PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

TIAGO MURER FURLANETTO

SEGURANÇA DA INFORMAÇÃO NA CADEIA DE SUPRIMENTOS DA SAÚDE: UMA ANÁLISE DAS PRÁTICAS DE PROTEÇÃO DE INFORMAÇÕES CRÍTICAS

Orientadora: Profa. Dra. Edimara Mezzomo Luciano

Porto Alegre

2016

TIAGO MURER FURLANETTO

SEGURANÇA DA INFORMAÇÃO NA CADEIA DE SUPRIMENTOS DA SAÚDE: UMA ANÁLISE DAS PRÁTICAS DE PROTEÇÃO DE INFORMAÇÕES CRÍTICAS

Dissertação apresentada à Pontifícia Universidade Católica do Rio Grande do Sul como requisito parcial para a obtenção do grau de Mestre em Administração.

Orientadora: Profa. Dra. Edimara Mezzomo Luciano

Porto Alegre

2016

Dados Internacionais de Catalogação na Publicação (CIP)

F985s Furlanetto, Tiago Murer
Segurança da informação na cadeia de suprimentos da saúde : uma análise das práticas de proteção de informações críticas / Tiago Murer Furlanetto. – Porto Alegre, 2016.
116 f.

Dissertação (Mestrado) – Faculdade de Administração, Contabilidade e Economia, PUCRS.
Orientador: Prof.ª Dr.ª Edimara Mezzomo Luciano

1. Segurança da Informação. 2. Gestão da Informação. 3. Logística (Administração). 4. Administração de Empresas. I. Luciano, Edimara Mezzomo. II. Título.

CDD 658.4038

Ficha Catalográfica elaborada por Loiva Duarte Novak – CRB10/2079

Tiago Furlanetto

Segurança da Informação na Cadeia de Suprimentos da Saúde: Uma Análise das Práticas de Proteção de Informações Críticas

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado em Administração e Negócios da Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Aprovado em 23 de março de 2016, pela Banca Examinadora.

BANCA EXAMINADORA:

Profa. Dra. Edimara Mezzomo Luciano
Orientadora

Profa. Dra. Mirian Oliveira
Presidente da sessão

Prof. Dr. Gustavo Dalmarco

Prof. Dr. Pietro Dolci

AGRADECIMENTOS

Em primeiro lugar, agradeço aos meus pais, Antonio e Lucia, por todo o carinho, confiança, apoio e incentivo desde o primeiro dia para que este trabalho fosse realizado.

À minha esposa, Dariane, por seu companheirismo, por sua paciência e compreensão, pelo menos na maior parte do tempo.

A Deus, pela força de seguir sempre em frente e pelo fantástico presente que me foi dado, minha filha Clara, que trouxe muita alegria e novas energias para finalizar este trabalho.

À minha irmã Anelise e demais parentes pelo apoio e compreensão pela ausência.

Ao Prof. Leonardo Rocha, pelos ensinamentos e orientação na primeira fase desta pesquisa.

À Profa. Dra. Edimara Luciano, pelas várias e construtivas conversas acerca dos melhores caminhos a seguir com a pesquisa, além da própria orientação na reta final do trabalho.

Ao Odirlei Magnagagno por seu apoio, com o qual tornou possível a coleta de dados desta pesquisa.

Aos meus colegas do mestrado pelas trocas de experiências e grandes ensinamentos.

Aos colegas de trabalho, pela compreensão dos períodos ausentes, além de alguns dias de humor “alterado”.

E a todos os demais amigos, pela compreensão quanto à ausência em diversos eventos, jogos do Grêmio, *happy hours*, jantares e outros encontros planejados.

Enfim, agradeço a todos que colaboraram de alguma forma, direta ou indiretamente, para que este trabalho acontecesse.

RESUMO

As informações das organizações são sempre importantes, seja por serem a base para a tomada de decisão, seja por serem informações confidenciais relacionadas aos clientes ou informações para um simples pedido à um fornecedor da quantia correta de produtos necessários para sua operação. Desta forma, proteger essas informações se torna uma necessidade para todas as organizações, independente do tamanho ou da área de atuação. Mas ao mesmo tempo que as organizações precisam investir para proteger suas informações, elas são constantemente cobradas por sua performance financeira, tendo que buscar melhores resultados com aumento de receita e redução de custo. Na busca por esses melhores resultados, organizações aperfeiçoaram seus relacionamentos com organizações parceiras das cadeias de suprimentos de que fazem parte. A Cadeia de Suprimentos da Saúde é uma das cadeias que vêm recebendo atenção, tanto pela necessidade de melhorias em sua performance como nas questões de segurança das informações que possui, visto que lida com informações bastante sensíveis de pacientes. Assim, o trabalho tem por objetivo, analisar as práticas em ações em Segurança da Informação na proteção de informações críticas das organizações na Cadeia de Suprimento da Saúde. Para atingir esse objetivo, foram realizadas 11 entrevistas semiestruturadas com profissionais de Administração e Tecnologia da Informação de 10 diferentes organizações participantes de Cadeias de Suprimento da Saúde, incluindo Laboratórios, Clinicas, Hospitais e Planos de Saúde na região sul do Brasil. O Roteiro de Entrevista foi elaborado após a revisão bibliográfica que resultou em um quadro com quatro dimensões base e 14 variáveis que auxiliaram a obtenção de informações para atingir o objetivo. Para a análise dos dados obtidos com as entrevistas, utilizou-se a técnica de análise de conteúdo com análise categorial para cada dimensão e variável, identificando as categorias conforme elas se apresentaram nas entrevistas transcritas. Dentre os resultados observados estavam o conhecimento das informações críticas para elas, principalmente relacionada aos dados dos pacientes, e dos processos internos das organizações sobre seus processos com fornecedores, mas que não se repetia fora da esfera da organização. As organizações pesquisadas não funcionam de forma integrada e colaborativa dentro da Cadeia de Suprimentos, elas não veem os demais elos da cadeia como parceiros para que possam contribuir um com o outro, assim não compartilham informações ou atividades para crescimento

conjunto. Além disso, demonstraram não ter métricas para controle dos impactos de possíveis ataques às suas informações para que possam planejar, investir e mitigar de forma preventiva a ocorrência destes ataques de forma adequada ao valor da informação a ser protegida. As organizações realizam investimentos em mitigação quanto a falhas, tanto em termos de sistemas como prevenção contra falhas humanas, mas esse investimento é feito de maneira genérica, sem a preocupação específica quanto as organizações mais críticas para suas operações. Este trabalho pode ser visto como um alerta às organizações da área de assistência à saúde, quanto à Segurança das Informações e dos possíveis impactos financeiros à elas e a cadeia da qual fazem parte.

PALAVRAS-CHAVE : Segurança da Informações, Investimento em Segurança da Informação, Gestão de Cadeia de Suprimentos; Cadeias de Suprimento da Saúde.

ABSTRACT

The organizations' information are always important, they can be the basis for decision-making, related to customers' confidential information or information to a simple request to a supplier about the correct amount of products needed for its operation. Thus, to protect this information becomes a necessity for all organizations, regardless of size or area of operation. But while organizations need to invest to protect their information, they are constantly charged by their financial performance, having to seek better results with revenue growth and cost reduction. Searching for these better results, organizations improved their relationships with partners' organizations in supply chains. Healthcare Supply Chain is one of the chains that have received attention, both by the need for improvements in their performance and in the Information Security issues, since they are dealing with very sensitive patient information. So, the research objective seeks to analyze the practices on Information Security in order to protect critical organizational information that is part of the Healthcare Supply Chain. To achieve this goal, there were 11 semi-structured interviews with professionals of Administration and Information Technology areas from 10 different organizations participating in the Healthcare Supply Chain, including Laboratories, Clinics, Hospitals and Healthcare Plans in Southern Brazil. The interview script was developed after a literature review, which resulted in four dimensions and 14 variables that help getting information needed to achieve the goal. For the analysis of the data obtained from the interviews, was used the content analysis technique and categorical data analysis for each dimension and variables identifying the categories as they were presenting themselves in the interview transcription. Among the finding results were the knowledge of the critical information, mostly related to the patients and its internal process related to their suppliers, which did not repeated outside the organization's boundaries. The research presented that the organizations surveyed do not work integrated and collaboratively within the supply chain, they can't see the other organizations in the supply chain as partners so that they can help each other to achieve better results, so they don't share information nor activities. Furthermore, they have no metrics to control the impacts of possible attacks to their information in order to plan, invest and mitigate preventively the occurrence of these attacks accordingly to the value of the information to be protected. The organizations perform investments to mitigate issues, both in systems and human, but the investment is done in a generic

way to all organization disregarding the importance of the information to their operations. This work can be seen as a warning to organizations of healthcare area, to the Information Security and the possible financial impact to the organizations and the supply chain of which they are part.

KEYWORDS: Information Security, Information Security Investments, Supply Chain Management; Healthcare Supply Chain.

LISTA DE FIGURAS

Figura 1 – Modelo SCOR – Nível 1 38

Figura 2 – Cadeia de Suprimentos de Medicamentos 43

Figura 3 – Cadeia de Suprimento da Saúde 50

Figura 4 – Modelo Conceitual 51

Figura 5 – Desenho de Pesquisa 56

Figura 6 – Número de Entrevistados na Cadeia da Suprimentos 65

Figura 7 – Cadeia de Suprimento Identificada na Pesquisa 74

Figura 8 – Práticas de Segurança da Informação Identificadas na Cadeia de Suprimento da Saúde 100

LISTA DE TABELAS

Tabela 1 – Ataques ocorridos em 2014 no Brasil 22

LISTA DE QUADROS

Quadro 1 - Ameaças à Segurança da CS.....29
Quadro 2 - Matriz de Dimensões 57
Quadro 3 - Variáveis x Questões 59
Quadro 4 - Caracterização dos Entrevistados 64
Quadro 5 - Categorias do Fluxo de Informações Interno à Organização 69
Quadro 6 - Categorias do Fluxo de Informações com Parceiros da CS.....71
Quadro 7 - Categorias do Papel da Organização na CS.....74
Quadro 8 - Categorias das Informações Críticas a Serem Protegidas.....78
Quadro 9 - Categoria do Acesso à Informação.....80
Quadro 10 - Categoria dos Meios de Comunicação com Parceiros.....81
Quadro 11 - Categorias das Reconhecimento de Ameaças e seus Impactos 84
Quadro 12 - Categorias das Ações de Mitigação em Sistemas 87
Quadro 13 - Categorias das Ações de Mitigação para Funcionários 88
Quadro 14 - Categorias de Monitoramento da Informação 89
Quadro 15 - Categorias das Avaliação de impacto de Ameaças 91
Quadro 16 - Quadro Resumo.....99

LISTA DE ABREVIATURAS E SIGLAS

APQC	*American Productivity & Quality Center*
CBV	Custo de Bens Vendidos
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
COSO	*Committee of Sponsoring Organizations*
CS	Cadeia de Suprimentos
CSCMP	*Council of Supply Chain Management Professionals*
CTGCS	Custo Total da GCS
DoS	*Denial of Service*
GCS	Gestão da Cadeia de Suprimentos
GRC	Governança, Risco e Conformidade
KPI	*Key Performance Indicator*
PCF	*Process Classification Framework*
SCC	*Supply Chain Council*
SCADA	*Supervisory Control and Data Acquisition*
SCMI	*Supply Chain Management Institute*
SCOR	*Supply Chain Operations Reference*
SGSCS	Sistema de Gestão de Segurança para a Cadeia de Suprimentos
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistemas de Informação
OCEG	*Open Compliance and Ethics Group*
TI	Tecnologia da Informação
TIC	Tecnologia de Informações e Comunicações

SUMÁRIO

1 INTRODUÇÃO 15

1.1 DELIMITAÇÃO DO TEMA 15

1.2 SITUAÇÃO PROBLEMÁTICA 20

1.3 OBJETIVOS 21

1.3.1 Objetivo Geral 21

1.3.2 Objetivos específicos 21

1.4 JUSTIFICATIVA DO TEMA 21

1.5 ESTRUTURA DO TRABALHO 24

2 REFERENCIAL TEÓRICO 25

2.1 SEGURANÇA DA INFORMAÇÃO 25

2.1.1 Investimentos em Segurança da Informação 30

2.1.2 Normas ISO 32

2.1.2.1 ISO 27000 32

2.1.2.2 ISO 28000 33

2.2 GERENCIAMENTO DA CADEIA DE SUPRIMENTOS 35

2.2.1 Modelo de Gestão de Cadeia de Suprimento 37

2.2.2 Gestão da Cadeia de Suprimento da Saúde 42

2.2.3 Governança, Risco e Conformidade 44

2.3 SEGURANÇA DA INFORMAÇÃO NA CADEIA DE SUPRIMENTOS DA SAÚDE 46

3 MODELO CONCEITUAL DA PESQUISA 50

4 MÉTODO DE PESQUISA 55

4.1 DEFINIÇÕES METODOLÓGICAS 55

4.2 ELABORAÇÃO E VALIDAÇÃO DO INSTRUMENTO 57

4.3 COLETA DOS DADOS 60

4.4 ANÁLISE DOS DADOS 61

5 ANÁLISE DOS RESULTADOS 63

5.1 CARACTERIZAÇÃO DOS RESPONDENTES 63

5.2 DIMENSÕES E VARIÁVEIS.....65

5.2.1 Estrutura da CS para um Melhor Fluxo de Informações 66

5.2.1.1 Fluxo de Informações Interno à Organização 66
5.2.1.2 Fluxo de Informações com Parceiros da Cadeia de Suprimento 69
5.2.1.3 Papel da Organização na Cadeia de Suprimento 72
5.2.1.4 Definição dos parceiros 74

5.2.2 Informações a Serem Protegidas 76

5.2.2.1 Informações Críticas a Serem Protegidas.....76
5.2.2.2 Acesso à Informação 79
5.2.2.3 Meios de Comunicação com Parceiros 80

5.2.3 Ameaças e ações de mitigação para a Segurança da Informação 82

5.2.3.1 Reconhecimento de Ameaças e seus Impactos 82
5.2.3.2 Ações de Mitigação em Sistemas.....85
5.2.3.3 Ações de Mitigação para Funcionários 87
5.2.3.4 Monitoramento da Informação.....89

5.2.4 Investimentos em Segurança da Informação.....89

5.2.4.1 Avaliação de impacto de Ameaças.....90
5.2.4.2 Orçamento Específico para Segurança da Informação 91
5.2.4.3 Impacto do Investimento na Performance Financeira Organizacional e da Cadeia de Suprimentos 92

5.3 ANÁLISE DAS PROPOSIÇÕES 93

5.3.1 Proposição 1 – Cadeia de Suprimentos Integrada e Colaborativa 93

5.3.2 Proposição 2 – Conhecimento das Informações Críticas 95

5.3.3 Proposição 3 – Métricas de Impacto para Ataques à Informação .96

5.3.4 Proposição 4 – Investimento em Segurança de Informações.....97

5.4 CONSOLIDAÇÃO DOS RESULTADOS 98

6 CONSIDERAÇÕES FINAIS.....102

6.1 CONTRIBUIÇÕES DA PESQUISA.....104

6.2 LIMITAÇÕES DA PESQUISA 106

6.3 PROPOSTAS PARA PESQUISAS FUTURAS 106

REFERÊNCIAS.....108

APÊNDICE A – ROTEIRO DE ENTREVISTA 115

APÊNDICE B – CARTA DE APRESENTAÇÃO.....116

1 INTRODUÇÃO

Neste capítulo serão apresentados os elementos introdutórios. Na seção 1.1 será apresentado o Tema e sua Delimitação. Na seção 1.2 será abordada Situação Problemática. Na seção 1.3, os Objetivos Geral e Específicos. Na seção 1.4 será justificado o tema proposto. Por fim, na seção 1.5, será apresentada a Estrutura do Trabalho.

1.1 DELIMITAÇÃO DO TEMA

O uso de tecnologias cresce em alta velocidade em todo o mundo e a medida em que mais pessoas e organizações utilizam esses meios eletrônicos para guardar suas informações ou trocá-las entre si, maior a visibilidade para mais pessoas buscarem formas para se aproveitar de falhas e obterem alguma vantagem sobre elas (GORDON *et al.*, 2015; SAFA *et al.*, 2016). Estima-se que o custo anual para a economia global a partir de ações referentes a crimes cibernéticos sejam mais de 400 bilhões de dólares (LOSSES, 2014). Mas os ataques contra as informações das organizações não ocorre da mesma forma em todos os tipos de organização. As organizações financeiras ficam em primeiro lugar, mas organizações de assistência à saúde, organizações de tecnologia e governamentais vêm logo a seguir entre as mais visadas para ataques (NAGURNEY e NAGURNEY, 2015).

Para se defender desses ataques cibernéticos, as organizações precisam investir em segurança onde o propósito, segundo Guttman e Roback (1995), é a proteção dos recursos das organizações, tais como informação, hardware e software. Com a escolha correta dos meios de proteção, esta segurança atua não apenas sobre os ativos físicos da empresa, mas também sobre seus recursos financeiros, informações de empregados, clientes e planos de negócios (GUTTMAN e ROBACK, 1995).

Quando se trata de informações, o ataque cibernético é apenas um dos meios para chegar à elas. Muitos ataques focam as pessoas para conseguir entrar em um sistema (GAUNT, 2000; ISO-IEC, 2014). Pessoas que não possuem o devido cuidado com as informações com as quais lidam no seu dia-

a-dia ou mesmo são relapsas com senhas, acessos inapropriados, compartilhamento de dados confidenciais, entre outros (SAFA *et al.*, 2016). Alguns autores indicam que os funcionários das organizações têm resistência quanto ao seu papel de protetor das informações, em parte, por sua não familiaridade com procedimentos e práticas de proteção ou mesmo as consequências causadas decorrente destas falhas à proteção (DINI, 2014). Idealmente, a Segurança da Informação deve combinar aspectos tecnológicos, segurança sistêmica e de equipamentos de TI (Tecnologia de Informação), com aspectos comportamentais das pessoas (SAFA *et al.*, 2016).

No momento em que as organizações passam a trabalhar de forma integrada, além da preocupação natural para as organizações com a segurança de suas informações, elas também passam a prestar atenção em como seus parceiros de negócio lidam com a questão de segurança, pois uma falha em uma organização pode comprometer o acesso a segunda (GORDON *et al.*, 2015). Esta integração inicia no momento em que as empresas deixam as questões de negociação, transporte e armazenagem de maneira particular, com cada uma das áreas sendo operacionalizada e gerida individualmente (BALLOU, 2006). Na busca de processos mais eficientes e menores custos, as organizações passam a trabalhar com um conceito de gestão coordenada de atividades inter-relacionadas, deixando de lado a gestão individual das áreas, identificando possíveis problemas e otimizando o fluxo da cadeia em busca de melhores negócios com fornecedores (CROOM *et al.*, 2000; BALLOU, 2006).

Esta inter-relação entre organizações exige um maior controle da logística das organizações para organizar os fluxos de materiais, produtos e informações (GOMES, 2004). O Gerenciamento da Cadeia de Suprimento (GCS) capta a essência da logística e destaca as interações do fluxo, e passa a coordenar efetivamente o que ocorre no processo da cadeia dentro da organização, e também no que tange os parceiros envolvidos, sejam clientes ou fornecedores (CHRISTOPHER, 2007). De maneira sistêmica, é importante identificar com clareza cada um desses integrantes e as informações mais significativas para cada organização da Cadeia de Suprimento (CS), pois com o conhecimento do processo completo, pode-se avaliar como cada um poderá ser influenciado, positiva ou negativamente, impactando o fluxo da cadeia (GOMES, 2004).

A GCS é um assunto que tem recebido atenção nas últimas décadas, tanto da academia como da prática de negócios (HASSINI *et al.*, 2012). Ela é vista como um ponto vital de sucesso, auxiliando organizações na busca de lucros e eficiência na gestão dos custos, seja com a diversificação dos fornecedores ou com o fortalecimento da relação entre as organizações (KETCHEN e HULT, 2007). Com a aproximação entre organizações e com atividades que podem ser compartilhadas, maior a quantidade de informações trafegadas entre estas organizações, as quais ocorrem, principalmente, por Sistemas de Informação (SI) (KETCHEN e HULT, 2007). Assim, cresce a necessidade por medidas que garantam a segurança dos dados e informações das organizações envolvidas (BOJANC e JERMAN-BLAŽIČ, 2008). Na busca por esta proteção, as organizações tem realizado cada vez mais investimentos em segurança (GORDON *et al.*, 2010; GORDON *et al.*, 2015).

Levando em consideração todo o leque de opções de fornecedores e clientes que se abre com o aperfeiçoamento das comunicações e sistemas logísticos, aumenta a pressão sobre os principais fornecedores em quase todos os setores, ocasionando um aumento da competitividade entre eles (CHRISTOPHER, 2007). Esse cenário logisticamente descentralizado também trás uma dependência das organizações em SI, e com ela a necessidade de aumentar a segurança contra ataques (GORDON *et al.*, 2015). Os sistemas utilizados pelas organizações, bem como os níveis de segurança aplicados às informações que trafegam dentro dela, trazem benefícios quanto a competitividade no mercado, pois a preocupação quanto a segurança torna-se um item importante na busca por parceiros de negócio (GORDON *et al.*, 2010).

A redução das barreiras ao comércio e desenvolvimento de uma infraestrutura de transporte, permitiu que empresas passassem a concentrar fábricas maiores em diferentes regiões ou até mesmo em diferentes países, próximo as matérias primas e com mão-de-obra com menor custo (BALLOU, 2006). Com essa distribuição de unidades e organizações, maior a quantia de atividades integradas e informações que precisam trafegar entre elas, consequentemente, maior a quantidade de ameaças e possibilidades para ataques cibernéticos (GIUNIPERO e ELTANTAWY, 2004). Assim, torna-se necessário um rigor maior com os processos internos da organização frente a

gestão da informação em CS, seja por recursos humanos, dispositivos eletrônicos, ou sistemas de informações (GUTTMAN e ROBACK, 1995; GOMES, 2004). Em caso de um ataque cibernético bem sucedido, além dos danos causados a organização, empresas parceiras também são afetadas (GORDON *et al.*, 2015). Além de informações sobre valores de negociação, muitas vezes confidenciais, poderem ficar expostos, existem outros riscos de danos como a manipulação de pedidos, onde um pedido realizado poderá não ser entregue ou um pedido inexiste poderá ser criado, gerando prejuízo para todos os participantes da cadeia (WARREN e HUTCHINSON, 2000).

No entanto, um gasto excessivo na busca pela proteção perfeita das informações pode impactar nos resultados financeiros da organização, assim, a busca por esse equilíbrio passa a ser um dos grandes desafios das organizações (GORDON e LOEB, 2002). Por mais que as tecnologias surjam sempre com novidades quanto a segurança das informações, o lado técnico tem ficado em segundo plano para muitos tomadores de decisão (BOJANC *et al.*, 2012). Ao invés de buscarem a melhor alternativa técnica, eles fazem primeiramente uma avaliação do ponto de vista econômico para então analisar os requisitos técnicos, assim encontram a melhor solução de proteção de maneira compatível com suas organizações (BOJANC *et al.*, 2012).

Todo este cenário descrito não é distante da área de assistência à saúde, é uma área que ainda está engatinhando se comparada a outras em termos de TI e de GCS, como a industrial, que já possuem vários anos de estudos a frente da saúde (HEDSTRÖM *et al.*, 2011; CHEN *et al.*, 2013). Já existem exemplos da saúde, como a indústria farmacêutica que, na definição de novas plantas fabris, buscam benefícios para as organizações se espalhando ao redor do planeta para adquirir componentes de menor custo para sua produção (MUSTAFFA e POTTER, 2009).

