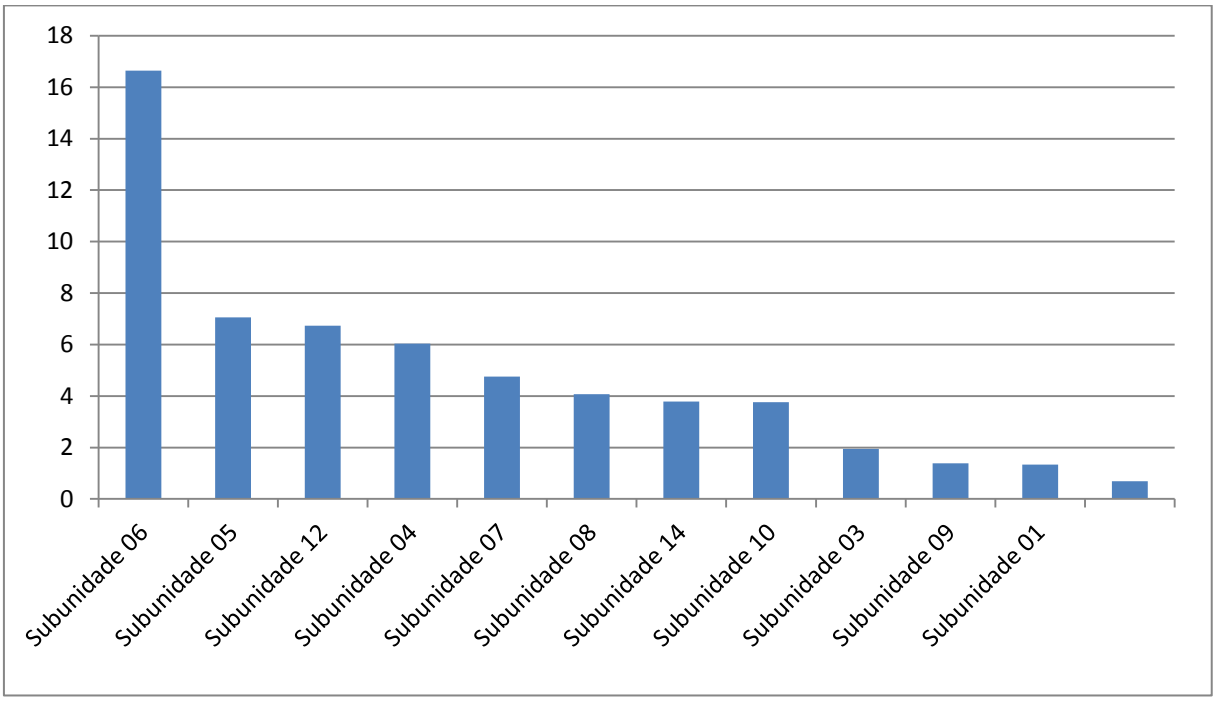


Figura 16 – Cobertura de percentual das subunidades para a tática de barganha.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

O uso das três táticas de compromisso é descrito pelo Entrevistado 09, que explica que algumas medidas são adotadas parcialmente (equilíbrio), algumas não são adotadas (pacificação) e outras são negociadas com a administração central da organização (barganha):

> Se a gente quer e a diretoria entende que não pode, que vai atrapalhar ou que vai causar algum ruído, então não faz. Quando faz, quando é uma coisa mais técnica, a gente vê se precisa de uma conscientização. Se for uma coisa obrigatória, uma coisa que o governo manda fazer, a gente tenta adotar. Só não adota se não tiver dinheiro ou gente para fazer. Se prejudicar o trabalho aqui, aí a gente tenta fazer uma coisa, dar uma solução, porque não pode parar o trabalho. Olha, quando é bom, a gente adota. Tem coisa que a gente adota em parte, e tem coisa que a gente não adota. Tem coisa que a gente negocia com a CGTI, tem também coisa que a gente vai lá brigar para não ter, então depende do caso. Cada caso é uma história. (ENTREVISTADO 09).

Os dados mostram que a tática de compromisso que teve mais referências foi a barganha, com 32 codificações. A tática de pacificação, por sua vez, teve 24, e o equilíbrio teve 13 referências identificadas no NVivo. A barganha, identificada em 12 subunidades, foi a tática mais difundida da resposta de compromisso. A pacificação teve referências de 11

subunidades, e o equilíbrio foi identificada em sete. Estes resultados mostram que a barganha é a tática mais utilizada para responder com compromisso e que há uma preferência por parte das subunidades de negociar a adoção das medidas de Segurança da Informação consideradas incoerentes ou cuja adoção não é possível no momento. Considerando suas três táticas, a resposta estratégica de compromisso teve 69 referências codificadas no NVivo.

A resposta estratégica de compromisso é considerada também uma resposta de conformidade (OLIVER, 1991; FREZATTI; AGUIAR; REZENDE, 2007) e representa uma expectativa de conformidade com os requisitos institucionais, visto que medidas de Segurança da Informação foram adotadas, apesar de não estarem funcionando como deveriam. Essa expectativa se mostra também quando parte das medidas exigidas pelos regulamentos foi adotada, e ainda quando houve uma negociação entre a subunidade e a administração central para que as medidas sejam adotadas de outra forma ou em outro momento.

Apenas a Subunidade 15 não respondeu com compromisso a pressões institucionais. Dentre as subunidades que apresentaram referências a esta resposta, a Subunidade 02 teve 21,65% de cobertura de percentual, a Subunidade 06 teve 16,65%, e a Subunidade 08 teve 15,54%. A Subunidade 13, com 1,80%, foi a que teve menor cobertura de percentual para a resposta de compromisso (Figura 17).

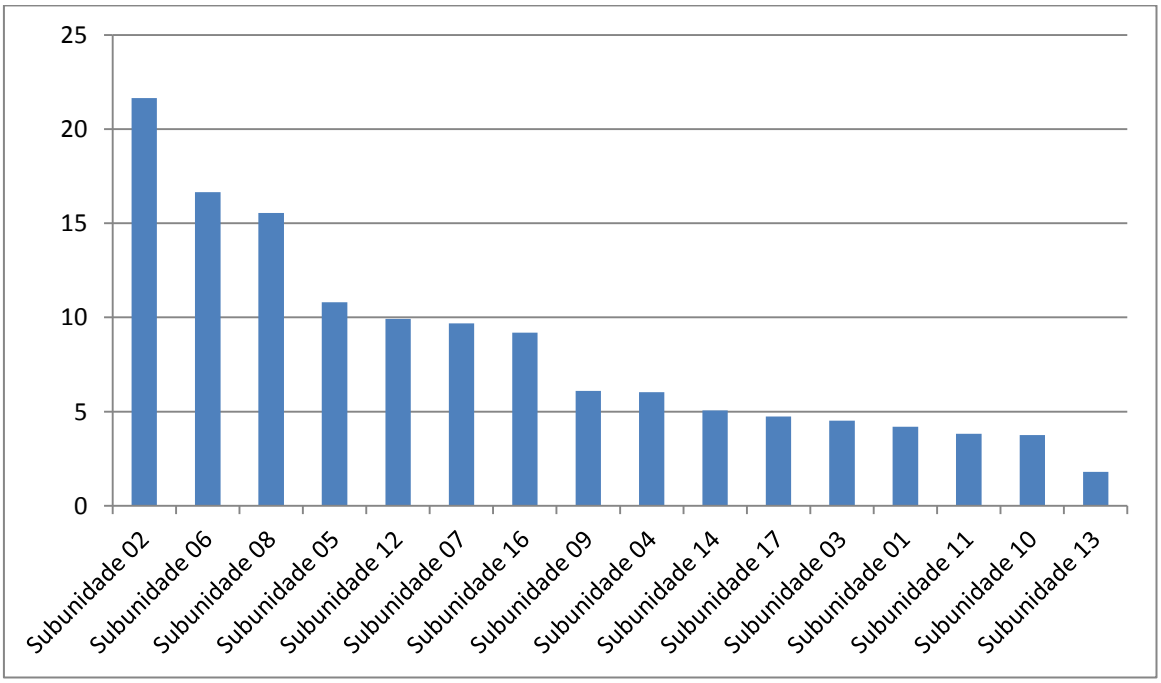


Figura 17 – Cobertura de percentual das subunidades para a tática de compromisso.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Quanto à quantidade de referências de codificação, a Subunidade 12 e a Subunidade 16 foram as que mais se destacaram, com oito referências identificadas para cada uma. A Subunidade 09 e a Subunidade 06 tiveram sete referências. A Subunidade 07 e a Subunidade 08 tiveram cinco, enquanto Subunidade 17, Subunidade 05 e Subunidade 02 apresentaram quatro referências. As subunidades que apresentaram menos referências à resposta estratégica de compromisso foram a Subunidade 04 e a Subunidade 13, ambas com apenas uma referência identificada (Figura 18). Isto mostra que a Subunidade 16 e a Subunidade 12 foram as que mais responderam com a tática de compromisso, adotando parcialmente ou negociando a adoção das medidas de Segurança da Informação.

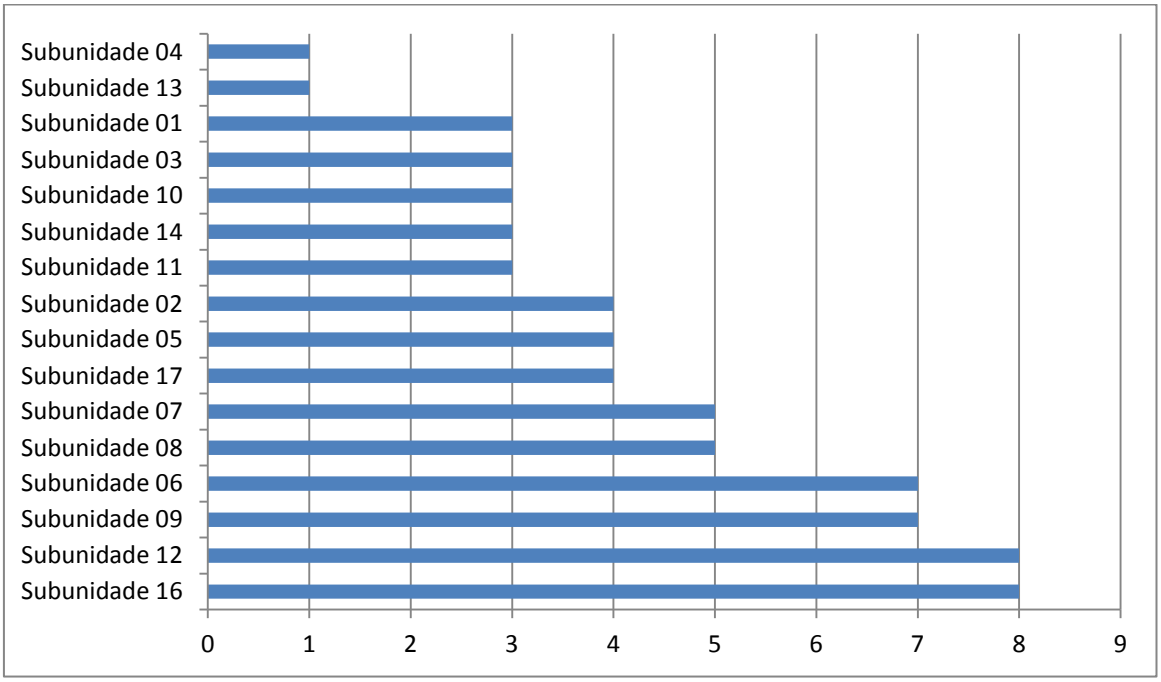


Figura 18 – Referências de codificação para a resposta de compromisso.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

6.7.3 Esquiva

A resposta estratégica de esquiva acontece quando a organização procura manter uma conformidade aparente com os requisitos do ambiente institucional, de acordo com Oliver (1991). Com a mesma lógica da dissociação entre política e prática discutida por Boxenbaum e Jonsson (2009), esta resposta estratégica é uma tentativa inequívoca de evitar a

conformidade com os requisitos institucionais. Oliver (1991) apresenta como táticas de esquiva a ocultação, o amortecimento e a fuga. Como as subunidades estão sujeitas a pressões tanto da administração central quanto de outros constituintes do ambiente institucional (OSMUNDSEN, 2005; BOSCHMAN, 2006; NETLAND; ASPELUND, 2014), podem utilizar qualquer uma das três táticas para evitar a conformidade com requisitos de Segurança da Informação conflitantes.

No caso da tática de ocultação, é criado um disfarce para a não conformidade, o que, segundo Meyer e Rowan (1977), pode garantir a legitimidade da organização no seu meio. Assim, a organização pode ter formalizado regulamentos e uma Política de Segurança da Informação, mas as medidas previstas podem não ser adotadas. Esta dissociação é prevista por Björck (2004), Lopes e Sá-Soares (2014) e Lapke e Dhillon (2015). Em organizações compostas por subunidades descentralizadas, a ocultação é uma tática que as subunidades podem utilizar para estar intencionalmente em conformidade cerimonial com os requisitos da administração central e do ambiente. No contexto da Segurança da Informação, as tecnologias podem ser implantadas sem as configurações necessárias, e programas, processos e regulamentos podem ser formalizados sem que sejam cumpridos.

A utilização da tática de ocultação através da implantação de uma tecnologia de forma superficial, sem a realização das configurações necessárias, é identificada na Subunidade 13. Ao relatar que houve a implantação recente de um *firewall* na subunidade, a despeito do avanço que foi a implantação do equipamento, o Entrevistado 13 afirmou que este não foi configurado de forma minuciosa:

> Na verdade, quando eu cheguei aqui, não tinha nem um *firewall*. Já que estamos falando de Segurança, não tinha nem *firewall* na rede. Então eu coloquei um [nome do fabricante do *firewall*], mas sem muita regra, porque tinha muitas outras coisas para fazer. Então só coloquei o *firewall* com o básico. (ENTREVISTADO 13).

A realização de uma configuração básica, da forma como o equipamento vem do fabricante, não é recomendável, pois pode expor a rede de computadores da subunidade, já que nem todas as necessidades da organização podem estar cobertas pela configuração básica (SENTHILKUMAR; ARUMUGAM, 2011). A Subunidade 13 teve ainda outro caso de ocultação relatado pelo entrevistado. Neste caso também houve a instalação de uma tecnologia de Segurança da Informação sem que houvesse sua implantação de fato – uma

solução tecnológica de controle de acesso lógico para controlar a autenticação e o acesso dos usuários à rede de computadores da subunidade:

> Não implantamos isso [senhas de acesso] ainda não. Nós usamos [nome de solução de autenticação] e a gente está com um problema de atualização com ele. O universo de usuários ainda é pequeno e a gente ainda vai decidir o que fazer quanto a isso aí. Essa parte não está completa ainda. (ENTREVISTADO 13).

A fim de tomar decisões sobre Segurança da Informação na Subunidade 13, um subcomitê foi instituído através de portaria da diretoria, mas o coordenador de TI da subunidade admite que não funciona como deveria, pois não tem se reunido e suas deliberações não são sequer apreciadas pela direção:

> Ele [o subcomitê de Segurança da Informação] existe, mas não está havendo reuniões. A última demanda do Comitê de Segurança foi justamente a normatização dos nomes das caixas postais [de correio eletrônico], que foi passado para a Diretoria, que vai definir. Existe formalmente um Comitê de Segurança, mas ele não tem se reunido com a frequência necessária. E o que foi feito pelo Comitê não deu em nada. Até agora a Diretoria não tomou uma decisão. Já fazem mais de dois anos que essa decisão está com a Diretoria. (ENTREVISTADO 13).

Com isto, a existência do Comitê na Subunidade 13 é apenas o cumprimento de uma exigência da administração central da organização, uma formalidade que não tem uma aplicação prática, caracterizando o uso da ocultação para responder com esquiva.

A Subunidade 13 tem uma biblioteca de acesso aberto ao público que oferece acesso à Internet aos visitantes, relata o Entrevistado 13. Os usuários da biblioteca são identificados na portaria da subunidade e dentro da biblioteca, mas não é feito o monitoramento nem controle de acesso lógico nos computadores disponibilizados nem do acesso que fazem à Internet, o que também configura a tática de ocultação, pois há um aparente controle sobre a identificação das pessoas:

> Uma coisa que poderia ser diferente é o acesso à biblioteca. A biblioteca daqui, por concepção, é uma biblioteca que o público externo pode ter acesso. Então a única forma de controlar o acesso dessas pessoas que são externas, dessas pessoas que não têm nenhum vínculo aqui, é através de crachá, que hoje todos são obrigados a utilizar. Mas a gente não tem controle algum do que as pessoas estão tendo acesso lá na biblioteca. (ENTREVISTADO 13).

A tática de ocultação foi utilizada pela Subunidade 04 em medidas de controle de acesso físico. Segundo o entrevistado, a subunidade tem a tecnologia necessária, mas não está funcionando, como visto no trecho a seguir:

> O controle [de acesso físico] é feito pelo porteiro [da entrada principal da subunidade]. Não existe um controle eletrônico, com nível de acesso aqui dentro. A gente já tem a estrutura tecnológica, mas nada foi implementado ainda. Compramos uma solução há mais ou menos cinco ou seis anos atrás. Tem roletas, cartões com níveis de acesso. (ENTREVISTADO 04).

O Entrevistado 04 acrescenta que esta situação já possibilitou a ocorrência de incidentes:

> Nós temos em uma das portas, a porta principal, uma fechadura de acesso biométrico ou através de senha. Como não existe uma recepção na entrada dos laboratórios, quando alguém vem fazer uma entrega, fica batendo na porta. É uma entrada principal e dentro do prédio tem vários serviços. Então as pessoas têm o costume de deixar a porta aberta. [...] Então houve um problema de segurança que foi relatado pelos próprios pesquisadores do laboratório [...]. (ENTREVISTADO 04).

Em outro momento da entrevista, o informante da Subunidade 04 mostrou que a implantação das medidas de controle de acesso físico é importante por outro motivo além da segurança física:

> São feitas algumas auditorias e por isso devem existir esses controles. Mas às vezes eles não são utilizados. Nós temos controles de acesso, e nós utilizamos, mas nos laboratórios acontecem esses problemas. As pessoas simplesmente não querem ficar levantando para abrir a porta, apenas deixam a porta aberta. Fixaram a porta aberta com um pedaço de madeira para não ficar abrindo a porta, para não ter que ficar levantando para abrir a porta. São realizadas algumas auditorias que exigem esse tipo de controle de acesso. (ENTREVISTADO 04).

A situação descrita pelo Entrevistado 04 mostra que a subunidade implantou controle de acesso físico de forma cerimonial, pois não está sendo utilizada adequadamente para a finalidade para a qual a tecnologia foi adquirida.

As câmeras de vigilância também são tecnologias que auxiliam o controle de acesso físico, mas que não estão implantadas adequadamente. O Entrevistado 04 relata que, quando foi necessário consultar as imagens das câmeras para elucidar um incidente, não foi possível: “As câmeras deveriam ter as imagens, e estão ali funcionando 24 horas por dia, e quando você precisa e solicita, as imagens não existem.” (ENTREVISTADO 04).

Sobre o cumprimento dos regulamentos e da Política de Segurança da Informação nas subunidades, o Entrevistado 12 deixa clara sua percepção de que a dissociação entre a Política e as medidas adotadas é uma realidade na organização: “De certa forma, as unidades são independentes, então nem todo mundo implementa, ou fala que implementa, mas não utiliza.” (ENTREVISTADO 12). Em outro momento da entrevista, ele reforça esta percepção: “O fato de dizer que tem uma Política, mas que não consegue monitorar nem aplicar as sanções necessárias para quem não cumpre, fica uma norma de gaveta, que não serve para nada, só para dizer que tem.” (ENTREVISTADO 12).

Nove subunidades utilizam a ocultação para evitar as pressões institucionais. A Subunidade 04 teve cinco referências de codificação identificadas para a tática de ocultação, seguida da Subunidade 17, com três referências, e da Subunidade 10, Subunidade 12 e Subunidade 13, cada uma com duas referências. Com 17,36%, a Subunidade 04 também a que apresentou maior cobertura de percentual para esta tática. A Subunidade 13, com 6,24%, a Subunidade 17, com 5,99%, e a Subunidade 03, com 5,68%, completam as quatro subunidades que se destacam na cobertura de percentual para ocultação (Figura 19). Esta tática foi identificada ainda na Subunidade 12, Subunidade 09, Subunidade 16, Subunidade 01 e Subunidade 11, mostrando que a dissimulação é uma prática comum entre as subunidades.

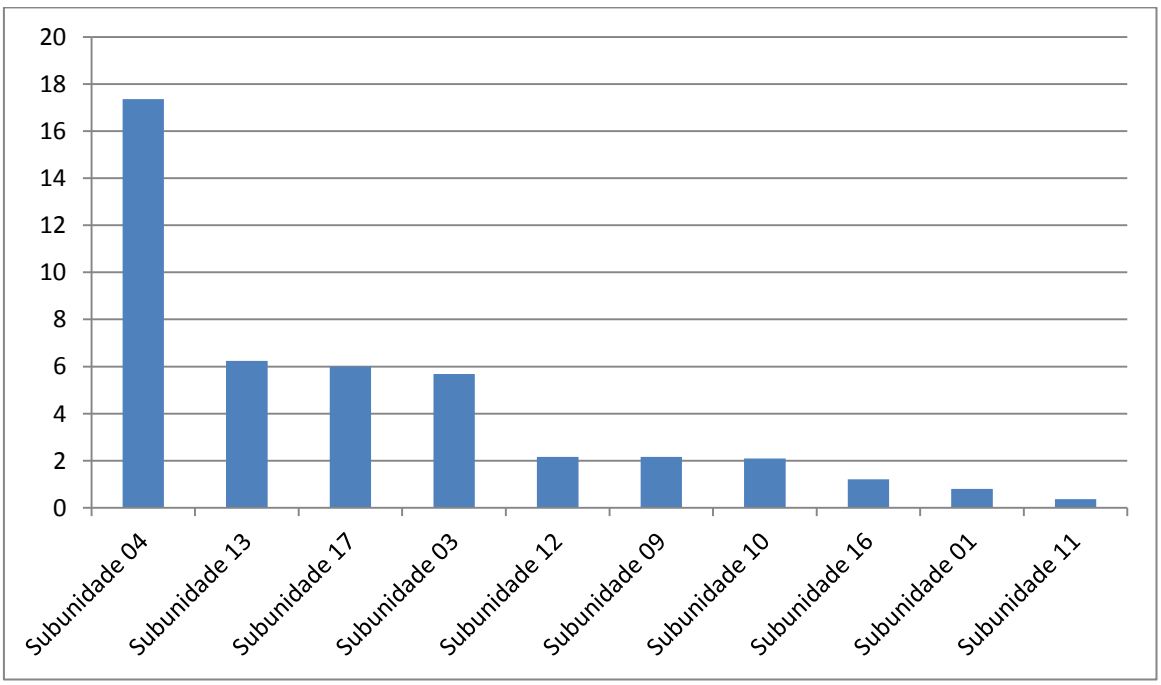


Figura 19 – Cobertura de percentual das subunidades para a tática de ocultação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

O amortecimento é uma tática que visa à redução do quanto a subunidade é inspecionada, controlada ou avaliada pela administração central ou outros constituintes do ambiente institucional (OLIVER, 1991). Esta tática caracteriza-se por uma redução dos vínculos existentes entre o ambiente interno e o ambiente externo (PFEFFER; SALANCIK, 1978; PARKS; WIGAND, 2014), que resulta em um afastamento entre o funcionamento interno e o que é inspecionado (AIER; WEISS, 2012). Enquanto a ocultação consiste em demonstrar uma conformidade que não existe, o amortecimento consiste em esconder a não conformidade das fontes de pressão institucional.

Esconder a ocorrência de incidentes de Segurança da Informação do ambiente externo, como descrito por Dhillon (2001), é uma forma de utilizar a tática de amortecimento. A outra forma é esconder do ambiente externo quais medidas de Segurança da Informação foram adotadas e quais não foram. Uma subunidade pode esconder a ocorrência de incidentes e a rejeição de medidas requisitadas tanto pela administração central quanto por outras organizações, evitando assim críticas e danos à sua imagem.

O amortecimento é utilizado pela Subunidade 04 ao esconder que uma medida de controle de acesso físico foi adquirida mas não é utilizada apropriadamente: “O auditor chegou aqui e a porta estava presa com um papelão. Aí perguntou: ‘vocês não têm controle de acesso?’ Tem e funciona. A gente fecha a porta e abre com controle de acesso biométrico, e abre na hora.” (ENTREVISTADO 04).

O entrevistado da Subunidade 06 assumiu que ajustes são realizados para que não conformidades não sejam percebidas em auditorias. O mesmo comportamento foi identificado na Subunidade 09. Já o Entrevistado 11 afirmou que há uma movimentação na sua subunidade para realizar ajustes antes das inspeções. O Entrevistado 10, por sua vez, declarou: “Às vezes, e até internamente aqui, a gente vê certos casos em que se quer só tapar um buraco para não ser pego em não conformidades em uma auditoria.”

Sobre a comunicação a respeito da ocorrência de incidentes à administração central, o Entrevistado 09 admitiu isto não acontece porque entende que os incidentes devem ser tratados pela equipe local e porque a comunicação prejudica a imagem da subunidade: “Nem sempre [a CGTI é comunicada sobre a ocorrência de incidentes]. Na verdade, nunca. Do que já aconteceu aqui, nunca avisamos nada. Porque é sempre uma coisa que não depende deles, que a gente tem de resolver por aqui mesmo. E vamos ser sinceros, vai ficar feio para a gente.” (ENTREVISTADO 09).

O entrevistado da Subunidade 16 também não comunica à administração central a ocorrência de incidentes, a não ser que necessite de algum apoio da CGTI:

> A gente não informa não [à sede a ocorrência de incidentes de Segurança da Informação]. Se for um caso de vírus mandando ataque para fora, aí vem uma mensagem do CAIS [Centro de Atendimento a Incidentes de Segurança, departamento da Rede Nacional de Ensino e Pesquisa – RNP], mas a gente não informa lá na FIOCRUZ não. Se tem um vírus, a gente não avisa não. Se tiver algum incidente mais sério, com perda de dados, por exemplo, a gente se resolve aqui e só avisa quando precisa de algum apoio. Ou quando tem alguma coisa de comportamento, quando um usuário faz uma bobagem, passa a senha para outro, a gente fala com ele, informa ao chefe dele, mas não tem essa coisa de passar para a FIOCRUZ não. (ENTREVISTADO 16).

Já o Entrevistado 11 afirmou que a administração central é informada da ocorrência, mas somente depois de o problema ter sido sanado. Em todas essas situações, fica caracterizado o uso da tática de amortecimento, pois a intenção das subunidades é manter um distanciamento entre a inspeção externa e sua realidade interna. Como consequência da não comunicação dos incidentes à sede, ações corretivas e preventivas podem não ser executadas tempestivamente e sistemas e informações compartilhados podem ser prejudicados. A falta de informações sobre a ocorrência de incidentes nas subunidades também pode prejudicar a tomada de decisões pelo Comitê e pelo Escritório de Segurança da Informação da organização.

A Subunidade 16 apresentou mais referências de codificação (quatro referências identificadas) e maior cobertura de percentual para a tática de amortecimento (4,32%). A Subunidade 09, por sua vez, teve 2,51% de cobertura de percentual e duas referências de codificação. Já a Subunidade 06, que teve 1,55% de cobertura, teve uma referência identificada, e a Subunidade 11, que teve 1,33% de cobertura de percentual, apresentou duas referências identificadas. A Figura 20 mostra o gráfico com a cobertura de percentual das subunidades que utilizaram a tática de amortecimento.

Armênio Neto e Machado-da-Silva (2009) esclarecem que a tática de fuga consiste em mudanças de atividades, objetivos ou do domínio no qual as pressões institucionais acontecem com a intenção de contornar a necessidade de estar em conformidade com os requisitos institucionais. Subunidades organizacionais podem evitar participar de projetos, iniciativas e ações da administração central para evitar a necessidade de estar em conformidade. Dessa forma, a implantação de tecnologias na sede que exigem a adoção de medidas de Segurança da Informação pelas subunidades pode levá-las a uma resposta de fuga

devido à incapacidade de adotar ou à inconsistência entre as medidas exigidas e seus objetivos ou atividades.

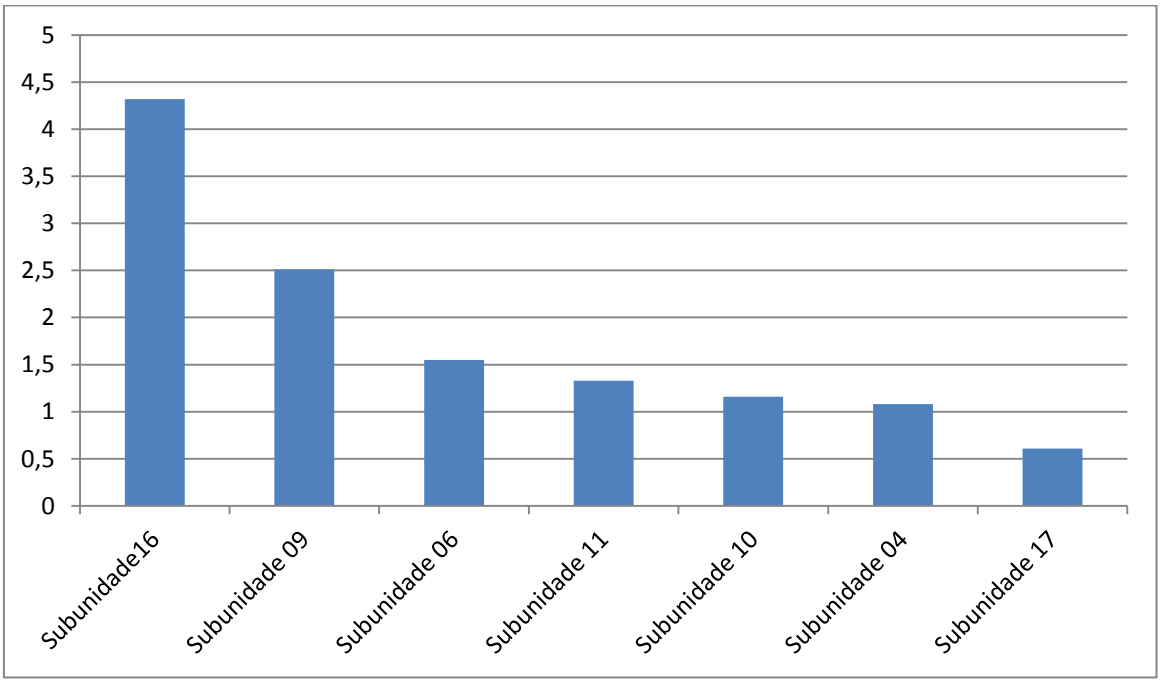


Figura 20 – Cobertura de percentual das subunidades para a tática de amortecimento.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Apenas três referências à tática de fuga foram identificadas nas entrevistas, e em apenas duas subunidades. A entrevista com o informante da Subunidade 16 mostrou que quando a administração central da organização executa um projeto que exige a adoção de medidas de Segurança da Informação, há uma avaliação quanto ao interesse da subunidade e à importância do projeto e das medidas: "Se for bom, se for interessante para a gente, nós entramos, participamos. Se envolve algum investimento, aí a gente pede ajuda, se não tiver recurso aqui. Tudo depende da utilidade, da importância disso para a gente. Se for bom, a gente faz. Aí o que precisa ser feito, alguma coisa de segurança, a gente faz também." (ENTREVISTADO 16). Caso a subunidade não possa adotar o que é exigido, o Entrevistado 16 esclarece: "Aí a gente não faz, não participa do projeto."

A integração da Subunidade 11 com outras organizações, o Governo Federal e a própria administração central da FIOCRUZ faz com que iniciativas decorrentes dessa integração pressionem para que medidas de Segurança da Informação sejam adotadas. Nessas

situações, o Entrevistado 11 afirmou que a subunidade avalia as medidas exigidas e as implicações para os usuários de TI, podendo levar à não adoção:

> Vamos supor que alguém de fora, da [nome de universidade federal] precisa acessar um dado ou um sistema nosso aqui, porque tem um projeto de um pesquisador daqui que tem colaboração com o pessoal de lá. Então eu tenho de pensar em como vou fazer para essa pessoa acessar o sistema, quais são as implicações disso. Talvez eu tenha de fazer algum tipo de documento para regular essa relação com a [nome de universidade federal], porque não posso simplesmente criar um *login* para ele, dar um acesso VPN para ele. É preciso ter um compromisso formal, e deve ficar bem claro o que ele vai acessar, para quê e até quando. E cada situação pode exigir uma solução diferente. E para o pesquisador, tem de liberar tudo. Ele não pensa nas implicações. Se o que querem for uma coisa impossível ou que esteja além dos nossos recursos, a gente tenta outra alternativa ou não libera [o acesso]. (ENTREVISTADO 11).

Em outro momento, o Entrevistado 11 fez a seguinte declaração a respeito da adoção de medidas exigidas por projetos e iniciativas de outras organizações:

> A gente avalia se é importante para nós, o custo de implementar o que é exigido, as implicações de não participar do projeto, se dá para participar sem implementar o que é exigido... Tudo isso pesa. Se realmente o que está sendo exigido for um problema, acho que a gente não participa. Se dá para fazer de outro jeito, participando sem se comprometer tanto quando à Segurança, a gente vai por esse caminho. (ENTREVISTADO 11).

Das duas subunidades que utilizaram a tática de fuga, a Subunidade 11 foi a que teve maior cobertura de percentual, com 4,92%. A Subunidade 16, por sua vez, teve 1,73% de cobertura de percentual. Das três referências de codificação identificadas, duas foram referentes à Subunidade 11 e uma à Subunidade 16. O resultado mostra que esta tática é pouco usual na organização, o que pode ser explicado pelo fato de as subunidades terem seu poder de decisão limitado pela subordinação hierárquica à administração central.

Das 17 subunidades que participaram da pesquisa, 11 responderam com esquiva. A estratégia de esquiva teve 34 referências identificadas nas entrevistas e documentos analisados. Dessas, 19 foram associadas à tática de ocultação, 12 à de amortecimento e três à fuga. A ocultação foi também a tática mais comum: dez subunidades utilizaram a tática. Já o amortecimento foi identificado em sete subunidades, enquanto a fuga foi identificada em apenas duas. Estes dados mostram que as subunidades que respondem com esquiva preferem manter uma conformidade aparente ou esconder das fontes de pressão institucional suas não conformidades do que mudar suas atividades e projetos para evitar a necessidade de estar em conformidade.

A Figura 21 apresenta as subunidades com maior cobertura de percentual para a resposta estratégica de esquiva. O destaque fica para a Subunidade 04, com 18,45%, seguida da Subunidade 11, com 6,63%, e da Subunidade 17, com 6,60%. Outras cinco subunidades responderam a pressões institucionais com esquiva.

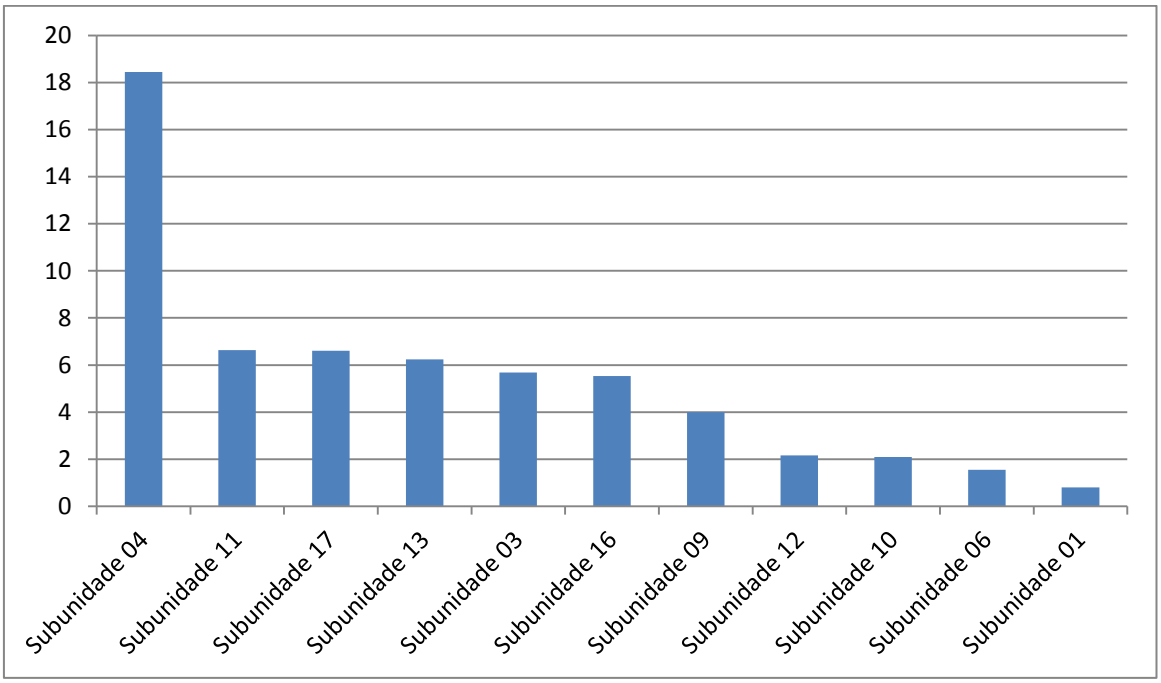


Figura 21 – Cobertura de percentual das subunidades para a resposta de esquiva.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Já a Figura 22 apresenta quantas referências à resposta estratégica de esquiva foram identificadas nas entrevistas. Neste caso, juntamente com a Subunidade 04, aparece a Subunidade 16 em primeiro lugar, com seis referências codificadas. A Subunidade 11, com cinco referências codificadas, e a Subunidade 17, com quatro referências, aparecem em seguida. Já a Subunidade 09 e a Subunidade 10 apresentaram três referências identificadas.

Os gráficos apresentados nas Figuras 21 e 22 mostram como a Subunidade 04 se destaca em tanto em cobertura de percentual quanto em número de referências codificadas para a resposta estratégica de esquiva, o que condiz com a percepção do Entrevistado 04 de que a adoção de medidas de Segurança da Informação é também uma questão de conformidade com os requisitos externos. A conformidade cerimonial, como entendem Meyer e Rowan (1977), é suficiente para legitimar a organização no seu ambiente institucional.

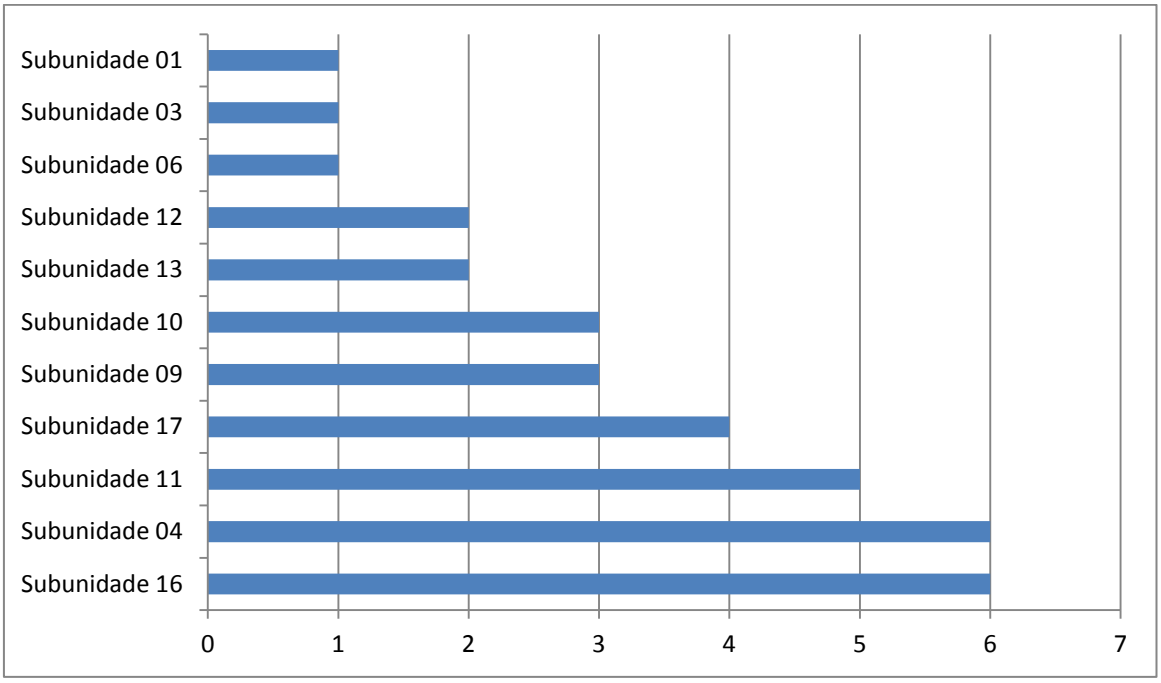


Figura 22 – Referências de codificação para a resposta de esquiva.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

Ao adotar tecnologias e definir políticas, regulamentos, processos e estruturas que afetam as atividades das subunidades, a administração central exerce poder coercitivo, e a impossibilidade de utilizar outras táticas pode levar as subunidades a fugir dessas iniciativas. No entanto, o poder que algumas subunidades podem ter sobre recursos importantes para a organização pode favorecer respostas mais agressivas de não conformidade, como será visto na seção seguinte.

6.7.4 Desafio

A resposta estratégica de desafio demonstra uma resistência ativa e inequívoca às pressões institucionais (OLIVER, 1991). As táticas desta resposta são rejeição, contestação e ataque. A rejeição significa que a organização decidiu ignorar as pressões, não adotando as regras exigidas pelos constituintes do ambiente institucional. A tática de contestação é um afastamento mais ativo, no qual a organização declara a rejeição das normas e valores institucionais. Já o ataque é uma oposição ainda mais agressiva, quando a organização desfere ataques às fontes de pressão institucional ou às pressões institucionais (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009).

Com base na proposta de Oliver (1991), em se tratando da adoção de medidas de Segurança da Informação em subunidades de uma organização, a resposta estratégica de desafio está associada à falta de controle por parte da administração central da organização e de outras fontes de pressão institucional, que permite que as subunidades desafiem a necessidade ou obrigação de estar em conformidade. De acordo com Standing, Sims e Love (2009), a estratégia tem também uma relação com o fato de as pressões virem de múltiplos constituintes do ambiente institucional e serem percebidas como ineficientes ou excessivamente restritivas pelas subunidades. A tática de rejeição, neste caso, consiste em ignorar os requisitos de Segurança da Informação, como regulamentos, leis, tecnologias, modelos e a Política de Segurança da Informação da organização. A contestação corresponde à rejeição declarada dos requisitos externos. Por fim, o ataque significa que a subunidade agiu contra os requisitos ou as fontes de pressão institucional, indicando uma postura ainda mais agressiva.

A tática de rejeição foi utilizada pelas 17 subunidades para responder às pressões institucionais com desafio. Ao analisar a não conformidade das subunidades com relação aos regulamentos de Segurança da Informação da FIOCRUZ, a auditoria interna constatou que pelo menos 21% das medidas previstas nos regulamentos não são adotadas, sendo a Norma Institucional SIC-005/CGTI/VPGDI (FIOCRUZ, 2013a) a que apresenta maior percentual de não conformidade (FIOCRUZ, 2015).

A adequação dos regulamentos da organização às necessidades e possibilidades das subunidades foi questionada nas entrevistas. O Entrevistado 11 declarou que as medidas previstas no regulamento que trata de *datacenters* (FIOCRUZ, 2013a) não foram adotadas e nem serão, pois o regulamento foi elaborado para as necessidades da CGTI e não se aplica à realidade das subunidades. Ele acrescenta que o custo envolvido não permite a adoção das medidas deste regulamento pelas subunidades: “Se a gente fosse implementar tudo o que está na norma de *datacenter*, o custo seria proibitivo”. (ENTREVISTADO 11). O regulamento que trata de acesso remoto às redes de computadores da organização (FIOCRUZ, 2013e) é também criticada por este informante, que argumenta que as medidas previstas limitam as possibilidades de os pesquisadores da subunidade trabalharem viajando ou mesmo de casa. Medidas previstas no regulamento de uso de serviços de correio eletrônico (FIOCRUZ, 2012d) também são alvo de críticas e o Entrevistado 11 admite que parte dessas medidas não é adotada.

Outras medidas, como o bloqueio do uso de serviços de armazenamento de dados em nuvem, a classificação de informações e a criação do Comitê de Segurança da Informação da subunidade também não foram adotadas. A Subunidade 11 não adota 38% das medidas previstas no regulamento de *datacenters* e 18% das medidas previstas no regulamento de acesso remoto (FIOCRUZ, 2015). Segundo o Entrevistado 11, não há uma preocupação constante das subunidades com a adoção de medidas de Segurança da Informação. Além disso, medidas que podem "prejudicar ou provocar um impacto muito grande" não são adotadas de imediato, podendo ser até rejeitadas, e medidas que podem causar uma reação negativa dos usuários de TI da subunidade são mais difíceis de serem adotadas. Por fim, o informante declara que "O importante é permitir que a unidade funcione. Se prejudica a unidade, a ideia é não adotar." (ENTREVISTADO 11). Com isto, o entrevistado mostra que medidas consideradas inadequadas às atividades desenvolvidas na subunidade não são adotadas.

O Entrevistado 02 também admite que nem todas as medidas são adotadas na sua subunidade: "Tem coisa que a gente adota em parte e tem coisa que a gente não adota. Tem coisa que a gente negocia com a CGTI, tem também coisa que a gente vai lá brigar para não ter, então depende do caso. Cada caso é uma história".

As necessidades da subunidade são consideradas ao avaliar as medidas as serem adotadas, segundo o Entrevistado 10. Nas palavras deste informante: "O que a gente procura fazer sempre aqui em [nome da subunidade] é entender a demanda do negócio. O negócio está em primeiro lugar." (ENTREVISTADO 10). Em outro trecho, ele apresenta os motivos pelos quais a subunidade não adota parte das medidas de Segurança da Informação exigidas:

> Isso leva tempo e, em alguns casos, precisa de orçamento mesmo. Pior agora que estamos em uma fase de crise, uma época de crise. E às vezes, não está de acordo com a visão de negócio mesmo. Nesse momento, pode não ser estrategicamente viável. (ENTREVISTADO 10).

O Entrevistado 16 relatou a rejeição de diferentes medidas tecnológicas em sua subunidade, como limitações de uso do serviço de correio eletrônico para envio de arquivos em anexo, utilização de serviços de armazenamento de arquivos em nuvem e remoção de caixas postais de correio eletrônico de pessoas que não têm mais vínculo com a subunidade. Sobre o bloqueio das contas de acesso à rede de computadores e a remoção de caixas postais de correio eletrônico de pessoas que perderam o vínculo com a subunidade, o informante

admitiu que as regras são desrespeitadas, mas explica que o interesse da subunidade é considerado:

> A gente sempre dá um prazo a mais para o aluno defender [dissertações e teses]. A bolsa [de estudos do aluno de pós-graduação] acaba muitas vezes antes da defesa e o certo seria bloquear. Então o que a gente faz? Segura o *login* ativo mais um pouco, até ele defender. O *email* também. Olha, tem pesquisador aposentado aqui há mais de dez anos que continua com *email*. A gente não apaga porque sabe que vai prejudicar a pesquisa dele. [...] Eu sei que manter ativo é contra as regras, mas bloquear é contra também aos interesses da [nome da subunidade], porque se a pesquisa dele continua, então ele deve continuar ativo. (ENTREVISTADO 16).

Em outro momento, o entrevistado complementou que as medidas são rejeitadas porque "não são coerentes com as atividades desenvolvidas pelos pesquisadores. [...] Se atrapalhar, a gente não faz. A gente não implementa, não adota, não elabora o documento, a regra." (ENTREVISTADO 16).

O Entrevistado 12 citou que a rejeição dos usuários impôs dificuldades para adotar algumas medidas, como a proibição da utilização de serviços de correio eletrônico particulares para fins de trabalho, o que é proibido pelo regulamento que trata de correio eletrônico (FIOCRUZ, 2012d). O entrevistado complementou que não é a existência de regulamentos externos que faz com que as medidas sejam adotadas na subunidade, mas ressaltou a importância de ações de conscientização:

> É no convencimento ainda. Nada externo, dizendo que tem que adotar. Olha que têm leis, decretos, normas complementares estabelecendo a questão de Segurança, acesso à informação e uma série de coisas que obrigam, mas isso não tem impacto. Vou ser sincero com você, o que eu tenho observado que tem impacto mesmo é o convencimento, de mostrar que tem que ser assim por conta disso, se não adotar tais procedimentos, pode impactar lá na frente em uma colaboração com uma universidade ou com outro órgão que faça parte de um projeto, que vê que a gente não tem essa questão da Segurança amadurecida. [...] Esses fatores externos, normativos, do Governo ou de forma geral, não vejo como tendo um impacto, uma influência. (ENTREVISTADO 12).

O bloqueio da utilização de serviços de armazenamento em nuvem é uma medida que a Subunidade 07 também não adotou pois os usuários da subunidade necessitam desse serviço, que não é oferecido pela organização. No entendimento do Entrevistado 07, o controle de acesso físico existe, mas não se aplica a todos os equipamentos da rede de computadores da subunidade – somente alguns equipamentos de TI ligados às atividades de pesquisa têm acesso físico controlado. Outras medidas também não são adotadas, como o monitoramento e o controle do acesso dos usuários à Internet.

Para o Entrevistado 05, devido às necessidades específicas das subunidades, as restrições impostas pelas medidas de Segurança da Informação podem limitar sua autonomia e resultar em rejeição.

O Entrevistado 04 acrescentou que também a falta de iniciativas de adoção na subunidade como causa da não adoção: "[Não adotar as medidas] acaba sendo um pouco de relaxamento [da subunidade]." (ENTREVISTADO 04). Além desse desinteresse, o Entrevistado 04 afirmou que as decisões tomadas pelo Comitê de Segurança da Informação não consideram as necessidades de todas as subunidades, pois não têm a participação de todas as subunidades, o que prejudica a adoção. Como exemplo, ele citou a tentativa de proibir a aquisição de equipamentos, considerada prejudicial às subunidades distantes e que dependem da sua própria infraestrutura de TI:

> A ideia de centralizar a infraestrutura tecnológica ou serviço de TI em um local na CGTI é boa, mas ela não funciona porque a CGTI não funciona em alguns lugares. Como ela vai prestar suporte ao usuário? Porque, se você está na [nome de outra subunidade], você tem que ter uma TI lá. Não teria como centralizar. Mesmo aqui dentro de Manguinhos não funciona. (ENTREVISTADO 04).

Da mesma forma, o Entrevistado 09 também entende que o regulamento que trata do *datacenter* (FIOCRUZ, 2013a) não se aplica às subunidades, tanto por falta de recursos para adotar as medidas previstas quanto por inadequação dessas medidas ao ambiente computacional das subunidades. Essa inadequação é percebida também quanto às medidas previstas no regulamento sobre acesso remoto, que, na opinião do entrevistado, prejudica as atividades de pesquisa. A falta de punição para o descumprimento dos regulamentos e medidas é também outra causa da rejeição nas subunidades, relatada pelo Entrevistado 09, Entrevistado 15 e outros cinco entrevistados. Quanto aos recursos necessários para adotar certas medidas de Segurança da Informação, o Entrevistado 09 afirmou:

> Aqui, algumas coisas não são implantadas porque a gente não tem condições de fazer. A norma do *datacenter* [Norma Institucional SIC-004/CGTI/VPGDI], a gente faz pouco do que está ali porque não tem dinheiro. [...] A gente não tem uma equipe de tratamento de incidentes de segurança, não tem uma pessoa que fique dedicada à segurança da informação. Isso a gente deveria ter, mas não tem ainda. Tem que fazer concurso ou contratar empresa para prestar o serviço. Aí fica difícil. Muita coisa a gente não faz por falta de dinheiro e de gente também. Quando tiver, faz essas coisas, adota. (ENTREVISTADO 09).

A Figura 23 mostra que a Subunidade 09, com 20,04%, foi a que teve maior cobertura de percentual para rejeição. A Subunidade 04 vem em segundo lugar, com 16,97% de cobertura de percentual, e a Subunidade 07, com 15,20%, ficou em terceiro lugar. Os resultados da pesquisa mostram que a tática de rejeição é difundida entre as subunidades e que os motivos principais da utilização desta tática são a inadequação das medidas às suas necessidades e a percepção de que não haverá punição caso haja descumprimento. Quanto ao número de referências de codificação, a Subunidade 12, com 12 referências identificadas, é a que mais apresentou evidências da tática de rejeição. A Subunidade 04, com nove referências identificadas, ficou em segundo lugar, seguida da Subunidade 11, com oito referências. A Subunidade 09 e a Subunidade 07, com sete referências cada, aparecem em seguida.

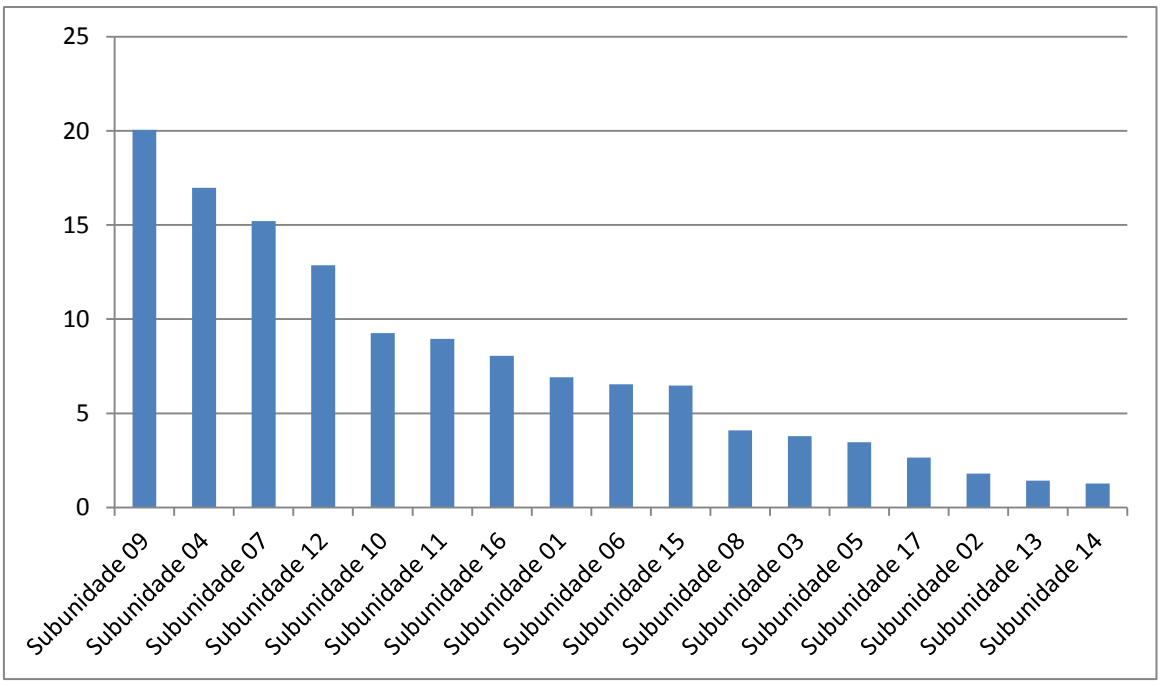


Figura 23 – Cobertura de percentual das subunidades para a tática de rejeição.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

A contestação como tática da resposta de desafio significa que a subunidade desafiou ativamente as pressões institucionais, declarando que não vai adotar as medidas. Esta tática foi identificada nas respostas de informantes de 11 subunidades. Nas entrevistas, foram identificadas 29 referências a esta estratégia, como a relatada pelo Entrevistado 09: "Minha diretoria já se posicionou contra algumas coisas." Em outro momento, o entrevistado informa que a contestação junto à administração central depende das medidas que a subunidade está sendo pressionada a adotar: "Olha, quando é bom, a gente adota. Tem coisa que a gente adota

em parte, e tem coisa que a gente não adota. Tem coisa que a gente negocia com a CGTI, tem também coisa que a gente vai lá brigar para não ter, então depende do caso.” (ENTREVISTADO 09). Este entrevistado reafirma o posicionamento da Subunidade 09 em outro momento da entrevista:

> Já aconteceu de [nome do Vice-Diretor de Gestão da subunidade] ser contra, participar de reunião e dizer que era contra para todo mundo. Claro, sempre justificando seu posicionamento. Se a coisa não é boa para nós, ele pode até chegar a fazer isso. Porque as coisas nem sempre são discutidas amplamente com as unidades. [...] Teve o caso de [a administração central da FIOCRUZ] tentar proibir de comprar servidor, equipamento de rede, essas coisas, e nosso vice [Vice-Diretor de Gestão] não aceitou. Discutiu na reunião, se posicionou contra, e desistiram disso. Tinha até uma portaria que ia ser publicada, mas desistiram. Não foi só a gente, mas outras unidades se rebelaram também. (ENTREVISTADO 09).

Como também mostraram outras entrevistas, diferentes subunidades utilizaram esta tática para desafiar pressões da administração central da organização. A necessidade de autorização e cadastro de equipamentos particulares para utilização da rede sem fio da Subunidade 17, como previsto na Norma Institucional SIC-002/CGTI/VPGDI (FIOCRUZ, 2012c), já foi alvo de críticas da direção da subunidade junto ao departamento de TI e à própria CGTI. Como consequência, a subunidade está estudando a implantação das tecnologias necessárias para prover esse acesso de outras maneiras: “A gente já fez o levantamento de custo dos equipamentos que podem ser utilizados para poder fazer essa melhoria nesse serviço que é disponibilizado.” (ENTREVISTADO 17).

O Entrevistado 17 relatou também o uso da tática de contestação quando a administração central da FIOCRUZ tomou iniciativas com a intenção de centralizar os serviços de TI de todas as subunidades no *datacenter*: “Já tentaram colocar os servidores [de rede de computadores] das unidades no *datacenter* da FIOCRUZ, mas [nome do Vice-Diretor de Gestão da subunidade] foi contra isso e esse posicionamento da Presidência [da FIOCRUZ] não foi adiante.” (ENTREVISTADO 17).

A reação negativa dos gestores da Subunidade 08 é relatada pelo responsável pela TI da subunidade. Segundo o entrevistado, quando houve a publicação de regulamentos de Segurança da Informação pela FIOCRUZ, os gestores contestaram a proibição do uso de sistemas correio eletrônico e computadores particulares para fins de trabalho:

> Os nossos gestores [...] tiveram reação negativa. [...] Teve gente aqui dentro que usava o [sistema privado de correio eletrônico] e não usava o *email* institucional. Tem uma [norma institucional] que trata de dispositivos móveis [Norma Institucional SIC-

> 007/CGTI/VPGDI], e aqui a gente não tinha uma rede separada para dispositivos móveis, então a pessoa chegava e ligava o computador pessoal na rede e usava. Eles reclamaram disso também. Da parte de gestão, a gente teve várias reclamações. (ENTREVISTADO 08).

De acordo com o coordenador de TI da Subunidade 04, como cada subunidade tem características específicas, é necessário avaliar a adequação das medidas à necessidade de cada uma antes de regulamentar e exigir sua adoção. A identificação das necessidades específicas para evitar a adoção indistinta de medidas de Segurança da Informação é prevista na literatura (DRESNER, 2011; ABNT, 2013; SÊMOLA, 2014). Nesse sentido, o Entrevistado 04 entende que o caminho mais apropriado é elaborar regulamentos menos restritivos, que se apliquem a todas as subunidades indistintamente, permitindo que cada uma regulamente assuntos específicos e adote as medidas mais adequadas. O entrevistado citou também a tentativa de proibir a aquisição de equipamentos como causa da contestação que algumas subunidades fizeram junto à administração central da organização:

> Teve uma circular sobre impedimento para compra de alguns tipos de equipamentos. Foi uma proposta levada ao conselho da FIOCRUZ [Conselho Deliberativo da FIOCRUZ], os diretores receberam e só chegou aos gestores de TI o negócio praticamente decidido. Os gestores, em conversa com seus vices [Vice-Diretores], começaram a discutir e apontar que não deve ser assim, que isso iria tirar autonomia das unidades, que a decisão vai deixar todo mundo sucateado. O estardalhaço, o grito foi tão grande de algumas unidades, e uma delas foi a nossa, que chegou lá batendo, que eles desistiram. Eles nem voltaram com aquela circular. (ENTREVISTADO 04).

As medidas previstas no regulamento da FIOCRUZ sobre acesso remoto (FIOCRUZ, 2013e) são percebidas pelo Entrevistado 16 como incoerentes com as necessidades da sua subunidade, o que levou sua direção a contestá-las junto à CGTI. O entrevistado complementa que as decisões da sede não consideram situações específicas de todas as subunidades, concordando com o entrevistado da Subunidade 04. Como exemplo, mais uma vez é citada a implantação do *datacenter* da organização, a proibição de adquirir equipamentos e a tentativa de centralizar os serviços de TI como medidas inadequadas, todas contestadas junto à CGTI. Sobre estas medidas, o entrevistado relatou:

> Quando tentaram colocar nossa rede lá no *datacenter*, aí conversamos com a diretoria [da subunidade], a gente conversou e decidiu que seria pior. Argumentei que não dava para prestar um bom serviço estando distante dos dados, dos servidores e dos serviços, que iria ser uma dependência muito grande da CGTI. Então ele concordou e avisou lá na Presidência [da FIOCRUZ] que não iria ser feito. É claro que justificou, explicou os motivos, aquilo que eu disse, mas não iria fazer e pronto. A mesma coisa foi quando queriam proibir a gente de comprar equipamentos. Pelo mesmo motivo: o *datacenter*.

> [...] Nesse caso, o nosso Vice-Diretor [de Gestão] se posicionou contra e disse que a gente iria comprar os equipamentos que fossem necessários. [...] Acho que outras unidades fizeram o mesmo. Então eles recuaram. Construíram o *datacenter*, mas não estão mais com essa política. (ENTREVISTADO 16).

A Subunidade 16 teve sete referências codificadas no NVivo para contestação, sendo a que apresentou maior quantidade de referências identificadas. Subunidade 01, Subunidade 04, Subunidade 08, Subunidade 09 e Subunidade 17 tiveram três referências de codificação cada. A Figura 24 mostra a Subunidade 16, com 9,55%, como a que apresentou maior cobertura de percentual para a tática de contestação. Em seguida, aparecem a Subunidade 04, com 7,94%, a Subunidade 01, com 7,80%, e a Subunidade 08, com 7,18%. As entrevistas mostraram que a tática de contestação foi utilizada quando houve a percepção de que as medidas não eram adequadas à realidade da subunidade, sendo citadas de forma recorrente as tentativas de proibir a aquisição de equipamentos de TI e Segurança da Informação e centralizar os serviços e recursos de TI das subunidades no *datacenter* da organização.

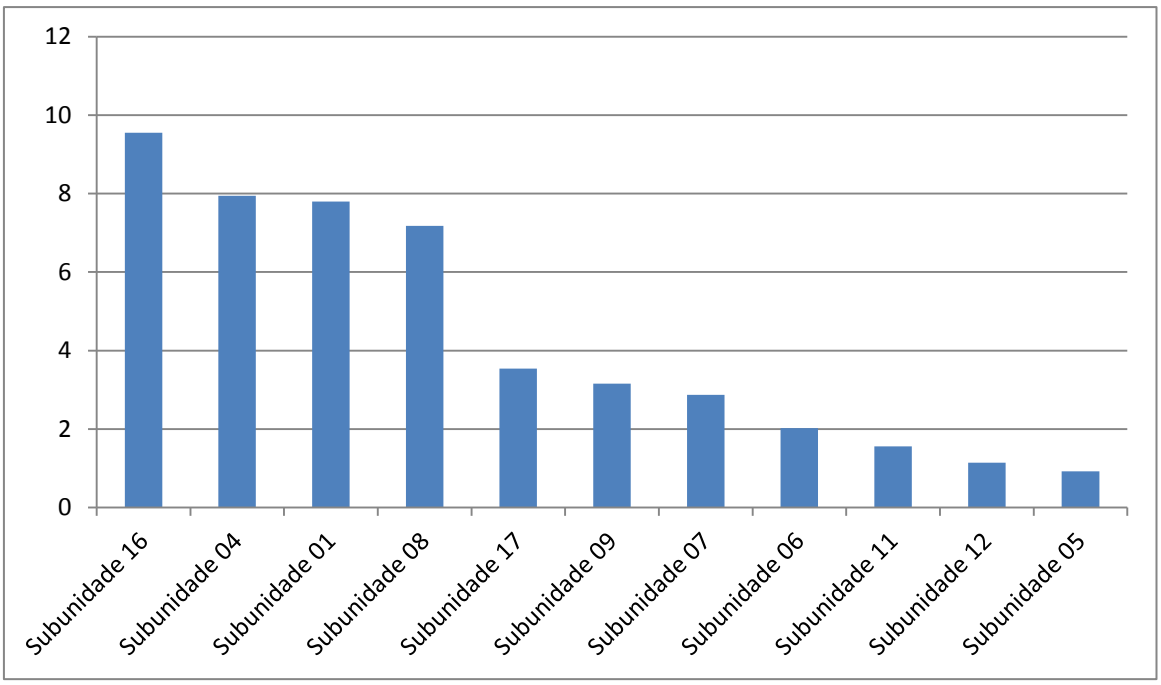


Figura 24 – Cobertura de percentual das subunidades para a tática de contestação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

A tática de ataque é uma forma de desafiar as pressões institucionais ou as fontes de pressão por haver discordâncias quanto aos requisitos institucionais (OLIVER, 1991). Medidas de Segurança da Informação exigidas pela administração central ou por outras organizações podem ser consideradas ineficientes ou restritivas demais para as subunidades. Os dados mostram que apenas duas subunidades utilizaram esta tática: a Subunidade 03 e a Subunidade 17.