Já em relação à TI, ela tem sido cada vez mais importante para a assistência da saúde, entregando as informações de maneira mais ágil e eficiente, mas sofre ao buscar dar mais proteção aos pacientes, seus dados e informações sobre seus procedimentos, controlando os custos do atendimento dado a ele (SAMY *et al.*, 2010; LANDOLT *et al.*, 2012). Profissionais da saúde precisam das informações de forma precisa e rápida sobre os pacientes e isso,

nem sempre, está alinhado com as restrições impostas para o acesso das informações (HEDSTRÖM *et al.*, 2011; HUANG *et al.*, 2014). No momento que as informações dos pacientes está inserida nos sistemas hospitalares, de clínicas, laboratórios e demais organizações de assistência à saúde, elas precisam ser protegidas, existe uma ética profissional a ser zelada e um comprometimento destas organizações para com seus clientes, os pacientes (BRAGANÇA, 2010). O prontuário do paciente é onde está contido todo o histórico do paciente durante seu atendimento e talvez possa ser considerado o documento no qual a organização devesse ter o maior desejo de proteger (MAGNAGNAGNO, 2015).

Além disso, ainda há a competividade na área assistencial, a qual requer um serviço eficiente, com respostas rápidas, capacidade de atendimento de qualidade e adaptabilidade em um meio que doenças e tratamentos estão constantemente surgindo (LEE *et al.*, 2011). E toda essa preparação, atendimento e controles de segurança, precisam estar estabelecidos dentro de parâmetros que sejam administrativamente e financeiramente aceitáveis para a organização (HUANG *et al.*, 2014). Os envolvidos nos processos dessas organizações assistenciais precisam estar cientes do valor da informação com a qual estão lidando, pois aquela informação é base para a tomada de decisões médicas e administrativas e se estiver corrompida, incorreta ou vazar de alguma forma, pode trazer consequências financeiras graves para a organização (MAGNAGNAGNO, 2015).

Neste controle é importante uma constante avaliação da gestão da organização. Um dos recentes modelos desenvolvido é o de “Governança, Risco e Conformidade” (GRC ou *Governance, Risk and Compliance)*. Nele, a gestão das informações consideram os três pilares do modelo Governança, Gerência de Riscos e Conformidade – em cada atividade dos fluxos de informações a longo da organização (OCEG, 2012).

A gerência de risco está presente não só em aspectos específicos da área de segurança, mas também na administração como um todo. Gestores, diretores, gerentes, em todos os níveis, avaliam as consequências das opções existentes antes de tomar uma decisão. O risco pode ser calculado para cada

uma das opções, bem como ações podem ser planejadas para mitigar a ocorrência de falhas.

Segundo Safa *et al.* (2016), as organizações geralmente preocupam-se com a segurança de suas informações e buscam alternativas para mitigar seus o riscos de falhas. Assim, este trabalho busca compreender as práticas empreendidas pelas organizações da área da saúde, a partir da percepção de seus gestores, quanto a segurança das informações com as quais lidam, sejam internas à elas ou da relação com parceiros participantes da CS.

1.2 SITUAÇÃO PROBLEMÁTICA

A partir da informatização e definição de métricas de performance, as organizações passaram a vislumbrar oportunidades de melhoria contínua e vantagem competitiva a partir de processos mais eficientes e seguros (CROOM *et al.*, 2000). A segurança também é necessária para informações hospitalares, como de pacientes, exames e tratamentos que são extremamente sigilosos e precisam ser protegidas da melhor forma possível (SAMY *et al.*, 2010).

Um pesquisa conduzida pelo IT Policy Compliance Group (ITPCG, 2013) apresenta que além dos bons resultados quanto a própria proteção das informações, o investimento em segurança também auxilia na manutenção dos clientes e da competitividade no mercado (HUANG *et al.*, 2014).

No meio acadêmico existem diversos estudos e pesquisas que envolvem Segurança da Informação, investimentos e CS. Estudos como Bojanc e Jerman-Blazic (2008), abordam um modelo econômico para avaliação de investimentos em segurança nas organizações. Já outros autores apresentam estudos que focam questões de desempenho (GUNASEKARAN *et al.*, 2004) e gerência de riscos (LAVASTRE *et al.*, 2012) na CS. No âmbito digital, existem diversos estudos sobre a segurança cibernética da informação das organizações, como Gordon (2015) e Atoum (2014). Muitos levam em consideração a dificuldade de mensuração desse tipo de investimento, foca os resultados indiretos para as organizações (HUANG *et al.*, 2014). Ao invés de olhar as métricas diretas sobre ataques malsucedidos, apresentam uma abordagem a longo prazo sobre benefícios de negócios para os organizações, pois passam a ser vistas como

seguras e conseguem uma vantagem no mercado para a conquista de novos parceiros e clientes (HUANG *et al.*, 2014).

Dada importância à Segurança da Informação e a avaliação de seus investimentos para que não onere a performance financeira das organizações, nem a da CS, o presente trabalho busca analisar as práticas em ações de Segurança da Informação na proteção de informações críticas na CS da Saúde. Assim, pretende-se responder a seguinte questão de pesquisa: Como as organizações baseiam suas decisões em ações de Segurança da Informação para proteger suas informações mais importantes?

1.3 OBJETIVOS

Nesta seção são apresentados o objetivo geral e os objetivos específicos deste trabalho.

1.3.1 Objetivo Geral

Analisar as práticas em ações em Segurança da Informação na proteção de informações críticas das organizações na Cadeia de Suprimento da Saúde.

1.3.2 Objetivos específicos

Objetivos específicos do trabalho são:

a) Identificar o fluxo de informações da Cadeia de Suprimento da Saúde;
b) Identificar as informações críticas da Cadeia de Suprimento da Saúde e o impacto na organização em caso de um ataque bem sucedido sobre a mesma;
c) Identificar as práticas de investimentos em Segurança da Informação.

1.4 JUSTIFICATIVA DO TEMA

Bojanc *et al.* (2012) consideram a Segurança da Informação como uma disciplina técnica na qual se atinja os níveis máximos de segurança. Mas é necessário que se tenha um olhar mais administrativo quanto a gestão da organização que analise os valores envolvidos nessa segurança, sua compatibilidade com a mesma e a expectativa da economia a ser feita ao realizar esse tipo de investimento (BOJANC *et al.*, 2012; GORDON *et al.*, 2015).

Os responsáveis por tomar decisões estão prestando mais atenção ao nível de segurança de informações de seus softwares e hardwares, além disso, também começaram a se preocupar com o nível de segurança que seus parceiros, principalmente os menores, com os quais trocam informações, cuidam da segurança (HUANG *et al.*, 2014). A dificuldade está na maneira de fazer essa avaliação financeira quanto ao investimento em segurança, pois nem sempre se consegue fazer medições precisas que comprovem a validade daquele investimento (GORDON e LOEB, 2002; BOJANC e JERMAN-BLAŽIČ, 2008; BOJANC *et al.*, 2012).

O grande problema das organizações que trocam informações é que se houver um elo mais fraco da cadeia, com níveis mais baixos de proteção entre as organizações, essa organização pode servir de entrada para ataques em todas as organizações dessa cadeia (HUANG *et al.*, 2014). E essa preocupação com a segurança não é algo pontual, ela deve ser acompanhada de forma constante pela organização (ÖĞÜTÇÜ *et al.*, 2016).

Para quantificar o risco atual que as empresas precisam lidar quanto a segurança das suas informações, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) possui dados referentes a ataques dos últimos 15 anos. Em 2012 ocorreram 466.029 ataques em território brasileiro, em 2013 foram 352.925 ataques e em 2014, 1.047.031 ataques (CERT.BR, 2015).

As estatísticas do CERT.br (2015) não apresentam todos os ataques individualmente, mas sumarizados, conforme pode ser verificado na Tabela 1, a qual apresenta os dados de ataques no ano de 2014.

Tabela 1 – Ataques ocorridos em 2014 no Brasil

Ataque	Ocorrências	Percentual	Descrição
Worm	42.191	4,03%	Propagação de códigos maliciosos na rede
DoS	223.935	21,39%	Tentativas de indisponibilizar serviços

Invasão	6.509	0,62%	Ataque bem-sucedido que permite o acesso não autorizado a um computador ou rede
Web	28.808	2,75%	Comprometimento de serviços web e ataques a páginas na *web*
Scan	263.659	25,18%	Tentativas de varrer a rede em busca de vulnerabilidades em computadores ou sistemas
Fraude	467.621	44,66%	Ato de má-fé que tenha por objetivo levar vantagem sobre os outros
Outros	14.308	1,37%	Os demais tipos de ataques
Total	**1.047.031**	**100,00%**	

Fonte: (CERT.BR, 2015)

Somado a este desafio de definição de valores de investimento em segurança, acompanha o crescimento das trocas de informações entre organizações de assistências da saúde e de toda a CS. Todos em busca de melhores resultados em qualidade e velocidade da prestação da assistência, mas também da redução de custos de logística (HEDSTRÖM *et al.*, 2011; HUANG *et al.*, 2014).

Para se fazer qualquer tipo de avaliação sobre a maneira como administradores de organizações ou responsáveis pelas áreas de TI tomam suas decisões de investimentos em segurança, torna-se necessário identificar como atualmente estes profissionais percebem e lidam com o assunto dentro de suas organizações. A CS na área da saúde auxilia o assunto Segurança da Informação devido à criticidade das informações que giram dentro dessa cadeia e quanto ao impacto que as organizações sofreriam no caso de um ataque bem sucedido às informações (HUANG *et al.*, 2014). É mais fácil calcular o tamanho do investimento a ser feito quando se lida com atualização de softwares e compra de novos equipamentos do que ao analisar o retorno dessa proteção em números (BOJANC *et al.*, 2012). Mas é importante que seja feita essa análise para que não sejam investidos valores superiores ao valor das informações que está se tentando proteger (BOJANC *et al.*, 2012; GORDON *et al.*, 2015).

Devido a essa dificuldade e importância quanto à mensuração dos investimentos em segurança, este estudo visa contribuir com uma perspectiva prática da avaliação de profissionais da área quanto a definição pelos

investimentos em ações de segurança para proteger suas informações e as informações que permeiam a CS da qual fazem parte. As organizações deveriam identificar suas informações críticas e procurar evitar que ela possa ser furtada, manipulada ou mesmo utilizada para, direta ou indiretamente, causar danos à elas e às demais organizações da CS dentro das possibilidades de cada organização.

1.5 ESTRUTURA DO TRABALHO

Este trabalho está subdividido em seis capítulos. O primeiro apresenta uma introdução com a delimitação do tema do trabalho, os objetivos e sua justificativa. O segundo capítulo traz a revisão da literatura com livros e artigos ligados a Segurança da Informação, Investimento em Segurança, GCS, CS da Saúde e conceitos sobre GRC. O terceiro capítulo apresenta o Modelo Conceitual e as Proposições a serem validadas com a pesquisa. O quarto capítulo apresenta o método utilizado no desenvolvimento do trabalho. O quinto capítulo apresenta as análises e os resultados da coleta de dados. E, finalmente, o sexto capítulo apresenta as considerações finais, bem como suas contribuições e propostas para pesquisas futuras.

2 REFERENCIAL TEÓRICO

Neste capítulo é desenvolvida a fundamentação teórica do trabalho. Na seção 2.1 são revistos conceitos sobre Segurança da Informação, incluindo normas ISO e trabalhos referente a investimentos em Segurança da Informação. Na seção 2.2 são revistos conceitos sobre Gerenciamento da Cadeia de Suprimentos (GCS), um modelo de GCS, conceitos sobre GCS da Saúde e também sobre o modelo GRC. A seção 2.3, é apresenta a relação da Segurança da Informação na CS da Saúde.

2.1 SEGURANÇA DA INFORMAÇÃO

Devido ao aumento da importância da TI nas atividades de negócios, as organizações passaram a ser mais dependentes deste recurso (GORDON e LOEB, 2002). Sistemas de TI evoluíram, principalmente para um papel mais estratégico, inclusive nas CS (GUPTA *et al.*, 2006). E as informações que estes sistemas lidam passaram a ser uma das principais preocupações das organizações (MONTESDIOCA e MAÇADA, 2015). O dinamismo da economia e o aumento da concorrência levaram a um crescimento na necessidade de proteger os dados e informações nas organizações contra ataques, cibernéticos ou não (GORDON *et al.*, 2015).

Mesmo que os sistemas tenham se aperfeiçoado nos últimos anos, vulnerabilidades continuaram existindo (GUPTA *et al.*, 2006; TEN *et al.*, 2008). Transações que ocorrem na internet entre empresas, aumentam a potencialidade de ataques nas informações trafegadas (TEN *et al.*, 2008). Em caso de sucesso em um ataque, há um potencial prejuízo para as organizações, tais como financeiro e quanto à imagem da organização perante o mercado (BOJANC e JERMAN-BLAŽIČ, 2008; TEN *et al.*, 2008). Para ainda aumentar a importância da proteção contra ataques, estes podem ser utilizados também para capturar informações de clientes, de fornecedores, ou mesmo para atacar as organizações eletronicamente interligadas (GORDON *et al.*, 2015). Mas quando suas informações estão mais seguras, as organizações tem outros benefícios, além da própria segurança: a imagem da organização, sua reputação

frente ao cliente e a abertura de caminho para novos negócios com outras organizações parceiras (HUANG *et al.*, 2014).

Uma das principais vulnerabilidades das organizações são as pessoas que fazem parte de seu quadro de funcionários (GAUNT, 2000; LUCIANO *et al.*, 2010). É necessário que eles recebam orientação de como lidar com as informações que manejam todos os dias, mas principalmente terem conhecimento dos tipo de ataques que podem sofrer por ações erradas cometidas por eles (FORWARD, 2010; MAGNAGNAGNO *et al.*, 2015). Um manual de comportamento é um ação bastante utilizada nas organizações, mas um dos problemas é que este manual, depois de entregue, não é mais revisitado ou atualizado (GAUNT, 2000). O treinamento constante dos funcionários é uma ação de segurança importante, mas também é dispendiosa, cabendo aos tomadores de decisões da empresa tratar do quando e como, ou mesmo se, realizar esses treinamentos (GAUNT, 2000; BOJANC e JERMAN-BLAŽIČ, 2008).

Os conceitos de violação de sistemas abrangem, basicamente, duas bases: (i) violação maliciosa intencional (como ataques internos (*insiders*), *hackers* ou terroristas); e (ii) violações não mal-intencionais, as quais, suas ações, não necessariamente afetam a segurança das informações (KRAEMER e CARAYON, 2007). Já o objetivo da gestão de segurança está na identificação e mitigação das possíveis falhas, de modo a garantir que, no momento de uma falha, os gestores tenham o conhecimento necessário para tomar a melhor decisão (BOJANC e JERMAN-BLAŽIČ, 2008). Nesta avaliação de segurança, procura-se proteger seis pilares principais referentes às informações da organização, conforme a ISO27000 (ISO-IEC, 2014):

- Confidencialidade: é a garantia de que apenas pessoas autorizadas terão acesso às informações em questão;
- Integridade: quando a informação é precisa, completa e consistente;
- Disponibilidade: é a garantia de que os sistemas estejam ininterruptamente a serviço dos usuários;
- Autenticidade: garantia de que o usuário ou informação são quem dizem ser;

- Não Repúdio: habilidade de provar a ocorrência do evento ou ação solicitada;
- Confiabilidade: propriedade que garante a consistência de informações e resultados.

Toda a informação capturada decorrente de ataques bem sucedidos pode ser utilizada das mais diversas formas, como fraudar transações que ocorrem entre organizações e bancos (WARREN e HUTCHINSON, 2000). Mesmo que a organização realize periódicas avaliações na sua área de TI, existem vulnerabilidades das próprias tecnologias que não estão ao alcance dela (GUPTA *et al.*, 2006). Todos os sistemas, de alguma forma, possuem falhas, vulnerabilidades que podem ser exploradas, as quais podem variar de acessos não autorizados às informações até a permissão da destruição da infraestrutura de TI da organização (GUPTA *et al.*, 2006).

Na busca por proteção ou pelo menos de uma análise sobre suas vulnerabilidades, as organizações fazem investimentos em diversas ações. Dentre elas, apresenta-se o gerenciamento de risco nas organizações, como primeira ação de segurança (PATEL *et al.*, 2008). Esse gerenciamento é indispensável para avaliar os pontos críticos dos processos de negócios e avaliar o impacto no caso de um ataque bem sucedido (BOJANC e JERMAN-BLAŽIČ, 2008). Alguns autores definem risco como a possibilidade de uma vulnerabilidade ser aproveitada, multiplicada pelo valor das informações, menos o percentual do risco mitigado por controles e pela incerteza do conhecimento dessa vulnerabilidade (PATEL *et al.*, 2008).

Todos os ataques tendem a atingir, direta ou indiretamente, um ou mais pilares de segurança (BOJANC e JERMAN-BLAŽIČ, 2008). Diferentes autores percebem de diferentes formas a abordagem quando se trabalha com Segurança da Informação, como será visto a seguir, indicando principais vulnerabilidade ou possibilidade de um ataque, as quais estarão sintetizadas no Quadro 1.

Dentre estes autores, pode ser citado o Consórcio *Forward,* que é uma iniciativa do Comissão Europeia para promover a colaboração e parcerias entre a academia e a indústria, com o objetivo principal de proteger a infraestrutura de

Tecnologia de Informações e Comunicações (TIC) (FORWARD, 2015). Em seu último relatório, o Consórcio *Forward* divulgou a lista das principais vulnerabilidades de TIC (FORWARD, 2010), que são:

- Rede: serviços de rede de comunicação;
- *Hardware* e Virtualização: *hardwares* e *softwares* que insiram novas funcionalidades;
- Complexidade: novos desenvolvimentos que adicionem complexidade aos atuais sistemas;
- Manipulação de Dados: por pessoas ou sistemas com acesso à grande quantidade e sensibilidade dos dados das organizações;
- Ataques à infraestrutura: ataques diretos à infraestrutura e sistema das organizações;
- Fatores humanos: trata das ameaças internas nas organizações, inclusive relacionados a ataques de engenharia social;
- Requisitos insuficientes de segurança: problemas, principalmente, de sistemas legados que não possuem um proteção adequada.

Já Gupta *et al.* (2006) apresenta um lista de sete categorias de vulnerabilidades. Elas são as principais e potenciais vulnerabilidades que estão presentes na maior parte dos sistemas de informações das organizações e em sua infraestrutura: (i) Design e Arquitetura do Sistema; (ii) Complexidade; (iii) Adaptação e Manipulação; (iv) Operação; (v) Exposição Indireta; (vi) Exposição Direta; (vii) Infraestrutura.

Kraemer e Carayon (2007) definem cinco elementos que podem contribuir para as falhas dos usuários: (i) erro individual; (ii) tarefas; (iii) ferramentas; (iv) tecnologias; (v) ambiente de trabalho e a própria organização.

Uma das vulnerabilidades mais citadas se trata das pessoas com acesso à informação nas organizações. Pessoas estão sempre aptas a falharem com a segurança dos sistemas e informações, cabe aos próprios sistemas auxiliarem os usuários, guiando-os a tomar decisões acertadas no que tange a segurança (KRAEMER e CARAYON, 2007). Mesmo assim, é necessário conscientizar os envolvidos. A conscientização é apontada como uma das mais fundamentais ações efetivas para a Segurança da Informação, pois mesmo que a organização

tenha diversas políticas e mecanismos para tentar auxiliar os usuários com essa segurança, se eles não colaborarem, nenhuma ação de segurança será realmente efetiva (LUCIANO *et al.*, 2010; MONTESDIOCA e MAÇADA, 2015).

Quadro 1 - Ameaças à Segurança da CS

Vulnerabilidades	Descrição	Autores
Infraestrutura	Direcionados ao Hardware da organização, bem como seu sistema de rede e comunicações	WARREN e HUTCHINSON (2000); GUPTA *et al.* (2006); TEN *et al.* (2008); FORWARD (2010); CERT.BR (2015); ISO28000
Complexidade de Sistemas	Direcionados as complexidades dos sistemas e suas interfaces	GUPTA *et al.* (2006); KRAEMER e CARAYON (2007); FORWARD (2010); CERT.BR (2015); ISO28000
Manipulação Dados	Qualquer tipo de alteração dos dados em sistemas	WARREN e HUTCHINSON (2000); GUPTA *et al.* (2006); FORWARD (2010); HEDSTRÖM *et al.* (2011); CERT.BR (2015); GORDON *et al.* (2015); SAFA *et al.* (2016); ISO28000
Fatores Humanos	Ações humanas que comprometam a segurança ou efetivamente causem o dano à organização. Desde falhas involuntárias que permitam um ataque, como ações mal intencionadas para roubo de informações	GAUNT (2000); GUPTA *et al.* (2006); KRAEMER e CARAYON (2007); FORWARD (2010); LUCIANO *et al.* (2010); LUCIANO *et al.* (2011); CERT.BR (2015); MONTESDIOCA e MAÇADA (2015); ISO27000; ISO28000
Requisitos insuficientes de segurança	Planos insuficientes de mitigação de falhas de segurança das informações, tanto com sistemas como de pessoal.	GUPTA *et al.* (2006); KRAEMER e CARAYON (2007); BOJANC e JERMAN-BLAŽIČ (2008); TEN *et al.* (2008); FORWARD (2010); ISO27000; ISO28000

Fonte: O Autor

Para exemplificar uma das responsabilidades dos usuários, é a sua identificação dentro do sistema, que é uma peça chave para a segurança do

sistema e de suas informações. Usuários não podem compartilhar acessos pois podem estar permitindo a pessoas não autorizadas o acesso à informações sigilosas, além de poder estar abrindo uma brecha para que seja possível instalar um programa malicioso no sistema (LIANG e XUE, 2009; BANG *et al.*, 2012).

As organizações buscam se proteger das vulnerabilidades e investem em segurança de forma a atingir dois principais objetivos (GUPTA *et al.*, 2006):

- Minimizar o número de potenciais vulnerabilidades em tecnologias de segurança;
- Reduzir custos de segurança para cobrir essas vulnerabilidades.

Em busca disso, as empresas seguem investindo em segurança para reduzir o risco de ataques, as quais dificilmente conseguirão se livrar totalmente (GUPTA *et al.*, 2006; BOJANC e JERMAN-BLAŽIČ, 2008). A grande dificuldade é para fazer um balanço da mitigação e das vulnerabilidades com seus sistemas o qual, normalmente, está baseado no custo dessas ações. Mas as vulnerabilidades, se corretamente mitigadas, poderão nunca vir a ser uma brecha de segurança (KRAEMER e CARAYON, 2007). Sistemas que são constantemente monitorados, por exemplo, têm menor chance de sofrerem um ataque (PATEL *et al.*, 2008). O mesmo ocorre para sistemas com menor número de interfaces de comunicação externa (PATEL *et al.*, 2008).

Devido a criticidade da necessidade de proteção de informações, modelos e regulamentações foram criados como guias para as organizações como os modelos ISO27000 para segurança cibernética e ISO28000 para segurança de CS (BOJANC *et al.*, 2012). Estas duas normas são apresentadas a seguir, juntamente com conceitos sobre investimento em Segurança da Informação.

2.1.1 Investimentos em Segurança da Informação

Diversos estudos apresentam os benefícios para as organizações protegerem suas informações, mas a maior parte deles não apresenta soluções para a otimização dos investimentos necessários para essa proteção (BOJANC *et al.*, 2012). Levando em consideração a dificuldade de mensuração desse tipo de investimento, eles focam em resultados indiretos para as organizações (HUANG *et al.*, 2014). Ao invés de olhar as métricas sobre ataques, apresentam

uma abordagem focando o longo prazo quanto a benefícios de negócios para as organizações, pois elas passam a ser vistas como seguras e conseguem vantagens no mercado para a conquista de novos parceiros e clientes (GUPTA *et al.*, 2006).

A avaliação e levantamento de segurança deve levar em consideração o valor da informação, um ponto de vista econômico, onde o custo para manter estas informações a salvo não seja maior que o prejuízo devido a uma falha (BOJANC e JERMAN-BLAŽIČ, 2008). Esta avaliação não é simples, pois existem diversas variáveis nessa fórmula, tal como a probabilidade de um ataque ou falha ocorrer e também na avaliação para atribuir ao sucesso da segurança qualquer tipo de crescimento organizacional (PATEL *et al.*, 2008; HUANG *et al.*, 2014).

Cada organização possui uma avaliação da importância das suas informações, e seus gestores podem avaliar quanto ao investimento necessário para protegê-las (GORDON e LOEB, 2002). Esta proteção envolve aspectos como: informações operacionais e de baixo valor que não precisam de muita proteção; informações táticas que podem ter uma consequência maior de dano em caso de ataque e precisariam ser melhor protegidas; e informações estratégicas, mais importantes para serem protegidas (GORDON e LOEB, 2002). A falta de proteção adequada para o tipo de informação que existe dentro dos processo dos hospitais, por exemplo, a deixam como potencial foco de ataques (SAMY *et al.*, 2010).

Existem três fatores chaves para as organizações referente aos investimentos em Segurança da Informação: (i) o valor a ser investido; (ii) em quais medidas de segurança investir; e (iii) como fazer o investimento ser eficiente (HUANG *et al.*, 2014).

O primeiro é, usualmente, definido através de análises tradicionais de risco versus retorno de investimento. Mas diferentemente dos demais investimentos, este não traz retornos diretos, tanto de lucro como prejuízo, mas sim do quanto se reduz do risco que a organização estaria correndo (HUANG *et al.*, 2014).

Após a definição do valor a ser investido, a organização precisa definir em quais ações de segurança o valor será investido (HUANG *et al.*, 2014). Por fim, precisa ser avaliada a performance desse investimento. É importante definir controles para averiguar se o investimento está dando o resultado que se espera, mas também verificar a possibilidade de readaptar esse investimento para momentos críticos para evitar ataques específicos e/ou cíclicos (HUANG *et al.*, 2014).

É importante que a informação não seja vista apenas como um ativo que gera custos, mas que sua integridade e proteção é essencial para todos os processos de negócios da organização (BOJANC *et al.*, 2012). E a partir do momento que se tem a identificação das informações críticas para o negócio da organização, tomadores de decisão podem elaborar planos e fazer análises necessárias em relação ao valor a ser aplicado para segurá-las (GORDON e LOEB, 2002; GORDON *et al.*, 2015). Quando valores tornam-se elevados demais para a proteção direta da segurança, uma das opções a ser considerada é a contratação de seguros, os quais cobririam o impacto financeiro do ataque bem sucedido (BOJANC e JERMAN-BLAŽIČ, 2008).

2.1.2 Normas ISO

2.1.2.1 ISO 27000

A ISO 27000 aborda padrões para sistemas de gerenciamento de segurança e é composta por uma série de quinze normas (ISO-IEC, 2014), que vão desde Sistemas de Gestão da Segurança da Informação (ISO/IEC 27001) até processos mais específicos como um Guia para implementação de processos de gerenciamento de riscos (ISO/IEC 27005).

A ISO 27000 foca em Sistemas de Gestão de Segurança da Informação (SGSI) e possui como objetivos (ISO-IEC, 2014):

- Definir requisitos para SGSI e para a certificação destes sistemas;
- Prover um direcionamento para implementar, estabilizar, manter e mesmo melhorar o SGSI;
- Endereçar guias específicos por áreas para SGSI;
- Endereçar avaliação de conformidade para SGSI.

A norma consiste em políticas, procedimentos, e guias para que a organização possa proteger seus ativos de informação. Os itens considerados fundamentais para o sucesso da implantação de uma SGSI são (ISO-IEC, 2014):

- Percepção da necessidade por Segurança da Informação;
- Definir responsáveis pela Segurança da Informação;
- Ter o comprometimento da gerência e de todos os envolvidos;
- Promover valores societários;
- Avaliar e determinar controles com níveis aceitáveis de riscos;
- Ter a segurança como um elemento essencial dos sistemas de informações;
- Ação preventiva e detecção de incidentes ligados a segurança;
- Garantir o entendimento acerca da Segurança da Informação;
- Avaliação contínua da Segurança da Informação.

A norma 27000 trata a segurança em SI de maneira geral, onde qualquer sistema da organização deveria ter suas definições sobre segurança, seus controles e classificações. Tendo esta norma como base para itens em SGSI, soma-se as informações presentes na norma 28000, que foca a segurança em cadeias de suprimento, para auxiliar no desenvolvimento deste trabalho.

2.1.2.2 ISO 28000

A norma ISO 28000 é uma norma relacionada às questões de segurança em cadeias de suprimentos. Ela detalha os cuidados necessários para segurança ao longo do fluxo da cadeia, referente às ações das pessoas envolvidas e aos sistemas de gestão. Ela apresenta um modelo de Sistema de Gestão de Segurança para a Cadeia de Suprimentos (SGSCS) abrangendo questões de conformidade com políticas de gestão, e apresentando opções para a auto avaliação constante avaliação das ações planejadas para a segurança das organizações (ABNT, 2013).

Como parte de suas recomendações e especificações, ela inicia com a avaliação do risco de segurança, onde a organização precisa estabelecer e manter ativos os procedimentos para identificação e avaliação da segurança.

Esta avaliação deve incluir a possibilidade de determinados eventos, tais como apresentados na ABNT (2013):

a. Ameaças e riscos materiais/equipamentos, como falha funcional, dano incidental, dano intencional ou ato terrorista e criminal;
b. Ameaças e riscos operacionais, incluindo o controle da segurança, fatores humanos e demais atividades que afetem o desempenho, situação ou segurança das organizações;
c. Eventos da natureza que possam tornar ineficientes as medidas e equipamentos de segurança;
d. Fatores externos ao controle da organização, tais como falhas em equipamentos/serviços terceirizados;
e. Ameaças e riscos às partes interessadas, como não atendimento aos requisitos reguladores ou dano à reputação ou à marca;
f. Projeto e instalação de equipamentos de segurança, incluindo substituição, e manutenção;
g. Gestão de dados, informações e comunicações;
h. Ameaças à continuidade das operações.

A partir da identificação das possíveis ameaças à segurança, deve se definir processos para gerenciar o risco de ocorrência. É importante que a organização mantenha clara a relação das ameaças, da avaliação, e dos processos de gestão da segurança. Com isso, em caso de ocorrência de ataque, pode ser adotada uma ação para proteção (ABNT, 2013).

A avaliação de ameaças e definição dos processos de gerência deve também considerar o custo e o tempo desses processos. Estabelecer a relação do custo de proteção com o prejuízo da ocorrência de um evento de segurança é desafio nas organizações (ABNT, 2013).

Também são previstas ações a serem tomadas na ocorrência de um evento de falha de segurança. É necessário que a organização esteja coberta por procedimentos para poder avaliar se medidas prévias de segurança não tenham sido eficazes contra um ataque. Além da detecção e ação contra a falha

de segurança, também é necessária uma investigação do incidente, para que ações preventivas possam ser postas em prática e evitar que volte a ocorrer. Além disto, é previsto um processo de acompanhamento destas ações, não apenas verificando a resolução do problema com as ações tomadas, mas também para garantir que as medidas preventivas tenham sido implementadas corretamente (ABNT, 2013).

2.2 GERENCIAMENTO DA CADEIA DE SUPRIMENTOS

A cadeia de suprimentos (CS) representa uma rede de organizações, com ligações entre atividades para desenvolvimento de processos para geração de produtos e serviços (CHRISTOPHER, 2007). Visto a dificuldade de uma única organização possuir todas as etapas da cadeia, a Gestão da Cadeia de Suprimentos (GCS) envolve o relacionamento das organização que fornecem e recebem os insumos e informações necessárias para a fabricação, montagem e desenvolvimento do produto ou serviço a ser disponibilizado ao consumidor final (BALLOU, 2006).

Toda a CS é baseada em processos definidos pelo relacionamento entre diversas organizações, controlando recursos humanos, materiais e informações, desde o fornecedor até o cliente final (GOMES, 2004). A GCS vem a ser a coordenação operacional e estratégica da integração dos fluxos de interação com as várias organizações envolvidas (BALLOU, 2006).

Com a profissionalização e o aumento da competitividade entre organizações, em um mercado quase que totalmente eletrônico, a velocidade e importância das informações ao longo da cadeia se tornam críticas (GUNASEKARAN e NGAI, 2004). São sistemas responsáveis pela organização da informação, mantendo os processos estáveis, em ordem, e garantindo a execução dos mesmos, de maneira veloz e segura, seja entre os setores internos da organização ou com fornecedores e clientes (GOMES, 2004).

A GCS é um conceito orientado a fluxos para integrar os recursos ao longo da cadeia (CHRISTOPHER, 2007). A partir do momento em que se identifica o potencial das vantagens competitivas que podem ser obtidas com uma GCS eficiente, as empresas perceberam a necessidade de indicadores e métricas

para auxiliar a monitorar seus processos, buscando melhores resultados (GUNASEKARAN *et al.*, 2001).

A GCS tem representado um novo e promissor desafio para empresas interessadas na obtenção de vantagens competitivas, e pode ser considerada uma visão expandida e atualizada da administração tradicional, abrangendo a gestão de toda a cadeia produtiva, de forma estratégica e integrada (GOMES, 2004). Christopher (2007) cita que a fonte da vantagem competitiva está na capacidade da organização de se diferenciar, aos olhos do cliente, de seus concorrentes.

Desta forma, torna-se um dos principais objetivo da GCS garantir a eficiência da cadeia para fornecer vantagens competitivas às organizações envolvidas (CHRISTOPHER, 2007). Para atingir este objetivo é necessário traçar estratégias e processos que auxiliem o fluxo de informações, produtos e serviços ao longo da cadeia (KETCHEN e HULT, 2007). Além dos processos de negócios para o correto funcionamento da cadeia, outros processos transversais suportam suas atividades, ou medem sua eficiência, em busca de melhorias, seja na agilidade, segurança ou custo de operações (GUNASEKARAN *et al.*, 2004).

A importância da GCS, somada às regulamentações e leis, como a redução de barreiras em nível global e a exigência por cuidados ambientais, faz com que ela passe a receber ainda mais atenção, seja para monitorá-la ou torná-la mais eficiente em relação a seus competidores (GUNASEKARAN *et al.*, 2004). Existe atualmente uma diversidade de métricas que suportam a GCS, nas mais diversas etapas da cadeia, como inventário, produção e distribuição (BEAMON, 1999). O aspecto financeiro talvez seja um dos mais importantes, por ser um dos fatores determinantes para um gestor na tomada de decisões e uma das principais métricas para medir a efetividade da cadeia (GUNASEKARAN *et al.*, 2004; CHRISTOPHER, 2007). Mas não se pode ignorar as vulnerabilidades de segurança que se apresentam ao longo da cadeia, principalmente na forma global como as GCS se apresentam, possuindo etapas ocorrendo em organizações menores ou com menores cuidado quanto a segurança dos processos da qual fazem parte (MARUCHECK *et al.*, 2011).

Estudos realizados referente ao âmbito financeiro e de segurança da GCS são significativos já há algum tempo (BALLOU, 2006; MARUCHECK *et al.*, 2011). As métricas para avaliar a cadeia evoluíram ao longo do tempo, tanto nos itens a serem medidos, como nos métodos de avaliação (BEAMON, 1999; SCC, 2010). Consequentemente, os modelos de GCS passaram a incorporar diferentes métricas que se mostravam importantes para as organizações, tais como perspectivas de custos, evolução de estratégias, níveis de segurança e métricas de operação, custo de inventário e combinação com a resposta do consumidor, prazos, possibilidade de esgotamento do estoque e taxas de entrega (BEAMON, 1999; GUNASEKARAN *et al.*, 2001). Dentro das métricas relacionadas à segurança, também incluem a segurança das informações que acompanham os processos e etapas ao longo da cadeia (ABNT, 2013). É necessário que sejam utilizadas ferramentas de monitoramento de risco e planos para mitigar a ocorrência de falhas que permitam o dano às informações e à GCS (MARUCHECK *et al.*, 2011).

Com a necessidade da avalição de desempenho para identificar oportunidades de melhorias nos processos da CS, estudos passaram a ser realizados, e modelos foram desenvolvidos (BALLOU, 2006). Um destes modelos é o SCOR (*Supply Chain Operations Reference Model*) que será apresentado a seguir. Nas seções posteriores ainda serão abordados conceitos da GCS aplicados à área hospitalar e da saúde como um todo e, por fim, na seção 2.2.3, será apresentado o conceito de GRC (Governança, Risco e Conformidade).

2.2.1 Modelo de Gestão de Cadeia de Suprimento

A GCS tem representado um novo e promissor desafio para empresas que buscam vantagens competitivas (GOMES, 2004). O sucesso das organizações podem depender de uma habilidade gerencial que organize e coordene as atividades que permeiam as fases e todas as organizações envolvidas (MIN e ZHOU, 2002). Isso fez com que diferentes organizações tenham criado modelos definindo processos e métricas para auxiliar na gestão. Nesta seção será analisado um dos modelos e um detalhamento sobre os indicadores de performance da GCS.

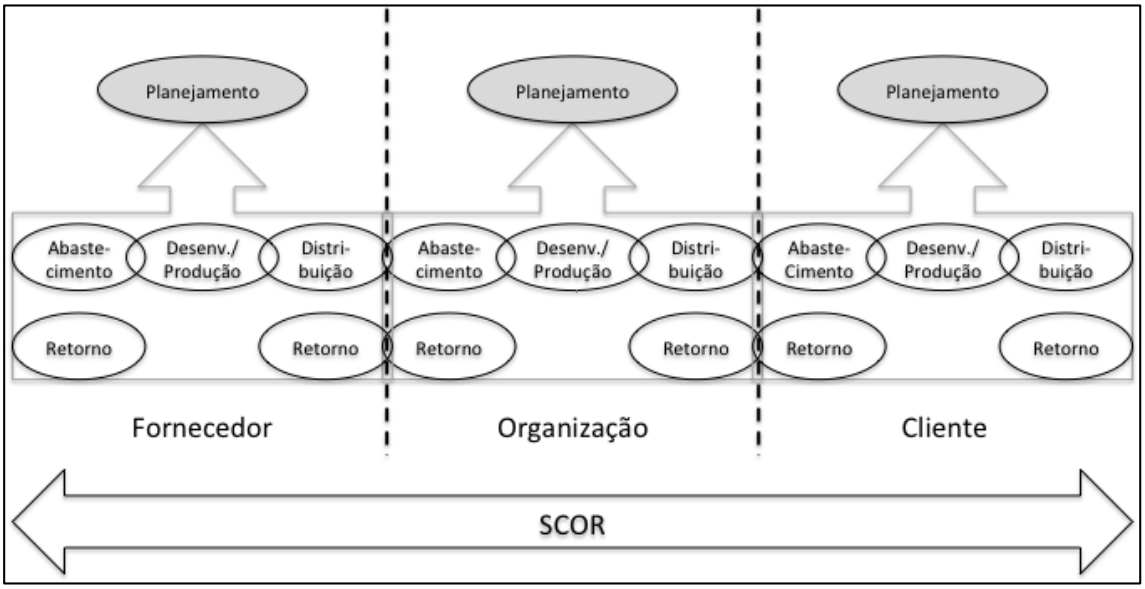
O modelo SCOR (*Supply Chain Operations Reference Model*) é um modelo criado pelo *Supply-Chain Council* (SCC), uma organização global, sem fins lucrativos, na qual a metodologia, diagnóstico e ferramentas de benchmarking ajudam organizações a realizarem melhorias em seus processos de negócios na CS buscando melhores lucros, qualidade e performance (SCC, 2010; LI *et al.*, 2011). O SCC estabelece o SCOR como um modelo para avaliação de evolução, comparação de atividades, e indicadores de performance de CS (SCC, 2010).

Segundo Ballou (2006):

> O modelo SCOR proporciona uma maneira de definir as atividades de cadeia de suprimentos em um formato padronizado, analisando a interorganizacionalidade da cadeia de suprimento no nível do produto, e comparando desempenho com estatísticas proporcionadas por empresas filiadas ao conselho (SCC).

O modelo SCOR é divido em quatro níveis, sendo que o Nível 1 é aquele que apresenta os processos de negócio principais do modelo (LOCKAMY III e MCCORMACK, 2004). O Nível 1 pode ser visualizado na Figura 1. Ele é decomposto em níveis inferiores para detalhamento das operações de cada organização (BALLOU, 2006). O Nível 2 trata da configuração dos processos e sua categorização. O Nível 3 é composto por processos elementares, é a decomposição dos processos do Nível 2. Por fim, o Nível 4, que é constituído do detalhamento das atividades internas de cada empresa, inclusive do que lhe dá vantagens frente a competidores, mas ele não é detalhado pelo modelo SCOR (SCC, 2010).

Figura 1 – Modelo SCOR – Nível 1



Fonte: SCC (2010)

O Nível 1 do SCOR compreende cinco processos. Estes processos, se repetem por todas as organizações da cadeia (Fornecedor – Intermediário – Cliente) e possuem pontos de integração entre essas organizações.

O primeiro processo é o de Planejamento. Ele descreve as atividades relacionadas com as operações da CS, e inclui os requisitos dos consumidores, a coleta de informações sobre a disponibilidade de recursos, e o balanço dos requisitos e recursos para determinar as capacidades da CS (LOCKAMY III e MCCORMACK, 2004; SCC, 2010).

O segundo processo é o Abastecimento, que descreve a ordem e o recebimento de produtos e serviços. Ele possui base em processos que incluem emissão de ordens de compra, agendamento de entregas, recebimentos, validação de expedição, armazenamento, e aceite de faturas de fornecedores. Além disso, ainda inclui o compartilhamento do planejamento e de informações com os fornecedores (LOCKAMY III e MCCORMACK, 2004; SCC, 2010).

O terceiro processo é o que define as atividades de Desenvolvimento e Produção das organizações. Ele descreve as atividades associadas com as conversões de materiais e/ou criação de conteúdos para serviços (SCC, 2010). As atividades são colaborativa entre os participantes da cadeia, desde o

fornecedor até o distribuidor e consumidor, estabelecendo parâmetros para a performance da cadeia (LOCKAMY III e MCCORMACK, 2004).

Distribuição é o quarto processo do modelo. Ele descreve as atividades associadas com a criação, manutenção e cumprimento das solicitações dos clientes, incluindo o recebimento, validação, criação das solicitações, agenda de entrega, empacotamento, envio e emissão da nota fiscal (LOCKAMY III e MCCORMACK, 2004; SCC, 2010).

O quinto e último processo é o de Retorno. O processo de Retorno descreve as atividades associadas com o fluxo dos produtos devolvidos pelos clientes. O processo de retorno inclui atividades como a identificação do que necessita devolução, agendamento da devolução, envio e recebimento do produto devolvido (SCC, 2010).

Cada um dos processos acima citados possuem uma vasta gama de indicadores. Estes indicadores procuram medir a performance de cada um dos processos acima citados.

A seção de Performance do SCOR baseia-se em dois elementos: (i) Atributos de Performance e (ii) Métricas. O (i) Atributo de Performance é composto por um grupo de Métricas, as quais são utilizadas para guiar as decisões estratégicas. Já as (ii) Métricas medem a habilidade da CS em atingir as estratégias definidas (SCC, 2010).

As métricas diagnosticam a saúde geral da CS com base em resultados estratégicos que auxiliam na definição de metas realistas na composição dos objetivos definidos pela organização. O SCC recomenda que as organizações definam, pelo menos, uma métrica para cada um dos Atributos de Performance definidos no modelo SCOR.

Os Atributos de Performance são: Confiabilidade, Capacidade de Resposta, Agilidade, Custo e Gerenciamento de Ativos.

Confiabilidade é um atributo focado no cliente e endereça a habilidade de realizar tarefas como são esperadas, de acordo com o previsto como saída do processo. Métricas de confiabilidade tipicamente incluem: pontualidade,

quantidades e qualidades corretas. O KPI (*Key Performance Indicator*) do SCOR considera o perfeito cumprimento da solicitação (SCC, 2010).

Capacidade de Resposta descreve a velocidade na qual as tarefas são executadas. O KPI do SCOR considera o tempo necessário para uma resposta, desde a solicitação, passando pelo recebimento até a resolução (SCC, 2010).

Agilidade descreve a habilidade de resposta por influências externas, tais como: aumento ou redução de demandas não previstas; fornecedores ou parceiros saindo do negócio; desastres naturais; atos de terrorismo ou cyber-terrorismo; disponibilidade de ferramentas financeiras; ou problemas trabalhistas. O KPI do SCOR inclui medições de flexibilidade e adaptabilidade para indicar se o atributo está atendendo corretamente o cliente (SCC, 2010).

O Gerenciamento de Ativos, que descreve a habilidade de utilização de ativos de forma eficiente e incluem redução de inventário e avaliação entre atividades internas e terceirizadas. As métricas incluem o número de dias para realização destas atividades (SCC, 2010).

Custo é o atributo que descreve o custo de operação do processo, tais como de trabalho, material e transporte. O KPI do SCOR para custos inclui custo de produtos, vendas e de GCS (SCC, 2010).

O atributo que avalia a saúde financeira da cadeia é o de Custos. Este indicador auxilia a medição da eficiência financeira da cadeia, onde cada uma das suas etapas é monitorada e medida para extrair resultados. Outro indicador de Custo é o de Custo de Mitigação de Riscos, que envolve o custo de mitigação de riscos ao longo da cadeia, ou mesmo o dano financeiro para a cadeia em caso de algum problema ocorrer.

Indicadores de Custos podem ser utilizados pelas organizações da CS da Saúde para medir seus esforços de investimentos em Segurança da Informação. Além disso, podem auxiliar a verificação da eficiência destes investimentos frente as possíveis impactos quanto aos riscos de um ataque ou falha ocorrer.

2.2.2 Gestão da Cadeia de Suprimento da Saúde

Cadeias de Suprimento da Saúde são um pouco diferentes de cadeias tipicamente industriais. Isso ocorre por uma série de fatores, como cita Chen *et al.* (2013):

- As operações precisam de materiais muito específicos para poder atender às diversas necessidades dos pacientes;
- Os Hospitais utilizam os mais diversos fornecedores, para adquirir todo o tipo de materiais, inclusive de alto valor;
- A área da saúde ainda não estabeleceu codificação padrão para todos os produtos que são consumidos, como já ocorre em outras áreas;
- A diversidade de suprimentos a serem adquiridos é grande, visto que é uma área de constante atualização quanto a novos procedimentos e novos medicamentos.

A CS da Saúde possui uma complexidade maior que as cadeias de outras áreas, mas isso não significa que não haja a mesma preocupação por seu aperfeiçoamento (MUSTAFFA e POTTER, 2009). Ela tem sido estudada e tem apresentado resultados importantes para a melhora da performance das organizações e da CS, prevenindo erros médicos, melhorando serviços de atendimento ao paciente e melhorando a eficiência operacional do hospital (LEE *et al.*, 2011).