O entrevistado da Subunidade 17 informou que os gestores se posicionaram contra a padronização de caixas postais de correio eletrônico e a utilização de senhas complexas para acesso a este serviço, medidas previstas na Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d), criticadas por serem consideradas ineficazes. O entrevistado citou também o ataque de membros da direção contra o projeto de integração de tecnologias de autenticação de usuários para acesso à rede de computadores, correio eletrônico e sistemas de informação, que permite reduzir a quantidade de senhas utilizadas pelos usuários por meio da centralização do controle de acesso lógico. As críticas direcionadas ao Comitê de Segurança da Informação tinham por base a alegação de que as medidas prejudicariam o trabalho desenvolvido nos laboratórios da subunidade, onde se tinha o hábito de vários usuários de TI compartilharem senhas de acesso à rede de computadores. Apesar dos ataques, o entrevistado relatou que as medidas não foram revogadas.

A direção da Subunidade 17 protagonizou ainda um ataque ao seu único regulamento de Segurança da Informação formalizado. O coordenador de TI afirmou que o regulamento, que fora elaborado e aprovado em 2008, sempre foi criticado dentro da subunidade, mas que as críticas não impediram a adoção das medidas técnicas previstas. Segundo o relato do Entrevistado 17, depois da publicação da Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d) pela administração central da FIOCRUZ, novos membros da diretoria da subunidade passaram a atacá-lo com mais veemência, o que resultou no seu enfraquecimento e na rejeição de parte das medidas adotadas.

O ataque da Subunidade 03 identificado na pesquisa não foi relatado pelo informante desta subunidade, mas identificado no relatório de auditoria (FIOCRUS, 2015). O relatório registra um apontamento referente ao uso de sistemas de correio eletrônico particulares na subunidade para fins de trabalho, um desrespeito à Norma Institucional SIC-003/CGTI/VPGDI (FIOCRUZ, 2012d). Diante da recomendação de observar o regulamento organizacional, a subunidade respondeu que está ciente do uso indevido, mas sugere a

centralização da gestão do correio eletrônico da organização, criticando o regulamento organizacional e a descentralização dos sistemas de correio eletrônico na organização.

A Subunidade 17 apresentou 6,94% de cobertura de percentual para a tática de ataque, enquanto a Subunidade 03 apresentou 2,93%. Os ataques identificados na entrevista com o coordenador de TI da Subunidade 17 foram contra medidas adotadas pela área de TI local e contra a administração central da FIOCRUZ sob a alegação de que prejudicavam o desenvolvimento das atividades na subunidade. Já o ocorrido na Subunidade 03 é contra o regulamento da organização, considerado incoerente com as necessidades da organização como um todo. A Subunidade 17 apresentou quatro referências de codificação, enquanto a Subunidade 03 apresentou uma referência.

Além das táticas de rejeição, contestação e ataque previstas por Oliver (1991), a pesquisa evidenciou ainda o **reconhecimento**, identificado nas respostas dos informantes da Subunidade 04, Subunidade 08 e Subunidade 15. Tal qual qualquer tática de desafio, o reconhecimento caracteriza a rejeição dos regulamentos institucionais, mas essa rejeição não é uma decisão estratégica, racional, no sentido de não adotar, mas está relacionada à falta de capacidade e ao fato de a subunidade não ter realizado ações no sentido da adoção. Nesse sentido, há um reconhecimento da necessidade e da importância da adoção, mas a subunidade, ainda assim, não adota.

Não adotar as medidas de Segurança da Informação devido à incapacidade da subunidade é uma situação reconhecida por membros do Comitê de Segurança da Informação da organização. O Entrevistado 18 entende que as subunidades tentam implantar as medidas de Segurança da Informação, mas encontram dificuldades: “A unidade não faz porque ela tem dificuldade de implementar, não porque não tenta implementar. Não é porque não se aplica à realidade dele.” O Entrevistado 19 reforça o entendimento de que a baixa conformidade das subunidades não é intencional, mas acrescenta que a falta de planejamento é a causa:

> Pelo que eu vejo o conhecimento sobre as regras, as normas, é notório. Eles sabem. [...] O problema está na fragilidade, ou na ausência de planejamento. O que nós fazemos com muita prática é apagar incêndio, e quando se apaga incêndio, a gente fica à margem, deixa de cumprir determinadas normas legais. Então eu acho que a falta de planejamento é um fator determinante para o descumprimento de normas, de regras. (ENTREVISTADO 19).

Quanto à afirmação do Entrevistado 19, a falta de planejamento pode ser entendida como falta de capacidade de planejar as ações de Segurança da Informação, o que é

condizente com a ausência de estruturas nas subunidades, como o Comitê de Segurança da Informação e o Escritório de Segurança da Informação, responsáveis por ações estratégicas e táticas de Segurança da Informação (CASEY, 2005; MARTIN; KHAZANCHI, 2006; MANOEL, 2014; SÊMOLA, 2014).

Sem relatar nenhuma ocorrência na sua subunidade, o Entrevistado 05 concorda que a falta de recursos prejudica a conformidade das subunidades. Da mesma forma, embora entenda que sua subunidade tem uma parcela de culpa por não ter agido para que a adoção das medidas de Segurança da Informação acontecesse, o Entrevistado 04 acredita que as mesmas não são adotadas por falta de recursos:

> A falta de recursos também não ajuda muito. Aí digo recurso, mas não é só verba. Recursos humanos. Muitas vezes a gente perde funcionário, o setor é reduzido, o trabalho não termina porque a pessoa que era competente para o trabalho sai. [...] Acho que é por falta de recursos. (ENTREVISTADO 04).

A Subunidade 08 não adota as medidas que limitam o acesso dos usuários a repositórios virtuais na Internet, mas há um entendimento de que elas são importantes e necessárias, embora nenhuma atitude tenha sido tomada para a adoção.

Para o Entrevistado 15, o fato de não ter adotado medidas de autenticação forte e outras previstas no regulamento de correio eletrônico da organização aumentam os riscos de incidentes. O entrevistado demonstra reconhecer a necessidade, mas a priorização das medidas a serem adotadas depende dos recursos que a subunidade dispõe: “Normalmente conseguimos adotar controles de acordo com necessidades técnicas mais latentes, porém priorizá-los depende também da estrutura de pessoal da área e dos custos envolvidos.” (ENTREVISTADO 15).

Os relatos desses entrevistados mostram que a adoção pode não ser possível, embora esteja nos planos das suas subunidades. Apesar de não demonstrar propriamente uma ação de desafio aos requisitos institucionais por não ser uma ação ou mesmo uma omissão intencional no sentido de não adotar, a utilização da tática de reconhecimento também não resulta em uma adoção cerimonial, parcial ou sequer a fuga da obrigação de adotar, como nas táticas da resposta de esquiva. Assim, a tática de reconhecimento pode ser inserida na resposta estratégica de desafio por representar uma maneira de não adotar as medidas de Segurança da Informação.

Os dados analisados no NVivo mostram que a Subunidade 05 apresentou 5,00% de cobertura de percentual para reconhecimento, enquanto a Subunidade 08 apresentou 1,82% e a Subunidade 04 apresentou 1,45%. Foram identificadas cinco referências à tática de reconhecimento nas entrevistas: duas na Subunidade 15, duas na Subunidade 04 e uma na Subunidade 08.

A resposta estratégia de desafio teve 108 referências codificadas no NVivo, tanto em documentos quanto nas entrevistas com os informantes das subunidades. A tática de rejeição teve 69 referências identificadas, a contestação teve 29, o ataque teve cinco e o reconhecimento, que emergiu dos dados da entrevista e cujo subnó correspondente no NVivo foi criado dentro do nó da estratégia de desafio, teve também cinco referências identificadas. A rejeição foi identificada em dados relacionados a 17 subunidades, a contestação em 11 subunidades, o ataque em duas, e o reconhecimento em três subunidades. Com isto, os dados mostram que a estratégia de desafio foi identificada nas 17 subunidades que participaram da pesquisa.

A maior cobertura de percentual apresentada para a estratégia de desafio foi da Subunidade 09: 22,43%. A Subunidade 04, por sua vez, apresentou uma cobertura de percentual de 22,09%, enquanto a Subunidade 07 teve 18,07% de cobertura de percentual para esta resposta estratégica. A Subunidade 16 teve 17,60% de cobertura de percentual, ficando em quarto lugar (Figura 25).

A Subunidade 04 e a Subunidade 12 foram as que tiveram mais referências à resposta estratégica de desafio: 14 referências para cada uma. A Subunidade 16 teve 12 referências identificadas e a Subunidade 09 teve 10 referências. Entre as que tiveram menos referências identificadas estão a Subunidade 02, a Subunidade 13 e a Subunidade 14, com uma referência codificada (Figura 26).

A Subunidade 04 se destaca por ser a que apresenta o segundo maior índice de cobertura de percentual e por ser também uma das que tiveram maior quantidade de referências à estratégia de desafio. Embora o relatório de auditoria (FIOCRUZ, 2015) não aponte esta subunidade como a que teve maior rejeição às medidas de Segurança da Informação previstas nos regulamentos da organização, os dados mostram que ela foi uma das que mais respondeu com rejeição, o que pode levar a questionamentos sobre as informações fornecidas na auditoria.

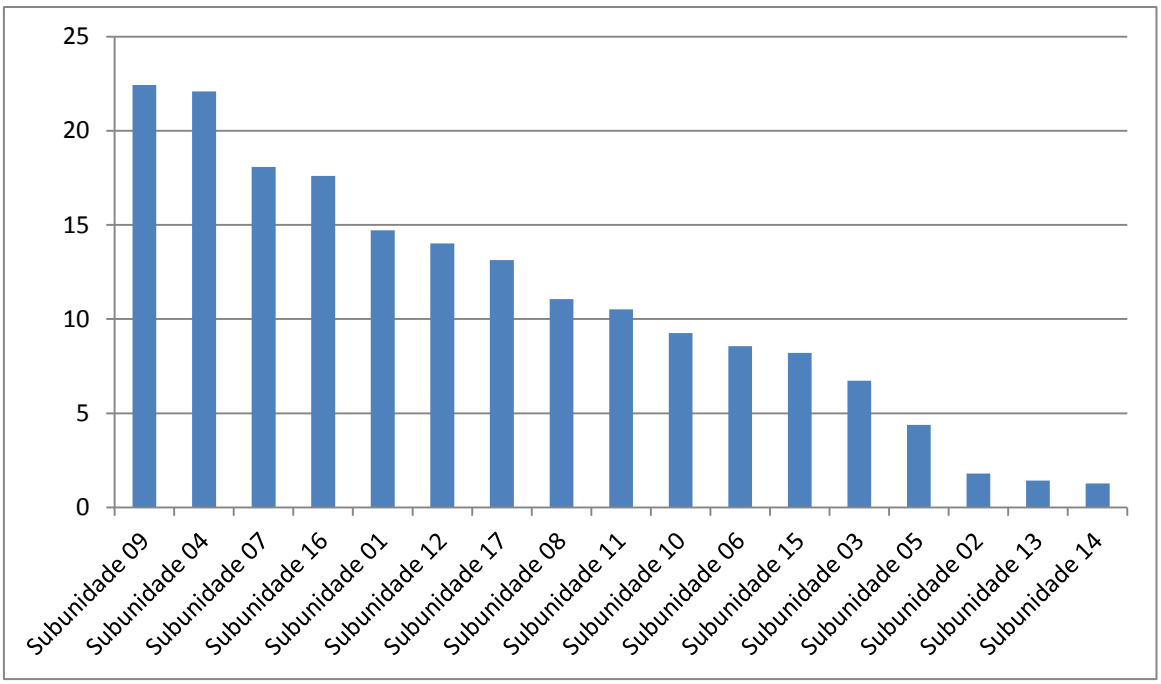


Figura 25 – Cobertura de percentual das subunidades para a resposta de desafio.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

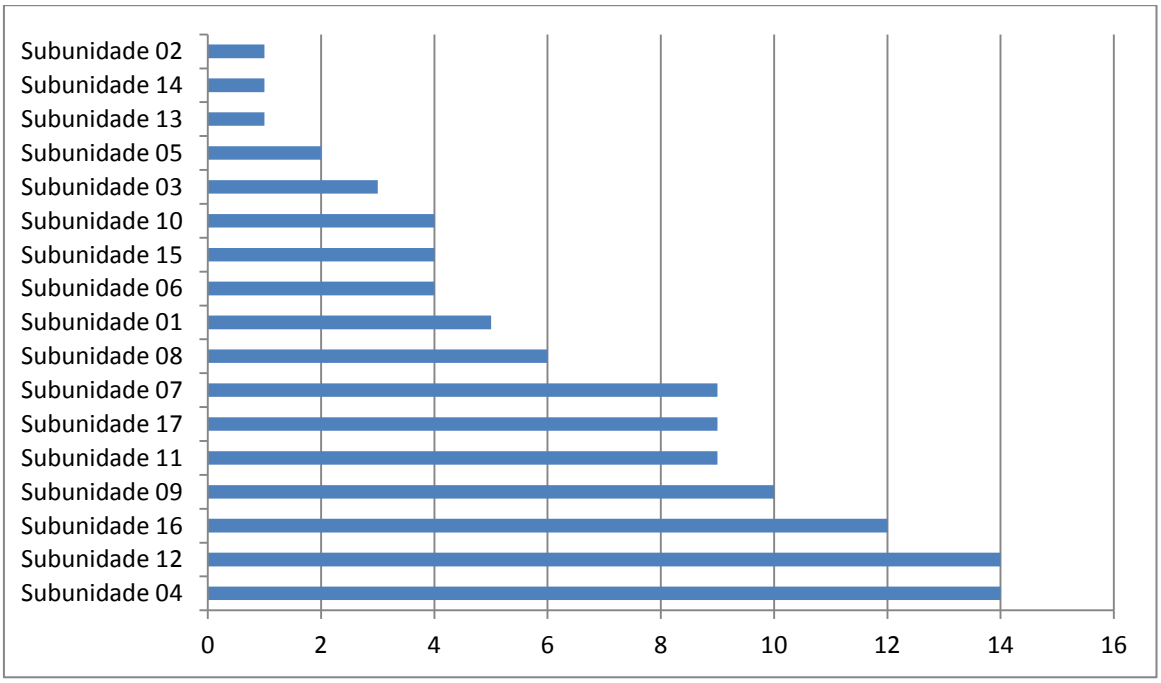


Figura 26 – Referências de codificação para a resposta de desafio.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

6.7.5 Manipulação

Oliver (1991) explica que a manipulação é a forma mais ativa de resistência. Sendo assim, a resposta estratégica de manipulação é associada por Standing, Sims e Love (2009) à existência de múltiplas demandas institucionais, à falta de autoridade das fontes de pressão institucional, à percepção de que os requisitos institucionais são pouco eficientes e à ausência de consequências relacionadas à não conformidade. As táticas desta estratégia são cooptação, influência e controle. Segundo Armênio Neto e Machado-da-Silva (1991), a cooptação é uma tentativa de persuadir membros do ambiente institucional para se aliarem à organização visando à neutralização da oposição dos constituintes do ambiente institucional. A influência envolve a tentativa de mudar as pressões institucionais através de mudanças na percepção dos constituintes do ambiente institucional quanto a valores, crenças e critérios de aceitação. O controle envolve uma tentativa de dominar os constituintes do ambiente institucional através do poder sobre eles.

Com base na descrição de Pfeffer (1974) e Dowling e Pfeffer (1975), para caracterizar a cooptação, membros da administração central da organização devem ser convidados a participar das decisões relacionadas a Segurança da Informação de uma subunidade organizacional com a intenção de conseguir apoio político. O entrevistado da Subunidade 11 declarou que trazer membros da administração central para ajudar nas decisões da subunidade pode fazer com que esta fique com um nível melhor de conformidade com os requisitos externos. O Entrevistado 09 também entende que a participação de membros da administração central nas decisões da subunidade seria positiva na promoção da conformidade na subunidade. Embora tenham essa percepção positiva, não foi possível identificar qualquer referência à tática de cooptação nas entrevistas e documentos analisados.

A tática de influência envolve o uso do prestígio da subunidade para fazer com que a administração central ou outras fontes de pressão institucional mudem exigências quanto à adoção de medidas para atender às suas necessidades e interesses. Não foram identificadas nas entrevistas ou documentos evidências de que tenha havido tentativas por parte das subunidades de influenciar constituintes do ambiente institucional além da administração central da organização.

A influência é reconhecida pelo Entrevistado 19, que afirma que há interferências das subunidades sobre o processo de decisão do Comitê de Segurança da Informação e que,

em alguns casos, a administração central não consegue evitá-las: “Sabemos que tem várias interferências que são políticas. [...] Nesse caso, são decisões políticas e a gente não tem condições de interferir.” (ENTREVISTADO 19). No entanto, o entrevistado não percebe essas influências como negativas, sejam no âmbito do Comitê de Segurança da Informação, sejam diretamente na Presidência da organização:

> Quando sai alguma norma, que pode ser até interna, que implique em mudança em procedimentos nas unidades, elas [as subunidades] costumam se posicionar de forma firme, pedindo revisão, ajustes. Então eu vejo uma atuação muito boa das unidades no caso específico do Comitê [de Segurança da Informação, uma atuação muito forte. No caso da gestão central da FIOCRUZ, as unidades estão sempre fazendo contato para rever determinada norma. (ENTREVISTADO 19).

Com a intenção de defender os interesses da sua subunidade, o Entrevistado 04 admitiu que tenta incluir profissionais de TI da subunidade nos grupos que tratam de assuntos de seu interesse: “Eu sempre tento colocar a nossa unidade com alguns membros em alguns grupos de trabalho, grupos de discussão, para que a gente faça parte disso. [...] Têm de colocar a gente nos grupos de trabalho. Participar das discussões.” (ENTREVISTADO 04). Além disso, ele declarou que entende que a direção da subunidade precisa atuar junto à presidência para defender seus interesses.

O Entrevistado 15 também entende que a subunidade deve atuar junto aos grupos que tomam decisões que afetam toda a organização. Para ele, os interesses da área de TI da subunidade precisam ser discutidos nos colegiados que aprovam os regulamentos de Segurança da Informação.

O entrevistado da Subunidade 16 relatou a ocorrência de influência da subunidade sobre a administração central e explicou que isso foi possível porque o Diretor da subunidade tem prestígio junto à presidência da organização e acesso direto ao Presidente.

O Entrevistado 14 entende que a participação dos funcionários da sua subunidade no Comitê de Segurança da Informação envolve interesses que vão além das decisões que afetam toda a organização, incluindo também a defesa dos interesses da subunidade. Essa atuação foi identificada também na Subunidade 12, quando o entrevistado admitiu que os gestores pressionaram a Presidência da FIOCRUZ tendo em vista os interesses da subunidade. Já o Entrevistado 10 não relatou esse tipo de influência, mas admitiu que soube de fatos ocorridos com pessoas de outras subunidades.

Segundo o Entrevistado 09, essas influências devem acontecer no Comitê de Segurança da Informação da FIOCRUZ. Ele relata que já compôs o Comitê, quando participou das discussões sobre três regulamentos da organização e que teve participação direta na elaboração de um regulamento, pois foi membro do grupo de trabalho responsável. O entrevistado afirmou que, ao discutir e votar quais medidas fariam parte dos regulamentos, ele considerava a possibilidade de implantação na sua subunidade: "Eu sempre pensava se era possível fazer aqui [na subunidade]. Como nem sempre era possível, às vezes eu me posicionava no sentido de minimizar o impacto para [nome da subunidade]. Se o impacto era grande, eu tentava convencer os outros para que a coisa ficasse menos exigente." (ENTREVISTADO 09). O entrevistado declarou que não havia uma orientação da direção para agir dessa forma, mas que tinha compreensão de que algumas medidas poderiam prejudicar a subunidade: "Não tinha nenhuma orientação da direção, mas eu sabia o que era possível, o que seria problema. Então eu tentava fazer com que as normas não fossem um problema para a gente." (ENTREVISTADO 09).

Por não ser mais membro do Comitê da organização, o Entrevistado 09 entende que esse tipo de influência é possível ainda através do Vice-Diretor de Gestão da subunidade, que participa de reuniões da Câmara Técnica de Gestão e Desenvolvimento Institucional da FIOCRUZ, colegiado que aprova os regulamentos discutidos no Comitê de Segurança da Informação. Segundo ele, o Vice-Diretor consulta a área de TI sobre Segurança da Informação, o que acaba por direcionar sua participação nas reuniões. Por fim, o Entrevistado 09 concluiu: "Poder, eu acho que não tem, mas tem a influência. [...] A gente pode influenciar no Comitê [de Segurança da Informação] se tiver participando, ou nas reuniões que têm a participação da direção da unidade." (ENTREVISTADO 09).

A já relatada tentativa de centralizar os serviços de TI das subunidades no *datacenter* da FIOCRUZ foi a situação que o Entrevistado 11 informou ter gerado uma resposta de manipulação através de influência por parte da sua subunidade:

> Eu falei para a diretoria o que a gente tinha, como a gente fazia, e que isso iria prejudicar a gente. Eu soube que conversaram lá na Presidência [da FIOCRUZ], que houve umas discussões na Câmara de Gestão, mas o caso é que parece que as diretorias da maioria das unidades não concordaram e fizeram com que o [nome do Vice-Presidente de Gestão e Desenvolvimento Institucional da FIOCRUZ] recuasse da ideia. (ENTREVISTADO 11).

Em outro momento da entrevista, o Entrevistado 11 complementou:

> A unidade se posicionou contra isso lá na Vice-Presidência [de Gestão e Desenvolvimento Institucional] e também na Câmara de Gestão. Foi no sentido de fazer pressão para que a exigência não fosse adiante. Não sei se conversar com a Vice-Presidência não surtiu o efeito desejado, mas na Câmara de Gestão a coisa ganhou corpo, com certeza. Os gestores conversaram com os de outras unidades, e aí a coisa funcionou. (ENTREVISTADO 11).

O Entrevistado 11 declarou que acredita que a participação das subunidades no Comitê de Segurança da Informação é importante para equilibrar as exigências da administração central com as necessidades das subunidades, mas acrescenta que todas as subunidades deveriam estar representadas no Comitê para que não fossem incluídas nos regulamentos medidas prejudiciais às suas atividades. Na opinião do informante, a influência das subunidades sobre a administração central a fim de defender seus interesses acontece na Câmara Técnica de Gestão e Desenvolvimento Institucional, concordando com o Entrevistado 09. Além disso, o Entrevistado 11 citou as reuniões entre os gestores das subunidades localizadas fora do Rio de Janeiro como local para influenciar a administração central, que "tem força para propor mudanças ou mudar situações lá na Presidência [da FIOCRUZ]." Para finalizar, o informante afirmou que acredita que uma subunidade sozinha não tem poder suficiente para influenciar a administração central, embora reconheça que duas subunidades desenvolvem atividades que têm um impacto grande para a população e que isso talvez dê a elas algum poder sobre a Presidência da organização.

O Entrevistado 17 também entende que o fórum de gestores das subunidades regionais, que tem discutido também Segurança da Informação, é um grupo através do qual pode haver influência da subunidade sobre as decisões que afetam toda a organização.

O entrevistado da Subunidade 17 relatou o ainda a ocorrência mais característica de influência com o intuito de mudar medidas de Segurança da Informação para adequá-las às necessidades da subunidade: a mudança de um regulamento já publicado pela organização. Por não concordar com medidas presentes no regulamento que trata da utilização de serviços de correio eletrônico (FIOCRUZ, 2012d) – especificamente, contra o bloqueio e exclusão de caixas postais de ex-funcionários e ex-alunos – e tendo já reduzido a efetividade das medidas presentes no regulamento da própria subunidade, a diretoria entrou em contato com a Presidência da organização argumentando que essas medidas fossem suspensas. O Entrevistado 17 afirmou que o bloqueio de caixas postais de pessoas que perdem o vínculo com a organização não está mais em vigor devido à influência da direção da subunidade sobre a administração central da organização. Este relato foi confirmado em consulta a documentos

pessoais que foram disponibilizados pelo entrevistado. Destes documentos, foi possível extrair o seguinte trecho:

> O tempo limite de 2 anos após a aposentadoria para desativação da conta [de correio eletrônico] (Portaria 433/2012-PR) cria um problema potencial para os pesquisadores que utilizaram o e-mail nos seus trabalhos. [...] Peço-lhes suspender a validade do item 5.3.2 [que trata do bloqueio da caixa postal] até que o assunto seja reavaliado. (DOCUMENTO PESSOAL DO ENTREVISTADO 17).

A pesquisa mostrou que as nove subunidades que utilizaram a tática de influência reagiram de forma contrária à tentativa da administração central de proibir a aquisição de equipamentos de TI com o objetivo de centralizar os serviços no *datacenter* da organização, seja atuando diretamente junto à Presidência da organização, seja na Câmara Técnica de Gestão e Desenvolvimento Institucional, seja no fórum no qual as subunidades regionais discutem assuntos em comum.

A Figura 27 mostra a cobertura de percentual que as respostas de cada entrevistado e os documentos analisados apresentaram para o subnó influência após a codificação. A Subunidade 11 teve 9,26%, sendo a que apresentou maior cobertura de percentual para a tática influência. A Subunidade 17 teve 7.08% de cobertura de percentual, ficando em segundo lugar. A Subunidade 09, com 6,36%, ficou em terceiro lugar, enquanto a Subunidade 15 apareceu em seguida, com 3,50%. Outras cinco subunidades também apresentaram referências a esta tática de manipulação. A Subunidade 09 teve sete referências de codificação identificadas, sendo a que apresentou maios quantidade e, portanto, a que mais utilizou a tática de influência. A Subunidade 11, com cinco referências, foi a que ficou em segundo lugar. Em terceiro lugar está a Subunidade 17, com quatro referências identificadas.

A tática de controle corresponde à utilização do poder das subunidades sobre a administração central da organização ou outras fontes de pressão institucional. A intenção é fazer com que os constituintes do ambiente institucional e a administração central exijam ou deixem de exigir a adoção de medidas de Segurança da Informação em benefício próprio. O poder das subunidades sobre as fontes de pressão institucional pode dar a elas oportunidade de controlar os constituintes do ambiente institucional e fazê-los mudar requisitos de Segurança da Informação conforme seus próprios interesses, mas não foram identificadas nas entrevistas e documentos analisados evidências de que tenha havido qualquer tentativa de controle das subunidades sobre a administração central ou mesmo outras organizações.

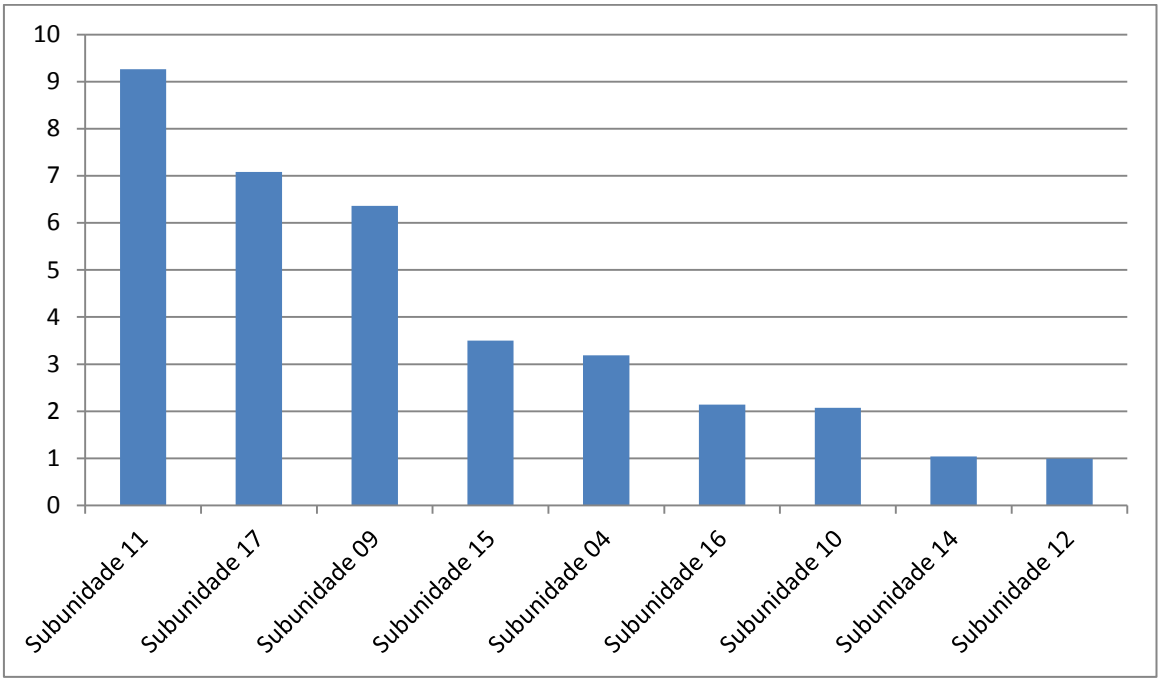


Figura 27 – Cobertura de percentual das subunidades para a tática de influência.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

A maior cobertura de percentual para a estratégia de manipulação foi identificada nos dados relacionados à Subunidade 11. Esta subunidade teve 9,26% de cobertura de percentual, seguida da Subunidade 17, com 7,08%, e da Subunidade 09, com 6,36%. A Subunidade 12 teve 0,99% de cobertura de percentual com relação a esta estratégia, sendo o menor percentual identificado (Figura 28).

A resposta estratégica de manipulação teve 27 referências codificadas, todas no subnó influência, pois não foram identificadas referências às táticas de cooptação e controle nos dados analisados. A Figura 29 mostra a Subunidade 09 como a que tem maior quantidade de referências de codificação para a resposta de manipulação. A Subunidade 11 aparece em segundo lugar, com cinco referências, seguida da Subunidade 17, com quatro. A Subunidade 10, a Subunidade 14 e a Subunidade 15 aparecem com apenas uma referência codificada, sendo as que têm menos codificações identificadas nos dados analisados.

A pesquisa mostrou até aqui uma variedade de medidas de Segurança da Informação adotadas, diferentes respostas estratégicas e diferentes julgamentos que as subunidades fazem sobre as medidas que são pressionadas a adotar. A seção seguinte discute a relação entre as pressões para adoção de medidas técnicas, formais e informais de Segurança da Informação e as respostas estratégicas.

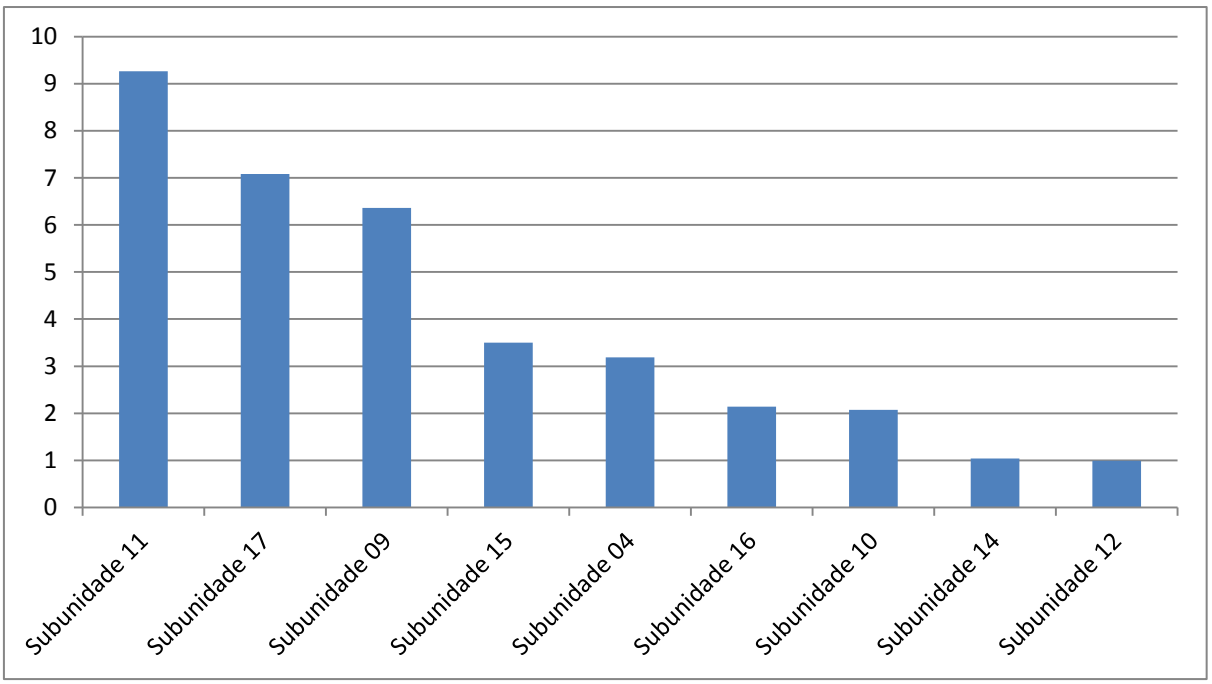


Figura 28 – Cobertura de percentual das subunidades para a resposta de manipulação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

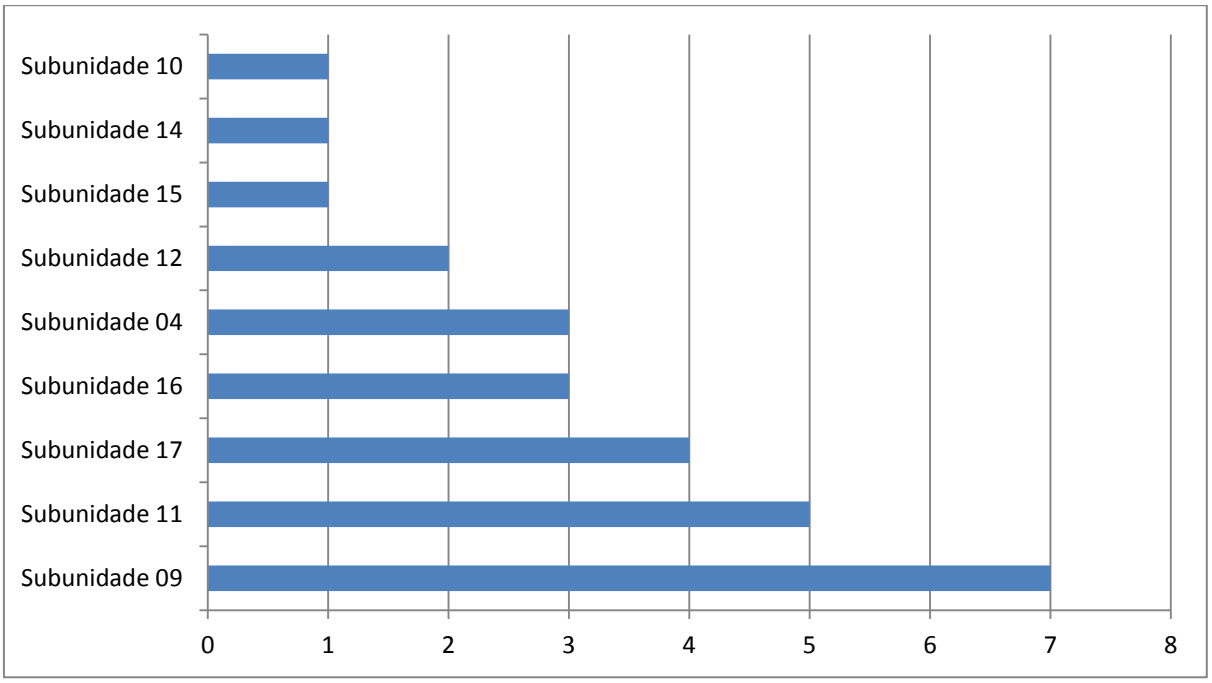


Figura 29 – Referências de codificação para a resposta de manipulação.
Fonte: Imagem criada pelo autor com dados da pesquisa analisados no NVivo 10.