Mesmo sendo áreas diferentes, algumas técnicas provenientes de outros segmentos estão sendo adotadas na CS da Saúde, apesar de que sua adoção enfrenta diversas barreiras de conhecimento para que seja mais largamente aceita (MUSTAFFA e POTTER, 2009). Analistas estimam que a GCS hospitalar, ou da área da saúde, está 10 anos atrás de outras cadeias como a CS de varejo e fabricação (CHEN *et al.*, 2013). Eles também discutem que há uma competição no mercado de CS contra CS ao invés de organizações contra organizações (KAZEMZADEH *et al.*, 2012).

A maioria dos estudos em GCS são aplicados à meios de produção e muito pouco coisa é feita voltada a saúde (CHEN *et al.*, 2013). Mesmo assim sistemas de saúde tem sofrido pressão internacionalmente por redução de

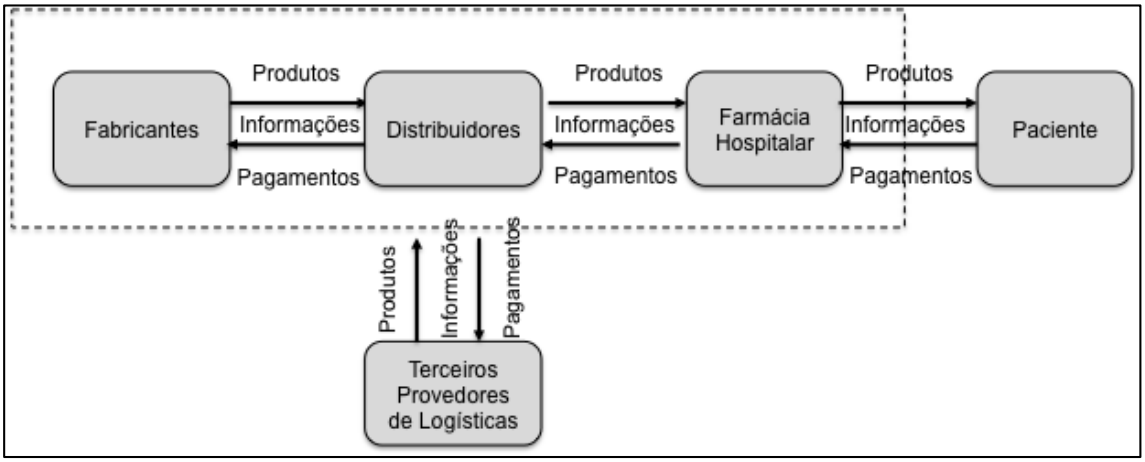
custos, melhora da qualidade e consistência no atendimento ao paciente (KAZEMZADEH *et al.*, 2012). Existe uma necessidade muito grande para que sejam avaliadas e estudadas as implicações de um processo de GCS na saúde, com a integração de vários participantes, bem como da performance desta cadeia (CHEN *et al.*, 2013).

A CS da Saúde possui três aspectos críticos a serem observados: Informação, Suprimentos e Finanças (KAZEMZADEH *et al.*, 2012). Desta forma, Kazemzadeh define CS da Saúde como:

> Informações, suprimentos e finanças envolvidas com a aquisição e a locomoção de produtos e serviços desde o fornecedor até o cliente final de maneira a melhorar o atendimento clínico enquanto se controla o custo.

A Figura 2 apresenta um modelo de CS da Saúde onde o foco são medicamentos. Este modelo é definido por Bhakoo e Chan (2011) na qual todos os participantes da cadeia possuem constante troca de informações entre eles em ambos sentidos, como por exemplo: Fabricantes enviam e recebem informações dos Distribuidores; ou Pacientes que trocam informações com o Hospital ou a Farmácia Hospitalar, informações estas que poderão ser, inclusive confidenciais, do estado de saúde do paciente. Já os produtos e serviços, seguem uma linha sequencial partindo do Fabricante até chegar ao Paciente. Por fim, o Dinheiro referente ao pagamento destes produtos ou serviços, percorrem o caminho contrário, partindo do Paciente até chegar ao Fabricante. Este modelo ainda conta com outro participantes, os Provedores de Logísticas, que atuam para transportar quaisquer dos três ativos principais da cadeia: Informações, Produtos ou Serviços e os Pagamentos. Alguns modelos colocam os Distribuidores como opcionais na cadeia, deixando a comunicação entre os Fabricantes e Hospitais de forma direta (KAZEMZADEH *et al.*, 2012).

Figura 2 – Cadeia de Suprimentos de Medicamentos



Fonte: (BHAKOO e CHAN, 2011)

A assistência à saúde passou a ser um problema: junto com erros médicos e segurança do paciente, existem os custos médicos para prestação da assistência (LEE *et al.*, 2011). Para apoiar no controle destes custos, entra a GCS para auxiliar o hospital na melhora de sua performance financeira e competitiva (LEE *et al.*, 2011). Estima-se que medicamentos farmacêuticos são os mais críticos para a prestação da assistência, pois precisam ser entregues dentro dos prazos requisitados e ser de alta qualidade pra uma assistência bem-feita (KAZEMZADEH *et al.*, 2012). Estima-se que 25 a 30% dos custos de hospitais sejam com medicamentos farmacêuticos, o que torna crítica a gerência destes produtos para a saúde financeira do hospital (KAZEMZADEH *et al.*, 2012). Este é um problema a ser alinhado com a GCS externa ao hospital, mas também controlado pelos setores internos da organização (LEE *et al.*, 2011).

2.2.3 Governança, Risco e Conformidade

GRC (Governança, Risco e Conformidade) é um *framework* que entrou rapidamente no mundo dos negócios (RACZ *et al.*, 2010). Independentemente, os três pilares separados (Governança, Gerência de Riscos e Conformidade) já eram difundidos e esclarecidos, mas em conjunto não eram unanimidade (RACZ *et al.*, 2010). Racz, Weippl e Seufert (2010) indicam GRC como:

> É a integração, aproximação de toda a organização com governança, gestão de risco e conformidade, garantindo que a organização aja com ética, dentro dos limites aceitáveis de riscos, políticas internas e externas, através do alinhamento das estratégias,

> processos, pessoas e tecnologia aperfeiçoando sua eficiência de toda a organização.

Atualmente o GRC está sendo mantido pela OCEG (*Open Compliance and Ethics Group*), a qual é composta por um grupo de especialistas de grandes organizações (OCEG, 2015). A OCEG se define como a organização que busca auxiliar as organizações a melhorar seu desempenho, aproximando as áreas de negócios, de forma a atingir os objetivos traçados, endereçando as adversidades e agindo de maneira íntegra (OCEG, 2012). O modelo da OCEG é dividido em duas partes (OCEG, 2012): (i) Resultados Universais e (ii) Componentes Integrados.

Resultados Universais são resultados esperados e observados, sendo composto por oito principais tipos (OCEG, 2012):

- Objetivos da organização;
- Melhoria da cultura organizacional;
- Aumento da confiança dos *stakeholders*;
- Preparar e proteger a organização;
- Prevenir, detectar e reduzir adversidades e fraquezas;
- Motivar e inspirar a conduta desejada;
- Melhorar a capacidade e eficiência das respostas;
- Otimização econômica e de valor social.

Componentes Integrados são os componentes que compõe o processo do GRC, e, embora sequenciais, podem ser definidos individualmente (OCEG, 2012):

- Contexto: cultura e os negócios da organização;
- Organização: organiza e supervisiona as capacidades da organização para atingir seus objetivos de maneira íntegra e endereçando incertezas;
- Avaliação: identificada as ameaças, oportunidades e requisitos de negócio;
- Pró Atividade: incentiva condições e eventos desejáveis, bem como previne que os indesejáveis ocorram;

- Detecção: identifica o progresso das atividades com base em controles e ações gerenciais;
- Resposta: responde a eventos desejáveis e corrige os indesejáveis;
- Mensuração: monitora e modifica as capacidades do GRC de forma periódica;
- Interação: captura, documenta e gerencia a informação do GRC.

GRC é constituído por quatro elementos: estratégia, processos, tecnologia e pessoas (RACZ *et al.*, 2010). Todos estes elementos devem ser vistos de forma integrada e holística por toda a organização, endereçando o GRC sempre alinhado com as operações de negócios (RACZ *et al.*, 2010). Com isso, pode-se atingir os principais objetivos do GRC, que tratam do comportamento ético e melhoria contínua da eficiência e eficácia de todos os processos envolvidos (RACZ *et al.*, 2010; OCEG, 2012).

Este *framework* tem sido incluído em sistemas grandes de ERP, como Oracle e SAP, para auxiliar as organizações nos seus controle e mitigação de riscos de forma coordenada com alinhamentos de governança de conformidade do mercado (SCHLEGEL e TRENT, 2014). Organizações participantes de CS na qual possuem processos utilizando conceitos de GRC, têm identificado uma melhor percepção quantos aos perigos do mercado ao qual estão diariamente expostos (SCHLEGEL e TRENT, 2014).

2.3 SEGURANÇA DA INFORMAÇÃO NA CADEIA DE SUPRIMENTOS DA SAÚDE

As informações presentes nos fluxos dos processos da GCS da Saúde são críticas, pois trata-se, dentre outras informações, da privacidade de seus pacientes, mas nem todos os funcionários percebem a necessidade de segurança da mesma forma (HEDSTRÖM *et al.*, 2011; MAGNAGNAGNO, 2015). O risco também existe para organizações parceiras, pois a exemplo dos fornecedores, poderiam ser lesados de alguma forma pela quebra de sigilo de negociações, ou mesmo receber ordens de compras inexistentes, que acarretaria em produção de equipamentos indesejados (WARREN e HUTCHINSON, 2000; GORDON *et al.*, 2015).

Organizações de assistência a saúde, estão começando a medir os impactos sobre problemas com a Segurança da Informação (HUANG *et al.*, 2014). Na maioria das vezes, quando é necessário escolher entre proteger as informações do paciente e a prestação da assistência a esse paciente, normalmente se opta pela segunda opção (HEDSTRÖM *et al.*, 2011). Quanto aos médicos, mesmo aceitando a responsabilidade de manter a confidencialidade dos dados dos pacientes, não tem a mesma percepção de responsabilidade de segurança quanto aos registros dentro dos sistemas do hospital (GAUNT, 2000). O que pode causar estranheza, pois esses registros estão diretamente relacionados a eles, são eles os principais profissionais de assistência e quem adiciona essas informações nos sistemas para posterior acesso a estas informações (GAUNT, 2000).

Consequência direta de qualquer investimentos é um acréscimo dos custos para o atendimento, mas é necessário verificar os possíveis investimentos quanto a vantagens que trarão para os hospitais (CHEN *et al.*, 2013). Com a gestão da informação, por exemplo, é necessário buscar um sistema que inclua segurança para a organização de forma adequada aos riscos que possam correr (LANDOLT *et al.*, 2012). Mas pra isso, estes riscos precisam ser levantados e analisados para que se chegue a medidas que possam mitigar os riscos dentro da capacidade da organização (LANDOLT *et al.*, 2012). As organizações tendem a buscar, de maneira isolada, formas de se proteger e arcam, muitas vezes, com elevados valores financeiros (HUANG *et al.*, 2014). As organizações menores acabam focando na proteção apenas das informações de pacientes, mas grandes organizações, como hospitais, deveriam ter um investimento mais abrangente, pois a possibilidade de prejuízo em caso de falhas ou ataques às informações pode ser muito significativo (HUANG *et al.*, 2014).

O balanceamento entre estes dois itens da avaliação de segurança (proteger e custo da proteção) é uma tarefa difícil (WARREN e HUTCHINSON, 2000). Apesar do extensivo número de pesquisas relacionadas à Segurança da Informação e as vulnerabilidades presentes nas organizações, há carência de estudos que aprofundem questões econômicas de segurança (GORDON e LOEB, 2002). Parte da dificuldade é devido à diversidade das empresas, visto que uma organização financeira precisa ter um cuidado maior com as

informações de clientes e suas contas, e hospitais tem uma preocupação maior quanto à informação dos pacientes (GUPTA *et al.*, 2006; CHEN *et al.*, 2013). Profissionais da saúde, em geral, pedem acesso a todas as informações do paciente para que realizem o atendimento, mesmo que não precisem de todos os dados (GAUNT, 2000). Os sistemas podem bloquear o acesso indevido às informações para garantir a integridade e confidencialidade das informações desse paciente, mas o balanceamento entre esses dois requisitos é o grande desafio (HEDSTRÖM *et al.*, 2011). Se estes sistemas receberem pouca atenção quanto a segurança dessas informações, o problema poderá ser ainda maior do que se não houvesse sistema algum (LANDOLT *et al.*, 2012).

Estudos sobre troca de informações de saúde classificam o investimento em segurança em três categorias: (i) o investimento individual da organização; (ii) a Segurança da Informação compartilhada; e (iii) o risco de propagação de um problema dentro do sistema de comunicação (HUANG *et al.*, 2014). Pela crescente importância da CS e a sistematização da mesma devido às necessidades de mercado, ela torna-se um alvo visado para ataques cibernéticos, aumentando ainda mais o risco de propagação dentro do sistema de comunicação da CS (WARREN e HUTCHINSON, 2000). Isso implica que ações de segurança em CS sejam cada vez mais reforçadas, embora isso também leve a um aumento de custo para a cadeia (GUPTA *et al.*, 2006). Quando organizações parceiras trabalham juntas para proteger suas informações, em geral, além de construírem uma segurança melhor para suas informações, normalmente ainda acabam reduzindo custos para implantar essa segurança (HUANG *et al.*, 2014).

Ações relacionadas a segurança da informação possuem diferentes frentes de ação para isolar vulnerabilidades (GUPTA *et al.*, 2006). Estas ações podem envolver atualização de tecnologia para minimizar vulnerabilidades, onde estendem-se os controles de segurança aos pontos de acessos de médicos e técnicos. Mas as organizações não costumam fazer avaliação e análise de riscos então, não percebem o tamanho do problema que estão deixando descoberto. Seria importante que analisassem os riscos de segurança e um dos guias existentes é a ISO 27000 (GAUNT, 2000; GUPTA *et al.*, 2006; SAMY *et al.*, 2010).

Outras ações estão relacionadas a processos de negócios. Talvez uma das ameaças mais significantes sejam os funcionários. Políticas precisam ser claras e consistentes para não resultar em confusão e causar danos aos pacientes, e precisam de programas de conscientização para que os funcionários não cometam falhas que causem danos aos sistemas de informação (MAGNAGNAGNO, 2015). As organizações da saúde costumam ter termos de responsabilidades para seus funcionários, mas dificilmente fazem uma revisão desses termos de forma periódica, confiando apenas nos contratos e códigos de conduta (GAUNT, 2000; GUPTA *et al.*, 2006).

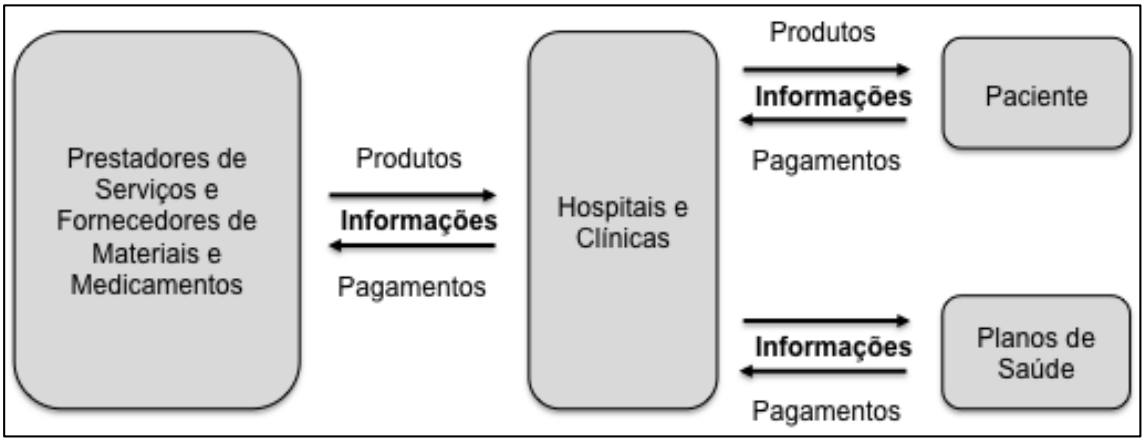
Assim que uma falha é identificada, ela precisa ser corrigida, evitando a possibilidade de reincidência (BOJANC e JERMAN-BLAŽIČ, 2008). Economicamente, isso pode não ser sempre viável, mas deve-se explorar as possibilidades (GORDON e LOEB, 2002). Vulnerabilidades não tratadas podem ser exploradas resultando em prejuízos para a organização (GUPTA *et al.*, 2006). Estes prejuízos podem não ser restritos ao aspecto financeiro, pois podem comprometer a credibilidade da organização no mercado frente aos seus clientes e fornecedores (WARREN e HUTCHINSON, 2000).

3 MODELO CONCEITUAL DA PESQUISA

Para a construção do modelo foram considerados conteúdos da revisão de literatura, tais como: Segurança da Informação e GCS voltada a área da saúde. A revisão apresenta que na busca por melhores resultados, as organizações passaram a organizar seus processos de maneira transversal e integrada entre organizações parceiras pertencentes a mesma CS (MIN e ZHOU, 2002; BALLOU, 2006). Essa integração inclui um compartilhamento de informações importantes para a CS que necessitam serem seguradas pelas organizações, mas não de forma unitária, mas conjunta dentro da cadeia (GOMES, 2004; GORDON *et al.*, 2015). Mesmo sendo mais complexa, a GCS da Saúde também busca constantemente por oportunidades de melhorias (LEE *et al.*, 2011; CHEN *et al.*, 2013). Hospitais e parceiros buscam uma relação mais próxima para aperfeiçoar seus processos e melhorar a performance da CS e assegurar as informações com as quais lidam para o atendimento ao paciente, bem como informações estratégicas para o negócio (MUSTAFFA e POTTER, 2009; LEE *et al.*, 2011; CHEN *et al.*, 2013).

Um modelo de CS para a saúde adaptado para a realidade brasileira, onde Planos de Saúde tem um papel importante, pode ser visualizada pela Figura 3.

Figura 3 – Cadeia de Suprimento da Saúde

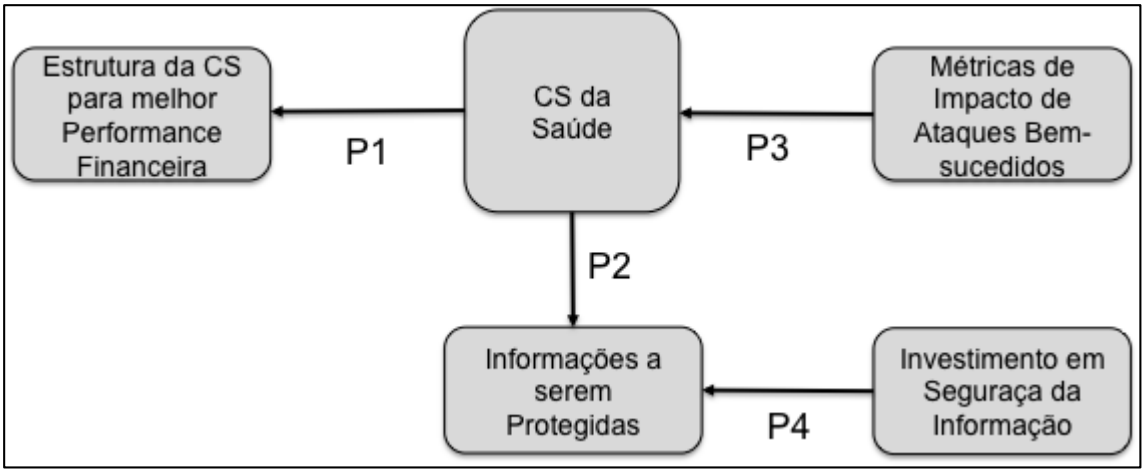


Fonte: Modelo elaborado a partir de Bhakoo e Chan (2011) e Kazemzadeh *et al.* (2012)

Os prestadores de Serviço e Fornecedores, principalmente de Materiais e Medicamentos para o atendimento aos pacientes, por mais que possam existir atravessadores, podem também possuir um canal direto de relacionamento com Hospitais, Clínicas e outros pontos de assistência à saúde (KAZEMZADEH *et al.*, 2012). Eles fornecem todos os materiais necessários para que as instituições assistenciais possam efetivamente atender aos pacientes, sejam com produtos cirúrgicos ou medicamentos (BHAKOO e CHAN, 2011). As organizações de atendimento à saúde do paciente, encontram-se mais centralizadas na cadeia, obtendo um contato direto para prestação de serviços, troca de informações e recebimento de pagamento com ele, que é o cliente final da cadeia (BHAKOO e CHAN, 2011; KAZEMZADEH *et al.*, 2012). No Brasil, há uma grande diversidade de Planos de Saúde que intermediam os pagamentos dos procedimentos efetuados em pacientes segurados e estes Planos de Saúde tem uma comunicação muito forte com instituições de assistência à saúde para efetivamente trocar informações e efetuar os pagamentos apropriados (MAGNAGNAGNO, 2015).

Partindo do modelo de CS da Saúde apresentada na Figura 3, busca-se a compreensão das suas ações relacionadas à Segurança da Informação como organizações e como CS. Assim, para auxiliar a busca dos objetivos propostos foi desenvolvido um modelo conceitual, apresentado a seguir pela Figura 4:

Figura 4 – Modelo Conceitual



Fonte: O Autor

Como visto anteriormente, Cadeias de Suprimentos buscam por uma gestão integrada de seus processo entre as organizações participantes de forma a serem mais colaborativas entre elas e obterem melhor resultados em suas operações, produtos e serviços (GUNASEKARAN e NGAI, 2004; BALLOU, 2006). Com essa premissa, formula-se a primeira proposição:

Proposição 1: As organizações pertencentes a Cadeia de Suprimento são integradas e colaborativas.

Diferentes e complexos sistemas para o controle de todas as atividades organizacionais, incluindo aspectos de CS, são constantemente adotadas pelas organizações (GUPTA *et al.*, 2006). Isso leva ao aumento na necessidade de proteger adequadamente as informações trafegadas nestes sistemas, para assegurar o sucesso da organização (GORDON *et al.*, 2015).

Ataques cibernéticos ocorrem em vulnerabilidades de sistemas, hardware ou pessoas (CERT.BR, 2015). As informações são a base para a tomada de decisão nas organizações, assim sendo, é de extrema importância que sejam íntegras e estejam disponíveis quando necessário, além de ficarem fora do alcance de pessoas não autorizadas (BRAGANÇA, 2010). Os ataques tendem a atingir, direta ou indiretamente estas informações, que sejam importantes para as organizações, pois são elas que trazem algum benefício competitivo para a organização (BOJANC e JERMAN-BLAŽIČ, 2008). Na CS da Saúde existem informações de fornecedores, pacientes, valores de transações, dados de entrega, entre outros (BALLOU, 2006; CHEN *et al.*, 2013). Cada uma destas informações tem uma importância específica e um risco de dano em cada organização (WARREN e HUTCHINSON, 2000; GORDON *et al.*, 2015). Com isto, apresentam-se a Proposição 2:

Proposição 2: As organizações conhecem as informações críticas a serem protegidas para a organização e para a Cadeia de Suprimento.

Na constante busca por melhores resultados, as organizações possuem diversas métricas para avaliarem seu desempenho (GUNASEKARAN e NGAI,

2004). Essas métricas auxiliam as organizações em suas avaliações individuais, mas também podem ajudar a medir a performance financeira da cadeia da qual fazem parte (SCC, 2010). Em paralelo, existe a preocupação com a proteção de suas informações, como as de pacientes que exigem confidencialidade, pois trata-se de informações delicadas dos mesmos, de seu estado e suas condições. Estas mesmas informações precisam estar sempre disponíveis e corretas para que os médicos possam utilizá-la para o tratamento do paciente (MAGNAGNAGNO, 2015). Sabendo que as organizações podem se tornar alvos de ataques ou mesmo sofrer com falhas internas de segurança, é necessária que elas considerem os riscos de falhas em suas informações ocorrerem e o impacto disso em sua performance financeira. Estas informações poderão ainda, auxiliar as organizações na tomada de decisão sobre as quantias financeiras cabíveis para investir na proteção destas informações (GORDON e LOEB, 2002; BOJANC e JERMAN-BLAŽIČ, 2008). Assim, apresenta-se a Proposição 3:

Proposição 3: As organizações possuem métricas dos impactos sobre a organização e sobre a Cadeia de Suprimento em caso de ataques à informações bem sucedidos.

As informações têm um papel importante nas organizações, seja para tomada de decisão ou para desenvolverem produtos ou serviços para seus clientes (GUNASEKARAN e NGAI, 2004). Além de informações estratégicas e financeiras, a CS da Saúde trata com dados de pacientes, os quais deve sempre estar fora do alcance de pessoas não autorizadas e ao mesmo tempo integralmente disponíveis para os prestadores de assistência (BALLOU, 2006; BRAGANÇA, 2010). Estas informações devem ser identificadas e tratadas de forma diferenciada pelas organizações, por isso é necessário que participantes da CS da Saúde possuam ações e investimentos específicos para garantir a segurança de suas informações, bem como as informações que trafegam ao longo da cadeia (BOJANC e JERMAN-BLAŽIČ, 2008; HUANG *et al.*, 2014). Com isso, é apresentada abaixo a Proposição 4:

Proposição 4: Informações críticas para a organização e para a Cadeia de Suprimento recebem investimentos em ações de Segurança da Informação de forma especializada.

Para a realização da verificação de cada uma das proposições acima, será efetuada uma pesquisa qualitativa em organizações pertencentes a CS da Saúde. O detalhamento do método desta pesquisa é apresentado no capítulo a seguir.

4 MÉTODO DE PESQUISA

A pesquisa científica é realizada quando se tem um problema e não há informações suficientes para solucioná-lo (CHIZZOTTI, 1991). A busca dessas informações pode ocorrer de diferentes formas, como por exemplo, a partir de observações, reflexões pessoais, de pessoas com experiência ou estudo, ou mesmo na própria literatura (CHIZZOTTI, 1991; KERLINGER, 2009). A utilização adequada destas fontes auxilia o pesquisador na delimitação do tema e provê meios para a resolução dos problemas da pesquisa (CHIZZOTTI, 1991).

Este capítulo apresenta aspectos metodológicos para o desenvolvimento da pesquisa, tal como a definição do método (seção 4.1), a elaboração e validação do instrumento (seção 4.2), coleta dos dados (seção 4.3) e, por fim, análise dos dados (seção 4.4).

4.1 DEFINIÇÕES METODOLÓGICAS

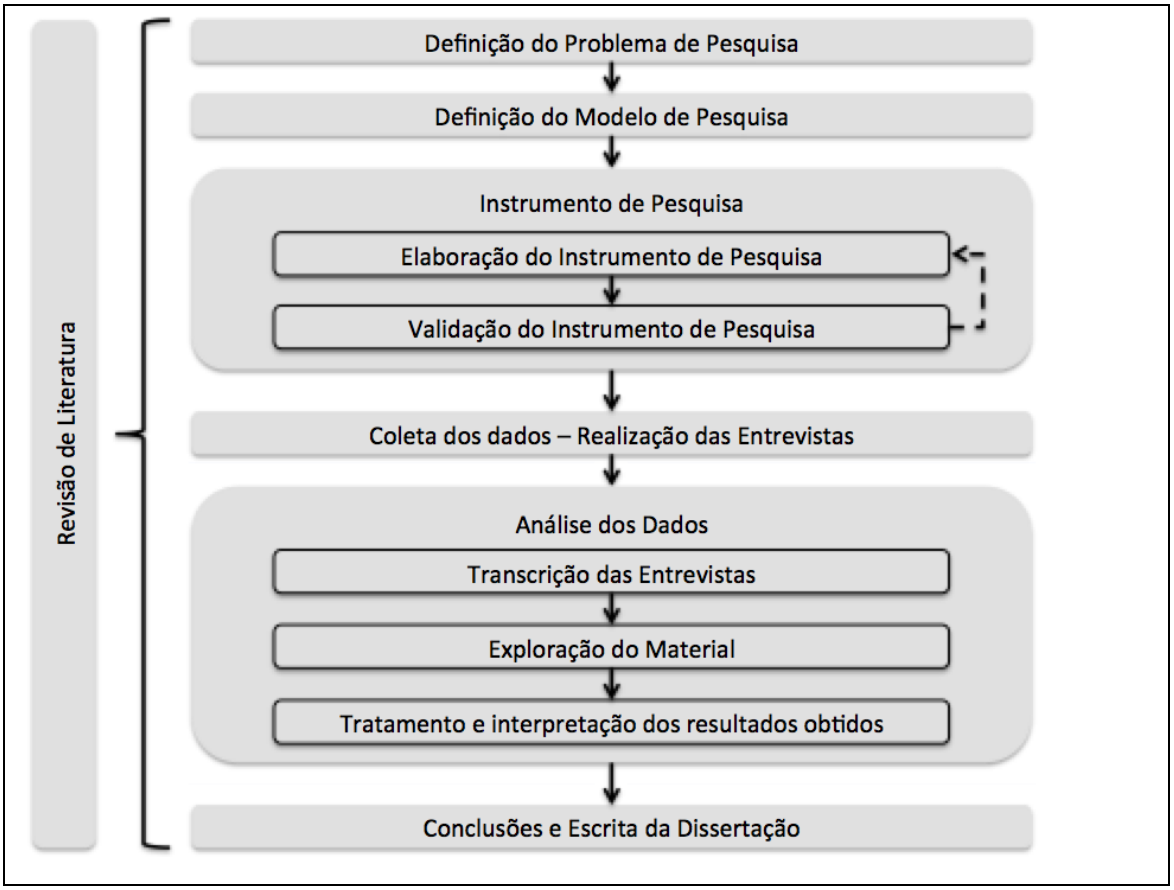
Existem duas estratégias de pesquisa: a (i) quantitativa, que se baseia em cálculos e estatísticas para números e dados obtidos durante o levantamento; e (ii) a qualitativa, que procura compreender e explicar práticas e situações que permeiam o meio em que estas práticas e situações estão dispostas (BARDIN *et al.*, 1979; CHIZZOTTI, 1991).

Para o desenvolvimento deste trabalho foi utilizada a estratégia de pesquisa qualitativa, pois os textos são seu material empírico e o interesse está, principalmente, nas perspectivas dos entrevistados, em suas práticas e conhecimento quanto à questão em estudo (FLICK, 2009). Neste modelo não existem hipóteses previamente definidas (SAMPIERI *et al.*, 2013). Ela se abstém de estabelecer conceitos bem definidos do que é estudado e suas proposições criadas não são exatas ou específicas (GIBBS, 2009; SAMPIERI *et al.*, 2013). Busca-se a experiência dentro do material analisado, bem como a interpretação desse material e das respostas colhidas nas entrevistas pelo pesquisador (GIBBS, 2009; SAMPIERI *et al.*, 2013). Após a coleta, não se utiliza medições numéricas para responder aos questionamentos, mas a interpretação das respostas coletadas (SAMPIERI *et al.*, 2013).

A técnica de entrevista é bastante utilizada em pesquisas de ciências sociais por ser adequada para a obtenção das informações que os entrevistados possuem acerca do assunto a ser estudado (GIL, 2010). A abordagem qualitativa busca abranger uma compreensão específica do assunto na visão do entrevistado (FLICK e NETZ, 2004). Na busca pela percepção dos profissionais da CS da Saúde, define-se que a unidade de análise da pesquisa serão os próprios profissionais, sua visão unitária da própria organização, do meio em que ela se encontra e das relações externas com seus parceiros.

O trabalho foi dividido em uma série de etapas sequenciais, desde a definição do problema, a coleta dos dados, sua análise e apresentação de resultados. Isso tudo sempre alinhado com a revisão da literatura. O desenho da pesquisa está representado pela Figura 5.

Figura 5 – Desenho de Pesquisa



Fonte: O Autor

O desenho de pesquisa auxilia o pesquisador com a esquematização das etapas da pesquisa, deixando mais claro o que deve ser feito ao longo do trabalho (FLICK, 2009). A primeira atividade realizada foi a definição do problema

de pesquisa. A partir deste ponto, iniciou-se a revisão da literatura para compreender melhor o cenário atual, as áreas envolvidas e o próprio problema a ser estudado. A mesma revisão foi também utilizada como um guia da pesquisa, mas que poderá ser revista no decorrer da pesquisa caso seja necessário (SAMPIERI *et al.*, 2013). Na etapa seguinte foi realizada a definição do instrumento de pesquisa, o qual deve auxiliar no alcance dos objetivos traçados, além da validação do mesmo (FLICK, 2009). O instrumento será utilizado para a realização das entrevistas que, segundo Gil (2010), possibilita a obtenção de dados em maior profundidade, além de permitir que o entrevistador possa esclarecer possíveis dúvidas dos entrevistados acerta dos questionamentos propostos. As etapas envolvendo a elaboração e validação do instrumento é detalhada na seção a seguir.

4.2 ELABORAÇÃO E VALIDAÇÃO DO INSTRUMENTO

O objetivo do roteiro de entrevista semiestruturado é capturar a percepção dos entrevistados de maneira aberta, sem um direcionamento que possa limitar suas respostas (FLICK, 2009). A partir da definição do modelo de pesquisa, foi realizado um estudo bibliográfico para identificação das principais características dos assuntos abordados no trabalho (Segurança da Informação, Investimento em Segurança, GCS da Saúde). Com estas características identificadas, cruzando estas informações com os objetivos traçados no trabalho e ainda as proposições criadas, foi possível desenvolver a matriz apresentada no Quadro 2. A matriz divide a pesquisa por dimensões, objetivos de cada uma destas dimensões e as variáveis que as envolvem para serem posteriormente analisadas contra os dados coletados. Grande parte da definição das variáveis da matriz, principalmente no que se refere à segurança e informações, foram elencadas com o auxílio do Quadro 1 sobre ameaças à Segurança da CS. A matriz ainda apresenta os autores que suportam cada uma destas dimensões e variáveis.

Quadro 2 - Matriz de Dimensões

Dimensões	Objetivos	Variáveis	Autores

Estrutura da CS para um melhor fluxo de informações	Identificar o papel da organização na cadeia e o fluxo de informação, interna e externamente	• Fluxo de informações interno à organização • Fluxo de informações com parceiros da CS • Papel da organização na CS • Definição dos parceiros (fornecedores e clientes)	CROOM *et al.* (2000); GUNASEKARAN *et al.* (2001); MIN e ZHOU (2002); BALLOU (2006); CHRISTOPHER (2007); SCC (2010); CHEN *et al.* (2013)
Informações a serem protegidas	Analisar informações de maior relevância na empresa e na CS e seu tratamento ao longo da CS;	• Informações críticas a serem protegidas • Acessos à informação • Meios de comunicação com parceiros	GUTTMAN e ROBACK (1995); GAUNT (2000); WARREN e HUTCHINSON (2000); GOMES (2004); GUNASEKARAN *et al.* (2004); BOJANC e JERMAN-BLAŽIČ (2008); GORDON *et al.* (2010); HEDSTRÖM *et al.* (2011); CHEN *et al.* (2013); HUANG *et al.* (2014); ISO-IEC (2014)
Ameaças e ações de mitigação para a Segurança da Informação	Identificar a compreensão de ameaças e ações para mitigá-las	• Reconhecimento de ameaças e seus impactos • Ações de mitigação em sistemas • Ações de mitigação para funcionários • Monitoramento da informação	GUTTMAN e ROBACK (1995); GAUNT (2000); WARREN e HUTCHINSON (2000); BOJANC e JERMAN-BLAŽIČ (2008); PATEL *et al.* (2008); TEN *et al.* (2008); BOJANC *et al.* (2012); LANDOLT *et al.* (2012); HUANG *et al.* (2014); CERT.BR (2015); FORWARD (2015); GORDON *et al.* (2015); SAFA *et al.* (2016)
Investimentos em Segurança da Informação	Analisar como são definidos os investimentos de Segurança da Informação	• Avaliação de impacto de ameaças • Orçamento específico para Segurança da Informação • Impacto do investimento na performance financeira organizacional e da CS	WARREN e HUTCHINSON (2000); GORDON e LOEB (2002); GUPTA *et al.* (2006); BOJANC e JERMAN-BLAŽIČ (2008); TEN *et al.* (2008); BOJANC *et al.* (2012); HUANG *et al.* (2014)
Dados Pessoais e Organizacionais dos Entrevistados	Identificar respondentes	• Idade e gênero do respondente • Área de formação • Tempo de atuação profissional • Cargo na empresa • Tempo na empresa • Envolvimento com CS ou Segurança da Informação • Porte da empresa • Atividade principal da empresa	

Fonte: O Autor

Cada variável está relacionada com uma ou mais questões do roteiro de entrevista (Apêndice A) e da mesma forma, com as proposições apresentadas no capítulo anterior, conforme pode ser visto no Quadro 3.

Quadro 3 - Variáveis x Questões

Dimensões	Variáveis	Proposições	Questões
Estrutura da CS para um melhor fluxo de informações	Fluxo de informações interno à organização	P1	1, 2
	Fluxo de informações com parceiros da CS	P1	1, 2, 4
	Papel da organização na CS	P1	3
	Definição dos parceiros (fornecedores e clientes)	P1	5, 6
Informações a serem protegidas	Informações críticas a serem protegidas	P2	7, 8
	Acessos à informação	P2	9
	Meios de comunicação com parceiros	P2	10
Ameaças e ações de mitigação para a Segurança da Informação	Reconhecimento de ameaças e seus impactos	P3	11
	Ações de mitigação em sistemas	P4	13, 14
	Ações de mitigação para funcionários	P4	12
	Monitoramento da informação	P4	15
Investimentos em Segurança da Informação	Avaliação de impacto de ameaças	P3	16, 19
	Orçamento específico para Segurança da Informação	P4	17
	Impacto do investimento na performance financeira organizacional e da CS	P4	18

Fonte: O Autor

A validação do instrumento busca analisar se o instrumento estava corretamente construído em relação ao texto, tempo de resposta, representação da área de estudo e a mensuração frente aos objetivos do trabalho.

O instrumento foi validado junto a dois especialistas, um da academia e outro profissional da área da saúde (um gerente de TI de um Hospital), os quais sugeriram um único ajuste referente a formalidade das políticas de seguranças (Questão 12), para a obtenção da informação mais concreta do entrevistado, bem como uma comprovação maior sobre a instrução aos funcionários da organização. O ajuste foi realizado antes das entrevistas iniciarem, sendo assim, o mesmo instrumento pôde ser aplicado desde a primeira entrevista. Segundo Sampieri (2013) a validade por especialistas está vinculada a validade de conteúdo e define: “Refere-se ao grau em que aparentemente um instrumento de mensuração mensura a variável em questão, de acordo com especialistas no tema”.

A próxima seção apresenta o detalhamento da coleta dos dados para a pesquisa.

4.3 COLETA DOS DADOS

A pesquisa qualitativa deste trabalho foi desenvolvida com entrevistas semiestruturadas, cujo instrumento foi desenvolvido com base na revisão de literatura. A entrevista semiestruturada tem atraído interesse de pesquisadores, pois acredita-se que o entrevistado possa colaborar mais se puder abordar os temas mais abertamente, ao invés de responder a questionamentos diretos (CHIZZOTTI, 1991; FLICK e NETZ, 2004).

A pesquisa busca uma avaliação abrangente do problema, assim, foram entrevistados profissionais de empresas participantes da CS da Saúde. Estes profissionais fazem parte de 10 diferentes empresas das cidades de Cascavel, no Paraná, e Porto Alegre, no Rio Grande do Sul. As empresas participantes da pesquisa são diversificadas dentro da cadeia, contendo Laboratórios, Hospitais, Clínicas e um Plano de Saúde. Todos os participantes pertenciam a alguma CS da Saúde, mas não necessariamente da mesma cadeia.

Os entrevistados são o foco da pesquisa, por isso precisavam ter conhecimento da CS de que a organização faz parte e de Segurança da Informação, pois busca-se a análise das práticas em segurança das informações que trafegam na cadeia. Além disto, os mesmos precisavam estar diretamente envolvidos no processo de decisão sobre os investimentos que a organização precisa fazer no que tange à Segurança da Informação. Assim, buscou-se profissionais com capacidade para oferecer convergência nas informações coletadas pois o foco da pesquisa está no conhecimento dos mesmos (FLICK e NETZ, 2004). Os entrevistados selecionados enquadraram-se dentre os seguintes perfis:

- Profissional de TI: Gerentes, coordenadores, diretores ou CIOs. Que provêm as informações e suas análises aos demais participantes da administração para que as decisões sejam tomadas;
- Profissional da área administrativa ou financeira: Gerentes, diretores ou CEOs. Que tenham uma visão abrangente do negócio e que possam avaliar os impactos sobre ações de Segurança da Informação.

Foram contatados 20 profissionais de 13 diferentes organizações que se enquadravam nos perfis identificados na literatura como organizações

participantes da CS da Saúde e de acordo com a possibilidade de contato com os mesmos. A definição das empresas nas cidades contatas se deu acordo com a conveniência do Autor. Todas as empresas procuradas fazem parte da CS da Saúde dentre as quais se encontravam Hospitais, Clínicas, Laboratórios e Planos de Saúde de ambas as cidades (Cascavel – PR e Porto Alegre – RS).

Os contatos foram feitos via e-mail, com a carta de apresentação do projeto de pesquisa presente no Apêndice B, ou telefone. Dentre os contatos realizados, 11 profissionais de 10 organizações se disponibilizaram para a realização das entrevistas, sendo 3 profissionais de TI e 8 profissionais da área Administrativa de suas organizações. Acredita-se que os respondentes podem colaborar na busca dos objetivos deste trabalho pelo conhecimento dos mesmos sobre as organizações e sobre a CS da Saúde, bem como a existência de respondentes dos principais nodos da cadeia: Laboratórios, Hospitais/Clínicas e Planos de Saúde.

As entrevistas ocorreram de forma presencial, no local de trabalho de cada entrevistado entre os meses de Outubro e Novembro de 2015. Todas as entrevistas foram gravadas para posterior transcrição e análise. As entrevistas totalizaram 5 horas e 43 minutos de gravação, com média de 31 minutos por entrevista e totalizaram em 39 páginas transcritas, realizadas pelo próprio pesquisador, que buscou a essência das respostas obtidas. O detalhamento sobre a análise dos dados obtidos é apresentado na seção a seguir.

4.4 ANÁLISE DOS DADOS

A análise dos dados foi realizada através de Análise de Conteúdo, a qual surgiu na busca da compreensão de comunicações e foi desenvolvida através de diferentes técnicas que auxiliam o pesquisador na classificação e interpretação do material disponível (BARDIN *et al.*, 1979). Considerando as práticas elencadas por Bardin (1979), a análise é dividida em três etapas: (i) pré-análise, (ii) exploração do material e (iii) tratamento e interpretação dos resultados obtidos.

A primeira etapa envolve a transcrição das entrevistas que ocorreram após a conclusão das mesmas. As transcrições, conforme já citado, foram

realizadas pelo próprio pesquisador. Após as transcrições, uma primeira análise nos dados foi realizada junto a uma avaliação superficial dos mesmos para verificar se haviam sido colhidos os dados necessários para a realização do trabalho.

A etapa seguinte foi realizada com auxílio do software computacional NVivo para a análise dos resultados coletados. Primeiramente, foram agrupados os trechos das respostas de todos os entrevistados com características similares de acordo com as variáveis e dimensões definidas no Quadro 2, apresentado anteriormente, mesmo que as mesmas se encontrassem em diferente pontos da entrevista.

Na última etapa, tratamento e interpretação dos resultados obtidos, foi realizada a interpretação do pesquisador frente ao material estruturado na etapa anterior. Também foi realizada uma Análise Categorial que, segundo Bardin (1979), é uma operação de classificação de elementos de um conjunto por diferenciação e então reagrupadas por critérios previamente definidos. A partir desse agrupamento, fez-se uma codificação aberta, onde foram identificadas categorias iniciais de cada uma das variáveis com base nas frases extraídas das entrevistas. Em um segundo momento, fez-se uma codificação axial, onde as categorias foram ajustadas e agrupadas por semelhança, obtendo-se categorias intermediárias. Finamente, fez-se uma codificação seletiva para identificar e consolidar as categorias finais e avaliar a frequência em que as mesmas se fizeram presentes nos textos (SAMPIERI *et al.*, 2013). O resultado estão dispostos nos Quadros presentes na seção de Análise dos Resultados.

Durante a etapa de tratamento e interpretações dos resultados obtidos, as informações foram validadas com base em uma triangulação das respostas dos entrevistados (FLICK e NETZ, 2004). Estas respostas ainda foram cruzadas com a revisão da literatura para, posteriormente, as proposições poderem ser avaliadas, bem como o próprio objetivo do trabalho.

5 ANÁLISE DOS RESULTADOS

Neste capítulo são apresentados os resultados obtidos através das entrevistas realizadas. O capítulo está divido em três seções: (i) caracterização dos respondentes da entrevista; (ii) as análises e interpretações do pesquisador sobre o material coletado e, posteriormente o cruzamento desta análise com as proposições criadas anteriormente; e (iii) considerações finais da análise quanto aos objetivos propostos para a pesquisa.

5.1 CARACTERIZAÇÃO DOS RESPONDENTES

Foram entrevistados 11 profissionais da área da saúde, em laboratórios, hospitais, clínicas e planos de saúde, com perfis de administradores a CEOs. Por questões de confidencialidade, seus nomes e os nomes das organizações da qual fazem parte foram suprimidos e cada entrevistado será identificado com um código (Ex).

O Quadro 4 apresenta o detalhamento de cada um dos entrevistados. Já as suas responsabilidades dentro das organizações são explicadas a seguir:

- Entrevistado 1 (E1): é o responsável pelas análises do laboratório, mas também por todas as decisões referentes à aquisição de equipamentos ou de novas políticas de Segurança da Informação;
- Entrevistado 2 (E2): é o responsável por todas as decisões estratégicas e operacionais e está nesta função há 1,5 ano;
- Entrevistado 3 (E3): é o responsável por todos os sistema da empresa e é o responsável técnico por toda a informação que é apresentada para a diretoria;
- Entrevistado 4 (E4): é a responsável pela administração geral da empresa para a qual foi contrata recentemente;
- Entrevistado 5 (E5): é o responsável por toda a parte técnica da TI, principalmente avaliações de novos produtos para proteção da informação interna da empresa e está nesta função há 10 anos;
- Entrevistado 6 (E6): é o responsável por toda a administração financeira do hospital e está nesta função há 15 anos;

- Entrevistado 7 (E7): é o responsável por todo o complexo hospitalar incluindo unidades fora da cidade de Cascavel e está nesta função há 3 anos;
- Entrevistado 8 (E8): é o responsável pela administração geral do hospital e está nesta função há 8 anos;
- Entrevistado 9 (E9): é o responsável por manter os sistemas em pleno funcionamento e suportar as questões técnicas para a tomada de decisão da diretoria;
- Entrevistado 10 (E10): é o responsável por analisar incidentes e propor melhoria dos processos internos e de segurança e está nesta função há 12 anos;
- Entrevistado 11 (E11): é o responsável pela administração e operação da empresa, além de ser o responsável pelas decisões administrativas que envolvem a área de TI e está nesta função há 10 anos.