6.8 ANÁLISE DAS RESPOSTAS DAS SUBUNIDADES

A pesquisa mostrou heterogeneidade quanto às respostas que as subunidades deram às pressões institucionais para adoção de medidas de Segurança da Informação, pois todos os tipos apresentados por Oliver (1991) foram identificados na pesquisa, sendo que sete subunidades responderam às pressões com as cinco estratégias.

Dados de oito subunidades apresentaram maior cobertura de percentual para a resposta estratégica de desafio, o que significa que essas oito subunidades apresentaram mais dados codificado para a resposta de desafio. Cinco subunidades apresentaram maior cobertura de percentual para a aquiescência, enquanto três tiveram o compromisso e uma teve a esquiva como as respostas que mais se destacaram em cobertura de percentual. Nenhuma subunidade teve a manipulação como a resposta com maior cobertura de percentual (Tabela 5). Isto significa que as transcrições e documentos não tinham ênfase em manipulação, evidenciando que essa estratégia é pouco utilizada, possivelmente porque as subunidades que participaram da pesquisa não têm poder sobre a administração central.

Tabela 5 – Cobertura de percentual para cada resposta estratégica.

SUBUNIDADE	COBERTURA DE PERCENTUAL (%)				
	Aquiescência	Compromisso	Esquiva	Desafio	Manipulação
Subunidade 01	13,26	4,20	0,80	**14,71**	0
Subunidade 02	3,18	**21,65**	0	1,80	0
Subunidade 03	**15,80**	4,52	5,68	6,72	0
Subunidade 04	3,77	6,03	18,45	**22,09**	3,19
Subunidade 05	**13,05**	10,81	0	4,38	0
Subunidade 06	13,44	**16,65**	1,55	8,56	0
Subunidade 07	10,27	9,68	0	**18,07**	0
Subunidade 08	10,42	**15,54**	0	11,06	0
Subunidade 09	19,91	6,10	3,99	**22,43**	6,36
Subunidade 10	**17,14**	3,76	2,10	9,26	2,07
Subunidade 11	5,31	3,83	6,63	**10,52**	9,26
Subunidade 12	8,79	9,93	2,16	**14,01**	0,99
Subunidade 13	5,78	1,80	**6,24**	1,43	0
Subunidade 14	**11,72**	5,07	0	1,28	1,04
Subunidade 15	**8,78**	0	0	8,21	3,50
Subunidade 16	8,86	9,20	5,53	**17,60**	2,14
Subunidade 17	8,11	4,74	6,60	**13,13**	7,08

Nota: Respostas estratégicas com maior cobertura de percentual destacadas para cada subunidade.
Fonte: Tabela criada com dados calculados no *software* NVivo 10.

As respostas de aquiescência e desafio também apresentaram mais referências identificadas nas entrevistas e documentos. Nove subunidades apresentaram a aquiescência como a resposta com maior quantidade de referências, sete apresentaram o desafio, duas tiveram o compromisso e uma teve a esquiva como resposta com mais referências de codificação. Cabe ressaltar que a Subunidade 08 teve tanto a aquiescência quanto o desafio como respostas com maior quantidade de referências de codificação, enquanto a Subunidade 13 teve a aquiescência e a esquiva. A manipulação, embora tenha sido identificada em nove subunidades, não foi a resposta estratégica mais identificada para nenhuma delas, o que pode ser explicado pelo fato de esta resposta ter como requisito uma relação de poder da subunidade sobre a administração central, ou de dependência da administração central com relação à subunidade. Assim, ainda que subunidades tenham exercido esta relação de poder, esta resposta ainda é incomum em comparação com as demais (Tabela 6).

Tabela 6 – Referências de codificação para cada resposta estratégica.

SUBUNIDADE	QUANTIDADE DE REFERÊNCIAS DE CODIFICAÇÃO				
	Aquiescência	Compromisso	Esquiva	Desafio	Manipulação
Subunidade 01	**8**	3	1	5	0
Subunidade 02	2	**4**	0	1	0
Subunidade 03	**6**	3	1	3	0
Subunidade 04	5	1	6	**14**	3
Subunidade 05	**7**	4	0	2	0
Subunidade 06	5	**7**	1	4	0
Subunidade 07	5	5	0	**9**	0
Subunidade 08	**6**	5	0	**6**	0
Subunidade 09	**11**	7	3	10	7
Subunidade 10	**10**	3	3	4	1
Subunidade 11	8	3	5	**9**	5
Subunidade 12	5	8	2	**14**	2
Subunidade 13	**2**	1	**2**	1	0
Subunidade 14	**4**	3	0	1	1
Subunidade 15	**5**	0	0	4	1
Subunidade 16	9	8	6	**12**	3
Subunidade 17	8	4	4	**9**	4
TOTAL	106	69	34	108	27

Nota: Respostas estratégicas com maior quantidade de referências destacadas para cada subunidade.
Fonte: Tabela criada com dados calculados no *software* NVivo 10.

Algumas divergências entre a cobertura de percentual e a quantidade de referências identificadas foram percebidas na análise. A Subunidade 01, que teve o desafio como resposta com maior cobertura de percentual, teve a aquiescência como resposta com mais referências. A Subunidade 08, que teve o compromisso com maior cobertura de

percentual, apresentou outras duas respostas como as que têm mais referências de codificação: aquiescência e desafio. A Subunidade 09, que teve a aquiescência como a resposta com maior quantidade de referências codificadas, apresentou o desafio como resposta com maior cobertura de percentual. Já a Subunidade 13, que teve a aquiescência e a esquiva como as respostas com mais referências de codificação, teve a esquiva também como resposta com maior cobertura de percentual. Embora apontem para diferentes respostas, esses resultados ainda mostram uma predominância de respostas de aquiescência e desafio, que representam a aceitação passiva e a resistência ativa às pressões institucionais.

No caso da Subunidade 13, a cobertura de percentual indica uma tendência à esquiva no discurso do entrevistado. As respostas de aquiescência e desafio, que tiveram a mesma quantidade de referências de codificação na Subunidade 08, figuraram também como coberturas de percentual altas para esta subunidade. Isso mostra que a subunidade tende a rejeitar os requisitos de Segurança da Informação que não são considerados eficientes ou coerentes, e que os requisitos considerados eficientes ou coerentes são adotados, mas que essa aceitação pode ser apenas aparente, como evidenciam os resultados para a resposta de esquiva.

Os dados revelam que a autonomia, que sete entrevistados apontaram como uma causa para a não conformidade das subunidades com os requisitos de Segurança da Informação, não está associada a respostas de desafio ou manipulação, visto que duas das quatro subunidades que não gozam de autonomia administrativa tiveram como resposta mais identificada nos dados o desafio, enquanto nove das 13 subunidades que têm autonomia administrativa apresentaram mais respostas de conformidade – a aquiescência foi a resposta mais identificada em sete subunidades, e o compromisso em duas (Quadro 15). Assim, tanto a percepção dos entrevistados quanto os argumentos de Pilato e Pedrini (2015) e Hernes e Erdvik (2014), de que as respostas das subunidades vão depender da sua autonomia, foram contrariadas pelos dados desta pesquisa.

Observando a cobertura de percentual das respostas do informante da Subunidade 05, nota-se que esta subunidade apresentou maior cobertura para a aquiescência, enquanto a Subunidade 09 apresentou evidências mais amplas de desafio. Já a partir da quantidade de referências de codificação, a Subunidade 09 aparece mais uma vez mais associada à aquiescência, e a Subunidade 04 e a Subunidade 12 são as que apresentam mais referências de codificação para a estratégia de desafio. Os dados mostram também que todas as subunidades responderam a pressões institucionais com aquiescência e desafio em algum momento. A

Figura 30 compara a quantidade de referências de codificação para cada resposta estratégica e mostra que não há uma resposta dominante entre as subunidades, mas duas: a aquiescência, que teve 106 referências codificadas, e o desafio, que teve 108 referências. Este resultado aponta para a tendência em aceitar pressões para adoção de medidas consideradas eficientes e adequadas, e rejeitar medidas ineficientes e inadequadas, a despeito dos interesses da administração central.

Quadro 15 – Relação entre respostas estratégicas e autonomia administrativa.

SUBUNIDADE	RESPOSTAS MAIS IDENTIFICADAS	AUTONOMIA
Subunidade 01	Aquiescência	Sim
Subunidade 02	Compromisso	Sim
Subunidade 03	Aquiescência	Sim
Subunidade 04	Desafio	Sim
Subunidade 05	Aquiescência	Não
Subunidade 06	Compromisso	Sim
Subunidade 07	Desafio	Não
Subunidade 08	Aquiescência/Desafio	Sim
Subunidade 09	Aquiescência	Sim
Subunidade 10	Aquiescência	Sim
Subunidade 11	Desafio	Sim
Subunidade 12	Desafio	Não
Subunidade 13	Esquiva	Não
Subunidade 14	Aquiescência/Esquiva	Sim
Subunidade 15	Aquiescência	Sim
Subunidade 16	Desafio	Sim
Subunidade 17	Desafio	Sim

Fonte: Elaborado pelo autor com dados da pesquisa analisados no NVivo 10.

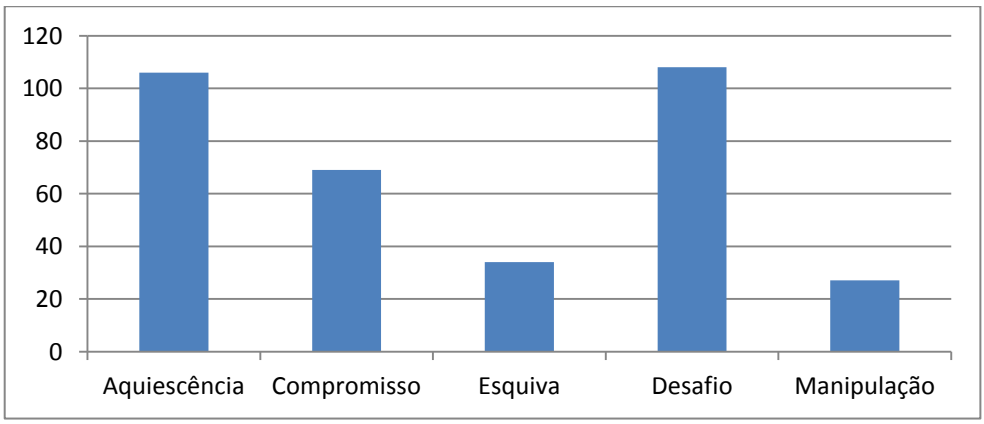


Figura 30 – Referências codificadas para as cinco respostas estratégicas.
Fonte: Imagem criada pelo autor a partir de dados da pesquisa.

Esses resultados evidenciam que essas duas respostas estratégicas antagônicas são dominantes. Apesar de as cinco respostas apresentadas por Oliver (1991) terem sido identificadas, todas as subunidades responderam a pressões institucionais tanto com desafio quanto com aquiescência. Há uma compreensão de que medidas de Segurança da Informação são importantes para garantir a confidencialidade, integridade e disponibilidade da informação e a conformidade da organização com os requisitos externos, mas muitas pressões institucionais têm como resposta o desafio, sendo esta a resposta estratégica que teve mais referências identificadas.

Nenhuma das subunidades adotou todas as medidas de Segurança da Informação que é pressionada a adotar – inclusive aquelas cujas pressões vêm de regulamentos cujo cumprimento é obrigatório, pois estes não são percebidos desta forma. As medidas de Segurança da Informação que dificultam as atividades desenvolvidas nas subunidades, as consideradas ineficientes, as que têm impacto negativo na imagem da subunidade ou que exigem recursos que as subunidades não dispõem são consideradas incoerentes e não são adotadas. A rejeição está associada à severidade das medidas exigidas e à preocupação com a eficiência das subunidades (KARYDA; KIOUNTOUZIS; KOKOLAKIS, 2005; HU; HART; COOKE, 2007; ABRAHAM; CHENGALUR-SMITH, 2011; SUN; AHLUWALIA; KOONG, 2011).

Os dados evidenciam que, apesar de a autonomia não determinar a resposta das subunidades, elas julgam as pressões institucionais antes de aceitarem ou rejeitarem as medidas que são objeto dessas pressões. Além disso, o fato de não haver sanções para o descumprimento dos regulamentos, como admitiram sete entrevistados, também pode influenciar as respostas estratégicas, corroborando com a teoria, que diz que a baixa incerteza quanto às consequências da não conformidade está associada à rejeição (STANDING; SIMS; LOVE, 2009).

Ao evidenciar respostas de manipulação, a pesquisa mostrou também que os entrevistados têm uma compreensão de que os gestores das subunidades podem influenciar diretamente a Presidência da organização a fim de atender aos interesses da subunidade. As subunidades podem influenciar a organização através da participação de seus membros no Comitê de Segurança da Informação, na Câmara Técnica de Gestão e Desenvolvimento Institucional e do fórum de gestores das subunidades. Essas influências serão tratadas na seção seguinte.

6.9 A INFLUÊNCIA DAS RESPOSTAS DAS SUBUNIDADES NA CONFORMIDADE DA ORGANIZAÇÃO

As pressões institucionais levam as organizações a formalizar políticas e regulamentos internos (DELMAS; TOFFEL, 2008; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014; PILATO; PEDRINI, 2015). Políticas e regulamentos internos são difundidos para as subunidades da organização (OSMUNDSEN, 2005), e para a organização estar em conformidade com os requisitos institucionais, é preciso que as subunidades os respeitem (BOSCHMAN, 2006). No contexto da Segurança da Informação, a Política e os regulamentos podem ser formalizados para atender a requisitos institucionais (BJÖRCK, 2004; LUESEBRINK, 2011; LOPES, 2012; NASUTION, 2012; LOPES; SÁ-SOARES, 2014; ALBUQUERQUE JUNIOR; SANTOS, 2015; ALBUQUERQUE JUNIOR *et al*., 2016). Nesse sentido, a pesquisa mostrou que a FIOCRUZ criou estruturas organizacionais e formalizou uma Política e outros regulamentos de Segurança da Informação para atender principalmente a leis e regulamentos.

A partir da formalização da Política, regulamentos e estruturas organizacionais de Segurança da Informação, a FIOCRUZ passou a difundir para as subunidades a necessidade de estar em conformidade, como argumentam diferentes autores (HOLLAND *et al*., 1994; TEO; WEI; BENBASAT, 2003; OSMUNDSEN, 2005) e como notado empiricamente nas entrevistas com membros do Comitê de Segurança da Informação da organização, especialmente o Entrevistado 18 e o Entrevistado 19. A análise dos dados coletados na pesquisa mostrou que a pressão exercida pela sede da organização, juntamente com pressões dos ambientes institucionais nos quais estão inseridas, incidem sobre as organizações, como previsto na literatura (TEMPEL *et al*., 2006; DELMAS; TOFFEL, 2008; AGUILERA-CARACUEL *et al*., 2012; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014; PILATO; PEDRINI, 2015).

A análise dos dados permitiu a identificação de pressões institucionais coercitivas, normativas e miméticas, sendo que as pressões coercitivas tiveram mais referências identificadas do que os demais tipos. Regulamentos e tecnologias adotados pela organização, a Política de Segurança da Informação organizacional e a realização de auditorias foram as pressões que tiveram mais referências identificadas, mas a publicação de recomendações

técnicas de Segurança da Informação e a realização de ações de conscientização tiveram também destaque entre as pressões normativas. A diversidade de pressões institucionais é uma causa que a literatura apresenta para a ocorrência de diferentes respostas estratégicas (BOSCHMAN, 2006; TEMPEL *et al*., 2006).

As pressões institucionais exigem que as subunidades adotem diferentes medidas formais, informais e técnicas de Segurança da Informação, mas parte dessas medidas é considerada incoerente com a realidade das subunidades institucionais. Foram identificadas medidas consideradas assim nas três categorias propostas por Dhillon (1999), mas houve a identificação de uma quantidade maior de medidas técnicas. Os entrevistados relataram que essas medidas são consideradas incoerentes devido à dificuldade em desenvolver as atividades das subunidades, a exigência de que as subunidades tenham recursos os quais não dispõem, a dificuldade em desenvolver as atividades do setor de TI, a insegurança das medidas e o prejuízo à imagem da subunidade. Medidas técnicas e medidas formais consideradas incoerentes com as necessidades das subunidades são assim avaliadas principalmente por dificultarem as atividades da subunidade. Já medidas informais são consideradas incoerentes por terem como requisitos pra adoção recursos que as subunidades não têm.

A percepção que as organizações têm quanto às pressões institucionais está relacionado ao seu comportamento com relação às respostas estratégicas, de forma que interpretação que fazem pode provocar diferentes respostas (GRAEFF, 2005; BOXENBAUM; JONSSON, 2009; LUNDBERG, 2013). De acordo com Netland e Aspelund (2014), ao serem submetidas a pressões institucionais conflitantes ou ineficientes, subunidades de uma mesma organização podem se comportar de maneiras distintas daquelas esperadas pela sua administração central. Esta pesquisa mostrou que há diferentes percepções quanto à coerência das medidas que as subunidades são pressionadas a adotar com suas atividades. Como consequência das diferentes pressões institucionais que recebem e das suas percepções quanto às medidas de Segurança da Informação, todas as subunidades adotaram mais medidas técnicas do que formais ou informais – os quatro tipos de medidas de Segurança da Informação que foram identificados em todas as subunidades que participaram da pesquisa são de natureza técnica. Entretanto, poucas subunidades adotaram todas as medidas previstas na literatura para qualquer uma das três categorias e nenhuma delas está em conformidade com todos os regulamentos de Segurança da Informação da organização.

As variações quanto à adoção podem ser explicadas pela diversidade de respostas estratégicas. Ao sofrerem múltiplas pressões e ao interpretarem essas pressões de formas distintas, as subunidades responderam com todas as estratégias propostas por Oliver (1991), corroborando com o que observaram Boschman (2006) e Tempel *et al*. (2006). Mas a análise dos dados para identificar as respostas estratégicas das subunidades mostrou que todas responderam com aquiescência a diferentes pressões institucionais, ainda que esta não tenha sido a única resposta identificada ou a resposta que teve mais referências. A aquiescência foi identificada em todas as subunidades que participaram da pesquisa, o que é coerente com o fato de todas terem adotado medidas de Segurança da Informação.

A adoção de medidas técnicas de Segurança da Informação como resultado de uma resposta de aquiescência significa que tecnologias foram implantadas para garantir a integridade, disponibilidade e confidencialidade das informações. Nesse sentido, medidas de segregação e monitoramento de redes de computadores, como *firewalls* e *proxies*, foram implantadas em todas as subunidades. Foram implantadas também medidas de redundância de dados, como *backups* de dados, que são realizados em todas as subunidades. Foram adotadas ainda medidas de prevenção contra códigos maliciosos, como utilização de antivírus e anti-spam, e medidas de controle de acesso lógico, como a utilização de *login* único para restringir acesso a funcionalidades de sistemas e recursos da rede de computadores. A adoção dessas medidas dificulta a ocorrência de incidentes relacionados a acessos não autorizados, perda de dados e infecções por vírus e outros códigos maliciosos.

Parte das subunidades tem regulamentos, processos, procedimentos e estruturas organizacionais voltados para a Segurança da Informação – em outras palavras, parte delas adotou medidas formais. Isso significa que algumas subunidades têm uma orientação formal para outras ações de Segurança da Informação. Embora nenhuma das subunidades tenha um Sistema de Gestão de Segurança da Informação, a organização tem o seu, que define como as subunidades devem organizar sua estrutura de Segurança da Informação. Nas subunidades que responderam com aquiescência à maior parte das pressões institucionais para adotar medidas formais, as responsabilidades estão definidas, há um direcionamento para as ações e há grupos responsáveis pelas decisões, o que facilita a adoção de medidas técnicas, informais e de outras medidas formais, reforçando a ideia de que as medidas são interdependentes, como descrito por Dhillon (1999) e Sveen, Torres e Sarriegi (2009).

A divulgação de regulamentos e da Política de Segurança da Informação e a realização de ações de conscientização na maioria das subunidades são também resultados de

respostas estratégicas de aquiescência. Essas medidas têm como benefício esperado a mudança do comportamento dos usuários TI, o que pode ser reforçado com treinamentos e usuários, como fazem algumas subunidades.

A identificação de 106 referências à resposta de aquiescência explica a quantidade de medidas técnicas adotadas por todas as subunidades e aponta para um comportamento de conformidade com os requisitos institucionais. Este comportamento, no entanto, é contraposto pela auditoria realizada pela organização, que mostrou que grande parte das medidas previstas nos regulamentos formalizados pela administração central não foi adotada (FIOCRUZ, 2015). Além disso, a pesquisa mostrou que muitas medidas formais e informais não são adotadas sequer pela metade das subunidades e muitas medidas técnicas não são adotadas por todas elas, o que reforça o resultado da auditoria.

No contínuo de respostas estratégicas apresentado por Oliver (1991), a segunda resposta é o compromisso. Caracterizado pela conformidade com parte dos requisitos institucionais e rejeição daqueles que não são considerados adequados às suas necessidades e interesses, o compromisso é também uma resposta de conformidade (FREZATTI; AGUIAR; REZENDE, 2007) e teve 56 referências identificadas. Das 17 subunidades que participaram da pesquisa, apenas uma não respondeu com compromisso. No entanto, apesar de a resposta de compromisso significar que a subunidade está buscando a conformidade, essa é apenas parcial (OLIVER, 1991), pois parte das medidas de Segurança da Informação não foi adotada completamente, ou parte delas foi adotada e parte não foi. A estratégia de compromisso mais utilizada pelas subunidades foi a barganha, o que reforça o entendimento de que, embora as subunidades tenham se comprometido a adotar medidas de Segurança da Informação, essa adoção ainda não aconteceu.

A explicação para as respostas de compromisso identificadas na pesquisa está na forma como as subunidades julgam as medidas de Segurança da Informação que são pressionadas a adotar. De acordo com Hernes e Erdvik (2014), as subunidades tomam decisões de forma descentralizada e com base em interesses e julgamentos próprios sobre a adoção de práticas em conformidade com as políticas da organização. As medidas de Segurança da Informação podem ser consideradas rígidas ou restritivas (KARYDA; KIOUNTOUZIS; KOKOLAKIS, 2005; ELLWANGER, 2009), o que pode resultar em uma rejeição de parte delas pelas subunidades. Como já discutido, os entrevistados relataram diferentes percepções quanto às medidas de Segurança da Informação, sendo que a dificuldade de desenvolver as atividades das subunidades é a causa mais apontada. Outros

motivos são a dificuldade de o setor de TI desenvolver suas atividades, a ineficiência (ou insegurança) das medidas e o prejuízo à imagem das subunidades.

A terceira resposta estratégica da tipologia de Oliver (1991) é a esquiva, que caracteriza-se por um afastamento entre a realidade da organização e os requisitos institucionais. No contexto da Segurança da Informação, a subunidade pode estar utilizando artifícios para evitar a adoção das medidas exigidas pelos constituintes do ambiente institucional. Foram identificadas 34 referências à resposta de esquiva em dados sobre 11 subunidades diferentes, sendo que em uma delas a esquiva foi a resposta mais recorrente. Através da esquiva, as subunidades ficam intencionalmente em conformidade cerimonial por terem adotado as medidas exigidas sem que a implantação tenha acontecido em profundidade, ou simplesmente fogem da necessidade de adotar.

A despeito de não ser uma das respostas mais comuns entre as subunidades, a esquiva pode significar a adoção parcial de medidas de Segurança da Informação, como a implantação de medidas técnicas sem as devidas configurações para que atendam aos requisitos de Segurança, e a criação de regulamentos e estruturas organizacionais que não são cobrados ou não funcionam, causando uma dissociação entre a política organizacional e as práticas implantadas nas subunidades (BJÖRCK, 2004; LOPES; SÁ-SOARES, 2014; LAPKE; DHILLON, 2015). A resposta de esquiva pode significar também que as subunidades esconderam da sede e de outras fontes de pressão institucional o nível de conformidade em que se encontram, ou mesmo a ocorrência de incidentes (DHILLON, 2001). Pode significar ainda que as subunidades evitaram participar de iniciativas da administração central para não serem obrigadas a adotar medidas de Segurança da Informação. Essas três situações foram identificadas nas entrevistas e mostram que parte das subunidades da organização em estudo esconde ou foge da necessidade.

Por terem a necessidade ou mesmo obrigação de adotar as medidas de Segurança da Informação exigidas pela administração central, mas por esconderem a sua realidade ou por fugirem da necessidade de adotar, as subunidades estão dissociando a Política organizacional das práticas internas, o que pode expor a organização a riscos de Segurança da Informação. Em outras palavras, essas subunidades, que compartilham sistemas, recursos computacionais e redes de computadores com outras subunidades e com a administração central, podem pôr em risco a organização devido à implantação inadequada de tecnologias e processos. O fato de dez subunidades responderem a pressões institucionais com esquiva mostra que há dissociação intencional entre a Política de Segurança da Informação da

organização e o comportamento dessas subunidades, caracterizando uma conformidade cerimonial (MEYER; ROWAN, 1977).

A quarta resposta estratégica proposta por Oliver (1991) é o desafio, que representa uma resistência ativa às expectativas institucionais. Todas as subunidades responderam a pressões institucionais com desafio, que foi também a resposta estratégica mais comum, com 108 referências identificadas. Isto explica a pequena quantidade de medidas informais e formais adotadas e também a rejeição de parte das medidas técnicas por algumas subunidades. Dados obtidos no relatório de auditoria (FIOCRUZ, 2015) mostram que uma grande parte das medidas requisitadas pelos regulamentos de Segurança da Informação da organização não foi adotada pelas subunidades, o que comporta a estratégia de desafio.

A resposta estratégica de desafio é associada por Standing, Sims e Love (2009) à falta de controle dos constituintes do ambiente institucional, à multiplicidade de demandas e à percepção de que as medidas são ineficientes ou inadequadas. Diferentes demandas institucionais foram identificadas na pesquisa, mas a maior parte dos entrevistados não reconhece pressões institucionais que não sejam da sede da organização. No entanto, o Entrevistado 19 reconhece que "Algumas unidades têm de respeitar regras nacionais, as regras da FIOCRUZ e as de outros países." Oliver (1991) associa o desafio à autonomia das organizações. No entanto, o desfio foi mais observado em subunidades que não têm autonomia administrativa, nos quais eram esperadas respostas de conformidade, enquanto subunidades autônomas tenderam a responder com aquiescência e compromisso.

Embora as pressões da administração central tenham sido reconhecidas pelos entrevistados, a falta de controle é relatada por diferentes pessoas, inclusive os sete entrevistados que afirmam que não há punição para o descumprimento dos regulamentos organizacionais. Esses regulamentos, por sua vez, não são sequer percebidos como obrigatórios, mas apenas como recomendações. Já o controle externo sobre as subunidades não é percebido pela maioria dos entrevistados como uma questão relacionada às subunidades, mas que incide apenas sobre a administração central da organização.

A pesquisa evidenciou que somente quatro tipos de medidas de Segurança da Informação foram adotados por todas as subunidades que participaram da pesquisa, enquanto 11 foram adotados por menos da metade, o que reforça o resultado da auditoria (FIOCRUZ, 2015). Apesar de as medidas técnicas terem sido mais adotadas do que as outras, apenas dez

entrevistados referiram que suas subunidades adotaram medidas de redundância de equipamentos e de controle de acesso físico, o que pode expor parte das subunidades a acessos indevidos aos equipamentos e a indisponibilidade de serviços de TI.

Como já citado, medidas formais importantes para definir a estrutura, os princípios, as necessidades e o funcionamento da Segurança da Informação nas subunidades são pouco adotadas. Em apenas uma subunidade há processo de classificação das informações quanto à necessidade de garantir confidencialidade. Apenas duas subunidades têm um processo de análise e avaliação de riscos. Além disso, poucas subunidades têm a estrutura organizacional necessária para tomar decisões estratégicas, táticas e operacionais de Segurança da Informação, pois apenas três delas têm Comitê de Segurança da Informação próprio, apenas uma tem um Escritório de Segurança da Informação e apenas três têm uma Equipe de Tratamento de Incidentes. Por fim, apenas duas subunidades têm uma Política de Segurança da Informação formal e apenas uma delas faz revisão periódica da sua Política.

Com isso, fica comprometida a adoção de outras medidas de Segurança da Informação adequadas à realidade de cada subunidade e em conformidade com os requisitos da administração central e do ambiente institucional. Treinamentos de usuários e profissionais de TI em Segurança da Informação não são realizados pela maioria das subunidades, o que pode resultar em incidentes provocados pelos próprios usuários, pois ações de divulgação da Política e dos regulamentos de Segurança da Informação e de conscientização sem treinamento podem não ser suficientes para garantir a mudança do comportamento.

Algumas medidas consideradas necessárias pela administração central e previstas em regulamentos organizacionais não foram adotadas por todas as subunidades. Com isso, informações da sede e de toda a organização podem ser expostas a riscos. Considerando que esses riscos sequer vêm sendo identificados e analisados em todas as subunidades, como expuseram os dados da pesquisa, os profissionais de Segurança da Informação vinculados à sede da organização não sabem os incidentes que podem acontecer nas subunidades nem podem estimar suas consequências.

A manipulação é a resposta estratégica mais ativa (OLIVER, 1991) e envolve a cooptação, o controle ou a influência da organização sobre a fonte de pressão institucional (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009). A pesquisa evidenciou a influência de nove subunidades sobre a administração central da organização. Standing, Sims e Love (2009) explicam que a resposta de manipulação está associada à pouca autoridade da sede da

organização sobre suas subunidades, à existência de múltiplas demandas institucionais, à baixa eficiência ou incoerência dos requisitos institucionais e à baixa incerteza quanto às consequências da não conformidade. Como já discutido, os regulamentos da administração central não são percebidos como obrigações, o que favorece a influência das subunidades sobre a sede.

A manipulação foi identificada em nove subunidades e teve 27 referências codificadas no NVivo. Embora seja pouco comum devido ao fato de ter como requisito o exercício do poder que as subunidades podem ter sobre a sede da organização, o Entrevistado 16 e o Entrevistado 19 reconheceram que as subunidades influenciam a administração central tendo em vista seus próprios interesses. Essa resposta foi identificada em relatos de situações nas quais as subunidades buscam incluir seus profissionais de TI nos grupos que tomam decisões de Segurança da Informação na organização, como a participação de pessoas das subunidades no Comitê de Segurança da Informação e a atuação de membros da direção das subunidades junto à Presidência da organização para revogar medidas de Segurança adotadas.