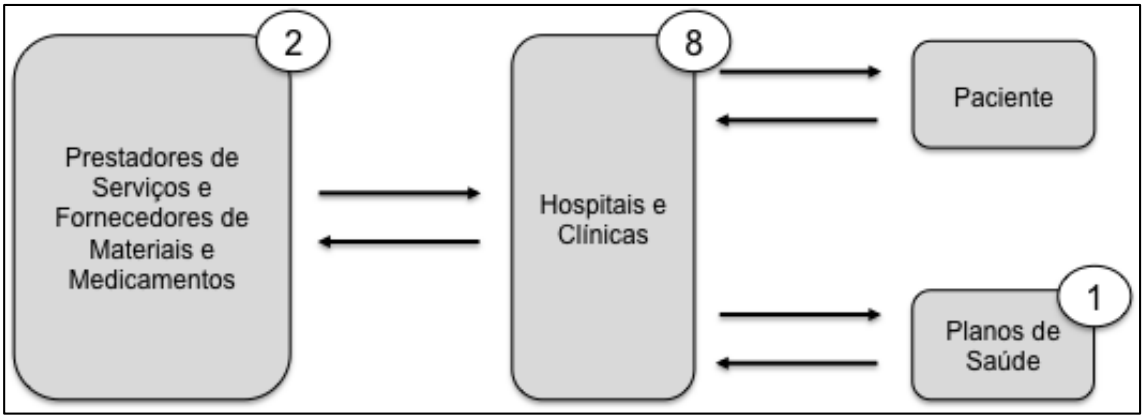
Quadro 4 - Caracterização dos Entrevistados

Código	Tipo de Empresa	Idade	Tempo de Atuação	Área de Formação	Cargo	Núm. Funcionários
E1	Laboratório A	62	30	Medicina	Sócio Proprietário	Até 100
E2	Laboratório B	45	21	Farmácia	CEO	101 à 500
E3	Clínica	30	15	Ciência da Computação	Coordenador de TI	Até 100
E4	Hospital A	37	10	Administração Hospitalar	Gerente Administrativa	Até 100
E5	Hospital A	39	20	Gestão da Informação	Coordenador de TI	Até 100
E6	Hospital B	50	38	Administração Hospitalar	Sócio Administrador	101 à 500
E7	Hospital C	37	14	Administração	Administrador Geral	501 à 1000
E8	Hospital D	43	19	Administração	Diretor Executivo	501 à 1000
E9	Hospital E	22	3	Sistemas de Informação	Administrador de Sistemas	101 à 500
E10	Hospital F	40	25	Administração Hospitalar	Consultor Técnico da Diretoria	2000
E11	Operadora de Plano de Saúde	47	16	Administração Hospitalar	Gestor de Operações	101 à 500

Fonte: Dados de Pesquisa (2016)

A Figura 6 apresenta a disposição dos entrevistados na CS da Saúde.

Figura 6 – Número de Entrevistados na Cadeia da Suprimentos



Fonte: O Autor

5.2 DIMENSÕES E VARIÁVEIS

Nesta seção será abordada a análise das entrevistas frente as dimensões e variáveis apresentadas anteriormente no Quadro 2. Cada variável será abordada individualmente e elas estão divididas dentre as quatro dimensões pré-definidas, quais sejam: (i) Estrutura da Cadeia de Suprimentos para melhor Performance Financeira, (ii) Informações a serem protegidas, (iii) Ameaças e ações de mitigação para a Segurança da Informação, e (iv) Investimento em Segurança da Informação.

Devido às perguntas serem abertas, muitas das informações providas pelos respondentes acabaram sendo mencionadas em diferentes questionamentos ou mesmo não aparecendo diretamente nas respostas fornecidas. Elas serão analisadas nas subseções a seguir de acordo com a dimensão e categoria de que fazem parte. A análise dos dados coletados assumirá diferentes óticas dentre as categorias tentando agrupar as repostas da melhor forma possível.

Ao final de cada subseção de dimensões, será realizada um análise da mesma abordando as variáveis abordadas, bem como uma análise categorial com as categorias identificadas de acordo com a exploração do material coletado através das entrevistas.

5.2.1 Estrutura da CS para um Melhor Fluxo de Informações

O objetivo desta dimensão era o de identificar o papel da organização na cadeia da qual as organizações fazem parte, além do fluxo de informação, interna e externa, e com seus parceiros (fornecedores e clientes).

5.2.1.1 Fluxo de Informações Interno à Organização

Todas as organizações possuem diversos processos para lidarem com as informações e operações do dia-a-dia, bem como com seus parceiros. Assim, os respondentes focaram em alguns destes processos para exemplificar o envolvimento na CS da organização. As análises foram divididas pelo tipo de organização: Laboratórios, Clínicas, Hospitais e Operadoras de Plano de Saúde.

Iniciando pelos laboratórios, o Entrevistado E1, devido a uma grande reformulação na organização, ainda não tem claro como será o processo adotado com a implantação de um novo sistema de gestão, segundo ele: *"Nesse momento, isso está confuso. Tudo é via papel, telefone e informações que os funcionários tem..."*. Já o Entrevistado E2, focou no seu processo básico de atendimento ao seu cliente, o paciente: *"...o ambulatorial, ele chega no cadastro e já é identificado e existe uma rastreabilidade do pré-analítico, analítico e do pós-analítico, ou seja, nós vamos até o resultado do exame... "*.

A clínica já focou seu processo de recepção, estoque e distribuição interno de medicamentos e materiais médicos, como comentado pelo Entrevistado E3:*"...temos uma pessoa responsável pelo almoxarifado que recepciona e separa, e a farmacêutica que responde pelos medicamentos. E agora estamos organizando a parte deste estoque, começamos a etiquetar tudo, já foi lançado no sistema e no começo do ano deve estar com todo esse fluxo..."*.

Ao entrarmos nos hospitais da CS, encontramos uma variedade maior de processos abordados pelos entrevistados, principalmente pelo maior número de empresas obtidas para a coleta de informações. De maneira geral, quase todos focaram seus processos que lidam com materiais médicos e medicamentos, como por exemplo o Entrevistado E8:

> [...] uma vez que é feita essa compra nós temos o TASY implantado em toda área administrativa do hospital integrado. Então... tanto faz comprar da

> Bionexo ou diretamente pelo hospital, ele vai gerar uma ordem de compra, essa ordem de compra vai cair de modo eletrônico, e também papel, esperando esse produto chegar no almoxarifado. Quando chegar, ele vai validar isso na nota fiscal, vai fazer com que dê entrada e o sistema vai fazer a confrontação da nota fiscal com a nota de compra... a ideia é lançar todas as notas no dia que ela chega, pra poder dar a entrada do produto no sistema e para abastecer o sistema de estoque. Depois o consumo disso: entra em caixa no almoxarifado e depois ele sai da caixa e é fracionado no CAF, que é o Centro de Abastecimento Farmacêutico, e do CAF ele abastece as farmácias. A gente tem farmácias satélites no centro cirúrgico, nas UTIs... e uma farmácia central... e essa farmácia central distribui por turno pra todas as alas, por paciente com rastreabilidade com código de barras pra tudo... o TASY vai baixado do estoque e vai dando ponto de pedido [...]

O sistema TASY, citado pelo Entrevistado E8, é um sistema de gestão administrativo com foco em serviços da saúde, desde laboratórios e clínicas, até hospitais e bancos de sangue (PHILIPS, 2015). Quase todos os hospitais pesquisados utilizam este mesmo sistema TASY para sua gestão que, conforme o Entrevistado E10, juntamente com o sistema MV (MV, 2015), utilizado pelo hospital em que atua, são considerados os principais sistemas de gestão do mercado: *"...toda a informação hoje, ela é dentro de um único sistema de gestão chamado MV. Que, acho que junto com o TASY, são os dois sistemas de maior volume, que tem em mais hospitais no Brasil..."*.

Já o sistema Bionexo, é um sistema que permite às organizações realizarem cotações e compras com uma grande base de fornecedores de insumos à hospitais e clínicas (BIONEXO, 2015). Seu funcionamento foi explicado pelo Entrevistado E9: *"...ela faz a solicitação pra Bionexo, ela publica como se fosse uma ordem de compra e aí os fornecedores alimentam aquele pedido com os valores... quase como uma licitação..."*.

Os processos abordados pelos hospitais, apresentaram a existência de responsáveis pelas cotações e compra dos materiais e medicamentos para os hospitais os quais, após serem entregues e entrados nos sistemas, são repassados para os setores competentes, por fim, são destinados aos setores que o utilizarão. Mas um dos respondentes também comentou de seu processo

com materiais que não são de uso constante dentro do hospital, órteses e próteses. O Entrevistado E10 diz:

> [...] quando vamos pra órteses e próteses... cada procedimento, cada evento dentro do hospital, que vai ser usado, o médico prescreve nos mínimos detalhes qual é a prótese que ele quer comprar: qual é o fabricante, qual é a marca, qual é o modelo, qual é a série, tudo, porque ela é extremamente específica[...]

O Entrevistado E10, também se diferenciou dos demais, além de ser o único a utilizar o sistema MV para a gestão do hospital, por ser um dos grandes hospitais a não efetuar as compras através do sistema Bionexo, mas através de práticas regulares de mercado, conforme informado pelo próprio Entrevistado: *"...a área de suprimento tem esse catálogo e essa normativa do que comprar com as características técnicas e geralmente é a prática de mercado normal, faz orçamento, 3 fornecedores, compra, entrega..."*.

Outro hospital que chamou atenção sobre seu fluxo interno, foi o do Entrevistado E6, que também é um grande hospital e não possui um sistema de gestão. Segundo ele: *"... eu tenho SPData (SPDATA, 2015) que me suporta na digitação da A.I.H. (Autorização de Internação Hospitalar), fazer o faturamento da A.I.H.... tenho o IDS (IDS, 2015) como o agendamento e arquivo de prontuário e aí a questão da contabilidade tem um arquivo/sistema específico, o RH tem um programa específico..."*.

Já a operadora de plano de saúde, por se tratar também de uma cooperativa, focou seu processo de atendimento do cooperado, conforme abordado pelo Entrevistado E11:

> Temos vários canais... quando a deliberação vem de um cooperado médico... eu tenho esse núcleo do cooperado... e ali é que tem a demanda, quando essa demanda vem, nós temos três gerências, a gerência de mercado, administrativa e operacional, eu sou operacional. Geralmente as demandas vem mais pra minha área, pode ser uma reclamação de tecnologia, não está funcionando em um consultório ou hospital. Aí vem essa demanda, por escrito, eu vou sentar com a área de TI, entender e aí vamos a campo, elaboramos uma resposta e devolvemos... se é prestador, eu tenho um outro canal, só com atendimento ao prestador, se é beneficiário, ou cliente, eu tenho a ouvidoria e a recepção [...]

Aplicando a técnica de análise categorial, chegou-se ao Quadro 5. E como pode-se verificar, os principais fluxos de informações considerados pelas organizações, quando se trata de CS, concentram-se nos processos de compra e rastreabilidade dos insumos, medicamentos e demais produtos utilizados. O que vai ao encontro da literatura que confirma que as organizações de CS e de hospitais tendem a focar suas atenções nos produtos manufaturados que circulam dentro delas (CHEN *et al.*, 2013). Ainda segundo a literatura, as organizações da CS da Saúde têm o conhecimento do que gera mais custo para sua operacionalização e possui um monitoramento destes custos para manter sua performance elevada ou mesmo sua saúde financeira estável (GUNASEKARAN *et al.*, 2001).

Quadro 5 - Categorias do Fluxo de Informações Interno à Organização

Categorias do Fluxo de Informações Interno à Organização	Frequência
Processo de Compra Insumos/Medicamentos	11
Rastreabilidade do Medicamento/Produto/Serviço	11
Processo de Compra Produto Especializado	9
Integridade da Informação	6
Sistema de Gestão	5
Rastreabilidade da Compra	4

Fonte: Dados de Pesquisa (2016)

Também foi citado pelos respondentes questões referentes aos sistemas de gestão e a preocupação com a integridade das informações. Sistemas de gestão são o centro de controle das organizações que gerenciam os processos de maneira mais eficiente, auxiliam o próprio funcionamento das organizações e ainda reforçam a segurança dessas informações, assim concordando com Min e Zhou (2002). Quanto à segurança, pode ser citado, a integridade das informações, visto que mantém o registro completo dos atendimentos a serem realizados e, principalmente, que estas informações sejam armazenadas de maneira legível aos seus usuários.

5.2.1.2 Fluxo de Informações com Parceiros da Cadeia de Suprimento

De maneira geral, poucas foram as informações identificadas que transitam entre os participantes da CS. As principais informações coletadas estão destacadas a seguir.

O Entrevistado E2 acabou se apresentando com uma das organizações com mais próximo relacionamento com um de seus clientes:

> Quando falo do segmento hospitalar... nós temos já uma integração com o sistema do [nome do hospital] que é o mesmo sistema do hospital [nome do hospital 2]... a gente tem uma integração total, ou seja, pacientes internados, pacientes no pronto-socorro, pacientes em rotinas de UTI... o paciente estando lá, já faz a identificação e já faz a solicitação através do sistema [...]

A grande maioria dos entrevistados destacou que com fornecedores são trocadas informações apenas de pedido de compra pelo sistema Bionexo, como informado pelo Entrevistador E3: "*(Quanto ao material médico) tudo isso é cotado no site da Bionexo... algumas coisas são consignadas, então o fornecedor deixa algumas coisas aqui, quando utiliza, já faz o repasse pra ele...".* Ou com operadoras de planos de saúde como citado pelo Entrevistado E6: *"...(a única informação que sai) é com os planos de saúde, com o próprio Ministério da Saúde onde você gerencia isso através dos arquivos fornecidos pelo próprio ministério..."*.

Dentre os hospitais, talvez o hospital do Entrevistador E10 tenha uma proximidade maior com algumas operadoras de plano de saúde, até por questões de circunstâncias: *"hoje, o mercado é muito regido pela operadora, são os planos de saúde que regem regras, normativas, valores, prazos, tudo são eles, então é aberto. Nas órteses e próteses em 100% delas o convênio fica sabendo o que, como, quando, o que foi comprado, porque ele paga sobre a nota fiscal de compra..."*.

Já sob a ótica da operadora do plano de saúde, há problema com a qualidade da informação, como citado pelo Entrevistado E11: *"O que nós mais sofremos é que nem sempre o que vem lá de fora realmente é, principalmente nessa área médica... nem sempre a informação que tem é certa, então você tem que depurar essa informação...".* Ele ainda comenta sobre as negociações e informações existentes entre a operadora e os provedores de assistência, como clínicas e hospitais, que ocorre todos os anos: *"...chama nossa atenção que, quando nós vamos negociar, a gente trás a vida dele (clínica ou hospital) toda... e agente nota que ele não tem. Então eu tenho essa informação e ele não tem*

essa informação, e não tem compartilhamento..." e ainda complementa: *"...na cadeia como um todo, se a relação fosse boa, e nem sempre ela é, você poderia compartilhar dados... o ideal é que tivesse esse compartilhamento*".

A análise categorial desta variável, Quadro 6, traz como item mais citado entre os entrevistados a comprovação da conclusão do pesquisador quanto aos relatos acima abordados: que as organizações da saúde não possuem um gerenciamento da CS propriamente dita, funcionam como um conjunto de organizações não colaborativas que dependem umas das outras.

Quadro 6 - Categorias do Fluxo de Informações com Parceiros da CS

Categorias do Fluxo de Informações com Parceiros da CS	Frequência
Falta de Relacionamento com Parceiros	8
Integridade da Informação	7
Sistema Cotação com Fornecedores	6
Compartilhamento de Informações	6
Relacionamento Direto	6
Cotação com Fornecedores	4

Fonte: Dados de Pesquisa (2016)

Como já afirmado, uma GCS envolve relacionamento das organização que fornecem e recebem os insumos necessário (BALLOU, 2006). A CS da Saúde existe pela definição pura do termo quando se ligam em busca da prestação de serviço, mas não há uma proximidade em busca de uma melhor relação entre as partes que, segundo Gunasekaran *et al.* (2001) e Christopher (2007), auxiliaria as organizações a atingirem melhores resultados.

A integridade das informações está presente novamente nesta variável como uma preocupação constante dos entrevistados. Mas o Compartilhamento de Informações e o Relacionamento Direto, apesar de estarem presentes entre os termos destacados não é positivo. Há uma negação da existência destas categorias, o que reforça a primeira categoria: a Falta de Relacionamento com Parceiros.

O Sistema de Cotação com Fornecedores é um ponto chave destacado pelos entrevistados para afastar o relacionamento entre as organizações. Estes sistemas funcionam como sites de leilão onde qualquer fornecedor se apresenta com o produto solicitado e o oferece a um preço que pode ser interessante pra organização e na próxima vez não será mais. Assim, não se criam vínculos entre

as organizações para uma maior integração entre as partes, o que é chave para uma melhora de performance entre os envolvidos (GUNASEKARAN *et al.*, 2001; MIN e ZHOU, 2002).

5.2.1.3 Papel da Organização na Cadeia de Suprimento

O questionamento voltado a coletar dados exclusivamente para essa variável (Qual a percepção quanto ao papel da empresa na CS?), mais uma vez demonstra o distanciamento entre as organizações. Inclusive, esse distanciamento foi perfeitamente explicitado pelo Entrevistado E2: *"(estamos) muito afastados... nós vivemos em continentes diferentes.."*.

A clínica compartilha desta visão, conforme comentado pelo Entrevistado E3: *"...com o uso da ferramenta (Bionexo), a gente diminuiu bastante o custo, mas assim, não tem hoje uma fidelização com o fornecedor específico... então fica meio na nuvem aquele negócio, meio nebuloso..."*.

Já os hospitais têm uma visão parecida em sua maioria, eles se veem como intermediários na cadeia, entre os mais diversos fornecedores e o cliente final, paciente, suportado pela fonte pagadora. O Entrevistado E7, comenta justamente da dificuldade desse papel:

> [...] (como ele vê o hospital na CS) Um grande absorvedor de problemas. Pelo seguinte, nós estamos no meio das duas pontas, uma que é a ponta que fabrica e comercializa e eu sou obrigado a comprar, porque eu preciso desse insumo, e na outra extremidade eu tenho quem paga. E aí, no meio está o hospital, que se vê por vezes necessário adquirir e não conseguir repassar a quem vai pagar, em especial SUS. Então a gente fica numa situação bastante complicada. Outra situação, o fornecedor de matéria prima tem o mercado livre, então ele determina o preço como ele melhor entender, só que na outra ponta eu tenha a ANS (Agência Nacional de Saúde) regulando quanto que o convênio poderá ter de reajuste e enfim, limitando as questões de cobrança [...]

Com uma abordagem parecida, mas destacando a percepção do cliente, o Entrevistado E8 diz: *"...ele (paciente) vem pra uma prestação de serviço... ele está preocupado em melhorar, ele quer o resultado, ele não está vendo o fornecedor do outro lado. Mas eu acho que é fundamental a gente ter produtos*

bons e fornecedores confiáveis... e fazer essa união. Só que na percepção do cliente final... ele não consegue enxergar isso.".

O entrevistado E10, corrobora com o E8 dizendo: *"... no mercado geral, o hospital é um atravessador, ele é um intermediador. O hospital desempenha um papel muito mais de farmácia do que hospital... o hospital vê muito do seu ganho no quanto ele compra de medicamentos e materiais e por quanto ele vende..."*, mas apresenta um plano do hospital para mudar um pouco essa abordagem: *"o [hospital]... puxou a discussão dizendo assim: eu não quero cobrar margem de comercialização, não me interessa... eu não quero ser o revendedor... mas eu quero ser muito bem pago pelo que eu faço e o que eu faço muito bem é assistência..."*, mas como ele mesmo complementa: *"...99% dos hospitais, eu vejo que eles são intermediadores dessa cadeia... o [hospital] como [outros hospitais no Brasil], estes hospitais estão buscando ser remunerados pela qualidade assistencial que fazem. Ainda é um paradigma...".*

Já o hospital de menor porte, tem uma percepção mais próxima da clínica. Segundo o Entrevistado E4:

> [...] não existe parceria... pelo que a gente consegue observar é que ele (empresa) não tem poder de compra tão grande, então ele acaba sendo mais um nesse processo da cadeia de fornecedores...mas hoje a gente compra ainda, pelo que eu pude observar, picado e as vezes isso que acaba nos deixando, frente aos fornecedores, como mais um [...]

Quanto à operadora do plano de saúde, o Entrevistado E11 abordou uma visão abrangente do tema em relação a operadora, colocando ela em vezes como provedora de serviços assistenciais e outras mais focada em ser cliente dessas organizações: *"... o primeiro problema hoje são as unidades da empresa... não tem um padrão de atendimento... então, em alguns lugares, ela é muito dependente do que a gente chama de prestadores, que são hospitais e clínicas, em outros lugares esses hospitais e clínicas são totalmente dependentes dela...".*

A análise categorial, apresentada no Quadro 7, confirma o que já foi citado pelos entrevistados acima sobre o relacionamentos entre os elos da CS: há pouco relacionamento entre as organizações da cadeia. Isso pode ser um reflexo

direto da inexistência de um gerenciamento desta CS da Saúde como indicado no atributo anterior. Eles buscam adquirir produtos e serviços para entregar os seus, mas não procuraram estreitar os laços de forma se aperfeiçoarem de maneira conjunta.

Outra categoria identificada pode ser vista como consequência da primeira: Foco em Resultados/Processos Internos. Se não há um relacionamento para um trabalho integrado e conjunto entre organizações, nada mais lógico que as organizações olharem pra dentro delas em busca do aprimoramento dos seus processos para obter melhores resultados.

Quadro 7 - Categorias do Papel da Organização na CS

Categorias do Papel da Organização na CS	Frequência
Relacionamento com outros Elos da CS	8
Foco em Resultados/Processos Internos	4
Intermediário na CS	4

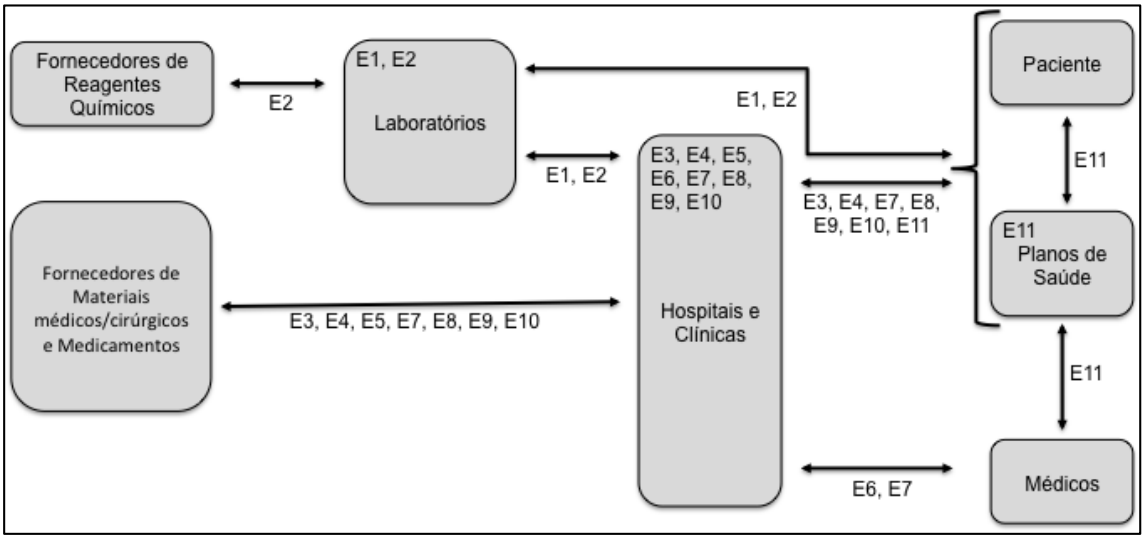
Fonte: Dados de Pesquisa (2016)

A última categoria, se destaca uma visão minimalista do processo da CS. Os entrevistados veem apenas seu contato direto com fornecedores e clientes e não possuem uma visão mais abrangente do que há além disto, como outros níveis de fornecedores, distribuidores ou cliente de seus clientes.