Essa atuação levou a Presidência da organização a desistir de centralizar os serviços de TI no *datacenter* da FIOCRUZ e houve ainda a suspensão de uma medida prevista em um dos regulamentos de Segurança da Informação da organização devido ao fato de, em ambos os casos, serem consideradas prejudiciais aos interesses e atividades das subunidades. A manipulação, nesses casos, levou a FIOCRUZ a desrespeitar o regulamento do Governo Federal que trata de credenciamento e controle de acesso em órgãos da administração pública federal, a Norma Complementar nº 7/IN01/DSIC/GSIPR (BRASIL, 2010). Considerando que os regulamentos da organização foram elaborados e formalizados para atender a requisitos externos de Segurança da Informação, a não conformidade das subunidades com esses regulamentos significa uma não conformidade da organização com esses requisitos externos.

Além das diferentes respostas estratégicas, foram identificadas também 20 situações em que dez subunidades adotaram medidas contrárias aos interesses da administração central. Subunidades adotaram tecnologias baseadas em *software* livre ou de outros fabricantes em detrimento da padronização feita pela administração central. Subunidades também bloquearam o acesso a redes sociais nas quais a organização tem atuação permitida e até mesmo incentivada.

O relatório de auditoria interna (FIOCRUZ, 2015) mostra que a Subunidade 02, da mesma forma que aconteceu com outras, apresentou não conformidades com regulamentos

da organização, mas a resposta à auditoria interna deixou claro que houve uma situação de conflito entre os regulamentos. O apontamento da auditoria diz: "Ausência de monitoramento sobre as responsabilidades do usuário quanto ao uso de senhas, equipamentos, mesa e tela limpa. Recomendação: manter, doravante, controle efetivo das responsabilidades dos usuários, na forma das Portarias da FIOCRUZ 069/11, 345/12, Norma SIC 001/12-VPGDI e incisos I a III da IN04-2010". A resposta da subunidade diz: "Está disponível na Intranet da unidade o [nome do regulamento que formaliza a Política de Segurança da Informação da subunidade] em que este ponto é tratado explicitamente. [...] No entanto, utilizaremos o constante nas portarias da FIOCRUZ 069/11, 345/12, Norma SIC 001/12-VPGDI e incisos I a III da IN04-2010." Como mostram as transcrições, a subunidade tinha um regulamento próprio que atendia às suas necessidades e procurou ficar em conformidade com ele, que foi motivo do apontamento dos auditores.

Há um entendimento na organização de que a conformidade com regulamentos externos é necessária para que a FIOCRUZ participe de projetos e políticas públicas, como expressou o Entrevistado 19: "Quando nós vamos atuar em programas e projetos, seja do CNPq [Conselho Nacional de Desenvolvimento Científico e Tecnológico] ou qualquer outro órgão nacional ou até estrangeiro, eles exigem da gente uma certa... não sei se é qualificação, mas uma estrutura suficiente para que a gente possa articular de forma mais segura essa relação." Essa percepção, no entanto, não impede a adoção pelas subunidades de medidas contrárias aos interesses da sede. Esse comportamento indica que, ao adotar medidas de Segurança da Informação, as subunidades buscam atender aos seus próprios interesses. Como consequência, ficam em não conformidade com os requisitos organizacionais e a organização fica em não conformidade com os requisitos externos. O Entrevistado 18 reconhece a os problemas de conformidade com regulamentos internos: "A gente tem problemas hoje, principalmente de *compliance* interno, com nossa Política de Segurança [da Informação da organização]."

A adoção de medidas contrárias aos interesses da organização, a manipulação da organização por parte das subunidades para mudar regulamentos em prol dos seus próprios interesses, e a ocorrência de diferentes respostas estratégicas nas subunidades mostram que os esforços da administração central da organização (formalização de uma Política e de nove regulamentos de Segurança da Informação, um Comitê de Segurança da Informação, um Sistema de Gestão de Segurança da Informação e uma Equipe de Tratamento de Incidentes de Segurança da Informação, e a realização de eventos de conscientização e divulgação desses

regulamentos) não são suficientes para garantir a conformidade das subunidades. Respostas de desafio, que tiveram mais referências do que a aquiescência, evidenciam também que esses esforços não resultaram nas respostas esperadas por parte das subunidades. Respostas de manipulação, que resultaram em mudanças de regulamentos organizacionais, e a adoção de medidas contrárias aos interesses da sede são evidências que devem ser consideradas ao analisar como as subunidades influenciam a conformidade da organização com os requisitos externos de Segurança da Informação.

Os discursos dos dois participantes que foram entrevistados como membros do Comitê de Segurança da Informação são de conformidade. O Entrevistado 18 deixa claro que a legitimidade da organização junto ao Governo Federal traz benefícios. No entanto, ele deixa claro também que há uma preocupação maior do que apenas a conformidade com os requisitos externos de Segurança da Informação ao declarar que os últimos regulamentos que têm sido discutidos mais recentemente não foram elaborados tendo em vista um regulamento externo, mas uma necessidade técnica interna. O discurso do Entrevistado 19 também é a favor da conformidade, que, segundo ele, permite o acesso a recursos e a participação de projetos e programas governamentais de interesse da organização.

Na auditoria realizada pelo TCU (2014), a organização respondeu que dispõe de uma política formal de cópias de segurança (*backup*) cujo cumprimento é obrigatório. A organização tem um regulamento que formaliza a realização de *backups*, mas este documento sequer é percebido como obrigatório pelas subunidades. O mesmo se aplica ao questionamento relativo ao processo de gestão de riscos de Segurança da Informação, cuja resposta é positiva, mas que não se sustenta ao analisar o comportamento das subunidades organizacionais. A pergunta sobre o processo de gestão de vulnerabilidades também teve uma resposta positiva, mas que não se aplica à organização como um todo, como mostrou a pesquisa. Processos de gestão de incidentes, também alvo de questionamentos do TCU e cuja resposta foi positiva, não é respeitado, pois parte dos entrevistados admitiu que sequer comunica à CGTI a ocorrência em suas subunidades.

Como a organização buscou a conformidade com os requisitos externos formalizando estruturas organizacionais e criando processos, regulamentos e uma Política de Segurança da Informação, e como isto não se traduziu em um comportamento de conformidade das subunidades, tem-se uma dissociação entre política e prática, tendo como consequência uma conformidade cerimonial da organização: ela está aparentemente em conformidade quanto a vários aspectos questionados na auditoria, pois formalizou

documentos, atribuiu responsabilidades e criou estruturas organizacionais, mas isto não é respeitado nas subunidades, que adotam as medidas que convêm, a depender do julgamento que fazem.

A conformidade cerimonial, neste caso, é diferente daquela prevista por Meyer e Rowan (1977) por não ser intencional. Apesar de haver a compreensão de que as medidas são importantes por motivos relacionados à eficiência quanto à Segurança da Informação, é recorrente nas entrevistas com o Entrevistado 18 e com o Entrevistado 19 a preocupação com a legitimidade junto ao Governo. Além disso, os dados mostram de que algumas subunidades não têm recursos necessários para adotar todas as medidas requisitadas pela administração central, sendo este o segundo maior motivo pelo qual as medidas foram consideradas incoerentes com as atividades e objetivos das subunidades e do setor de TI. A falta de capacidade da organização de estar em conformidade com os requisitos institucionais foi prevista na literatura (COLE, 2005, 2012; LIM; TSUTSUI, 2012; BROMLEY; POWELL, 2012).

Assim, a causa identificada na pesquisa para a dissociação entre a Política de Segurança da Informação da organização e as medidas adotadas é o comportamento das subunidades, que respondem às pressões institucionais conforme seus próprios interesses e julgamentos sobre as medidas de Segurança da Informação. A seção seguinte discute as proposições teóricas frente aos achados empíricos do trabalho.

6.10 DISCUSSÃO DAS PROPOSIÇÕES DA PESQUISA

A conformidade das organizações com os requisitos institucionais de Segurança da Informação vai depender de como elas julgam e interpretam esses requisitos quanto à eficiência e adequação às suas atividades e objetivos (HU; HART; COOKE, 2007). No contexto das subunidades organizacionais, há o julgamento quanto à coerência das pressões institucionais com suas necessidades e interesses, em detrimento das necessidades e interesses da administração central da organização (DELMAS; TOFFEL, 2008; BOXENBAUM; JONSSON, 2009; HERNES; ERDVIK, 2014; NETLAND; ASPELUND, 2014), e também quanto à existência de conflitos entre diferentes pressões da administração central e do ambiente institucional (BOXENBAUM; JONSSON, 2009).

A pesquisa mostrou que as subunidades estão sujeitas a pressões coercitivas, normativas e miméticas do ambiente institucional, sendo que a maioria das pressões referenciadas é coercitiva. A pesquisa mostrou também que há mais adoção de medidas técnicas do que das demais. No entanto, nem todas as medidas técnicas, formais e informais foram adotadas por todas as subunidades. Essa rejeição é explicada pela forma como as medidas são julgadas pelas subunidades. Foram identificadas evidências de que medidas técnicas foram consideradas incoerentes com a realidade das subunidades por dificultarem suas atividades, por exigirem recursos que não dispõem e por dificultarem as atividades de TI. Medidas formais e informais também foram julgadas incoerentes por dificultarem as atividades das subunidades e por exigirem recursos que elas não têm, mas também por serem consideradas inseguras (ou ineficientes) e por prejudicarem a imagem das subunidades.

Como consequência, foram identificadas as cinco respostas estratégicas apresentadas por Oliver (1991). Embora os dados tenham mostrado que as respostas de aquiescência e desafio sejam mais comuns do que as demais, a pesquisa revelou que nem todas as subunidades tiveram essas respostas como as mais identificadas: uma subunidade apresentou mais referências para esquiva, enquanto outra teve o compromisso como resposta mais utilizada. A partir disso, apresenta-se novamente a primeira proposição da pesquisa:

Proposição 1: As subunidades organizacionais respondem às pressões institucionais através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre a eficiência e adequação das medidas de Segurança da Informação.

Quanto à sustentação empírica da Proposição 1, é possível afirmar que **os dados a sustentam empiricamente.**

As respostas às pressões para adoção de tecnologias ou práticas de gestão de TI dependem também da percepção que se tem e do tipo de pressão (ARMÊNIO NETO; MACHADO-DA-SILVA, 2009; STANDING; SIMS; LOVE, 2009; AIER; WEISS, 2012). Considerando que decisões sobre medidas técnicas, medidas formais e medidas informais são de responsabilidade de diferentes áreas das organizações (SÊMOLA, 2014), e que a adoção de cada uma dessas categorias está relacionada a diferentes pressões institucionais (ALBUQUERQUE JUNIOR *et al*., 2016), havia uma expectativa de que as pressões para adoção de medidas formais, informais e técnicas resultassem em diferentes respostas estratégicas das subunidades.

Os dados evidenciam que houve mais adoção de medidas técnicas, que têm como benefício percebido a garantia da confidencialidade, integridade e disponibilidade das informações. Quatro tipos diferentes de medidas técnicas foram adotados por todas as subunidades, e pelo menos 58,82% delas adotaram os demais tipos. Isto mostra que as subunidades tendem a responder com aquiescência às pressões para adotar medidas técnicas. No entanto, a percepção de inadequação de 14 dessas medidas à realidade das subunidades também foi identificada nas entrevistas.

Esse resultado é particularmente estranho devido ao fato de a adoção ser uma responsabilidade dos profissionais de TI das subunidades e de não haver subcomitês de Segurança da Informação na maioria delas, fazendo com que as decisões sobre a adoção não sejam discutidas ou sejam tomadas considerando critérios principalmente técnicos. A explicação para este resultado está no fato de a adoção das medidas que podem gerar impacto nas atividades desenvolvidas nas subunidades ser objeto de discussões entre os profissionais de TI e os gestores das subunidades, o que minimiza a ausência de escritórios e subcomitês de Segurança da Informação. No entanto, como não há participação de outros setores das subunidades, as decisões podem não considerar necessidades específicas de Segurança da Informação.

Medidas formais de nove tipos foram consideradas incoerentes com as atividades das subunidades. Nesse sentido, o Sistema de Gestão de Segurança da Informação, uma medida formal, não foi identificado nas subunidades. Comitês e sistemas de gestão de Segurança da Informação são raros, o que prejudica a elaboração de regulamentos e o direcionamento de ações nas subunidades.

Já as medidas informais foram identificadas em 11 subunidades. Apenas duas medidas informais foram consideradas incoerentes com as atividades das subunidades. Por serem consideradas importantes devido à possibilidade de mudarem o comportamento das pessoas, essas medidas têm melhor aceitação do que as formais entre as subunidades.

Em suma, medidas técnicas são mais adotadas do que as demais, mas apresentam uma maior quantidade de tipos considerados incoerentes com as subunidades. Medidas formais são menos adotadas, mas há uma percepção de que são coerentes por estarem associadas à conformidade com os requisitos externos de Segurança da Informação. Medidas informais são consideradas importantes e são pouco associadas à incoerência com os objetivos e atividades das subunidades, mas são menos adotadas do que as técnicas.

Embora medidas técnicas sejam mais adotadas, não é possível afirmar que sejam julgadas mais coerentes ou eficientes do que as demais, pois as medidas mais rejeitadas pelas subunidades são justamente técnicas. Além disso, parte das subunidades se destaca na adoção de medidas técnicas, enquanto outras se destacam na adoção de medidas formais.

Enquanto respostas de manipulação ocorreram quando as pressões exigiam a adoção de medidas técnicas, como o bloqueio de caixas postais de pessoas que perderam o vínculo com as subunidades, ou a elaboração de medidas formais, como regulamentos no Comitê de Segurança da Informação da organização, as respostas de desafio foram mais associadas a medidas formais, embora pressões para adoção de medidas técnicas tenham tido respostas de desafio também. As subunidades responderam com esquiva e compromisso a pressões que exigiam a adoção de medidas técnicas e formais. Já a resposta de aquiescência foi mais associada a pressões para adotar medidas técnicas.

Desta forma, a análise das entrevistas e documentos não trouxe evidências de que pressões para adotar medidas de certa categoria vão resultar em respostas específicas. Assim, retomando as proposições da pesquisa, a segunda proposição estabelecida foi a seguinte:

Proposição 2: Pressões para adoção de medidas formais, medidas informais e medidas técnicas vão resultar em diferentes respostas estratégicas por parte das subunidades organizacionais.

Considerando que não foi possível identificar elementos que mostrem que pressões para adoção de medidas informais, formais e técnicas resultam diferentes respostas estratégicas das subunidades, **os dados não dão sustentação empírica para a Proposição 2.**

A influência das subunidades sobre a administração central é citada por Osmundsen (2005) e Delmas e Toffel (2008). Hernes e Erdvik (2014) acrescentam que essa influência tem consequências na conformidade da organização com os requisitos institucionais. Neste sentido, as decisões descentralizadas tomadas no âmbito das subunidades são baseadas em seus próprios interesses e julgamentos.

Como as medidas previstas na Política e nos regulamentos de Segurança da Informação da organização podem ser percebidas como ineficientes (NETLAND; ASPELUND, 2014), as subunidades podem responder com diferentes estratégias (PILATO; PEDRINI, 2015). Como resultado de diferentes percepções e respostas estratégicas, parte das subunidades pode não adotar as medidas de Segurança da Informação, o que prejudica as intenções da administração central de padronizar o comportamento das subunidades

(BOSCHMAN, 2006; AGUILERA-CARACUEL *et al*., 2012) e, consequentemente, de estar em conformidade com os requisitos institucionais.

Se a organização criou estruturas organizacionais e formalizou regulamentos e uma Política de Segurança da Informação para ficar em conformidade com os requisitos externos (NETLAND; ASPELUND, 2014), mas parte das subunidades desrespeita os regulamentos da organização, a conformidade é cerimonial, pois a Política de Segurança da Informação da organização é dissociada da realidade existente nas suas subunidades. Neste caso, a conformidade cerimonial não é intencional, mas uma decorrência do comportamento das subunidades da organização. Devido ao fato de a conformidade ser cerimonial, é possível que a organização não sofra as consequências da não conformidade, mas pode estar exposta a riscos devido ao fato de não ter adotado medidas que atendam aos seus requisitos de Segurança da Informação.

Assim, a conformidade da organização com os requisitos externos só é possível se todas as subunidades estiverem em conformidade com os requisitos internos. O oposto dessa situação é a não conformidade, que acontece quando há um evidente desrespeito da organização com relação aos requisitos externos de Segurança da Informação. No entanto, esta pesquisa mostrou que esse desrespeito pode também ser uma decorrência do comportamento das subunidades, pois a manipulação da administração central pode levar a organização a mudar regulamentos e a Política de Segurança da Informação em benefício de uma ou mais subunidades, fazendo com que a organização como um todo desrespeite requisitos externos. Em suma, as diferentes respostas das subunidades às pressões institucionais podem fazer com que a organização fique em conformidade, em não conformidade ou em conformidade cerimonial com os requisitos institucionais.

A influência das respostas das subunidades sobre as medidas adotadas pela organização foi identificada nos dados da pesquisa. As subunidades utilizam sistemas de informação da organização e compartilham rede de computadores e dados com a sede e outras subunidades. Respostas estratégicas de desafio ou esquiva, com rejeição ou implantação parcial, expõem a organização a riscos que podem comprometer as atividades desenvolvidas por todas as subunidades. A ausência de medidas formais para orientar as ações de Segurança da Informação específicas para cada subunidade pode também fazer com que medidas técnicas necessárias não sejam adotadas.

Medidas que têm implicações mais claras para toda a organização foram adotadas por todas as subunidades, como a segregação de redes de computadores, prevenção contra códigos maliciosos e controle de acesso lógico. No entanto, a ocorrência de respostas de esquiva, como as identificadas na implantação de *firewall* em duas subunidades, e a não atualização dos antivírus devido à expiração da licença de uso, são também causas potenciais de incidentes que podem comprometer a organização. Além disso, a esquiva é uma resposta típica de conformidade cerimonial, pois implica em esconder ou fugir da obrigação de estar em conformidade.

A pesquisa mostrou que a maioria das subunidades não adotou medidas formais importantes, que orientam a adoção de outras medidas de Segurança da Informação. Responsabilidades, processos e procedimentos também não foram formalizados em todas as subunidades. Como poucas têm um processo de análise e avaliação de riscos formal, poucas fizeram classificação das suas informações, poucas têm um Comitê de Segurança da Informação e poucas têm Política de Segurança da Informação, a tomada de decisões específicas para cada subunidade fica prejudicada. Assim, a não adoção de medidas formais pode provocar um direcionamento equivocado para as ações de Segurança da Informação, podendo fazer com que medidas técnicas e informais não sejam adotadas adequadamente. Ainda que a organização esteja em conformidade com os requisitos externos, com todos os regulamentos, processos, estruturas organizacionais e documentos formalizados, a ausência de uma preocupação com o direcionamento correto das ações de Segurança da Informação nas subunidades aponta que há uma dissociação entre política e prática, o que significa que a organização está em conformidade cerimonial.

Ações de conscientização e divulgação da Política e dos regulamentos de Segurança da Informação tiveram mais referências identificadas do que treinamentos de profissionais e usuários de TI. Em nenhum dos casos, as medidas previstas foram adotadas por todas as subunidades. A falta de treinamento pode causar uso indevido de sistemas de informação corporativos por imperícia dos usuários e profissionais de TI, o que pode comprometer as informações das subunidades e mesmo da organização. Independentemente do risco potencial de os usuários e profissionais de TI não estarem devidamente capacitados, as subunidades não estão em conformidade com os requisitos da organização, que são decorrentes de exigências externas.

A manipulação é a resposta mais ativa dentro do contínuo de respostas estratégicas de Oliver (1991) e, ainda que nem todas as tentativas de manipular a

administração central da organização tenham sido consumadas, o fato de algumas terem sido já põe a conformidade da organização sob suspeita. A manipulação levou a Presidência da organização a mudar seus planos de centralizar os diversos equipamentos de TI das subunidades em seu *datacenter*. Levou também à suspensão de uma medida que obrigada as subunidades a controlar o acesso dos usuários através da vigência dos vínculos deles com a organização. Ainda que a necessidade de abrigar todos os servidores de rede e serviços oferecidos pelos setores de TI das subunidades em um só *datacenter* seja questionável, como observado nas entrevistas, o ganho em termos de Segurança da Informação é inquestionável, visto que um *datacenter* necessariamente tem diversas medidas de controle de acesso físico e proteção ambiental. Como nem todas as subunidades dispõem de *datacenter*, isso já seria positivo para a organização como um todo. Quanto à mudança realizada no regulamento de correio eletrônico da organização, houve uma implicação clara, que foi a desobediência de regulamentos do Governo Federal. Assim, fica caracterizada a não conformidade da organização com esses regulamentos.

A terceira proposição do trabalho foi a seguinte:

Proposição 3: As respostas das subunidades às pressões que sofrem influenciam no nível de conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional.

Assim, quanto à sustentação empírica da terceira proposição da tese, é possível afirmar que **os dados dão sustentação empírica para a Proposição 3.**

Os dados da pesquisa mostraram que duas proposições construídas com base na teoria têm sustentação empírica, visto que: as subunidades respondem às pressões institucionais através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre as medidas de Segurança da Informação, e essas as respostas das subunidades influenciam o nível de conformidade organizacional com os requisitos de Segurança da Informação do ambiente institucional. No entanto, não foram identificadas evidências de que pressões para adoção de medidas formais, informais e técnicas de Segurança da Informação resultam em diferentes respostas das subunidades.

Com isto, a pesquisa mostrou que a adoção de medidas de Segurança da Informação pelas subunidades organizacionais não depende da autonomia, mas do julgamento quanto à adequação e eficiência das medidas que são pressionadas a adotar. Mostrou também que a conformidade da organização com os requisitos institucionais e, consequentemente, a

Segurança da Informação na organização dependem de como as subunidades respondem às pressões institucionais. O capítulo a seguir apresenta as considerações finais do trabalho.

7 CONSIDERAÇÕES FINAIS

Esta tese teve o objetivo de explicar como as respostas estratégicas das subunidades organizacionais às pressões externas influenciam a conformidade da organização com os requisitos externos de Segurança da Informação. Para isto, foi realizado um estudo de caso integrado na FIOCRUZ, organização composta por diferentes subunidades autônomas e descentralizadas geograficamente.

Para alcançar este objetivo, foram identificadas as medidas formais e informais adotadas pela organização, que seriam a base das pressões coercitivas e normativas da administração central sobre as subunidades. No entanto, a pesquisa mostrou que medidas técnicas adotadas pela sede também pressionam as subunidades a adotarem medidas de Segurança da Informação.

Depois de identificadas as medidas adotadas pela sede, foram identificadas as pressões institucionais que incidem sobre as subunidades. As medidas adotadas pelas subunidades em decorrência dessas pressões foram também identificadas, o que permitiu conhecer as respostas das subunidades a essas pressões.

Por fim, foi feita uma análise dos efeitos das respostas das subunidades sobre as medidas de Segurança da Informação adotadas pela administração central como uma forma de conhecer a influência das subunidades sobre a conformidade da organização.

A pesquisa partiu do pressuposto de que as organizações estão sujeitas a pressões coercitivas, normativas e miméticas do ambiente externo, como preconiza a Teoria Institucional. Esta abordagem explica como as organizações assimilam características do ambiente no qual estão inseridas. No entanto, a abordagem prevê como possíveis respostas organizacionais a essas pressões a aceitação (e a conformidade, como resultado) e a rejeição (e a não conformidade). Devido a esta limitação, a Teoria Institucional é criticada por não explicar outros tipos de resposta, a depender dos seus interesses e do julgamento que as organizações fazem das pressões que sofrem.

Além de ampliar a compreensão sobre dissociação entre política e prática e sobre a conformidade cerimonial da organização com os requisitos institucionais, a tipologia de respostas estratégicas acrescenta à aceitação (ou aquiescência) e rejeição (ou desafio) as

respostas de compromisso, esquiva e manipulação. Com isto, a tipologia trouxe outras possibilidades de análise do comportamento organizacional à abordagem institucional.

No contexto da Segurança da Informação, a Teoria Institucional explica como as organizações adotam diferentes medidas de Segurança da Informação como resultado das pressões do ambiente externo. Como resultado dessas pressões, as organizações podem adotar medidas formais, informais e técnicas e ficar em conformidade com os requisitos institucionais, ou não adotar as medidas exigidas pelo ambiente institucional e ficar expostas a riscos e às consequências da falta de legitimidade.

Estudar a Segurança da Informação em organizações com estrutura descentralizada utilizando a tipologia de Oliver (1991) ampliou o conhecimento sobre o tema, pois as subunidades podem ter autonomia administrativa e decidir com base nas suas necessidades e interesses. O estudo permitiu conhecer não somente as respostas das subunidades às pressões institucionais, mas também os efeitos dessas respostas sobre a organização, o que é pouco abordado em estudos sobre Segurança da Informação.

O estudo identificou não só medidas formais e informais adotadas pela administração central da organização, mas também medidas técnicas, que implicam em adoção de outras medidas pelas subunidades. Assim, além da Política de Segurança da Informação, de regulamentos e de estruturas organizacionais voltados para esse fim, a organização realizou treinamentos e ações de divulgação e conscientização e implantou medidas de redundância, segregação e monitoramento de redes de computadores, prevenção contra códigos maliciosos, controle de acesso lógico e físico, autenticação, criptografia e proteção ambiental.

A tese mostrou a conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional não como uma decisão racional, mas como uma decorrência das respostas das suas subunidades. Com a elaboração de um *framework* baseado na Teoria Institucional e na tipologia de respostas estratégicas, a tese possibilitou compreender como uma organização que busca a conformidade pode ficar em conformidade cerimonial com os requisitos externos.

Os resultados da pesquisa evidenciam que as subunidades são pressionadas pela sua administração central e pelo ambiente institucional, mas que seu foco são as pressões que vêm da sede da organização. Regulamentos e uma Política formalizados por um Comitê de Segurança da Informação, a implantação de tecnologias que exigem a adoção de medidas de

Segurança da Informação, a realização de auditorias internas de conformidade, a publicação de recomendações e ações de conscientização são os meios pelos quais as pressões da administração central são exercidas. No entanto, mesmo reconhecendo a sede como uma fonte de pressão institucional, essas são percebidas como meras recomendações, cujo cumprimento é opcional. Essa percepção é reforçada por não haver penalidade para o descumprimento das regras presentes nos regulamentos e na Política de Segurança da Informação.

Entre as medidas adotadas pelas subunidades destacam-se as técnicas, que têm ampla adesão, sendo que as mais adotadas são de redundância de dados, segregação e monitoramento de redes de computadores, prevenção contra códigos maliciosos e controle de acesso lógico. Dentre as informais, os destaques são as ações de divulgação e de conscientização. Entre as formais, os processos e procedimentos de Segurança da Informação e os regulamentos internos são os tipos de medidas mais adotados pelas subunidades.

O trabalho permitiu identificar o reconhecimento, uma tática associada à resposta de desafio, que é caracterizada pela rejeição dos requisitos institucionais, que foi assim considerada por não ser uma decisão estratégica, mas o resultado da falta de capacidade e da falta de ações para que a adoção aconteça, embora seja reconhecida sua necessidade.

Como o trabalho evidenciou, as subunidades respondem às pressões através das cinco respostas estratégicas da tipologia de Oliver (1991), mas a aquiescência e o desafio foram as respostas mais identificadas na pesquisa. O fato de haver um equilíbrio na quantidade de referências de codificação dessas respostas antagônicas ajuda a explicar a conformidade parcial das subunidades com os regulamentos da organização, como evidenciado na análise do relatório de auditoria interna disponibilizado pela organização. Como resultado dessas respostas, as subunidades adotaram medidas de todos os tipos das três categorias, mas diversas medidas formais e parte das medidas informais têm pouca adesão, o que prejudica o planejamento de ações de Segurança da Informação e, como consequência, a adoção de outras medidas.

Essa diversidade de respostas estratégicas e a resultante rejeição de medidas formais, informais e técnicas influenciam na Segurança da Informação da organização, expondo a sede e todas as subunidades a riscos. Respostas de manipulação influenciam diretamente na adoção de medidas de Segurança da Informação pela administração central, alterando regulamentos vigentes e frustrando planos da sede da organização de tornar o ambiente computacional mais seguro hospedando equipamentos, dados e sistemas de

informação das subunidades em um mesmo *datacenter*, uma medida cuja implantação tem um custo alto e pode ser inviável para as subunidades. Com isso, a organização apresenta uma conformidade cerimonial com os requisitos externos de Segurança da Informação.

Os dados da pesquisa dão sustentação empírica a duas das três proposições da tese, pois as subunidades julgam as pressões institucionais conforme seus interesses e respondem de diferentes formas, e suas respostas influenciam a conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional, mas não houve elementos que sustentassem que as pressões para adoção de medidas formais, informais e técnicas resultaram em diferentes respostas estratégicas das subunidades.

A tipologia de Oliver (1991) permite conhecer como as organizações respondem às pressões institucionais, sem entrar no mérito do comportamento intraorganizacional e sua influência sobre a conformidade organizacional. A partir da compreensão de que as subunidades podem se comportar de formas distintas e, com isso, apresentar diferentes respostas às pressões recebidas, os resultados desta pesquisa demonstram que o *framework* também pode ser utilizado para análise de organizações com subunidades autônomas e a influência do comportamento dessas sobre a conformidade organizacional. Mais especificamente, o *framework* mostra como a dissociação entre a Política de Segurança da Informação e as medidas adotadas pelas subunidades acontece devido às respostas dessas subunidades.

A partir do conhecimento das respostas das subunidades, a organização tem subsídios para minimizar os efeitos dessas respostas sobre sua conformidade com os requisitos externos de Segurança da Informação.

7.1 LIMITAÇÕES DA PESQUISA

Uma limitação desta pesquisa está no fato de terem sido entrevistados apenas os responsáveis pela TI ou pela Segurança da Informação nas subunidades, o que restringe o acesso a informações a partir de outros pontos de vista, como de usuários e gestores. Essa limitação é minimizada pelo fato de dois membros do Comitê de Segurança da Informação que não representam subunidades organizacionais terem sido entrevistados. Com isso, a pesquisa permitiu obter informações sob o ponto de vista da organização, sem o viés dos representantes das subunidades.

A pesquisa não envolveu todas as subunidades da organização, o que é também uma limitação. Se houvesse a participação de todas as subunidades, a pesquisa traria o panorama geral da organização, enriquecendo os resultados. No entanto, por ter envolvido 17 subunidades diferentes de um total de 21 existentes na organização, e pelo fato de atuarem na prestação de serviços para a sociedade, na realização de pesquisas científicas, na produção de insumos para a saúde e na formação e qualificação de recursos humanos, a pesquisa garantiu uma diversidade de perspectivas para coleta de dados.

Outra limitação é não ter havido observação das subunidades, o que foi minimizado pela análise de diversos documentos, como relatórios de auditorias, políticas de Segurança da Informação e regulamentos das subunidades. Cabe registrar que muitas subunidades não disponibilizaram ou simplesmente não tinham esses documentos, o que limitou a abrangência da pesquisa documental.

A pesquisa poderia ter envolvido também a observação de reuniões do Comitê de Segurança da Informação da organização e dos subcomitês de três subunidades. No entanto, não houve reuniões desses comitês durante o período em que foram realizadas as entrevistas. Além disso, aguardar a realização das reuniões poderia gerar um atraso na conclusão da pesquisa. Esta aparente limitação é minimizada pelo fato de nove dos onze membros da composição vigente do Comitê de Segurança da Informação da FIOCRUZ terem sido entrevistados – dois como representantes do Comitê e os demais como representantes das suas subunidades.

7.2 RECOMENDAÇÕES PARA PESQUISAS FUTURAS

A pesquisa investigou a influência das respostas estratégicas das subunidades às pressões institucionais sobre a conformidade da organização. Para isto, o estudo utilizou um *framework* que representa o processo de adoção de medidas de Segurança da Informação que contempla as pressões do ambiente institucional e da administração central da organização, as respostas das subunidades, a adoção de medidas de Segurança da Informação e as consequências dessas respostas na conformidade da organização. Como foi um estudo de caso único, a primeira recomendação é a realização da pesquisa em outras organizações, o que permitirá verificar se esses resultados se confirmam. Empresas multinacionais e organizações de grande porte compostas por diferentes unidades de negócio, universidades com diferentes

campi e organizações públicas com presença em diferentes cidades e estados são possíveis casos que permitem a replicação do estudo.

A influência de pressões coercitivas, normativas e miméticas do ambiente institucional sobre as subunidades pode ser melhor explorada em estudos futuros, visto que esta pesquisa teve um foco na relação entre as subunidades e sua administração central. Investigar a relação entre o ambiente e as subunidades pode esclarecer inclusive como questões locais, como leis, regulamentos e cultura, podem influenciar a Segurança da Informação nessas subunidades.

Esta pesquisa investigou a conformidade organizacional com base no comportamento das suas subunidades, mas não investigou a influência do comportamento das pessoas sobre a Segurança da Informação na organização. A perspectiva institucional, amparada pela tipologia de respostas estratégicas, abre possibilidades para a realização de investigações sobre o comportamento das pessoas em resposta a pressões da organização, possibilitando compreender a relação entre as pressões coercitivas, normativas e miméticas e as respostas dos indivíduos.

O *framework* utilizado para realizar esta pesquisa pode ser adaptado para investigar o mesmo fenômeno em organizações cujas subunidades não têm autonomia, de forma que seja possível identificar se esta determina as respostas das subunidades. Além disso, pode ser utilizado também para investigar organizações que não tenham um setor de TI ou de Segurança da Informação.

Por fim, outras possibilidades seriam investigar como aspectos de cultura, poder e legitimidade interna e externa podem influenciar nas respostas das subunidades às pressões institucionais e, consequentemente, a conformidade da organização com seus requisitos externos de Segurança da Informação.

REFERÊNCIAS

ABRAHAM, Sherly; CHENGALUR-SMITH, Indushobha. The role of conflict resolution in designing and implementing information security policies: an institutional perspective. In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS, 17., 2011. Detroit. **Proceedings...** Atlanta: AIS, 2011.

ADEBAYO, Adewale O.; OMOTOSHO, Olawale J.; ADEKUNLE, Yinka A. Statistical insight into breach data toward improved countermeasures. **Information and Knowledge Management**, v.2, n.8, p.40-51, 2012.

AGUILERA-CARACUEL, Javier; ARAGON-CORREA, Juan A.; HURTADO-TORRES, Nuria E.; RUGMAN, Alan M. The effects of institutional distance and headquarters' financial performance on the generation of environmental standards in multinational companies. **Journal of Business Ethics**, v.105, n.4, p.461-474, 2012.

AHMAD, Atif; MAYNARD, Sean B.; SHANKS, Graeme. A case analysis of information systems and security incident responses. **International Journal of Information Management**, v.35, n.6, p.717–723, 2015.

AIER, Stephan; WEISS, Simon. An institutional framework for analyzing organizational responses to the establishment of architectural transformation. In: EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 13., 2012. Barcelona. **Proceedings...** Atlanta: AIS, 2012.

AL-HAMDANI, Wasim A. Three models to measure information security compliance. In: NEMATI, Hamid R. (Ed.). **Security and privacy assurance in advancing technologies: new developments**. Nova York: Information Science Reference, 2011, p.351-373.

AL-QIRIM, Nabeel. An empirical investigation of an e-commerce adoption-capability model in small businesses in New Zealand. **Electronic Markets**, v.15, n.4, p.418-437, 2005.

ALBERTIN, Alberto L. Valor estratégico dos projetos de Tecnologia da Informação. **Revista de Administração de Empresas**, v.41, n.3, p.42-50, 2001.

ALBRECHTSEN, Eirik. **Friend or foe?** Information Security management of employees. Trondheim, 2008. 182f. Tese (Doutorado em Economia Industrial e Gestão da Tecnologia) – Norwegian University of Science and Technology, Trondheim, 2008.

ALBUQUERQUE JUNIOR, Antonio Eduardo; SANTOS, Ernani M. Produção científica sobre Segurança da Informação em anais de eventos da ANPAD. In: ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO, 4., 2013. Bento Gonçalves. **Anais...** Rio de Janeiro: ANPAD, 2013.

_____; _____. Produção científica sobre Segurança da Informação em eventos científicos brasileiros. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT, 11., 2014. São Paulo. **Anais...** São Paulo: TECSI/FEA/USP, 2014a.

_____; _____. Análise das publicações brasileiras sobre Segurança da Informação sob a ótica social em periódicos científicos entre 2004 e 2013. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM ADMINISTRAÇÃO, 38., 2014. Rio de Janeiro. **Anais...** Rio de Janeiro: ANPAD, 2014b.

_____; _____. Adoção de medidas de Segurança da Informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica**, v.5, n.2, 2014c.

_____; _____. Adoption of Information Security measures in public research institutes. **Journal of Information Systems and Technology Management**, v.12, n.2, p.289-316, 2015.

_____; _____; OLIVEIRA, Rodrigo César R.; SILVA, Adriano S. R.; ALMEIDA, Laercio M. A influência do ambiente institucional na adoção de controles formais, informais e técnicos de Segurança da Informação. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM ADMINISTRAÇÃO, 40., 2016. Costa do Sauípe. **Anais...** Rio de Janeiro: ANPAD, 2016.

ALEXANDRIA, João Carlos S. **Gestão de Segurança da Informação**– uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

ALHIRZ, Hisham; SAJEEV, A. Sayed Muhammed. Factors influencing symbolic adoption of ERP systems in the Middle-East. In: ENTERPRISE SYSTEMS CONFERENCE, 1., 2013. Cape Town. **Proceedings…** Piscataway: IEEE, 2013.

ALJAREH, Salem; ROSSITER, Nick. A task-based security model to facilitate collaboration in trusted multi-agency networks. In: ACM SYMPOSIUM ON APPLIED COMPUTING, 2002. Madrid. **Proceedings…** New York: ACM, 2002, p.744-749.

ALKALBANI, Ahmed; DENG, Hepu; KAM, Booi. A conceptual framework for Information Security in public organizations for E-Government development. In: AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS, 25., 2014, Auckland. **Proceedings...** Auckland, 2014.

_____; _____; _____. Organisational security culture and information security compliance for e-Government development: the moderating effect of social pressure. In: PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS, 19., 2015. Singapura. **Proceedings...** Atlanta: AIS, 2015.

ALLEN, Bryce. **Information Tasks**: toward a user-centered approach to information systems. Orlando: Academic Press, 1996.

ALVARENGA NETO, Rivadávia C. D. **Gestão do conhecimento em organizações:** proposta de mapeamento conceitual integrativo. Belo Horizonte, 2005. 400f. Tese (Doutorado em Ciência da Informação) – Universidade Federal de Minas Gerais, Belo Horizonte, 2005.

AMORIM, Fabiana B.; TOMAÉL, Maria I. Gestão da informação e gestão do conhecimento na prática organizacional: análise de estudos de casos. **Revista Digital de Biblioteconomia e Ciência da Informação**, v.8, n.2, p.1-22, 2011.

ANDERSON, James M. Why we need a new definition of information security. **Computers & Security**, v.22, n.4, p.308-313, 2003.

ANDERSON, Ross. Why information security is hard – an economic perspective. In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 17., 2001, New Orleans. **Proceedings...** New Orleans, 2001.

ANTHONY, Denise L.; APPARI, Ajit; JOHNSON, M. Eric. Institutionalizing HIPAA compliance: organizations and competing logics in U.S. Health Care. **Journal of Health and Social Behavior**, v.55, n.1, p.108-124, 2014.

ANYANWU, Long O. Factorial management of global information systems. **Journal of International Information Management**, v.6, n.2, p.73-83, 1997.

APPARI, Ajit; ANTHONY, Denise L.; JOHNSON, M. Eric. HIPAA compliance: an examination of institutional and market forces. In: WORKSHOP ON ECONOMICS OF INFORMATION SYSTEMS, 8., 2009, London. **Proceedings...** London: WEIS, 2009.

_____; JOHNSON, M. Eric. Information security and privacy in healthcare: current state of research. **International Journal of Internet and Enterprise Management**, v.6, n.4, p.279-314, 2010.

_____; _____; ANTHONY, Denise L. The Neo-Institutional view of HIPAA compliance in home health care. In: WORKSHOP ON INFORMATION SECURITY & PRIVACY, 4., 2009. Phoenix. **Proceedings...** Atlanta: AIS, 2009.

ARMÊNIO NETO, João; MACHADO-DA-SILVA, Clóvis L. Institucionalização e desinstitucionalização de práticas sociais: o caso das tecnologias VoIP e Circuit Switched. **Revista Eletrônica de Sistemas de Informação**, v.8, n.2, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013**: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, 2013.

BACKHOUSE, James; DHILLON, Gurpreet S. Structures of responsibility and security of information systems. **European Journal of Information Systems**, v.5, n.1, p.2-9, 1996.

_____; HSU, Carol W.; SILVA, Leiser. Circuits of power in creating de jure standards: shaping an international information systems security standard. **MIS Quarterly**, v.30, SI, p.413-438, 2006.

BAPTISTA, Paulo; PINHEIRO, Gabriela; ALVES, Pedro. **Sistemas de gestão de segurança alimentar**. Guimarães: Forvisão, 2003.

BARMAN, Scott. **Writing information security policies**. Indianapolis: New Riders, 2001.

BASKERVILLE, Richard. Risk analysis: an interpretive feasibility tool in justifying information systems security. **European Journal of Information Systems**, v.1, n.2, p.121-130, 1991.

BEAL, Adriana. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BÉLANGER, France; CROSSLER, Robert E. Privacy in the digital age: a review of information privacy research in information systems. **MIS Quarterly**, v.35, n.4, p.1017–1042, 2011.

BELASCO, Kent; WAN, Siaw-Peng. Online retail banking: Security concerns, breaches, and controls. In: BIDGOLI, Hossein (Org.). **Handbook of Information Security**: threats, vulnerabilities, prevention, detection, and management. New Jersey: John Wiley & Sons, vol.1, 2006, p.37-48.

BENBASAT, Izak; GOLDSTEIN, David K.; MEAD, Melissa. The case research strategy in studies on Information Systems. **MIS Quarterly**, v.11, n.3, p.369-386, 1987.

BERNARD, Ray. Information Lifecycle Security Risk Assessment: a tool for closing security gaps. **Computers & Security**, v.26, n.1, p.26-30, 2007.

BEVERLAND, Michael; LUXTON, Sandra. Managing integrated marketing communication (IMC) through strategic decoupling: how luxury wine firms retain brand leadership while appearing to be wedded to the past. **Journal of Advertising**, v.34, n.4, p.103–116, 2005.

BISHOP, Matthew A. **Computer security**: art and science. Boston: Addison-Wesley, 2003.

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

_____. **Discovering Information Security Management**. Estocolmo, 2005. 300f. Tese (Doutorado em Segurança da Informação) – Stockholm University, Estocolmo, 2005.

BOIRAL, Olivier. Corporate greening through ISO 14001: a rational myth? **Organization Science**, v.18, n.1, p.127-146, 2007.

BOOKER, Robert. Re-engineering enterprise security. **Computers & Security**, v.25, n.1, p.13-17, 2006.

BORGES, Diego E.; DUTRA, Luiz C.; SCHERER, Flávia L. Meio ambiente e estratégia: um estudo multicaso no setor vitivinícola da região central do Rio Grande do Sul sob a perspectiva da Teoria Institucional. **Revista de Administração da UFSM**, v.7, número especial, p.40-54, 2014.

BORKO, Harold. Information science: what is it? **American Documentation**, v.19, n.1, p.3–5, 1968.

BOSCHMAN, Geke. **Strategic responses of multinational organizations concerning human rights dilemmas**. Eindhoven, 2006. 83f. Dissertação (Mestrado em Administração) – Tilburg University, Tilburg, 2006.

BOWERSOX, Donald J.; CLOSS, David J.; COOPER, M. Bixby; BOWERSOX, John C. **Gestão logística da cadeia de suprimentos**. Porto Alegre: Bookman, 2ª Ed., 2014.

BOXENBAUM, Eva; JONSSON, Stefan. Isomorphism, diffusion and decoupling. In: GREENWOOD, Royston; OLIVER, Christine; SAHLIN, Kerstin; SUDDABY, Roy (Orgs.). **The SAGE handbook of organizational institutionalism**. Los Angeles: SAGE, 2009, p.78-99.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**, Brasília, DF, n.114, s.1, p.78-79, 14 jun. 2000.

_____. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. **Diário Oficial da União**, Brasília, DF, n.115, s.1, p.6-7, 18 jun. 2008a.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 2/IN01/DSIC/GSIPR, de 13 de outubro de 2008. Metodologia de Gestão de Segurança da Informação e Comunicações. **Diário Oficial da União**, Brasília, DF, n.115, s.1, p.6-7, 18 jun. 2008b.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 3/IN01/DSIC/GSIPR, de 30 de junho de 2009. Diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**, Brasília, DF, n.125, s.1, p.11-12, 03 jul. 2009a.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 5/IN01/DSIC/GSIPR, de 14 de agosto de 2009. Disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. **Diário Oficial da União**, Brasília, DF, n.156, s.1, p.8-10, 17 ago. 2009b.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 6/IN01/DSIC/GSIPR, de 11 de novembro de 2009. Estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. **Diário Oficial da União**, n.223, s.1, p.20-21, 23 nov. 2009c.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 7/IN01/DSIC/GSIPR, de 06 de maio de 2010. Estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. **Diário Oficial da União**, n.86, s.1, p.6-8, 07 maio 2010.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012. Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial da União**, n.30, s.1, p.3, 10 fev. 2012a.

_____. Departamento de Segurança da Informação e Comunicações. Gabinete de Segurança Institucional. Norma Complementar nº 15/IN01/DSIC/GSIPR, de 11 de junho de 2012. Estabelece diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. **Diário Oficial da União**, n.119, s.1, p.3, 21 jun. 2012b.

_____. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013. Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. **Diário Oficial da União**, Brasília, DF, n.32, s.1, p.5-6, 18 fev. 2013a.

_____. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 3, de 6 de março de 2013. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. **Diário Oficial da União**, Brasília, DF, n.50, s.1, p.2-3, 14 mar. 2013b.

BROADBENT, Marianne; BUTLER, Carey. Managing Information Technology infrastructure capability for international business operations. In: PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS, 3., 1997. Brisbane. **Proceedings...** Atlanta: AIS, 1997.

BROMLEY, Patricia; POWELL, Walter W. From smoke and mirrors to walking the talk: decoupling in the contemporary world. **The Academy of Management Annals**, v.6, n.1, p.483-530, 2012.

_____; HWANG, Hokyu; POWELL, Walter W. Decoupling revisited: common pressures, divergent strategies in the U.S. nonprofit sector. **Management**, v.15, n.5, p.468-501, 2012.

BUCKLAND, Michael K. **Information and Information Systems**. New York: Greenwood, 1991.

BULGURCU, Burcu; CAVUSOGLU, Hasan; BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly**, v.34, n.3, p.523-548, 2010.

BURD, Steffani A. **The impact of Information Security in academic institutions on public safety and security**: assessing the impact and developing solutions for policy and practice. Washington, DC: National Institute of Justice, 2006.

BUSANELO, Ernani C. Um estudo epistemológico da Teoria Neo-Institucional. In: ENCONTRO DE ESTUDOS ORGANIZACIONAIS, 6., 2010. Florianópolis. **Anais...** Rio de Janeiro: ANPAD, 2010.

CARNEIRO, Alberto. **Introdução à segurança de sistemas de informação**. Lisboa: FCA, 2002.

CARTON, Fergal; ADAM, Frederic. Towards a model for determining the scope of ICT integration in the enterprise: the case of Enterprise Resource Planning (ERP) Systems. **The Electronic Journal of Information Systems Evaluation**, v.13, n.1, p.17-26, 2010.

CASAL, Jordi M.; MANUEL, A.; MATEU, Enrique M.; MARTIN, Marga J. Biosecurity measures on swine farms in Spain: perceptions by farmers and their relationship to current on-farm measures. **Preventive Veterinary Medicine**, v.82, n.1–2, p.138–150, 2007.

CASEY, Eoghan. Case study: network intrusion investigation – lessons in forensic preparation. **Digital Investigation**, v.2, n.4, p.254-260, 2005.

CASILE, Maureen; DAVIS-BLAKE, Alison. When accreditation standards change: factors affecting differential responsiveness of public and private organizations. **Academy of Management Journal**, v.45, n.1, p.180-195, 2002.

CASTELLS, Manuel. **A sociedade em rede – a era da informação**: economia, sociedade e cultura. São Paulo: Paz e Terra, v.1, 8ª. ed., 2005.

CAVUSOGLU, Huseyin; CAVUSOGLU, Hasan; SON, Jai-Yeol; BENBASAT, Izak. Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. **Information & Management**, v.52, n.4, p.385-400, 2015.

CEPIK, Marco; CANABARRO, Diego R.; POSSAMAI, Ana Júlia. A institucionalização do SISP e a Era Digital no Brasil. In: CEPIK, Marco; CANABARRO, Diego R. **Governança de TI**: transformando a Administração Pública no Brasil. Porto Alegre: UFRGS, 2014. p.37-78.

CHANG, Shuchih E.; HO, Chienta B. Organizational factors to the effectiveness of implementing information security management. **Industrial Management & Data Systems**, v.106, n.3, p.345-361, 2006.

CHIEOCHAN, Oran; LINDLEY, David; DUNN, T. Factors affecting the use of Information Technology in Thai agricultural cooperatives: a work in progress. **Electronic Journal of Information Systems in Developing Countries**, v.2, n.1, p.1-15, 2000.

CHOU, Shin-Yi; LIU, Jin-Tan; HAMMITT, James K. National Health Insurance and technology adoption: evidence from Taiwan. **Contemporary Economic Policy**, v.22, n.1, p.26-38, 2004.

COLES-KEMP, Lizzie. Information Security Management: an entangled research challenge. **Information Security Technical Report**, v.14, n.4, p.181-185, 2009.

COOPER, Donald R.; SCHINDLER, Pamela S. **Métodos de pesquisa em Administração**. Porto Alegre: AMGH, 12ª ed., 2016.

COOPER, Michael H. Information security training: what will you communicate? In: ANNUAL ACM SIGUCCS FALL CONFERENCE, 37., 2009, St. Louis. **Proceedings…** ACM, 2009, p.217-222.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. Porto Alegre: Artmed, 3ª ed., 2010.

COLE, Wade M. Sovereignty relinquished? Explaining commitment to the international human rights covenants, 1966–1999. **American Sociological Review**, v.70, n.3, p. 472–495, 2005.

_____. Human rights as myth and ceremony? Reevaluating the effectiveness of human rights treaties, 1981–2007. **American Journal of Sociology**, v.117, n.4, p.1131–1171, 2012.

CORDEIRO, Claudia C. R. **Evolução do conceito de segurança nas relações internacionais: uma análise das políticas de segurança alimentar** – caso Bolívia. São Paulo, 2013. 169f. Dissertação (Mestrado em Ciência Política) – Universidade de São Paulo, São Paulo, 2013.

CULNAN, Mary J.; WILLIAMS, Cynthia C. How ethics can enhance organizational privacy: lessons from the Choicepoint and TJX data breaches. **MIS Quarterly**, v.33, n.4, p.673–687, 2009.

CUMMINGS, Maeve L.; GUYNES, Jan L. Information System activities in transnational corporations: a comparison of U.S. and non-U.S. subsidiaries. **Journal of Global Information Management**, v.2, n.1, p.12-26, 1994.

DAMODARAN, Aswath. **Strategic risk taking** – a framework for risk management. Upper Saddle River: Prentice Hall, 2008.

DAVENPORT, Thomas H. **Ecologia da Informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

DELMAS, Magali A.; TOFFEL, Michael W. Organizational responses to environmental demands: opening the black box. **Strategic Management Journal**, v.29, n.10, p.1027-1055, 2008.

DEVAUJANY, François-Xavier; CARTON, Sabine; MITEV, Nathalie; ROMEYER, Cécile. Applying and theorizing institutional frameworks in IS research: a systematic analysis from 1999 to 2009. **Information Technology & People**, v.27, n.3, p.280-317, 2014.

DHILLON, Gurpreet S. Managing and controlling computer misuse. **Information Management & Computer Security**, v.7, n.4, p.171-175, 1999.

_____. Violations of safeguards by trusted personnel and understanding related information security concerns. **Computers & Security**, v.20, n.2, p.165-172, 2001.

_____; BACKHOUSE, James. Information System Security Management in the new millennium. **Communications of the ACM**, v.43, n.7, p.125-128, 2000.

_____; _____. Current directions in IS security research: towards socioorganizational perspectives. **Information Systems Journal**, v.11, n.2, p.127-153, 2001.

_____; MOORES, Steve. Computer crimes: theorizing about the enemy within. **Computers & Security**, v.20, n.8, p.715-723, 2001.

DIAS, Alcina; HERAS, Inaki. Efficiency of ISO 9001 in Portugal: a qualitative study from a holistic theoretical perspective. **International Journal for Quality Research**, v.7, n.1, p.31-62, 2013.

DIMAGGIO, Paul J.; POWELL, Walter W. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. **American Sociological Review**, v.48, n.2, p.147-160, 1983.

DOHERTY, Neil F.; FULFORD, Heather. Aligning the information security policy with the strategic information systems plan. **Computers & Security**, v.25, n.1, p.55-63, 2006.

DONNER, Marcos L.; OLIVEIRA, Leonardo R. Análise de satisfação com a segurança no uso de internet banking em relação aos atuais recursos disponíveis no canal eletrônico. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 32., 2008. Rio de Janeiro. **Anais...** Rio de Janeiro: ANPAD, 2008.

DOWLING, John; PFEFFER, Jeffrey. Organizational legitimacy: social values and organizational behavior. **The Pacific Sociological Review**, v.18, n.1, p.122-136, 1975.

DRESNER, Daniel G. **A study of standards and the mitigation of risk in Information Systems**. Manchester, 2011. 276f. Tese (Doutorado em Informática) – The University of Manchester, Manchester, 2011.

DRETSKE, Fred I. **Knowledge and the flow of information**. Cambridge: MIT Press, 1983.

DRUCKER, Peter F. The coming of the new organization. **Harvard Business Review**, v.66, p.45-53, 1988.

DWIVEDI, Yogesh K.; WADE, Michael R.; SCHNEBERGER, Scott L. **Information Systems Theory** – explaining and predicting our digital society. New York: Springer, 2012.

ELKY, Steve. **An introduction to Information System Risk Management**. Bethesda: SANS Institute, 2006.

ELLWANGER, Cristiane. **Impacto da utilização de técnicas de endomarketing na efetividade das Políticas de Segurança da Informação**. Santa Maria, 2009. 134f. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal de Santa Maria, Santa Maria, 2009.

ELOFF, Mariki M.; VON SOLMS, Sebastiaan H. Information Security Management: a hierarchical framework for various approaches. **Computers & Security**, v.19, n.3, p.243-256, 2000.

ELSBACH, Kimberly D.; SUTTON, Robert I. Acquiring organizational legitimacy through illegitimate actions: a marriage of institutional and impression management theories. **Academy of Management Journal**, v.35, n.4, p.699–738, 1992.

EMINAGAOGLU, Mete; UÇAR, Erdem; EREN, Saban. The positive outcomes of information security awareness training in companies – a case study. **Information Security Technical Report**, v.14, n.4, p.223–229, 2009.

ESTERHAZY, Rachelle. **Strategic responses to the German Excellence Initiative**: a case study of Berlin Humboldt University. Dissertação (Mestrado em Educação Superior) – University of Oslo, Oslo, 2014.

FACHINI, Gilson J. **Análise do nível de formalização da Política de Segurança da Informação à luz da NBR ISO/IEC 17799:2005 nas empresas de Tecnologia da Informação de Blumenau, SC**. Dissertação (Mestrado em Ciências Contábeis) – Universidade Regional de Blumenau, Blumenau, 2009.

_____; FERNANDES, Francisco C.; FARIA, Ana 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., 2011. Porto Alegre. **Anais...** Rio de Janeiro: ANPAD, 2011.

FARN, Kwo-Jean; LIN, Shu-Kuo; FUNG, Andrew R. W. A study on Information Security Management System evaluation – assets, threat and vulnerability. **Computer Standards & Interfaces**, v.26, n.6, p.501-513, 2004.

FENG, Nan; LI, Minqiang. An information systems security risk assessment model under uncertain environment. **Applied Soft Computing**, v.11, n.7, p.4332–4340, 2011.

FLICK, Uwe. **Introdução à pesquisa qualitativa**. 3ed. Porto Alegre: Artmed, 2009.

FONTANA, Rafaela M.; IAROZINSKI NETO, Alfredo. ERP systems implementation in complex organizations. **Journal of Information Systems and Technology Management**, v.6, n.1, p.61-92, 2009.

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

FORCHT, Karen A.; AYERS, Walter C. Developing a computer security policy for organizational use and implementation. **Journal of Computer Information Systems**, v.41, n.2, p.52-57, 2001.

FRANGOPOULOS, Evangelos D.; ELOFF, Mariki M.; VENTER, Lucas M. Psychosocial risks: can their effects on the security of information systems really be ignored? **Information Management & Computer Security**, v.21, n.1, p.53-65, 2013.

FREZATTI, Fábio; AGUIAR, Andson B.; REZENDE, Amaury J. Respostas estratégicas às pressões institucionais e sucesso no atingir metas no orçamento: um estudo em uma empresa multinacional. **Organizações & Sociedade**, v.14, n.43, p.141-158, 2007.

FUNDAÇÃO OSWALDO CRUZ. **FIOCRUZ –** uma instituição a serviço da vida. Rio de Janeiro: Editora FIOCRUZ, 2010.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 069/2011-PR**, de 21 de fevereiro de 2011. Institui a Política de Segurança da Informação e Comunicações (POSIC), visando assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações da FIOCRUZ. Rio de Janeiro, 21 fev. 2011a.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 070/2011-PR**, de 25 de fevereiro de 2011. Institui o Modelo de Gestão do Sistema de Segurança da Informação e Comunicações da FIOCRUZ. Rio de Janeiro, 21 fev. 2011b.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 114/2011-PR**, de 07 de abril de 2011. Institui a Coordenação de Gestão de Tecnologia da Informação – CGTI, vinculada à Vice-Presidência de Gestão e Desenvolvimento Institucional – VPGDI. Rio de Janeiro, 07 abr. 2011c.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 116/2011-PR**, de 07 de abril de 2011. Designa servidor para a função que especifica. Rio de Janeiro, 07 abr. 2011d.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 143/2011-PR**, de 28 de abril de 2011. Institui o Comitê de Segurança da Informação e Comunicações da FIOCRUZ. Rio de Janeiro, 22 abr. 2011e.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 345/2012-PR**, de 17 de abril de 2012. Aprova a Norma Institucional SIC-001/CGTI/VPGDI, que dispõe sobre as responsabilidades do usuário quanto ao uso de senhas e equipamentos, mesa limpa e tela limpa. Rio de Janeiro, 17 abr. 2012a.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 347/2012-PR**, de 17 de abril de 2012. Define a nova composição do Comitê de Segurança da Informação e Comunicações da FIOCRUZ. Rio de Janeiro, 17 abr. 2012b.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 432/2012-PR**, de 11 de maio de 2012. Aprova a Norma Institucional SIC-002/CGTI/VPGDI, que dispõe sobre as regras de segurança relativas ao uso do serviço de Internet. Rio de Janeiro, 11 maio 2012c.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 433/2012-PR**, de 14 de maio de 2012. Aprova a Norma Institucional SIC-003/CGTI/VPGDI, que dispõe sobre as regras de segurança relativas ao uso do serviço de correio eletrônico. Rio de Janeiro, 14 maio 2012d.

_____. Presidência da Fundação Oswaldo Cruz. **Portaria 153/2013-PR**, de 15 de fevereiro de 2013. Aprova a Norma Institucional SIC-004/CGTI/VPGDI, que dispõe sobre as regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em Data Centers na FIOCRUZ, aprova a Norma Institucional SIC-005/CGTI/VPGDI, que estabelece as diretrizes para a geração de cópias de segurança das informações e sua recuperação em um tempo aceitável, e aprova a Norma Institucional SIC-006/CGTI/VPGDI, que estabelece as diretrizes de segurança para aquisição, desenvolvimento e manutenção de sistemas de informação. Rio de Janeiro, 15 fev. 2013a.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Portaria 002/2013-VPGDI**, de 01 de março de 2013. Institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR. Rio de Janeiro, 01 mar. 2013b.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Portaria 003/2013-VPGDI**, de 11 de março de 2013. Institui o Modelo de Gestão de Incidentes de Segurança da Informação e Comunicações da FIOCRUZ. Rio de Janeiro, 11 mar. 2013c.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Portaria 007/2013-VPGDI**, de 12 de abril de 2013. Institui o Modelo de Gestão de Continuidade de Negócios de Tecnologia da Informação da FIOCRUZ. Rio de Janeiro, 12 abr. 2013d.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Portaria 017/2013-VPGDI**, de 23 de setembro de 2013. Aprova a Norma Institucional SIC-007/CGTI/VPGDI, que estabelece as diretrizes para a realização de acesso à rede de dados da FIOCRUZ a partir de um local externo. Rio de Janeiro, 23 set. 2013e.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Portaria 018/2013-VPGDI**, de 23 de setembro de 2013. Aprova a Norma Institucional SIC-008/CGTI/VPGDI, que estabelece diretrizes para o uso das redes sociais nos aspectos relativos à Segurança da Informação e Comunicações no âmbito da FIOCRUZ. Rio de Janeiro, 23 set. 2013f.

_____. Vice-Presidência de Gestão e Desenvolvimento Institucional da Fundação Oswaldo Cruz. **Norma Institucional SIC-009/CGTI/VPGDI**, que estabelece as diretrizes e fornece orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações no âmbito da FIOCRUZ. Rio de Janeiro, 07 nov. 2013g.

_____. Coordenação de Gestão de Tecnologia da Informação. **Análise da conformidade das unidades da FIOCRUZ à Política de Segurança da Informação e Comunicações**. Rio de Janeiro: FIOCRUZ, 2014.

_____. Coordenação de Gestão de Tecnologia da Informação. **Análise da conformidade das unidades da FIOCRUZ à Política de Segurança da Informação e Comunicações - 2015**. Rio de Janeiro: FIOCRUZ, 2015.

_____. Coordenação de Gestão de Tecnologia da Informação. **Quem somos – CGTI**. Rio de Janeiro: FIOCRUZ, 2016a. Disponível em: <https://cgti.fiocruz.br/novo_portal/pages/quemsomos/index.php>. Acesso em: 20 out. 2016.

_____. Coordenação de Gestão de Tecnologia da Informação. **Segurança – CGTI**. Rio de Janeiro: FIOCRUZ, 2016b. Disponível em: <https://cgti.fiocruz.br/novo_portal/pages/seguranca/index.php>. Acesso em: 20 out. 2016.

_____. **Organograma**. Rio de Janeiro: FIOCRUZ, 2016c. Disponível em: <http://portal.fiocruz.br/pt-br/content/organograma>. Acesso em: 20 out. 2016.

_____. **Unidades e escritórios**. Rio de Janeiro: FIOCRUZ, 2016d. Disponível em: <http://portal.fiocruz.br/pt-br/content/unidades-e-escritórios>. Acesso em: 20 out. 2016.

GIL, Antonio C. **Estudo de caso**. São Paulo: Atlas, 2009.

GORAYEB, Diana M. C. **Gestão de Continuidade de Negócios aplicada ao ensino presencial mediado por recursos tecnológicos**. São Paulo, 2012. 153f. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de São Paulo, São Paulo, 2012.

GORDON, Lawrence A.; LOEB, Martin P. The economics of information security investment. **ACM Transactions on Information and Systems Security**, v.5, n.4, p.438-457, 2002.

_____; _____. Budgeting process for information security expenditures. **Communications of the ACM**, v.49, n.1, p.121-125, 2006.

GORDON, Steven R.; GORDON, Judith R. Organizational options for resolving the tension between IT departments and business units in the delivery of IT services. **Information Technology & People**, v.15, n.4, p.286-305, 2002.

GRAEFF, Júlia F. **Pressões ambientais e respostas estratégicas na institucionalização do plantio direto no Paraná**. Curitiba, 2005. 209f. Dissertação (Mestrado em Administração) – Universidade Federal do Paraná, Curitiba, 2005.

GREENAWAY, Kathleen E.; CHAN, Yolande E. Theoretical explanations for firms' information privacy behaviors. **Journal of the Association for Information Systems**, v.6, n.6, p.171-198, 2005.

GUARIDO FILHO, Edson R.; MACHADO-DA-SILVA, Clóvis L.; GONÇALVES, Sandro A. Institucionalização da Teoria Institucional no contexto dos Estudos Organizacionais no Brasil. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 33., São Paulo, 2009. **Anais...** Rio de Janeiro: ANPAD, 2009.

GUSMÃO, Ana Paula H.; SILVA, Lúcio C.; SILVA, Maisa M.; POLETO, Thiago; COSTA, Ana Paula C. S. Information security risk analysis model using fuzzy decision theory. **International Journal of Information Management**, v.36, n.1, p.25–34, 2016.

GUTIÉRREZ-RINCÓN, Viviana. Beyond the internal dynamics of organizational responses to conflicting institutional demands. **Estudios Gerenciales**, v.30, n.133, p.376-383, 2014.

HAGEN, Janne M.; ALBRECHTSEN, Eirik; HOVDEN, Jan. Implementation and effectiveness of organizational information security measures. **Information Management & Computer Security**, v.16, n.4, p.377-397, 2008.

HAMEED, Mumtaz Abdul; ARACHCHILAGE, Nalin Asanka G. A model for the adoption process of Information System Security innovations in organisations: a theoretical perspective. In: AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS, 27., Wollongong, 2016. **Proceedings...** Atlanta: AIS, 2016.

_____; COUNSELL, Steve; SWIFT, Stephen. A conceptual model for the process of IT innovation adoption in organizations. **Journal of Engineering and Technology Management**, v.29, n.3, p.358-390, 2012.