5.2.1.4 Definição dos parceiros

Nesta variável são abordados principalmente os fornecedores e clientes de cada tipo de organização. Com base nas respostas providas pelos entrevistados, foi possível desenvolver a Figura 7 que representa a cadeia por eles citada. Cada conexão entre os participantes possui a identificação do entrevistado que dá suporte àquela conexão.

Figura 7 – Cadeia de Suprimento Identificada na Pesquisa



Fonte: Dados de Pesquisa (2016)

Uma observação a ser feita no modelo é referente aos médicos. Alguns entrevistados deram certeza quanto ao fato do médico ser um cliente do hospital, como foi o caso do Entrevistador E6: *"... meu cliente são os médicos, quem me manda o paciente é médico..."*. Da mesma forma o Entrevistado E7, também considera o médico como um cliente:

> [...] eu não posso ignorar que o médico é um cliente, porque se ele desejar (pode) levar os pacientes que ele tem lá na clínica dele pro hospital A ao invés do hospital B... então eu preciso enxergar ele como cliente, apesar de que algumas correntes entenderem que o médico não é um cliente, então temos que enxergar de duas formas, ora ele é cliente, ora ele é prestador de serviço ou ora ele é um mero operário da instituição [...]

Mas o Entrevistado E8, apresenta a compreensão desta visão, mas prefere uma abordagem contrária:

> [...] cliente interno, o médico, é um cliente na visão da qualidade, embora o médico não possa ser o foco do hospital, o foco do hospital tem que ser o paciente. Se eu considerar que o médico é o cliente do hospital único, tem uma lógica, ele diz assim: eu sou cliente do hospital, porque eu trago o paciente pra cá e eu posso levar pra outro hospital, mas nesse sentido, ele como se fosse um agente de viagem... então eu acho que o médico tem que ser um parceiro do hospital, mas eles querem ser tratados como clientes e eu aprendi na Administração Hospitalar

> que temos que tratar o médico como cliente, era uma coisa conveniente na época, mas está mudando um pouco isso, temos que colocar o centro da atenção no paciente [...]

Nem todos os entrevistados dos hospitais têm uma percepção clara do papel dos médicos na cadeia da qual participam, nem mesmo do papel administrativo dentro da própria organização. O que chama a atenção, é que mesmo o assunto ser abordado na formação destes administradores, como foi comentado pelo E8, de que seriam clientes, suas ações de atendimento dentro das dependências do hospital cria uma "camuflagem" sobre seu papel: colaborador, prestador de serviços ou cliente? Segundo E8, nem mesmo a literatura é clara em relação a estes profissionais.

5.2.2 Informações a Serem Protegidas

O Objetivo desta dimensão é analisar informações de maior relevância na empresa e na CS e seu tratamento ao longo da CS.

5.2.2.1 Informações Críticas a Serem Protegidas

Iniciando com os laboratórios, representados por E1 e E2, eles concordam quanto à principal informação a ser protegida: a identificação do paciente. Mas abordando informações críticas para a cadeia, o Entrevistado E2 comenta: *"... nós temos que ter as informações fidedignas, então assim, tanto do plano de saúde como do hospital, nós precisamos ter o básico (informações do paciente)... para que a gente entregue um resultado fidedigno, como a gente pertence ao mesmo grupo, ao mesmo setor, eu acredito que isso tem que ter uma confidencialidade entre nós...".*

Já a clínica, do Entrevistado E3, se assemelha a maioria dos hospitais quanto a essas informações mais críticas para serem protegidas (E4, E5, E8, E9 e E10): o prontuário médico. Pois, como comentado pelo Entrevistado E8: *"...prontuário do paciente, com certeza, ele é sigiloso e regido por legislação...".* Mas outro tipo de informação também foi citada por alguns respondentes: informações comerciais, ou de preço de compra de produtos como informado pelo Entrevistado E7: *"Informações comerciais, informações relacionadas a atendimento, informações e indicadores econômico-financeiros... Então todos*

esses a gente acaba observando de forma bastante crítica...”. Uma observação a ser feita é que esse tipo de informação foi mais frequentemente citada pelos entrevistados, quando questionados sobre informações críticas na CS. O Entrevistado E8 comenta exatamente isso: *“Preço é crítico. Porque tu acaba com a concorrência se tu abrir o preço de um pra outro, isso é crítico. Então eu tenho poucas pessoas que lidam com essa situação. Se abrir o preço, vai atrapalhar minha negociação, e pode dar margem para corrupção...”*. No mesmo sentido, o Entrevistado E4 aborda também o tema:

> Hoje nós temos uma preocupação muito grande em relação a política e o sigilo das informações de um fornecedor pra outro. Tanto que a política que nós passamos hoje... para central de compras, enfim, é nunca abrir preço de um fornecedor pra outro... Essa é a nossa grande preocupação porque hoje o valor que pode ser negociado aqui comigo pode cair no ouvido de um outro, enfim, e eu acabo perdendo em uma negociação: olha isso que eu estou fazendo, é só pra você. Então esse sigilo a gente procura também manter [...]

Mas indo no sentido oposto quanto às informações de comercialização com fornecedores, o Entrevistado E10 apresenta uma visão completamente diferente: *“... não tem nada que eu peça pro fornecedor que eu peça sigilo, por exemplo... de segurança, que tem, que eu preciso, é que as características técnicas do que foi pedido é o que deva ser entregue... (sigilo de preço) não, nenhuma.”*. Como ele mesmo complementa: *“...eventualmente, eu chamo um fornecedor em algum momento e digo assim: olha, tá muito caro. E ele: vou te dar um desconto, mas não fala pra ninguém que é só pra ti. Mas a gente sabe que é lábia, é o mesmo valor que ele tá falando pros outros...”*.

Analisando a criticidade de informações e sua segurança na ótica da operadora do plano de saúde, temos questões mais administrativas. Segundo o Entrevistado E11: “*Depende da área. Pegando na nossa área aqui, nós monitoramos muito o nosso planejamento orçamentário interno das áreas, quanto que cada um pode gastar ou não, isso tem um orçamento... e também tem o orçamento de quanto tu pode gastar com os principais fornecedores...*”. Ele ainda complementa detalhando mais as questões financeiras da organização: “*O que move, como cooperativa, é sinistralidade. Quanto do sinistro, de cada R$100 que entrou, quanto eu gastei. Então isso a gente*

monitora regularmente, então as informações que a gente não abre muito lá pra fora é quanto que está esse pagamento, gira internamente essa discussão...". Mas, em um alinhamento, quando a não colaboração das organizações como CS, ele ainda acrescenta:

> [...] tem dois lados da moeda, tem hoje, que tá muito em voga que é essas ameaças de entrarem pra capturar teu banco de dados, etc. Então tu tem que investir nessa segurança. Tu tem a vulnerabilidade dos dados... qualquer um pode pegar uma planilha... tu tem essa vulnerabilidade interna... na cadeia como um todo, se a relação fosse boa, e nem sempre ela é, você poderia compartilhar dados... eu poderia ter o resultado dos exames, o laboratório liberar pra mim e eu poderia liberar pro laboratório a quantidade de exames que foram feitos... mas como a relação não é de confiança e de transparência, ninguém tem isso.

Na análise categorial desta variável, Quadro 8, o que mais se apresentou nas respostas dos entrevistados foi o Prontuário Médico. Nele constam os dados do paciente e todos os detalhes dos exames e procedimentos executados, materiais e remédios utilizados. Ele é a informação citada pelos entrevistados como a mais crítica a ser protegida. E isso vai de acordo com autores que citam os problemas de vazamento de dados dos pacientes dentre de instituições assistenciais trazendo diversos prejuízos às organizações, seja financeira, da imagem ou da confiabilidade de seus usuários (LUCIANO *et al.*, 2011; HUANG *et al.*, 2014; MAGNAGNAGNO *et al.*, 2015).

Quadro 8 - Categorias das Informações Críticas a Serem Protegidas

Categorias das Informações Críticas a Serem Protegidas	Frequência
Prontuário Médico	10
Resultado de Atendimento	3
Informações Comerciais	3
Dados Financeiros	2

Fonte: Dados de Pesquisa (2016)

Informações comerciais e dados financeiros também apareceram dentre as categorias citadas, indicando que existe a preocupação quanto a informações financeiras e acordos comerciais. Estas informações estão na rede, por isso realmente precisam ser seguradas, pois em caso de ataque, podem trazer complicações às organizações como fraudes ou mesmo espionagem de

concorrentes diretos (BOJANC e JERMAN-BLAŽIČ, 2008; GORDON *et al.*, 2010).

5.2.2.2 Acesso à Informação

Todas as organizações pesquisadas possuem sistemas e controles de acesso configurados para serem acessadas de acordo com a função de cada funcionário. As variações ficam em pequenas peculiaridades quanto a restrições específicas dentro dos processos da organização como citado pelo Entrevistado E10: *"... por exemplo, o técnico de radiologia que antes tinha acesso à área de diagnóstico, ele não tem mais. O sistema foi fragmentado em preparo, execução e laudo, o mais restritivo de todos é o laudo. Quem tem acesso ao laudo, é o médico que está laudando, o médico que realizou o exame..."*. Já o Entrevistado E9, levanta uma preocupação exatamente quanto a necessidade dessas configurações no seu sistema:

> [...] quanto ao acesso do prontuário, eu falo que ele é falho pelo seguinte: ...na minha visão, você técnico de enfermagem devia poder ver o que você escreveu, ele não deveria ver o que o médico escreveu, o que o enfermeiro escreveu... Ele estará prestando assistência o paciente, vai estar fazendo o trabalho de assistência nele, então não é necessário ler...ele é falho nessa questão.

O Entrevistado E9 ainda explica que já houve uma tentativa de mudança, mas houve uma decisão administrativa para que continuasse assim, permitindo o acesso de todos os envolvidos às informações:

> Mas hoje o chefe de enfermagem, e o diretor clínico, deixa todo o prontuário aberto, então se você é medico, você vai entrar, vai ver a evolução do técnico de enfermagem, vai ver evolução do enfermeiro... vai ver a evolução de todo mundo. Se o enfermeiro entrar ele vai ver a informação do médico, então assim, ele vai ter acesso a todo o prontuário [...]

Além disso, a organizações maiores possuem sistemas mais robustos que auxiliam, inclusive, no rastreamento dos acessos e num controle maior do conteúdo acessado por seus funcionários, como comentado pelo Entrevistado E8: *"Nós usamos o TASY, da Philips... o sistema tem níveis de acesso e senhas e ele deixa rastros. Eu posso fazer qualquer coisa no sistema que eu tenha autorização pra fazer... qualquer coisa que eu fizer, fica registrado..."*.

O Quadro 9 apresenta a análise categorial desta variável. Nele pode-se confirmar o que foi abordado a pouco em que os principais métodos de proteção encontram-se no Acesso Individual aos Sistemas das organizações, juntamente com restrições de acordo com perfis ou atividades de que os funcionários precisam do acesso para execução de suas funções. Ação esta, que é bastante abordada na literatura (BOJANC e JERMAN-BLAŽIČ, 2008; BANG *et al.*, 2012; ISO-IEC, 2014).

Quadro 9 - Categoria do Acesso à Informação

Categoria do Acesso à Informação	Frequência
Acesso Individual ao Sistema	11
Perfis de Acesso Conforme Função	10
Monitoramento de Acessos	8

Fonte: Dados de Pesquisa (2016)

Outra categoria que se fez presente no material colhido foi o Monitoramento de Acessos, onde os entrevistados comentaram sobre a rastreabilidade dos acessos com históricos dentro de seus sistemas de gestão. Isso é uma ação providencial para segurar a informação de dentro da organização onde, tendo a identificação dos acessos, é possível tomar atitudes para evitar que voltem a se repetir ou mesmo ocasionem incidentes graves para a organização (BOJANC e JERMAN-BLAŽIČ, 2008). Ainda dentro desta mesma categoria, foram citados problema relacionados às informações fora dos sistemas, aqueles que circulam em papel dentro das organizações, as quais são ainda mais difíceis de serem controladas ou mesmo verificadas quanto a quem está vendo aquela informação, o que, confirme Hedström *et al.* (2011), pode trazer prejuízos igualmente consideráveis para as organizações.

5.2.2.3 Meios de Comunicação com Parceiros

Os meios de comunicação das organizações visitadas com seus parceiros são bastante diversificados. O Entrevistado E1 informou que é, principalmente por telefone, enquanto o Entrevistado E2 informou que estão desenvolvendo um novo aplicativo: *"...os canais (de comunicação), são internet, aplicativo que a gente está desenvolvendo e já está terminando..."*.

O Entrevistado E3, da clínica, já havia comentado que o contato com fornecedores se dá através do Bionexo, assim como vários hospitais, e olhando

para o cliente: *“...a parte de solicitação (de exame) é tudo web com os convênios, pelo site dos convênios, mas acontece de ter que ligar pra coisas que não são liberadas...”*.

Os hospitais falam de comunicações variadas. A maioria utiliza o Bionexo para tratar com fornecedores, como explicado anteriormente, mas ainda há outros meios, como informado pelo E8: *“Geralmente por e-mail, se usa muito e-mail. Muito pouco fax... e a plataforma (Bionexo), acho que é 80% da comunicação... Os que estão fora da plataforma é e-mail e telefone...”*.

Já o Entrevistado E5 fala da mudança pelo qual sua organização está passando nesse sentido: *“...estamos implantando um processo de [nome do processo] que é o fornecedor entrar no meio pra ajudar a gente no processo de licitação, cotação e compras, hoje está basicamente na questão de e-mail...”*.

Mas um dos hospitais tem uma comunicação mais próxima com o laboratório que utilizam, conforme o Entrevistado E10: *“... eu tenho uma comunicação, uma integração muito grande no sistema de gestão como um todo, porque pra eu cobrar uma conta, que tenha exame de laboratório, lá quando eles fizerem o exame de laboratório, lançaram no sistema deles e, automaticamente, tem que cair na conta do paciente...”.*

Já a operadora do plano de saúde, o Entrevistado E11 apresentou apenas a comunicação com a unidade integradora do convênio: *“nós somos obrigados a mandar os dados todos os meses, o ERP é deles, então é o mesmo que o nosso. Pelo ERP deles, é como se estivessem aqui dentro... eles tem o acesso.*”.

A análise categorial resultou no Quadro 10 apresentado abaixo. O meio de comunicação mais citado entre os entrevistados, para comunicação entre organizações, demonstra a utilização principal de *E-mails* ou *Sites Web*. Um dos sistemas que foi bastante comentado entre os entrevistados, também apareceu na lista, o sistema Bionexo, como Sistema de Compras.

Quadro 10 - Categoria dos Meios de Comunicação com Parceiros

Categoria dos Meios de Comunicação com Parceiros	Frequência

E-mail/Site Web	8
Telefone/Fax	7
Sistema de Compras	4
Pessoal	4
Integração de Sistema	4

Fonte: Dados de Pesquisa (2016)

Uma categoria que chama atenção é a Pessoal. Essa categoria engloba as citações de pessoas que levam papéis entre organizações ou CDs físicos com arquivos digitais destas informações. O que, em termos se segurança, é um ponto de alta vulnerabilidade. Ainda dentre as categorias encontradas, está a Integração de Sistemas que, se houvesse um melhor relacionamento entre as organizações da cadeia, talvez tivesse uma frequência mais elevada se comparada com as demais categorias.

5.2.3 Ameaças e ações de mitigação para a Segurança da Informação

O objetivo desta dimensão é identificar a compreensão de ameaças e ações para mitigá-las.

5.2.3.1 Reconhecimento de Ameaças e seus Impactos

De forma unânime, todos os entrevistados confirmaram que as organizações reconhecem a existência de ameaças à Segurança da Informação. Mas nem todos conseguiram descrever um possível impacto na organização em caso de alguma ocorrência.

Visto que o foco dos questionamentos estavam mais voltados aos resultados da organização, o foco principal dos respondentes, quando falando de impactos, foi da imagem da organização no mercado, em quase todos os tipos de organização. O Entrevistado E1, de um laboratório comentou: *"...a imagem da empresa fica ruim também. Uma clinica que manda exames pra gente, já ia pensar duas vezes antes de mandar, então o impacto é grande"*.

O Entrevistado E3, da clínica, considerou a ameaça de ataque aos sistemas, onde o impacto resultaria na indisponibilidade das informações no âmbito operacional:

> Se hoje parar, dois minutos, qualquer coisa aqui, não tem mais atendimento... como está tudo centralizado ali, se a gente sair a noite e alguém invadir o sistema,

> fazer aquele bloqueio por senha que o pessoal tem feito... no outro dia a gente chegar aqui e não tiver nada funcionando, basicamente, a clínica não funciona. Ninguém vai saber quem é o paciente que vai ser atendido, porque tudo é centralizado, todas as informações hoje, dessa questão de atendimento, está dentro do sistema, não tem nada fora. Então assim, seria irreparável, porque vai saber quanto tempo você vai levar? Eu tenho copia todos os dias, mas tu vai perder um dia de movimento [...]

Os Entrevistados E4, E5, E8 e E10 comentaram sobre os impactos sobre a imagem da organização. O Entrevistado E10, inclusive relatou um episódio que ocorreu no hospital onde um funcionário se aproveitou da vulnerabilidade do sistema e capturou informações confidenciais sobre um paciente: *"...em primeiro lugar, tem o risco da imagem. Nós tivemos um público e notório caso do [nome jogador de futebol], que veio fazer um exame e um profissional da radiologia falou o resultado, não sei se pra mídia... o exame era mais sério do que parecia...então deteriorou a imagem do hospital."*. Mas ele também focou o âmbito judicial: *"...Na questão judicial, completamente passível, se tu te achas lesado por alguma questão que infringiu a tua imagem, ou segurança, tu entra contra o hospital, e o hospital tem que arcar com tudo."*.

O Entrevistado E6, foi direto na resposta sobre o impacto quanto a indisponibilidade das informações, relatando um caso ocorrido no hospital: *"Desespero total, caos absoluto. Nós tivemos há uns dois anos atrás uma manhã que não entrou o sistema, simplesmente eu mandei embora 600 pacientes. Não tem o que fazer. Eu dependendo exclusivamente de um arquivo, pelo menos pra localizar a ficha do paciente..."*.

O Entrevistado E8, além de falar sobre a imagem, também comentou sobre o impacto no relacionamento na CS com fornecedores:

> [...] pode dar um prejuízo, pode gerar uma crise...pode ser prejudicado até por expor um fornecedor, pois se eu exponho o preço dele no mercado... os outros hospitais vão querer o mesmo preço que eu tenho...eles fazendo pressão em cima desse fornecedor, esse fornecedor vai dizer: olha, infelizmente não vou mais poder fazer esse preço pra ti, pois tu abriu o preço pros outros [...]

O entrevistado da operadora do plano de saúde, E11, comentou de um evento de que participou, sua percepção sobre segurança e dos impactos na organização:

> [...] estou vindo de um evento em Curitiba semana passada, nós estamos discutindo os *datacenters e backup* de *datacenters*, onde estão ficando esses *datacenters* e quantidade de investimento. Por mais que tu tenhas investimento, a partir do momento que tu consegue ter ataques na casa branca e algo parecido, é uma grande bobagem dizer que estamos totalmente seguros... a gente procura precaver e estar sempre simulando e monitorando... conforme o tipo de ataque que houver, tu pode deixar a [nome da empresa] lenta ou tu pode até parar a [nome da empresa], e não tenha dúvida que pra marca, também, ela pesa [...]

A análise categorial desta variável, Quadro 11, apresenta como principais preocupações dos entrevistados, o vazamento de informações e a indisponibilidade de sistemas. Conforme apresentado anteriormente por seus relatos, eles tem a preocupação quanto ao vazamento de dados de resultados de procedimento de seus pacientes. As consequências para as organizações dessas falhas podem variar de prejuízos financeiros diretos ou indiretos, como na imagem que pode ser afetada levando dúvidas aos pacientes sobre serem atendidos naquela instituição (BOJANC e JERMAN-BLAŽIČ, 2008; HUANG *et al.*, 2014). Já a indisponibilidade de sistemas ocasiona um prejuízo imediato, visto que a dependência de sistemas impede das organizações identificarem seus pacientes e assim não conseguirem dar o encaminhamento necessário para que qualquer tipo de procedimento seja realizado.

Quadro 11 - Categorias das Reconhecimento de Ameaças e seus Impactos

Categorias do Reconhecimento de Ameaças e seus Impactos	Frequência
Vazamento Informações	7
Indisponibilidade Sistemas	7

Ataque Interno	5

Fonte: Dados de Pesquisa (2016)

Outra preocupação, bastante presente na literatura, é referente aos ataques internos, que ocorrem com auxílio, voluntário ou não, do corpo interno da organização (FORWARD, 2010). Segundo Gaunt (2000): "*A ameaça mais significante à Segurança da Informação em uma organização, é o seu pessoal*".

Em relação aos impactos destas ameaças, não foi possível construir uma análise propriamente dita. Os entrevistados reconhecem a existência das ameaças, sabem o que elas podem atingir na organização, mas não conseguem quantificar que tipo de impacto elas podem causar em suas organizações de forma sistemática.

5.2.3.2 Ações de Mitigação em Sistemas

As ações de mitigação dos sistemas informados pelos entrevistados, estão voltados para suas organizações, apenas um dos entrevistados, o Entrevistado E9 é que indicou uma preocupação e um processo de mitigação quanto a comunicação com parceiros: *"...a gente publica o nosso banco (de dados), ele está publicado em um endereço de IP, mas o que acontece, a gente fez um bloqueio para que nem todos os IPs de fora possam ver nosso banco, somente o nosso parceiro..."*.

Os entrevistados dos laboratórios foram bastante distintos em suas abordagens. Enquanto o Entrevistado E1: *"...A gente tenta se proteger da melhor forma possível. Equipamentos sempre atualizados, sistemas de antivírus... o backup, ele é diário, protegido..."*, o Entrevistado E2 comentou sobre as restrições no sistemas e sobre a mitigação para a CS: *"...Não, nós protegemos os nossos aqui, nossos servidores..."*.

O Entrevistado E3, da clínica, tem um sistema mais complexo na estrutura de seus dados para auxiliar na proteção de suas informações:

> [...] elas (informações) estão espalhadas em vários servidores hoje. Então isso dificulta um pouco. Não está tudo em um servidor e nos servidores não são a mesma senha. Então tem um processo que tenta dificultar um pouco... eu tenho vários servidores com bancos de dados diferentes. As informações gerenciais da clínica e recepção estão em um banco

> de dados, as informações dos exames e imagens estão em outro banco de dados e fotos de pacientes estão em outro banco de dados e cada um deles está em um servidor.