HANDGRAAF, Annemarijn. **Institutional pressures & strategic responses**: the case of Shell and the Ogoni struggle. Amsterdam, 2012. 111f. Dissertação (Mestrado em Administração de Empresas) – Vrije Universiteit, Amsterdam, 2012.

HASAN, Ragib; YURCIK, William. A statistical analysis of disclosed storage security breaches. In: ACM WORKSHOP ON STORAGE SECURITY AND SURVIVABILITY, 2., 2006. Alexandria. **Proceedings...** New York: ACM, 2006.

HEDSTRÖM, Karin; KOLKOWSKA, Ella; KARLSSON, Fredrik; ALLEN, J. P. Value conflicts for information security management. **Journal of Strategic Information Systems**, v.20, n.4, p.373-384, 2011.

HERAS-SAIZARBITORIA, Iñaki. **An empirical study on the ceremonial adoption of ISO 9000 in Basque organizations**. Orkestra Working Paper Series in Territorial Competitiveness, n.2011-R02, 2011.

_____; BOIRAL, Olivier. Symbolic adoption of ISO 9000 in small and medium-sized enterprises: the role of internal contingencies. **International Small Business Journal**, v.33, n.3, p.299-320, 2015.

HERATH, Tejaswini; HERATH, Hemantha; BREMSER, Wayne G. Balanced Scorecard implementation of Security strategies: a framework for IT Security Performance Management. **Information Systems Management**, v.27, n.1, p.72-81, 2010.

HERNES, Helge; ERDVIK, Grete K. Compliance and non-compliance with a superordinate directive document. **Public Organization Review**, v.14, n.1, p.65-81, 2014.

HITCHINGS, Jean. Deficiencies of the traditional approach to information security and the requirements for a new methodology. **Computers & Security**, v.14, n.5, p.377-383, 1995.

HOLGATE, Janine A.; WILLIAMS, Susan P.; HARDY, Catherine A. Information Security Governance: investigating diversity in critical infrastructure organizations. In: BLEDECONFERENCE, 25., 2012. Bled, 2012. **Proceedings...** Bled, 2012, p.379-393.

HOLLAND, Christopher P.; LOCKETT, Geoff; RICHARD, Jean-Michel; BLACKMAN, Ian. The evolution of a global cash management system. **Sloan Management Review**, v.35, n.1, p.37-47, 1994.

HÖNE, Karin; ELOFF, Jan H. P. Information security policy – what do international information security standards say? **Computers & Security**, v.21, n.5, p.402-409, 2002.

HONG, Kwo-Shing; CHI, Yen-Ping; CHAO, Louis R.; TANG, Jih-Hsing. An integrated system theory of information security management. **Information Management & Computer Security**, v.11, n.5, p.243-248, 2003.

HOPPÉ, Norman. Achieving consistent security controls throughout a multinational organization. **Computers & Security**, v.13, n.1, p.23-29, 1994.

HSU, Carol W.; LEE, Jae-Nam; STRAUB, Detmar W. Institutional influences on Information Systems Security innovations. **Information Systems Research**, v.23, n.3, p.918-939, 2012.

HU, Qing; HART, Paul; COOKE, Donna. The role of external influences on organizational Information Security practices: an institutional perspective. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 39., 2006. Kauai. **Proceedings...** Big Island: HICSS,2006.

_____; _____; _____. The role of external and internal influences on Information Systems Security – a neo-institutional perspective. **Journal of Strategic Information Systems,** v16, n.2, p.153-172, 2007.

INGERSOLL, Richard M. Loosely coupled organizations revisited. **Research in the Sociology of Organizations**, v.11, p.81-112, 1993.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 13335-1:2004**: Information Technology – Security Techniques – Management of Information and Communications Technology Security. ISO/IEC: Genebra, 2004.

JEWER, Jennifer; MCKAY, Kenneth N. Antecedents and consequences of board IT governance: institutional and strategic choice perspectives. **Journal of the Association for Information Systems**, v.13, n.7, p.581-617, 2012.

JUELS, Ari. Encryption basics. In: BIDGOLI, Hossein (Org.). **Handbook of Information Security**: threats, vulnerabilities, prevention, detection, and management. New Jersey: John Wiley & Sons, vol.2, 2006, p.469-478.

KAM, Hwee-Joo; KATERATTANAKUL, Pairin; EMERICK, Gerald. Impact of external pressures on Information Security Policy compliance in the banking industry. In: INTERNATIONAL CONFERENCE ON INFORMATION RESOURCES MANAGEMENT, 6., 2013. Natal. **Proceedings...** Atlanta: AIS, 2013.

_____; _____; GOGOLIN, Greg; HONG, Soongoo. Information Security Police compliance in higher education: a Neo-Institutional perspective. In: PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS, 17., 2013. Jeju Island. **Proceedings…** Seoul: KMIS, 2013.

KARABACAK, Bilge; SOGUKPINAR, Ibrahim. ISRAM: Information Security risk analysis method. **Computers & Security**, v.24, n.2, p.147-159, 2005.

KARIMI, Jahangir; KONSYNSKI, Benn R. The Information Technology and Management Infrastructure Strategy – Globalization and information management strategies. In: GALLIERS, Robert D.; LEIDNER, Dorothy E. (Orgs.). **Strategic Information Management** – challenges and strategies in managing Information Systems. Oxford: Butterworth-Heinemann, 2003, p.89-112.

KARYDA, Maria; KIOUNTOUZIS, Evangelos; KOKOLAKIS, Spyros. Information Systems Security Policies: a contextual perspective. **Computers & Security**, v.24, n.3, p.246-260, 2005.

KAYO, Eduardo K.; KIMURA, Herbert; MARTIN, Diógenes M. L.; NAKAMURA, Wilson T. Ativos intangíveis, ciclo de vida e criação de valor. **Revista de Administração Contemporânea**, v.10, n.3, p.73-90, 2006.

KIELY, Laree S.; BENZEL, Terry V. Systemic Security Management. **IEEE Security & Privacy**, v.4, n.6, p.74-77, 2006.

KILLCRECE, Georgia; KOSSAKOWSKI, Klaus-Peter; RUEFLE, Robin; ZAJICEK, Mark. **State of the practice of computer security incident response teams (CSIRTs)**. Technical Report, CMU/SEI-2003-TR-001. Carnie Mellon University, 2003.

KING, Christopher M.; DALTON, Curtis E.; OSMANOGLU, T. Ertem. **Security architecture**: design, deployment, and operations. Berkeley: McGraw-Hill, 2001.

KOSTOVA, Tatiana; ZAHEER, Srilata. Organizational legitimacy under conditions of complexity: the case of the multinational enterprise. **Academy of Management Review**, v.24, n.1, p.64–81, 1999.

KOTULIC, Andrew G.; CLARK, Jan G. Why there aren't more information security research studies. **Information & Management**, v.41, n.5, p.597–607, 2004.

KRAHMANN, Elke. Beck and beyond: selling security in the world risk society. **Review of International Studies**, v.37, n.1, p.349-372, 2011.

KRITZINGER, Elmarie; SMITH, Elmé. Information security management: an information security retrieval and awareness model for industry. **Computers & Security**, v.27, n.5-6, p.224-231, 2008.

LAPKE, Michael; DHILLON, Gurpreet S. Disassociations in security policy lifecycles. **International Journal of Information Security and Privacy**, v.9, n.1, p.62-77, 2015.

LARSON, Eric C. **The impact of the demand for integration in the large multi-business unit firm on the IT Organization structure**. Minneapolis, 2012. 275f. Tese (Doutorado em Administração de Empresas) – University of Minnesota, Minneapolis, 2012.

LEBRE, Marcelo. Medidas de segurança e periculosidade criminal: medo de quem? **Responsabilidades**, v.2, n.2, p.273-282, 2013.

LEE, R. Daniel. **Developing effective information systems security policies**. Bethesda: SANS Institute, 2001.

LIM, Alwyn; TSUTSUI, Kiyoteru. Globalization and commitment in corporate social responsibility: cross-national analyses of institutional and political-economy effects. **American Sociological Review**, v.77, n.1, p.69–98, 2012.

LO, Chi-Chun; CHEN, Wan-Jia. A hybrid information security risk assessment procedure considering interdependences between controls. **Expert Systems with Applications**, v.39, n.1, p.247–257, 2012.

LOPES, Isabel M. **Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal**. Braga, 2012. 437f. Tese (Doutorado em Tecnologias e Sistemas de Informação, Engenharia e Gestão de Sistemas de Informação) – Universidade do Minho, Braga, 2012.

_____; SÁ-SOARES, Felipe. Institutionalization of Information Systems Security Policies adoption: factors and guidelines. **International Journal on Computer Science and Information Systems**, v.9, n.2, p.82-95, 2014.

LOPEZ, Daniel M. **Respostas estratégicas dos sindicatos patronais do comércio de bens, serviços e turismo do Brasil às pressões institucionais**. Rio de Janeiro, 2012. 97f. Dissertação (Mestrado Profissional em Gestão Empresarial) – EBAPE/Fundação Getúlio Vargas, Rio de Janeiro, 2012.

LORENS, Evandro M. **Aspectos normativos da Segurança da Informação**: um modelo de cadeia de regulamentação. Brasília, 2007. 145f. Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília, Brasília, 2007.

LUESEBRINK, Michael. **The Institutionalization of Information Security Governance structures in academic institutions**: a case study. Tallahassee, 2011. 257f. Tese (Doutorado em Comunicação e Informação) – Florida State University, Tallahassee, 2011.

LUNDBERG, Viktor. **Performance Management Systems in Swedish banks**: a longitudinal study through the deregulations' first quarter of a century. Gothenburg, 2013. 69f. Tese (Doutorado em Negócios) – Gothenburg University, Gothenburg, 2013.

LUO, Xin; BRODY, Richard; SEAZZU, Alessandro; BURD, Stephen. Social Engineering: the neglected human factor for Information Security Management. **Information Resources Management Journal**, v.24, n.3, p.1-8, 2011.

MACHLUP, Fritz; MANSFIELD, Una. Semantic quirks in studies of information. In: MACHLUP, Fritz; MANSFIELD, Una (Orgs.). **The study of information**: interdisciplinary messages. New York: John Wiley, 1983, p.641-671.

MANDIA, Kevin; PROSISE, Chris; PEPE, Matthew. **Incident response & computer forensis**. New York: McGraw-Hill, 2a.ed., 2003.

MANOEL, Sergio S. **Governança de Segurança da Informação**: como criar oportunidades para seu negócio. Rio de Janeiro: Brasport, 2014.

MARCIANO, José L. P. **Segurança da Informação** – uma abordagem social. Brasília, 2006. 211f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MARKUS, M. Lynne. Power, politics, and MIS implementation. **Communications of the ACM**, v.26, n.6, p.430-444, 1983.

MARTIN, Andrew P.; KHAZANCHI, Deepak. Information availability and Security Policy. In: AMERICAS CONFERENCE ON INFORMATION SYSTEMS, 12., 2006. Acapulco. **Proceedings…** Atlanta: AIS, 2006.

MARTINS, Alaíde B.; SANTOS, Celso A. S. Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **Journal of Information Systems and Technology Management**, v.2, n.2, p.121-136, 2005.

MAYNARD, Sean B.; RUIGHAVER, Anthonie B. What makes a good information security policy: a preliminary framework for evaluating security policy quality. In: ANNUAL SECURITY CONFERENCE, 5., 2006. Las Vegas. **Proceedings...** Las Vegas: Information Institute, 2006.

MCKAY, Ruth B. Organizational responses to an environmental bill of rights. **Organization Studies**, v.22, n.4, p.625-568, 2001.

MECHANIC, David. Sources of power of lower participants in complex organizations. **Administrative Science Quarterly**, v.7, n.3, p.349-364, 1962.

MELLO, Luiz B. B.; VASCONCELLOS, Lais A.; BRAGANÇA, Lívia R.; MOTTA, Otávio M. Contribuição para gestão de ativos intangíveis organizacionais: proposição de um modelo baseado no Balenced Scorecard. In: CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO, 6., 2010. Niterói. **Anais...** Niterói: CNEG, 2010.

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

MIGNERAT, Muriel; RIVARD, Suzanne. Positioning the institutional perspective in information technology research. **Journal of Information Technology**, v.24, n.4, p.369-391, 2009.

MILES, Raymond E.; SNOW, Charles C. **Organizational strategy, structure, and process**. New York: McGraw-Hill, 1978.

MITNICK, Kevin D.; SIMON, William L. **Mitnick – A arte de enganar** - Ataques de hackers: controlando o fator humano na Segurança da Informação. São Paulo: Makron Books, 2003.

MOORE, Gary C.; BENBASAT, Izak. Development of an instrument to measure the perceptions of adopting an Information Technology innovation. **Information Systems Research**, v.2, n.3, p.192-222, 1991.

MOREIRA, Herivelto; CALEFFE, Luiz G. **Metodologia da pesquisa para professor pesquisador**. Rio de Janeiro: Lamparina, 2ª ed., 2008.

MOREIRA, Nilton S. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books , 2001.

NAIDOO, Pravine. **Isomorphism, institutional entrepreneurship and Total Quality Management**: a case study in the implementation of Quality Management standards and

excellence models in South African developmental local government. Grahamstown, 2010. 1060f. Tese (Doutorado em Administração de Empresas) – Rhodes University, Grahamstown, 2010.

NAKAMURA, Emilio T. **Um modelo de Segurança de Redes para ambientes cooperativos**. Campinas, 2000. 281f. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Campinas, Campinas, 2000.

NASUTION, Muhamad F. F. A. **Institutionalization of Information Security**: case of the Indonesian banking sector. Richmond, 2012. 303f. Tese (Doutorado) – Virginia Commonwealth University, Richmond, 2012.

NETLAND, Torbjørn H.; ASPELUND, Arild. Multi-plant improvement programmes: a literature review and research agenda. **Journal of Operations & Production Management**, v.34, n.3, p.390-418, 2014.

NOBRE, Anna Cláudia S.; RAMOS, Anatália S. M.; NASCIMENTO, Thiago C. Adoção de práticas de Gestão de Segurança da Informação: um estudo com gestores públicos. **Reuna**, v.16, n.4, p.95-113, 2011.

OLIVER, Christine. Strategic responses to institutional processes. **Academy of Management Review**, v.16, n.1, p.145-179, 1991.

_____. The antecedents of deinstitutionalization. **Organization Studies**, v.13, n.4, p.563-588, 1992.

ORTON, J. Douglas; WEICK, Karl E. Loosely coupled systems: a reconceptualization. **Academy of Management Review**, v.15, n.2, p.203–223, 1990.

OSBORNE, Mark; SUMMITT, Paul M. **How to cheat at managing information security**. Rockland: Syngress, 2006.

OSMUNDSEN, Tonje C. **Becoming global** – the troublesome integration process. Trondheim, 2005. 257f. Tese (Doutorado em Administração) – Norwegian University of Science and Technology, Trondheim, 2005.

OZKAN, Sevgi; KARABACAK, Bilge. Collaborative risk method for information security management practices: a case context within Turkey. **International Journal of Information Management**, v.30, n.6, p.567-572, 2010.

PACHE, Anne-Claire; SANTOS, Filipe. When worlds colide: the internal dynamics of organizational responses to conflicting institutional demands. **Academy of Management Review**, v.35, n.3, p.455-476, 2010.

PANKO, Raymond R. Digital signatures and electronic signatures. In: BIDGOLI, Hossein (Org.). **Handbook of Information Security**: threats, vulnerabilities, prevention, detection, and management. New Jersey: John Wiley & Sons, vol.3, 2006, p.562-570.

PAPADIMITRIOU, Antigoni; WESTERHEIJDEN, Don F. Adoption of ISO-oriented quality management system in Greek universities: reactions to isomorphic pressures. **The TQM Journal**, v.22, n.3, p.229-241, 2010.

PARK, Cheol-Soon; JANG, Sang-Soo; PARK, Youg-Tae. A study of effect of Information Security Management System [ISMS] certification on organization performance. **International Journal of Computer Science and Network Security**, v.10, n.3, p.10-21, 2010.

PARKS, Rachida F. **A study of organizational responses to information privacy threats in the healthcare context**. Tese (Doutorado em Ciências e Tecnologias da Informação) – Pennsylvania State University, Centre County, 2012.

_____; CHU, Chao-Hsien; XU, Heng; ADAMS, Lascelles. Understanding the drivers and outcomes of healthcare organizational privacy responses. In: INTERNATIONAL CONFERENCE ON INFORMATIION SYSTEMS, 32., 2011. Shanghai. **Proceedings…** Atlanta: AIS, 2011.

_____; WIGAND, Rolf T. Organizational privacy strategy: four quadrants of strategic responses to information privacy and security threats. **Journal of Information Privacy and Security**, v.10, n.4, p.203-224, 2014.

PATRICK, Walter F. **Creating an information systems security policy**. Bethesda: SANS Institute, 2001.

PAVLOU, Paul A. State of the information privacy literature: where are we now and where should we go. **MIS Quarterly**, v.35, n.4, p.977–988, 2011.

PECI, Alketa. A Nova Teoria Institucional em Estudos Organizacionais: uma abordagem critica. **Cadernos EBAPE.BR**, v.4, n.1, 2006.

PELTIER, Thomas R. **Information security risk analysis**. Boca Raton: Auerbach Publications, 2005.

PERKEL, Jeffrey. Cybersecurity: how safe are your data? **Nature**, v.464, p.1260-1261, 2010.

PERROW, Charles B. **Complex organizations**: a critical essay. New York: McGraw-Hill, 3ª ed., 1993.

PFEFFER, Jeffrey. Co-optation and the composition of electric utility boards of directors. **Pacific Sociological Review**, v.17, n.3, p.333-363, 1974.

_____; SALANCIK, Gerald R. **The external control of organizations**: a resource dependence perspective. New York: Harper & Row, 1978.

PILATO, Viviana; PEDRINI, Matteo. The Institutional Triality of MNE's subsidiaries CSR strategy: the role of institutional pressures, legitimacy and autonomy in home versus host country contexts. In: CONVEGNO NAZIONALE ACADEMIA ITALIANA DI ECONOMIA AZIENDALE, 37., 2015. Pacienza. **Proceedings…** Bologna: AIDEA, 2015.

PINHEIRO, Joziane; ZEITOUNE, Regina C. G. Hepatite B: conhecimento e medidas de biossegurança e a saúde do trabalhador de enfermagem. **Revista de Enfermagem**, v.12, n.2, p.258-264, 2008.

POSEY, Clay; ROBERTS, Tom L.; LOWRY, Paul B.; HIGHTOWER, Ross T. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. **Information & Management**, v.51, n.5, p.551-567, 2014.

POSTHUMUS, Shaun; VON SOLMS, Rossouw. A framework for the governance of information security. **Computers & Security**, v.23, n.8, p.638-646, 2004.

POWELL, Walter W. Institutional effects on organizational structure and performance. In: ZUCKER, Lynn G. (Ed.). **Institutional patterns and organizations**: culture and environment. Cambridge: Ballinger, 1988, p.115-136.

POWER, Michael. The audit society – second thoughts. **International Journal of Auditing**, v.4, n.1, p.111-119, 2000.

PRESSMAN, Jeffrey L.; WILDAVSKY, Aaron. **Implementation**: how great expectations in Washington are dashed in Oakland. Berkeley: University of California Press, 1984.

PUHAKAINEN, Petri. **A design theory for information security awareness**. Oulu, 2006. 156f. Tese (Doutorado em Ciência de Processamento da Informação) – University of Oulu, Oulu, 2006.

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

QURESHI, Muhammad S. **Measuring efficacy of Information Security policies**: a case study of UAE based company. Estocolmo, 2011. 48f. Dissertação (Mestrado em Segurança em Sistemas de Informação e Comunicações) – Stockholm University, Estocolmo, 2011.

RYAN, Julie J. C. H.; MAZZUCHI, Thomas A.; RYAN, Daniel J.; DE LA CRUZ, Juliana L.; COOKE, Roger. Quantifying information security risks using expert judgment elicitation. **Computers & Operations Research**, v.39, n.4, p.774–784, 2012.

_____; RYAN, Daniel J. Expected benefits of information security investments. **Computers & Security**, v.25, n.8, p.579-588, 2006.

SÁ, Virgínio. A influência do ambiente institucional sobre a estrutura das organizações educativas: entre a aquiescência e a manipulação. In: CONGRESSO PORTUGUÊS DE SOCIOLOGIA, 5., 2004. Braga. **Anais…** Lisboa: APS, 2004.

SÁ-SOARES, Filipe. **Interpretação da segurança de sistemas de informação segundo a Teoria da Acção**. Braga, 2005. Tese (Doutorado em Tecnologias e Sistemas de Informação) – Universidade do Minho, Braga, 2005.

SALEH, Mohamed S.; ALFANTOOKH, Abdulkader. A new comprehensive framework for enterprise Information Security risk management. **Applied Computing and Informatics**, v.9, n.2, p.107–118, 2011.

SALTZER, Jerome H.; SCHROEDER, Michael D. The protection of information in Computer Systems. **Communications of the ACM**, v.17, n.7, p. 388-402, 1974.

SCHAEFER, Robert. The epistemology of Computer Security. **ACM SIGSOFT Software Engineering Notes**, v.34, n.6, p. 8-10, 2009.

SCOTT, W. Richard. Health care organizations in the 1980s: the convergence of public and professional control systems. In: MEYER, John W.; SCOTT, W. Richard (Orgs.). **Organizational environments**: ritual and rationality. Beverly Hills: SAGE, 1983, p.99-113.

_____. **Organizations: rational, natural, and open systems**. New Jersey: Prentice-Hall, 3ª ed., 1992.

_____. Institutional Theory: contributing to a theoretical research program. In: SMITH, Ken G.; HITT, Michael A. (Orgs.). **Great minds in management**: the process of theory development. Oxford: Oxford University Press, 2005, p.460-484.

_____. **Institutions and organizations**: ideas and interests. 3ª ed., Los Angeles: SAGE, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva. Rio de Janeiro: Campus, 2ª ed., 2014.

SENTHILKUMAR, P.; ARUMUGAM, S. Policy verification, validation and troubleshooting in distributed firewalls. **International Journal of Computer Science and Information Security**, v.9, n.10, p.135-137, 2011.

SHAFIU, Ibrahim. **Information Security compliance behavior in supply chain security**. Auckland, 2015. 249f. Tese (Doutorado em Administração de Empresas) – Auckland University of Technology, Auckland, 2015.

SHAW, R. S.; CHEN, Charlie C.; HARRIS, Albert L. The impact of information richness on information security awareness training effectiveness. **Computers & Education**, v.52, n.1, p.92-100, 2009.

SHEENAN, Kim B.; HOY, Mariea G. Dimensions of privacy concern among online consumers. **Journal of Public Policy & Marketing**, v.19, n.1, p.62-73, 2000.

SILIC, Mario; BACK, Andrea. Information Security: critical review and future directions for research. **Information Management & Computer Security**, v.22, n.3, p.279-308, 2014.

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

SILVA, Edna L.; MENEZES, Estera M. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: Laboratório de Ensino à Distância da UFSC, 3ed., 2001.

SILVA NETTO, Abner; SILVEIRA, Marco A. P. Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Journal of Information Systems and Technology Management**, v.4, n.3, p.375-397, 2007.

SCHMITTLING, Ron; MUNNS, Anthony. Performing a security risk assessment. **ISACA Journal**, v.1, 2010.

SCHULTZ, E. Eugene; PROCTOR, Robert W.; LIEN, Mei-Ching.; SALVENDY, Gavriel. Usability and security – an appraisal of usability issues in information security methods. **Computers & Security**, v.20, n.7, p.620-634, 2001.

SMITH, H. Jeff; DINEV, Tamara; XU, Heng. Information privacy research: an interdisciplinary review. **MIS Quarterly**, v.35, n.4, p.989–1016, 2011.

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

STANDING, Craig; SIMS, Ian; LOVE, Peter. IT non-conformity in institutional environments: e-marketplace adoption in the government sector. **Information & Management**, v.46, n.2, p.138-149, 2009.

STERGIOU, Theodoros; LEESON, Mark S.; GREEN, Roger J. An alternative architectural framework to the OSI security model. **Computers & Security**, v.23, n.2, p.137-153, 2004.

STERNE, Daniel F. On the buzzword 'security policy'. In: IEEE COMPUTER SOCIETY SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, 2., 1991. Oakland. **Proceedings...** Oakland: IEEE, 1991.

SUCHMAN, Mark C. Managing legitimacy: strategic and institutional approaches. **Academy of Management Review**, v.20, n.3, p.571-610, 1995.

SUN, Jun; AHLUWALIA, Punit; KOONG, Kai S. The more secure the better? A study of information security readiness. **Industrial Management & Data Systems**, v.111, n.4, p.570-588, 2011.

SVEEN, Finn O.; TORRES, Jose M.; SARRIEGI, Jose M. Blind information security strategy. **International Journal of Critical Infrastructure Protection**, v.2, n.3, p.95-105, 2009.

TAMJIDYAMCHOLO, Alireza; BABA, Mohd S. B.; SHUIB, Nor L. M.; ROHANI, Vala A. Evaluation model for knowledge sharing in information security professional virtual community. **Computers & Security**, v.43, p.19-34, 2014.

TEJAY, Gurvirender P. S.; BARTON, Kevin A. Information System Security commitment: a pilot study of external influences on senior management. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 46., 2013, Maui. **Proceedings...** Manoa, 2013.

TEMPEL, Anne; EDWARDS, Tony; FERNER, Anthony; MULLER-CAMEN, Michael; WÄCHTER, Hartmut. Subsidiary responses to institutional duality: collective representation practices of US multinationals in Britain and Germany. **Human Relations**, v.59, n.11, p.1543-1570, 2006.

TEO, Hock H.; WEI, Kwok K.; BENBASAT, Izak. Predicting intention to adopt interorganizational linkages: an institutional perspective. **MIS Quarterly**, v.27, n.1, p.19-49, 2003.

THONG, James Y. L. An integrated model of Information Systems adoption in small businesses. **Journal of Management Information Systems**, v.15, n.4 p.187-214, 1999.

_____; YAP, Chee S. CEO characteristics, organizational characteristics and information technology adoption in small businesses. **Omega**, v.23, n.4, p.429-442, 1995.

THORPE, Stephen W. Extranets: applications, development, security, and privacy. In: BIDGOLI, Hossein (Org.). **Handbook of Information Security**: threats, vulnerabilities, prevention, detection, and management. New Jersey: John Wiley & Sons, vol.1, 2006, p.215-225.

TOLBERT, Pamela S.; ZUCKER, Lynne G. Institutional sources of change in the formal structure of organizations: the diffusion of Civil Service Reform, 1880-1935. **Administrative Science Quarterly**, v.28, n.1, p.22-39, 1983.

_____; _____. A institucionalização da Teoria Institucional. In: CLEGG, Stewart R.; HARDY, Cynthia; NORD, Walter R. (Orgs.). **Handbook de estudos organizacionais**. São Paulo: Atlas, 1999, vol. 1, p.196-219.

TRIBUNAL DE CONTAS DA UNIÃO. **Levantamento de Governança de TI 2010** – Resultado retornado para a instituição respondente: Fundação Oswaldo Cruz. Brasília: TCU, 2010. Disponível em: <https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/relatorio_de_levantamento_de_governanca_de_ti_2010.pdf>. Acesso em: 07 out. 2016.

_____. **Levantamento de Governança de TI 2012** – Resultado retornado para a instituição respondente: Fundação Oswaldo Cruz. Brasília: TCU, 2012. Disponível em: <https://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/relatorio_sobre_levantamento_de_governanca_de_ti_2012.pdf>. Acesso em: 07 out. 2016.

_____. **Levantamento de Governança de TI 2014** – Resultado individual: Fundação Oswaldo Cruz. Brasília: TCU, 2014. Disponível em: <http://portal.fiocruz.br/sites/portal.fiocruz.br/files/documentos/relatorio_de_analise_-_2014_-_2012.pdf>. Acesso em: 07 out. 2016.

TSAI, S.-H. Terence; CHILD, John. Strategic responses of multinational corporations to environmental demands. **Journal of General Management**, v.23, n.1, p.1-22, 1997.

TURNER, Patrick; GOTZE, John; BERNUS, Peter. Architecting the firm – coherency and consistency in managing the enterprise. In: BERNUS, Peter; DOUMEINGTS, Guy; FOX, Mark (Orgs.). **Enterprise architecture, integration and interoperability**. Berlin: Springer, 2010, p.1-10.

ULVIN, Kim. **The ISO 9001:2000 standard**: legitimization, fashion or actual quality improvement? Oslo, 2007. 62f. Dissertação (Mestrado em Gestão de Saúde) – Universitetet I Oslo, Oslo, 2007.

VASCONCELOS, Isabella F. G.; VASCONCELOS, Flávio C. ISO 9000, consultants and paradoxes: a sociological analysis of Quality Assurance and Human Resource techniques. **Revista de Administração Contemporânea**, v.7, n.1, p.173-194, 2003.

VON SIMSON, Ernest M. The 'centrally decentralized' IS organization. **Harvard Business Review**, v.68, n.4, p.158-162, 1990.

VOXTED, Søren; LIND, Jens. New principles of management in modern organizations. In: INTERNATIONAL INDUSTRIAL RELATIONS ASSOCIATION EUROPEAN CONGRESS, 9., 2010. Copenhagen. **Proceedings…** Geneva: ILO, 2010.

WAHYUDI, Imam. **Symbolism, rationality and myth in organizational control systems**: an ethnographic case study of PBS Jakarta Indonesia. Wollongong, 2004. 365f. Tese (Doutorado em Administração) – University of Wollongong, Wollongong, 2004.

WAWRZYNIAK, Dariusz. Information security risk assessment model for risk management. In: FISCHER-HÜBNER, Simone; FURNELL, Stevel; LAMBRINOUDAKIS, Costas (Orgs.). **Trust and Privacy in Digital Business**. Berlin: Springer, 2006, p.21-30.

WEERAKKODY, Vishanth; DWIVEDI, Yogesh K.; IRANI, Zahir. The diffusion and use of Institutional Theory: a cross-disciplinary longitudinal literature survey. **Journal of Information Technology**, v.24, p.354–368, 2009.

WEICK, Karl E. Educational institutions as loosely coupled systems. **Administrative Science Quarterly**, v.21, n.1, p.1–19, 1976.

WESTPHAL, James D.; ZAJAC, Edward J. Decoupling policy from practice: the case of stock repurchase programs. **Administrative Science Quarterly**, v.46, n.2, p.202-228, 2001.

WHITMAN, Michael E. Enemy at the gate: threats to Information Security. **Communications of the ACM**, v.46, n.8, p.91-95, 2003.

WILLIAMS, Paul. Information Security Governance. **Information Security Technical Report**, v.6, n.3, p. 60-70, 2001.

WILLIAMS, Susan P.; HARDY, Catherine A.; HOLGATE, Janine A. Information Security Governance practices in critical infrastructure organizations: a socio-technical and institutional logic perspective. **Electronic Markets**, v.23, n.4, p.341-354, 2013.

WILLSON, Phyl; POLLARD, Carol. Exploring IT Governance in theory and practice in a large multi-national organisation in Australia. **Information Systems Management**, v.26, n.2, p.98-109, 2009.

WILSON, Piers. Positive perspectives on cloud security. **Information Security Technical Report**, n.16, p. 97-101, 2011.

WINKLER, Ira S.; DEALY, Brian. Information security technology?... Don't rely on it – a case study in social engineering. In: USENIX UNIX SECURITY SYMPOSIUM, 5., 1995. Salt Lake City. **Proceedings...** Berkeley: USENIX, 1995.

WOOD, Charles C. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. **Computer Fraud & Security**, v.2004, n.1, p.16-17, 2004.

WOOD JR., Thomaz; CALDAS, Miguel P. Importação de tecnologia gerencial no Brasil: o divórcio entre substância e imagem. In: ENCONTRO DA ASSOCIAÇÃO NACIONAL DE PÓS-GRADUAÇÃO E PESQUISA EM ADMINISTRAÇÃO, 21., 1997. Rio das Pedras. **Anais…** Rio de Janeiro: ANPAD, 1997.

WORKMAN, Michael. Gaining access with Social Engineering: an empirical study of the threat. **Information Systems Security Journal**, v.16, n.6, p.315–331, 2007.

_____; BOMMER, William H.; STRAUB, Detmar W. Security lapses and the omission of information security measures: a threat control model and empirical test. **Computers in Human Behavior**, v.24, n.6, p.2799-2816, 2008.

WRIGHT, Barry. Quiescent Leviathan? Citizenship and national security measures in late modernity. **Journal of Law and Society**, v.25, n.2, p.213–236, 1998.

WU, Yu A.; SAUNDERS, Carol. Governing information security: governance domains and decision rights allocation patterns. **Information Resources Management Journal**, v.24, n.1 p.28-45, 2011.

XU, Heng; DINEV, Tamara; SMITH, H. Jeff; HART, Paul. Examining the formation of individual's privacy concerns: toward an integrative view. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS, 29., 2008. Paris. **Proceedings...** Atlanta: AIS, 2008.

YEH, Quey-Jen; CHANG, Arthur Jung-Ting. Threats and countermeasures for information system security: a cross-industry study. **Information & Management**, v.44, n.5, p.480-491, 2007.

YIN, Robert K. **Estudo de Caso:** planejamento e métodos. Porto Alegre: Bookman, 4ª ed., 2010.

APÊNDICE A

PROTOCOLO DE ESTUDO DE CASO

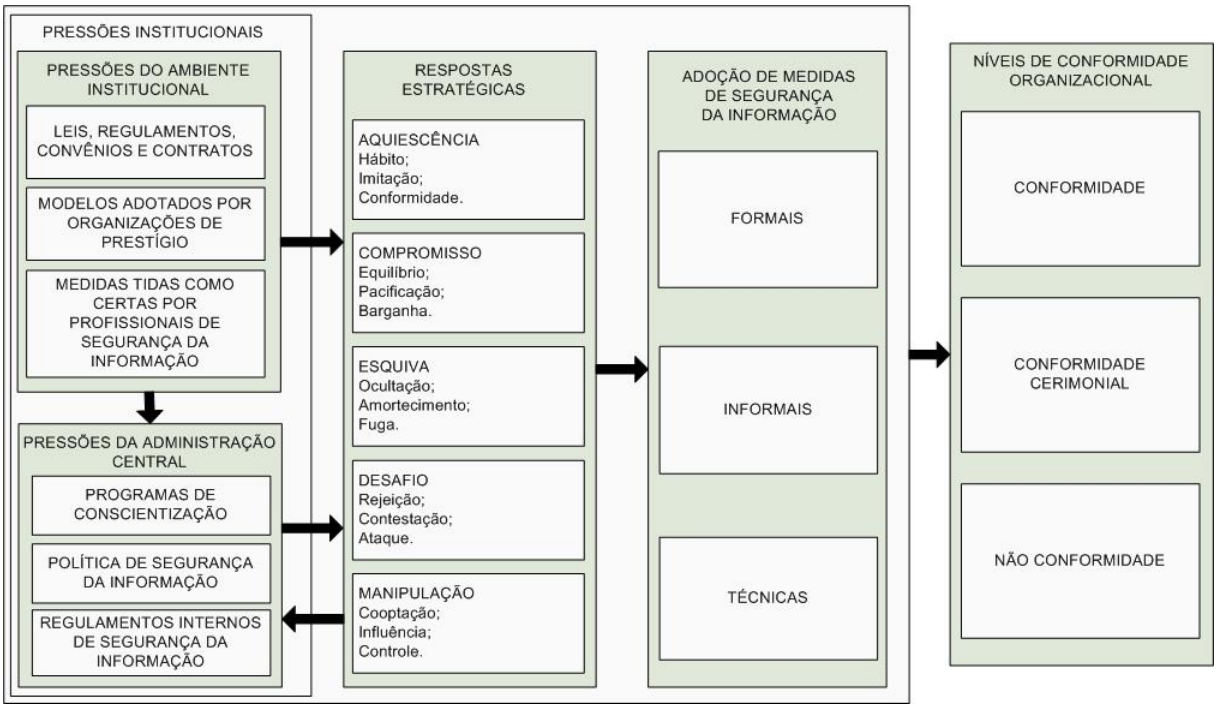
1 ASPECTOS GERAIS

1.1 Objetivo Geral: Explicar como as respostas estratégicas das subunidades organizacionais às pressões externas influenciam a conformidade da organização com os requisitos externos de Segurança da Informação.

1.2 Questão de pesquisa:

Como as respostas estratégicas das subunidades às pressões que sofrem influenciam a conformidade da organização com os requisitos externos de Segurança da Informação?

1.3 *Framework* de pesquisa:



1.4 Construtos e indicadores da pesquisa:

CONSTRUTOS		INDICADORES	AUTORES DE REFERÊNCIA
Pressões Institucionais		Programas de conscientização, regulamentos e Política de Segurança da Informação formalizados na organização	Ellwanger (2009), Eminagaoglu, Uçar e Eren (2009), Shaw, Chen e Harris (2009), Bulgurcu, Cavusoglu e Benbasat (2010), Alkalbani, Deng e Kam (2015)
Resposta Estratégica de Aquiescência	Hábito	Adoção inconsciente de medidas tidas como certas pelas subunidades, independentemente de terem sido adotadas por outras organizações ou subunidades	Chou, Liu e Hammitt (2004), Standing, Sims e Love (2009), Turner, Gotze e Bernus (2010), Parks e Wigand (2014)
	Imitação	Cópia inconsciente ou consciente pelas subunidades das medidas adotadas por outras organizações ou subunidades	Standing, Sims e Love (2009), Hsu, Lee e Straub (2012), Tejay e Barton (2013), Parks e Wigand (2014), Albuquerque Junior e Santos (2015), Albuquerque Junior *et al*. (2016)
	Conformidade	Adoção consciente pelas subunidades das medidas exigidas visando à obtenção benefícios decorrentes da conformidade	Posthumus e Von Solms (2004), Ryan e Ryan (2006), Standing, Sims e Love (2009), Perkel (2010), Parks e Wigand (2014)
Resposta Estratégica de Compromisso	Equilíbrio	Adoção pelas subunidades de medidas conflitantes com outras medidas ou com seus objetivos e atividades realizando ajustes na implementação para que não haja descumprimento	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Sun, Ahluwalia e Koong (2011), Abraham e Chengalur-Smith (2011), Parks e Wigand (2014)
	Pacificação	Adoção pelas subunidades de parte das medidas exigidas e rejeição de outras consideradas conflitantes entre si ou com seus objetivos e atividades	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Sun, Ahluwalia e Koong (2011), Parks e Wigand (2014)
	Barganha	Negociações entre as subunidades e as fontes de pressão visando à alteração do quando ou o quanto as medidas devem ser adotadas	Karyda, Kiountouzis e Kokolakis (2005), Ellwanger (2009), Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Esquiva	Ocultação	Implantação de tecnologias pelas subunidades sem realizar as configurações e ações necessárias ou previstas nos regulamentos e na Política de Segurança da Informação da organização; criação de políticas e regulamentos nas subunidades sem que haja cobrança quanto ao seu cumprimento	Björck (2004), Standing, Sims e Love (2009), Parks e Wigand (2014), Lopes e Sá-Soares (2014), Lapke e Dhillon (2015)
	Amortecimento	Ações da subunidade com o objetivo de esconder das fontes	Dhillon (2001), Hasan e Yurcik (2006), Standing, Sims e Love

		de pressão o nível real de conformidade e a ocorrência de incidentes	(2009), Aier e Weiss (2012), Adebayo, Omotosho e Adekunle (2012), Parks e Wigand (2014)
	Fuga	Ações da subunidade para não participar de iniciativas que exijam a adoção de medidas de Segurança da Informação	Armênio Neto e Machado-da-Silva (2009), Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Desafio	Rejeição	Rejeição das medidas exigidas ou tidas como certas pela administração central e outras organizações	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Contestação	Ações da subunidade para desafiar as pressões através de críticas à sua eficiência ou rigor	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Ataque	Ataques deferidos pela subunidade às fontes de pressão ou às próprias pressões por considerá-las ineficientes ou rigorosas demais	Standing, Sims e Love (2009), Parks e Wigand (2014)
Resposta Estratégica de Manipulação	Cooptação	Tentativas de fazer com que membros do Comitê ou do Escritório de Segurança da Informação da administração central ou membros de outras fontes de pressão participem das decisões sobre Segurança da Informação da subunidade para neutralizar as pressões sofridas	Standing, Sims e Love (2009), Parks e Wigand (2014)
	Influência	Utilização pela subunidade de prestígio para influenciar a administração central ou outras fontes de pressão para mudarem requisitos de Segurança da Informação	Delmas e Toffel (2008), Standing, Sims e Love (2009), Parks e Wigand (2014), Hernes e Erdvik (2014)
	Controle	Utilização pela subunidade de poder sobre a administração central ou outras fontes de pressão para que exijam a adoção de medidas que a beneficiem	Tempel *et al*. (2006), Standing, Sims e Love (2009), Parks e Wigand (2014)
Adoção de Medidas de Segurança da Informação		Medidas técnicas, formais e informais adotadas pelas subunidades	Farn, Lin e Fung (2004), Björck (2005), Casey (2005), Martins e Santos (2005), Belasco e Wan (2006), Juels (2006), Doherty e Fulford (2006), Thorpe (2006), Panko (2006), Park, Jang e Park (2010), Gorayeb (2012), Manoel (2014), Sêmola (2014)
Níveis de Conformidade Organizacional		Tratamentos distintos às pressões para adoção de medidas formais, informais e técnicas nas subunidades; adoção pelas subunidades de medidas formais, informais e técnicas contrárias aos objetivos e interesses da	Björck (2004), Sá (2004), Wahyudi (2004), Boschman (2006), Armênio Neto e Machado-da-Silva (2009), Standing, Sims e Love (2009), Aguilera-Caracuel *et al*. (2012), Aier e Weiss (2012), Lopes e Sá-Soares (2014), Netland e

	administração central; ocorrência de respostas de conformidade e não conformidade pelas subunidades; ocorrência de alterações em regulamentos e na Política de Segurança da Informação devido a ações promovidas pelas subunidades para atender aos seus interesses; discurso de conformidade da administração central	Aspelund (2014), Hernes e Erdvik (2014), Lapke e Dhillon (2015), Pilato e Pedrini (2015)

1.5 Proposições da pesquisa:

PROPOSIÇÃO	CONTEÚDO
Proposição 1	As subunidades organizacionais respondem às pressões institucionais através de diferentes estratégias e atendendo aos seus próprios interesses e julgamentos sobre a eficiência e adequação das medidas de Segurança da Informação
Proposição 2	Pressões para adoção de medidas formais, medidas informais e medidas técnicas vão resultar em diferentes respostas estratégicas por parte das subunidades organizacionais
Proposição 3	As respostas das subunidades às pressões que sofrem influenciam no nível de conformidade da organização com os requisitos de Segurança da Informação do ambiente institucional

1.6 Fontes de informação:

Entrevistas semiestruturadas: gestor de Segurança da Informação da organização, membros do Comitê de Segurança da Informação e responsáveis pela TI e Segurança da Informação nas subunidades organizacionais.

Documentos: organogramas da organização e das subunidades organizacionais, Política de Segurança da Informação, normas complementares, regulamentos e orientações de Segurança da Informação, Sistema de Gestão de Segurança da Informação, Plano Diretor de TI, portarias que instituem o Comitê de Segurança da Informação e subcomitês das subunidades, relatórios de auditorias realizadas nas subunidades e na organização, relatórios de gestão da organização.

1.7 Critérios para seleção da organização:

Comitê de Segurança da Informação formalizado;

Política de Segurança da Informação formalizada

Sistema de Gestão de Segurança da Informação documentado;

Escritório de Segurança da Informação;

Equipe de tratamento de incidentes de Segurança da Informação;

Regulamentos internos de Segurança da Informação.

1.8 Procedimentos para realização das entrevistas:

Identificar e entrar em contato com os informantes;

Marcar entrevistas com os informantes;

Alinhar expectativas da entrevista com os informantes;

Alinhar tecnologia para realização das entrevistas (gravador, Skype e Facetime).

1.9 Procedimentos de análise dos dados:

Transcrever gravações das entrevistas;

Ler as transcrições e fazer anonimização;

Importar transcrições e documentos para o *software* QSR NVivo 10;

Criar hierarquia de nós e subnós no NVivo;

Categorizar trechos das entrevistas e documentos nos nós e subnós do NVivo com base nos indicadores da pesquisa;

Identificar novas categorias de análise a partir dos dados;

Analisar o resultado da categorização;

Confrontar resultados das entrevistas com dados dos documentos.

1.10 Hierarquia preliminar de *nodes* e *subnodes* para análise dos dados no *software* QSR NVivo:

NÓS	SUBNÓS
Pressões institucionais	Programas de conscientização
	Regulamentos de Segurança da Informação
	Política de Segurança da Informação
Aquiescência	Hábito
	Imitação
	Conformidade
Compromisso	Equilíbrio
	Pacificação
	Barganha
Esquiva	Ocultação
	Amortecimento
	Fuga
Desafio	Rejeição
	Contestação
	Ataque
Manipulação	Cooptação
	Influência
	Controle
Adoção de medidas de Segurança da Informação	Medidas técnicas adotadas
	Medidas formais adotadas
	Medidas informais adotadas
Níveis de conformidade	Ocorrência de respostas distintas
	Tratamentos distintos às pressões para medidas técnicas, formais e informais
	Adoção de medidas contrárias aos objetivos e interesses da sede
	Ocorrência de alterações em regulamentos e na Política de Segurança
	Ocorrência de respostas de conformidade

2 – ROTEIRO DE ENTREVISTA SEMI-ESTRUTURADA – SUBUNIDADES

INTRODUÇÃO

O objetivo desta pesquisa é compreender como as respostas estratégicas das subunidades organizacionais influenciam a Segurança da Informação da sua organização. Os procedimentos aplicados nesta pesquisa não visam à identificação dos entrevistados nem das subunidades organizacionais nas quais trabalham e não se pretende utilizar qualquer informação que possibilite essa identificação. A entrevista será gravada e transcrita literalmente e os resultados das transcrições serão enviados para os respectivos entrevistados para confirmação e validação das respostas. O entrevistado poderá desistir ou interromper a entrevista a qualquer momento bem como não responder a qualquer uma das perguntas. Caso não queira mais participar da pesquisa, o entrevistado pode entrar em contato com o pesquisador a qualquer momento e solicitar a devolução dos dados ou mesmo sua destruição. A **Parte 1** trata da caracterização do entrevistado e da subunidade da organização em que trabalha. A **Parte 2** visa identificar as medidas de Segurança da Informação adotadas pela sua subunidade, sem entrar em detalhes quanto às tecnologias utilizadas. E a **Parte 3** tem perguntas mais específicas sobre o comportamento da subunidade quanto à adoção de medidas de Segurança da Informação.

PARTE 1

Características gerais do entrevistado

Qual é o seu cargo dentro da carreira da organização? _____

Entre funções mais técnicas ou de chefia, que tenham gratificação ou cargo comissionado, que função você exerce na organização? _____

Há quanto tempo você está na organização? _____

Qual é a sua formação, incluindo pós-graduação, se houver? _____

Características gerais da unidade descentralizada

Quantos usuários de TI tem sua subunidade, aproximadamente? _____

Como está posicionada a área de TI na estrutura organizacional da subunidade?

_____

_____

Quantas pessoas trabalham exclusivamente com Segurança da Informação na subunidade?

_____

Quantas pessoas trabalham conciliando Segurança da Informação com outras atividades?

_____

PARTE 2

Considere que medidas formais de Segurança da Informação são aquelas administrativas, que têm o objetivo de mudar o comportamento das pessoas e da organização através de regras e estruturas organizacionais.

Quais são as Medidas Formais/Administrativas relativas a Segurança da Informação adotadas pela sua subunidade?

(Medidas a serem identificadas na resposta: Política de Segurança da Informação formal, Comitê ou Subcomitê de Segurança da Informação formalmente instituído na subunidade, regulamentos ou normas internas de Segurança da Informação formalizados na unidade, processos e procedimentos internos de Segurança da Informação da unidade documentados, equipe própria de tratamento de incidentes de Segurança da Informação, escritório de Segurança da Informação formalmente instituído na subunidade, processo documentado de análise e avaliação de riscos de Segurança da Informação, processo documentado de classificação das informações da subunidade, Sistema de Gestão de Segurança da Informação formalizado na subunidade, processo documentado de revisão da Política de Segurança da Informação da subunidade).

As medidas informais de Segurança da Informação são aquelas que têm o objetivo de mudar o comportamento das pessoas e da organização através da conscientização.

Quais são as Medidas Informais relativas a Segurança da Informação adotadas pela sua subunidade?

(Medidas a serem identificadas na resposta: programas ou ações de treinamento de profissionais de TI em Segurança da Informação realizados na subunidade, programas ou ações de treinamento de usuários de TI em Segurança da Informação realizados na subunidade, campanhas ou ações de divulgação de regulamentos de Segurança da Informação da subunidade, campanhas ou ações de divulgação da Política de Segurança da Informação da subunidade, campanhas ou ações de divulgação de regulamentos de Segurança da Informação da organização, campanhas ou ações de divulgação da Política de Segurança da Informação da organização, campanhas ou ações de conscientização de usuários e profissionais de TI sobre Segurança da Informação).

As medidas técnicas são as que afetam o funcionamento dos recursos tecnológicos, as que são implantadas nos recursos tecnológicos e que visam protegê-los, bem como aquelas que afetam o ambiente onde esses recursos e dispositivos funcionam.

Quais são as Medidas Técnicas relativas a Segurança da Informação adotadas pela sua subunidade?

(Medidas a serem identificadas na resposta: redundância de dados, como backup, espelhamento de dados e storage; segregação de redes de computadores, como firewall, proxy, switch de conteúdo; redundância de peças de equipamentos, como fontes, discos, RAID, processadores, memórias, placas, e outras partes redundantes; prevenção contra códigos maliciosos, como antivírus, anti-spam e filtro de conteúdo; controle de acesso lógico, como a definição de níveis de permissão a arquivos e sistemas e a funcionalidades e conteúdos; transmissão e armazenamento seguros de dados, como aquelas utilizando VPN ou criptografia em transmissão ou armazenamento de dados; autenticação forte utilização de senhas fortes, tokens, PINs, biometria ou smartcards para prover acesso a sistemas e equipamentos; redundância de equipamentos, como servidores redundantes, clusters, espelhamento de servidores e

sites backup; controle de acesso físico, como restrição de acesso a CPDs, datacenters, salas de equipamentos, equipamentos e servidores apenas para pessoal de TI e funcionários identificados e autorizados; proteção ambiental contra incêndio, inundação e fumaça, uso de no-breaks e geradores, uso de salas-cofre e cofres para armazenamento de dados e mídias).

PARTE 3

PRESSÕES DA ADMINISTRAÇÃO CENTRAL

P1 – Como sua subunidade é pressionada a adotar medidas de Segurança da Informação?
P2 – Que mudanças ocorreram na sua subunidade depois da publicação dos regulamentos e da Política de Segurança da Informação da organização?

RESPOSTA ESTRATÉGICA DE AQUIESCÊNCIA

A1 – Como a adoção de medidas de Segurança da Informação realizada por outras organizações ou subunidades influencia as decisões de sua subunidade?
A2 – Como você descreve a relação da sua subunidade com outras organizações, com sua sede ou com outras subunidades em termos de uso de sistemas e compartilhamento de dados?
A3 – Como a relação da sua subunidade com outras organizações, com a sede ou outras subunidades influencia na adoção de medidas de Segurança da Informação?
A4 – Em quais momentos sua subunidade adotou medidas de Segurança da Informação com relação à publicação de regulamentos ou da Política de Segurança da Informação?
A5 – Foram consultadas Políticas de outras organizações ou subunidades durante a elaboração da Política da sua subunidade?
A6 – O que levou sua subunidade a fazer essas consultas?
A7 – Quais benefícios a adoção de medidas de Segurança da Informação trouxe para sua subunidade?
A8 – De onde vêm esses benefícios?
A9 – Por quais motivos medidas de Segurança da Informação foram adotadas por sua subunidade?

RESPOSTA ESTRATÉGICA DE COMPROMISSO

C1 – Como você avalia a coerência das medidas de Segurança da Informação exigidas pela sede ou por outras organizações com as atividades de sua subunidade?
C2 – Como as medidas adotadas pela administração central da organização influenciam o desenvolvimento das atividades ou o alcance dos objetivos da sua subunidade?
C3 – Como a adoção de medidas de Segurança da Informação limita ou restringe as atividades desenvolvidas em sua subunidade?
C4 – Quais atividades sua subunidade deixa de executar por ter adotado medidas de Segurança da Informação?
C5 – Como você percebe a relação entre as medidas de Segurança da Informação exigidas e a disponibilidade dos recursos necessários para sua subunidade adotá-las? Considere recursos humanos, capital, infraestrutura e quaisquer outros recursos.

C6 – Como sua subunidade se comporta quando sofre pressões para adotar medidas que são contrárias às suas atividades ou contraditórias com outras medidas também exigidas?

RESPOSTA ESTRATÉGICA DE ESQUIVA

E1 – Quais medidas de Segurança da Informação foram adotadas na sua subunidade conforme os requisitos ou exigências externas ou da organização?
E2 – A adoção dessas medidas ocorreu em que momento com relação à existência desses requisitos e exigências?
E3 – O que acontece na subunidade quando há uma auditoria de Segurança da Informação?
E4 – Há algum movimento para melhorar a conformidade em função ou em decorrência da auditoria?
E5 – Como agem os envolvidos com a Segurança da Informação quando ocorre um incidente?
E6 – O que acontece quando sua subunidade é convidada a participar de um novo programa, projeto ou ação da administração central que exige a adoção de medidas de Segurança da Informação?

RESPOSTA ESTRATÉGICA DE DESAFIO

D1 – Como sua subunidade se posiciona perante a administração central ou outras organizações quando é pressionada a adotar medidas de Segurança da Informação ineficientes ou prejudiciais às suas atividades?

RESPOSTA ESTRATÉGICA DE MANIPULAÇÃO

M1 – Comente sobre a participação do Comitê de Segurança da Informação ou do Escritório de Segurança da Informação da organização nas decisões de Segurança da Informação da sua subunidade.
M2 – Quais vantagens a subunidade tem ou teria com a participação de pessoas da área de Segurança da Informação da sede em suas decisões?
M3 – Comente agora sobre a participação da subunidade nas decisões de Segurança da Informação da administração central, do governo ou de outras organizações que regulam a Segurança da Informação.
M4 – Como os membros da sua subunidade são orientados para participarem dessas decisões?
M5 – Você considera que a subunidade tem algum poder ou influência sobre sua sede, o governo ou outras organizações que regulamentam a Segurança da Informação?
M6 – Comente sobre a utilização pela sua subunidade do poder ou da influência que tem sobre a sede ou outras organizações quanto à criação, alteração ou extinção de regulamentos de Segurança da Informação.

ADOÇÃO DE MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

S1 – Quando há uma obrigação ou necessidade de adotar tecnologias de Segurança da Informação, como são tomadas as decisões em sua subunidade?
S2 – Quando há uma obrigação ou necessidade de adotar medidas formais de Segurança da Informação, como são tomadas as decisões em sua subunidade?
S3 – Quando há uma obrigação ou necessidade de adotar medidas informais de Segurança da Informação, como são tomadas as decisões em sua subunidade?

NÍVEIS DE CONFORMIDADE ORGANIZACIONAL

O1 – Houve mudanças em regulamentos e na Política de Segurança da Informação da organização decorrentes da adoção de medidas pela sua subunidade?
O2 – Quais foram as medidas adotadas que provocaram essas mudanças?
O3 – Quais foram as mudanças ocorridas nos regulamentos e na Política de Segurança da Informação?

3 – ROTEIRO DE ENTREVISTA SEMI-ESTRUTURADA – MEMBROS DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

INTRODUÇÃO

O objetivo desta pesquisa é compreender como as respostas estratégicas das subunidades organizacionais influenciam a Segurança da Informação da sua organização. Os procedimentos aplicados nesta pesquisa não visam à identificação dos entrevistados nem das subunidades organizacionais nas quais trabalham e não se pretende utilizar qualquer informação que possibilite essa identificação. A entrevista será gravada e transcrita literalmente e os resultados das transcrições serão enviados para os respectivos entrevistados para confirmação e validação das respostas. O entrevistado poderá desistir ou interromper a entrevista a qualquer momento bem como não responder a qualquer uma das perguntas. Caso não queira mais participar da pesquisa, o entrevistado pode entrar em contato com o pesquisador a qualquer momento e solicitar a devolução dos dados ou mesmo sua destruição. A **Parte 1** trata da caracterização do entrevistado e da subunidade da organização em que trabalha. A **Parte 2** visa identificar as medidas de Segurança da Informação adotadas pela sua subunidade, sem entrar em detalhes quanto às tecnologias utilizadas. E a **Parte 3** tem perguntas mais específicas sobre o comportamento da subunidade quanto à adoção de medidas de Segurança da Informação.

PARTE 1

Características gerais do entrevistado

Qual é o seu cargo dentro da carreira da organização? _____

Entre funções mais técnicas ou de chefia, que tenham gratificação ou cargo comissionado, que função você exerce na organização? _____

Há quanto tempo você está na organização? _____

Qual é a sua formação, incluindo pós-graduação, se houver? _____

PARTE 2

Considere que medidas formais de Segurança da Informação são aquelas administrativas, que têm o objetivo de mudar o comportamento das pessoas e da organização através de regras e estruturas organizacionais.

Quais são as Medidas Formais/Administrativas relativas a Segurança da Informação adotadas pela organização?

(Medidas a serem identificadas na resposta: Política de Segurança da Informação formal, Comitê ou Subcomitê de Segurança da Informação formalmente instituído na subunidade, regulamentos ou normas internas de Segurança da Informação formalizados na unidade, processos e procedimentos internos de Segurança da Informação da unidade documentados, equipe própria de tratamento de incidentes de Segurança da Informação, escritório de Segurança da Informação formalmente instituído na subunidade, processo documentado de análise e avaliação de riscos de Segurança da Informação, processo documentado de classificação das informações da subunidade, Sistema de Gestão de Segurança da Informação formalizado na subunidade, processo documentado de revisão da Política de Segurança da Informação da subunidade).

As medidas informais de Segurança da Informação são aquelas que têm o objetivo de mudar o comportamento das pessoas e da organização através da conscientização.

Quais são as Medidas Informais relativas a Segurança da Informação adotadas pela organização?

(Medidas a serem identificadas na resposta: programas ou ações de treinamento de profissionais de TI em Segurança da Informação realizados na subunidade, programas ou ações de treinamento de usuários de TI em Segurança da Informação realizados na subunidade, campanhas ou ações de divulgação de regulamentos de Segurança da Informação da subunidade, campanhas ou ações de divulgação da Política de Segurança da Informação da subunidade, campanhas ou ações de divulgação de regulamentos de Segurança da Informação da organização, campanhas ou ações de divulgação da Política de Segurança da Informação da organização, campanhas ou ações de conscientização de usuários e profissionais de TI sobre Segurança da Informação).

As medidas técnicas são as que afetam o funcionamento dos recursos tecnológicos, as que são implantadas nos recursos tecnológicos e que visam protegê-los, bem como aquelas que afetam o ambiente onde esses recursos e dispositivos funcionam.

Quais são as Medidas Técnicas relativas a Segurança da Informação adotadas pela organização?

(Medidas a serem identificadas na resposta: redundância de dados, como backup, espelhamento de dados e storage; segregação de redes de computadores, como firewall, proxy, switch de conteúdo; redundância de peças de equipamentos, como fontes, discos, RAID, processadores, memórias, placas, e outras partes redundantes; prevenção contra códigos maliciosos, como antivírus, anti-spam e filtro de conteúdo; controle de acesso lógico, como a definição de níveis de permissão a arquivos e sistemas e a funcionalidades e conteúdos; transmissão e armazenamento seguros de dados, como aquelas utilizando VPN ou criptografia em transmissão ou armazenamento de dados; autenticação forte utilização de senhas fortes, tokens, PINs, biometria ou smartcards para prover acesso a sistemas e equipamentos; redundância de equipamentos, como servidores redundantes, clusters, espelhamento de servidores e sites backup; controle de acesso físico, como restrição de acesso a CPDs, datacenters, salas de equipamentos, equipamentos e servidores apenas para pessoal de TI e funcionários identificados e autorizados; proteção ambiental contra incêndio, inundação e fumaça, uso de no-breaks e geradores, uso de salas-cofre e cofres para armazenamento de dados e mídias).

PARTE 3

Pergunta 1: Quais são os benefícios que a adoção de medidas de Segurança da Informação traz para a FIOCRUZ?

Pergunta 2: O governo publica regulamentos que obrigam a FIOCRUZ a adotar medidas de Segurança da Informação. Por favor, fale sobre a coerência entre os objetivos e estratégias da FIOCRUZ e essas medidas que ela é obrigada a adotar.

Pergunta 3: Quais são as limitações ou prejuízos que a FIOCRUZ tem ao adotar certas medidas de Segurança da Informação?

Pergunta 4: Porque medidas de Segurança da Informação são adotadas pela FIOCRUZ?

Pergunta 5: A FIOCRUZ consulta outras organizações sobre as medidas de Segurança da Informação que elas adotam? Como é feita a consulta?

Pergunta 6: Como a interconectividade da FIOCRUZ com outras organizações ou suas subunidades influencia na adoção de medidas de Segurança da Informação?

Pergunta 7: Como foi o processo de elaboração da Política de Segurança da Informação da FIOCRUZ?

Pergunta 8: Como foi a criação do Comitê de Segurança da Informação da FIOCRUZ?

Pergunta 9: Como foi a criação dos regulamentos de Segurança da Informação da FIOCRUZ?

Pergunta 10: Fale sobre o comportamento das subunidades diante da política e dos regulamentos de Segurança da Informação da FIOCRUZ.

Pergunta 11: Por quais motivos as subunidades adotam ou deixam de adotar medidas de Segurança da Informação?

Pergunta 12: Quais são os interesses das subunidades ao adotarem medidas de Segurança da Informação?

Pergunta 13: Como você descreve a situação da FIOCRUZ quanto à conformidade com os requisitos externos de Segurança da Informação?

APÊNDICE B

MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

MEDIDAS FORMAIS	
Política de Segurança da Informação	-
Comitê de Segurança da Informação	-
Regulamentos internos de Segurança da Informação	Regulamento de uso de correio eletrônico Regulamento de uso de dispositivos móveis Regulamento de acesso a recursos da rede de computadores Regulamento de segurança no desenvolvimento de sistemas Regulamento de uso de equipamentos particulares Regulamento de acesso à Internet Regulamento de participação em redes sociais na Internet Regulamento de acesso remoto à rede de computadores Regulamento de responsabilidades dos usuários Regulamento de continuidade do negócio Política de senhas Política de uso de chaves de criptografia Política de uso de computação em nuvem
Processos e procedimentos de Segurança da Informação	Processo de credenciamento de usuários Processo de descredenciamento de usuários Processo de autorização de acesso Procedimento de realização de *backup* Procedimento de restauração de *backup* Procedimento de descarte de dados e mídias de armazenamento Procedimento de identificação de visitantes Processo de concessão de acesso a dados sigilosos Procedimento de instalação segura de *softwares* Procedimento de configuração segura de servidores Processo de revisão de regulamentos de Segurança da Informação Procedimento de recuperação de servidores Processo de inventário e mapeamento de ativos de informação Procedimento para alteração de configurações em equipamentos e sistemas de Segurança da Informação Procedimento de tratamento de registros e evidências
Equipe 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 periódica da Política de Segurança da Informação	-

MEDIDAS TÉCNICAS	
Redundância de dados	Replicação de dados Espelhamento de discos *Backup* Armazenamento de mídias em cofres contra água e fogo
Segregação e monitoramento de redes de computadores	*Firewalls* *Proxies* *Switches* de conteúdo VLAN IPS IDS
Redundância de peças de equipamentos	Fontes redundantes Discos redundantes Interfaces redundantes
Prevenção contra códigos maliciosos	Anti-spam Antivírus *Antimalware* Atualização de sistemas
Controle de acesso lógico	Listas de controle de acesso à *web* Listas de controle de acesso a arquivos Listas de controle de acesso a sistemas de informação Listas de controle de acesso à Internet *Login* único Registro (*log*) de acesso
Transmissão e armazenamento seguros de dados	Criptografia de mensagens VPN Criptografia de dados armazenados em disco
Autenticação forte	Senhas complexas Quantidade mínima de caracteres em senhas Biometria Frase secreta *Token* *Pin*
Redundância de equipamentos	Espelhamento de servidores *Failover* ativo-ativo *Failover* ativo-passivo *Cluster*
Controle de acesso físico	Definição de perímetros Cabo de segurança Fechadura Fechadura eletrônica Fechadura biométrica Câmeras de vigilância Segurança patrimonial
Proteção ambiental	Detector de fumaça Sistema contra incêndio Proteção contra inundação Ar condicionado Detector de calor *No-break* *UPS* Gerador elétrico Redes elétricas redundantes Extintor de incêndio

MEDIDAS INFORMAIS	
Treinamento de profissionais de TI	Cursos de capacitação em tecnologias de Segurança da Informação Cursos de capacitação em equipamentos e sistemas de Segurança da Informação Especialização em Segurança da Informação Treinamentos em gestão de Segurança da Informação
Treinamento de usuários de TI	Treinamentos voltados para os usuários sobre o uso seguro de sistemas de informação
Divulgação de regulamentos e da Política de Segurança da Informação	Campanhas ou ações de divulgação da Política de Segurança da Informação da organização Campanhas ou ações de divulgação da Política de Segurança da Informação da subunidade Campanhas ou ações de divulgação de regulamentos de Segurança da Informação da organização Campanhas ou ações de divulgação de regulamentos de Segurança da Informação da subunidade
Ações de conscientização	Palestras e seminários de conscientização em Segurança da Informação da organização