Dentre os hospitais, um destaque ao representado pelo Entrevistado E6, o qual não possui uma área de TI específica, mas uma empresa terceirizada que presta o suporte necessário: *"...nós temos uma assessoria externa que faz esse backup de hora em hora para a gente, tem os servidores externos..."*.

Os hospitais tratam da segurança principalmente no que tange as permissões de acesso nos sistemas internos, parametrizando da melhor forma possível, como comentado pelo Entrevistado E7:

> [...] o que a instituição faz para poder ter uma certa segurança nesses dados, afinal de contas, os funcionários estão usando, por mais que a gente restrinja os sistemas, restrinja o uso do USB pra pessoa não ter acesso a relatórios e enfim, hoje nós temos os e-mails que podem ser utilizados pra vazar informação e você tem a própria pessoa, então, na verdade hoje, o hospital utiliza-se da restrição do uso do celular dentro da instituição [...]

Já o Entrevistado E8 falou sobre o arquivamento de documentos:

> [...] (sobre a área de TI) tem redundância, máquinas virtuais com redundâncias, tem *nobreaks*, tem sistema de *backup* fora, em outros locais, então se cair um raio e explodir aqui e pegar fogo, eu consigo fazer funcionar em outro lugar... tem servidores separados por sistema, que é o coração do hospital... é uma coisa separada do sistema de comunicação do hospital... tem este tipo de organização [...]

A operadora de plano de saúde, apresentou não seus recursos de mitigação, mas o procedimento que efetuam para validar se os mesmos estão funcionando. Segundo do Entrevistado E11: *"A gente faz simulações, no sentido de: pra tudo, ver se vai entrar o outros servidor aonde eu tenho backup, onde eu tenho isso ou tenho aquilo... mas eu não deixo os backups na mesma área, tenho toda uma outro sala, fora aqui do prédio contra fogo..."*.

Dentre as categorias identificadas para a variável Ações de Mitigação em Sistemas, apresentadas no Quaro 12, está a utilização de Sistemas de Mercado. Poucas são as organizações que utilizam sistemas internos para efetuarem suas

transações ou mesmo a gestão administrativa da mesma. Segundo o Consórcio *Forward* (2010), organizações correm maior risco de falhas e ataques em sistemas caseiros do que sistemas mais robustos de mercado, pois existe uma atenção especializada no sistema que irá atender a inúmeras organizações.

Quadro 12 - Categorias das Ações de Mitigação em Sistemas

Categorias das Ações de Mitigação em Sistemas	Frequência
Sistemas de Mercado	8
Backups/NoBreaks	7
Sistemas Internos	3
Redundância de Servidores	3
Antivírus	2

Fonte: Dados de Pesquisa (2016)

As demais categorias identificadas, foram a utilização de *Backups* e *NoBreaks* nos servidores, a utilização de Redundância de Servidores e o uso de Antivírus nas organizações. São medidas simples, mas essenciais na proteção das informações nas organizações (ISO-IEC, 2014; CERT.BR, 2015).

5.2.3.3 Ações de Mitigação para Funcionários

A maioria das organizações visitadas possuem regras e normas estabelecidas e explícitas aos funcionários. Elas também contam com contratos ou termos de responsabilidade, sigilo e/ou responsabilidade dentro da organização. Mas não são todas, os Entrevistados E1 e E6 não possuem nada deste tipo. Enquanto os Entrevistados E3 e E4, informaram que existem políticas informais dentro da organização, e estão trabalhando para a sua formalização conforme informado pelo Entrevistado E3: *“Com relação também a política de segurança interna, essa semana a gente comentou com o nosso RH, que a gente vai escrever um termo de responsabilidade, de utilização de internet, utilização das máquinas internas, utilização de informações da instituição...”*.

Mas nem todos possuem um processo de revisitação destas políticas de tempos em tempos para relembrar seus funcionários, o que pode ser um erro grande para a organização pelos inúmeros problemas que podem ocorrer causados pelos descuidos por parte dos funcionários, conforme alertado por Gaunt (2000). Mas o Entrevistado E10, comentou de um processo um pouco diferente de como eles trabalham essa recordação dos processos internos:

> [...] não é bem um treinamento, mas é de uma eficácia enorme. Nós temos um grupo teatral de funcionários dentro do hospital... e eles, de tempo em tempo... apresentam uma peça teatral satirizando as questões que deram errado no meu processo...depois disso dito... eles relatam o caso que de fato que aconteceu no hospital: assim, assim e assim, a conduta foi certo, legal, por isso, ou a conduta, neste caso, foi errada, a gente não pode repetir [...]

O Quadro 13 apresenta as categorias referentes às Ações de Mitigação contra a Segurança da Informação para os Funcionários das organizações. Para muitos autores, o elo mais frágil dentre os existentes para a Segurança da Informação (KRAEMER e CARAYON, 2007; FORWARD, 2010; LUCIANO *et al.*, 2010). Isso ocorre devido a uma séria de fatores, como interfaces muito complexas para o entendimento do usuário, usuários que deliberadamente causam danos à organização ou ainda aqueles que são manipulados ou enganados para não propositalmente permitir um ataque à organização (FORWARD, 2010; CERT.BR, 2015).

Quadro 13 - Categorias das Ações de Mitigação para Funcionários

Categorias das Ações de Mitigação para Funcionários	Frequência
Código de Conduta	7
Termo de Responsabilidade	5
Regras não Formalizadas	4
Auditoria Interna	2
Revisão do Manual	2

Fonte: Dados de Pesquisa (2016)

As categorias mais citadas foram a existência de um Código de Conduta e um Termo de Responsabilidade, os quais são apresentados aos novos funcionários no momento de sua contratação, o que é valioso, mas é necessário uma revisão e treinamentos de pessoal para que ele seja efetivo, como indicado por Gaunt (2000) e Landolt *et al.* (2012), e esta categoria (Revisão do Manual), se apresentou apenas duas vezes.

Ainda mais crítico, foi a aparição de Regras não Formalizadas onde a organização não tinha qualquer guia de comportamento para que seus funcionários segurem a informação com as quais lidam no seu dia-a-dia. Isso implica que os mesmos, por desconhecimento, criem senhas fracas,

compartilhem acesso, acessem site não confiáveis ou mesmo deixem seus computadores desprotegidos para que outros possam ter acesso durante sua ausência (BOJANC e JERMAN-BLAŽIČ, 2008; LANDOLT *et al.*, 2012).

5.2.3.4 Monitoramento da Informação

O monitoramento das informações, na maior parte das organizações visitadas existem de alguma forma, como sistemas de backup, conforme informado pelo Entrevistado E5: *"...trabalhamos com agentes... e sistemas de backups, e testes de backup..."*.

Mas não são todos, a clínica, do Entrevistado E3, por exemplo, não cuida especificamente das informações: *"...não tem nada específico, o monitoramento sou eu. A única coisa que eu recebo notificação hoje, é do meu sistema de storage, onde eu faço meus backups, e se acontece alguma coisa ele me notifica..."*.

A análise categorial desta variável, apresentada o Quadro 14, pouco pode ser extraído. A maioria dos entrevistados não tinha o conhecimento específico dos tipo de monitoramento que a organização possuía, apenas informaram que "Existe" um monitoramento, com exceção dos entrevistados elencados acima.

Quadro 14 - Categorias de Monitoramento da Informação

Categorias de Monitoramento da Informação	Frequência
Existe	6
Não Soube Informar	2
Não Há	2

Fonte: Dados de Pesquisa (2016)

Houve aqueles que não souberam informar, talvez por suas funções mais administrativas na organização. Mas chama atenção, a existência da categoria "Não há", onde os entrevistados afirmaram não existir qualquer tipo de monitoramento em seus servidores. Isso implica em risco de ser atingido por um ataque e demorar até perceber o problema, o que pode incrementar seus prejuízos (ISO-IEC, 2014; CERT.BR, 2015).

5.2.4 Investimentos em Segurança da Informação

O objetivo desta dimensão é analisar como são definidos os investimentos de Segurança da Informação

5.2.4.1 Avaliação de impacto de Ameaças

Dentre todas as organizações, apenas um tem uma avaliação sobre impacto de ameaças, a operadora do plano de saúde. Conforme o E11:

> [...] primeiro porque eles trabalham com orçamento, quanto que eles podem gastar e depois nós trabalhamos com quanto eu posso vir a perder, de marca, de dados e qual o impacto disto. É amarrado aqui na [nome da empresa], o planejamento orçamentário, o gasto que pode ter, o quanto foi gasto e o quanto pode perder.

E sobre as métricas utilizadas para os cálculos, o entrevistado E11 complementa: *"É um percentual do faturamento, tanto para gastos quanto para perda."*.

Todas as demais organizações não possuem esta avaliação, pelo menos não formal, como disse o Entrevistado E5: *"Formal, não. Informal, extraoficial, pode acontecer isso, aquilo, aquilo, resultando nesta problemática, mas formalizado, não."*. E questionando sobre algum tipo de métrica sobre essa discussão informal: *"...é tudo no achismo. Eu acho que vai parar e tanto de prejuízo. Até uma impressora hoje, me dá uma mensuração de prejuízo, mas a estrutura geral parada, é complexo demais."*.

Mas eles concordam quanto a essa complexidade de fazer esse tipo de cálculo e também de que o impacto de algo assim ocorrer causaria um grande dano à organização. Como comentado pelo Entrevistado E7: *"Não é formal, não. A gente sabe que isso pode gerar um dano muitas vezes irreversível"*. Mais tarde, ele complementa:

> [...] mas é fato, a instituição sabe muito bem disso, que um dia ou horas parado no sistema de informação, ou no seu *datacenter*, isso ocasiona em um prejuízo enorme em relação aos controles internos, dispensação de itens via sistema, possibilidade de prejuízo no atendimento ao paciente, porque hoje é tudo eletrônico, a prescrição nossa, ela é eletrônica. Então a gente já sabe dos impactos, mas não o cálculo desse impacto.

Uma das formas existentes para que as organizações possam se prevenir contra ataques a Segurança das Informações, é a contratação de seguros. Assim, as organizações reduzem o risco do prejuízo em caso de ataques bem

sucedidos, transferindo esse risco à seguradoras (BOJANC e JERMAN-BLAŽIČ, 2008). Mas de acordo com as informação coletadas nas entrevistas, dentre todas as organizações, nenhuma delas possui seguros para suas informações ou sequer ocorreu do assunto ter sido tratado ou discutido dentro de suas organização. Inclusive, grande parte dos entrevistados, não tinham o conhecimento da existência de seguros para as informações de uma organização.

Quanto à análise categorial apresentada no Quadro 15, fica aparente a falta de uma análise envolvendo ataques à Segurança da Informação. Como categoria mais frequente, está o Prejuízo Imensurável, que de forma geral, tenta explicar a segunda categoria mais frequente: Não há Análise de Impacto Formal. As organizações não fazem o estudo de impacto sobre suas informações e assim, ficam completamente às cegas sobre as consequências no caso de um ataque ocorrer. Isso também traz como consequência a inexistência de planos de contingência, pois não há avaliação sobre esses prejuízos.

Quadro 15 - Categorias das Avaliação de impacto de Ameaças

Categorias das Avaliação de impacto de Ameaças	Frequência
Prejuízo Imensurável	14
Não há Análise de Impacto Formal	10
Dano à Imagem	6

Fonte: Dados de Pesquisa (2016)

A terceira categoria mais frequente, traz a percepção sobre qual seria um dos principais impactos de uma falha de Segurança da Informação: a imagem da organização. Esse dano, pode impactar não apenas a organização em que houve o ataque, mas de seus parceiros que se relacionam e possuem um vínculo perante aos pacientes (HUANG *et al.*, 2014). Não é exatamente uma análise, pois os entrevistados não possuíam dados para medir esse impacto, foi apenas uma percepção dos entrevistados em relação aos principais problemas por eles imaginados.

5.2.4.2 Orçamento Específico para Segurança da Informação

Nenhuma das organizações avaliadas possui qualquer tipo de tratamento diferenciado em seu orçamento quando se trata de ações de Segurança da Informação. Todas seguem suas definições padrões de investimento em

quaisquer medidas. Se são orçamentos pré-definidos por setor, o setor de TI, recebe o valor e distribui como achar conveniente, seja com segurança ou não, como comentado pelo Entrevistado E10: *"Orçamento é pra TI e ela define o que é segurança, o que é infra..."*.

Os valores para esses investimento, também podem ser captados após uma avalição técnica, ou consultoria externa, indicando a necessidade de fazer determinado investimento e então o mesmo é discutido e, se for o caso, aprovado. Como é o caso informado pelo Entrevistado E4:

> [...] estamos com um rapaz que está fazendo pra nós, como se fosse uma consultoria... ele vai estar avaliando pra nós, em que situação nós nos encontramos, o que nós precisamos pra nos adequar e ele vai apontar pra nós, exatamente, quais são os riscos que nós, hoje, estamos correndo da maneira como estamos... ele vai dar uma avaliação pra nós pra gente poder, também, comparar com o que a gente tem da avaliação da nossa TI, pra gente poder chegar numa decisão [...]

Seguindo a abordagem de forma parecida, o Entrevistado E7 comenta:

> [...] a gente utiliza, qual a necessidade, qual é o objetivo real do investimento naquele tipo e projeto. Não é porque eu tenho uma verba destinada que eu vou usar, por que está lá definida. Ou vou deixar de fazê-lo, porque eu não tenho uma verba estipulada, ao contrário. A gente prefere trabalhar em cima de necessidades reais [...]

Como as organizações não possuem definição exclusiva quanto o orçamento utilizado para ações de Segurança da Informação, não foi possível avaliar a maneira como os mesmos são definidos, como métricas e itens que seriam levados em consideração.

5.2.4.3 Impacto do Investimento na Performance Financeira Organizacional e da Cadeia de Suprimentos

Esta variável buscava captar dos entrevistados suas percepções da relação custo-benefício dos investimentos em Segurança da Informação versus o impacto de um ataque ou falha na organização ou na CS. Mas como visto nas análises das variáveis anteriores, ainda dentro da dimensão de Investimentos em Segurança da Informação, os entrevistados não possuem o conhecimento

preciso dos impactos de ataques à suas organizações e também não possuem foco orçamentário para a Segurança da Informação.

É possível que o Entrevistado E11, tenha sido feliz em traduzir em palavras uma percepção geral dos demais entrevistados:

> Alguns dados até se consegue, mas a gente vai caminhar muito pra um campo intangível. Então se a gente vai mais pra contabilidade, até mensura isso, mas tem muita coisa que é intangível... do outro lado, também do custo, a gente consegue. Intangivelmente, a gente consegue colocar o quanto a gente deixou de gastar ou quanto a gente gastou, mas não dá pra ser tão pontual, nessa ciranda, tu tem muito intangível [...]

Esta variável tinha por objetivo compreender o relacionamento entre os impactos à performance financeira da organização e da CS em relação aos investimentos realizados para a Segurança da Informação. Como não há uma análise do impactos à organização, nem à CS, e também não há um planejamento de investimento específico para a Segurança da Informação, não é possível realizar uma análise propriamente dita desta variável.

5.3 ANÁLISE DAS PROPOSIÇÕES

Esta seção busca, a partir de todo o levantamento e análise realizada a partir dos dados coletados nas entrevistas, suportar as proposições criadas ou procurar uma explicação para sua não aplicabilidade.

5.3.1 Proposição 1 – Cadeia de Suprimentos Integrada e Colaborativa

Segundo a Proposição 1, as organizações pertencentes a CS são integradas e colaborativas em busca de uma melhor performance financeira.

O crescimento e especialidade da GCS nos últimos anos decorreu de uma série de fatores, principalmente externos às organizações como maior disponibilidade de informações (GUNASEKARAN *et al.*, 2004). A integração entre as organizações da área da saúde também buscam melhorar seus resultados e sua performance (CHEN *et al.*, 2013). Nos casos avaliados, vemos a melhora da performance na integração dos resultados de exames entre alguns laboratórios e hospitais, mas esta performance é de iniciativa individual e não

integrada e colaborativa em que se buque melhores resultados da cadeia como um todo.

Os entrevistados tinham clara a visão sobre seus parceiros, mas não quanto a um trabalho compartilhado em que buscassem uma relação mais eficiente de ganha-ganha. Inclusive, isso apareceu explicitamente em alguns momentos da coleta de dados, como com o Entrevistado E2, que é de um laboratório: *"... a gente tem muita oportunidade, e a gente vive em ilhas separadas. A gente tinha que estar no mesmo continente... eu defendo que, quanto mais próximo a gente estiver, melhor a gente vai ter uma performance em toda a cadeia..."*

Outro relato, neste mesmo sentido veio do Entrevistado E11, da operadora de plano de saúde:

> Parceria não existe. Um coisa que falta e eu vejo, pelo menos na região em que estamos, é compartilhamento e reciprocidade. Então como a coisa nem sempre é colocado clara, ou por falta de profissionalismo ou porque não é séria, tu não tens e todos poderiam ganhar [...]

Ele ainda procura uma resposta para sua própria pergunta:

> Mas por que isso não se dá? Como nós estamos em um sistema capitalista... nem sempre esse laboratório, é interesse dele, que eu tenha o resultado de todos os exames, porque talvez, eu tendo o resultado dos exames, e eu ver que esse paciente fez um exame ontem, não é meu interesse que tu faças o exame hoje, porque eu vou deixar de ganhar... mas por trás, eu estou com uma máquina que precisa trabalhar... então não quer dizer que tudo que é feito, é realmente necessário... Então, eu não pago melhor porque é feito o desnecessário, em contrapartida, pra tu compensar o que eu não te pago melhor, tu faz além do necessário, então todos nós perdemos.

Assim, a Proposição 1 confirma a busca por melhores resultados, mas de maneira individualizada, com baixo nível integração e colaboração. Por mais que as organizações presentes na pesquisa pertençam a mesma CS, elas não são integradas e colaborativas em busca de uma melhor performance financeira para a cadeia. Apenas possuem um relacionamento em que buscam o fornecimentos dos materiais ou informações de que precisam para prestar seus serviços. Se

falarmos dos hospitais, que possuem um papel mais central na CS para o atendimento ao paciente, eles estão envolvidos com este atendimento e deixando em segundo plano a administração do próprio hospital e não prestando atenção aos resultados da cadeia.

5.3.2 Proposição 2 – Conhecimento das Informações Críticas

A Proposição 2 afirmava que as organizações conheciam as informações críticas para a organização e para a CS.

Os entrevistados concordaram que as principais informações de suas organizações, portanto também para a CS, tratam-se das informações dos pacientes, seja resultados de exames, procedimentos ou mesmo a própria identificação do mesmo. Outra informação importante constatada foram informações comerciais de fornecedores, mesmo que não tenha sido uma unanimidade.

O Entrevistado E8 já havia dito sobre a criticidade de informações do paciente: *"...prontuário do paciente, com certeza, ele é sigiloso e regido por legislação..."*. Mas também comentou sobre negociação com fornecedores: *"Preço é crítico. Porque tu acaba com a concorrência se tu abrir o preço de um pra outro, isso é crítico."*. Isso é corroborado com o Entrevistado E7 que também fala da confidencialidade de informações comerciais, mas vai de encontro com o Entrevistado E10: *"... não tem nada que eu peça pro fornecedor que eu peça sigilo..."*

É importante que as organizações saibam quais suas informações primordiais, seja para seu funcionamento ou para obtenção de vantagem competitiva no mercado (BOJANC e JERMAN-BLAŽIČ, 2008). A partir dessa identificação, fica mais claro onde investir esforços para proteger o que realmente precisa dentro das organizações (BOJANC *et al.*, 2012). Informações sobre pacientes acabam sendo o mais críticas, não apenas por questões legais, mas também por todo o impacto indireto que pode ocorrer, sejam por ações na justiça ou pela imagem arranhada devido ao comprometimento das informações (HEDSTRÖM *et al.*, 2011; HUANG *et al.*, 2014).

Assim, conclui-se que a Proposição 2 pôde ser confirmada pela pesquisa realizada. As organizações conhecem as informações críticas pra elas e para a cadeia da qual fazem parte.

5.3.3 Proposição 3 – Métricas de Impacto para Ataques à Informação

Segundo a Proposição 3, as organizações possuem métricas dos impactos sobre a organização e sobre a CS em caso de ataques à informações bem sucedidas.

Conforme o Entrevistado E3, da clínica:

> Na questão de segurança, eu acho que é falho em muitas coisas, que tem que melhorar... Banco hoje é uma segurança diferente e mesmo assim eles sofrem ataques... a saúde em si, ela não tem muito investimento nessas áreas, a maioria deixa de lado, a não ser grandes centros ou grandes serviços. O resto tenta ir mascarando.

E questionado sobre o porquê disto:

> [...] talvez por falta de informação do que pode acontecer. De repente teria que fazer pesquisa e ver o que está acontecendo ... e mostrar pra eles (médicos) o quão vital são estas informações. Porque as vezes eles, talvez, não tenham noção do que é aquilo... não sabem o perigo disso de cair na mão de alguém.

O Entrevistado E3 traduz bem as respostas encontradas durante as entrevistas. Todos os entrevistados tinham uma ideia do que seria impactado no caso de uma falha de segurança das informações, mas era uma opinião muito mais pessoal do entendimento deles sobre esse impacto do que análises ou métricas existentes em suas organizações. Eles não possuíam um estudo formal, nem mesmo informal, das consequências de um ataque ou falhas sobre suas informações. Tanto é que o principal impacto citado foi o da imagem da organização, mas sem conseguirem traduzir esse impacto para números, nem mesmo aproximados. Demonstração disto pode ser visto na análise categorial, onde a categoria mais frequente foi “Prejuízo Imensurável”, mesmo existindo diversos estudos que auxiliam a medir esse tipo de impacto como Gupta *et al.* (2006), Bojanc *et al.* (2012) e Gordon *et al.* (2015).

Os entrevistados tem uma noção da existência de impactos em caso de ataques bem sucedidos ocorrerem, mas não tem informações específicas do tamanho deste impacto para planejarem ações de mitigação apropriadas. Assim, conclui-se que esta proposição não pode ser confirmada com a pesquisa realizada.

5.3.4 Proposição 4 – Investimento em Segurança de Informações

A quarta e última proposição buscava o cruzamento das proposição anteriores com investimentos em Segurança da Informação. A Proposição 4 afirmava que informações críticas da CS recebem investimentos em ações de Segurança da Informação de forma especializada.

A Proposição 1 pôde ser confirmada de forma parcial devido a baixa integração e colaboração das organizações da cadeia quanto às informações compartilhadas, consequentemente, baixa é a colaboração quanto à investimentos em Segurança da Informação. A Proposição 2 pôde ser confirmada, as organizações sabem quais as informações críticas para elas e, consequentemente, para a CS da Saúde. Por fim, a Proposição 3, não pôde ser confirmada, pois as organizações não possuem avaliações para levantamento de dados sobre o impacto de possíveis falhas na segurança de suas informações. Desta forma, a Proposição 4 resulta na existência de investimentos individuais das organizações quanto a Segurança da Informação, que inclui suas informações críticas, mas o investimento não é especializado de acordo com o valor da informação.

A não especialização do investimento em segurança para as informações não é exclusividade da CS. Mesmo excluindo análise sobre a CS da Saúde, buscando analisar apenas a organização singular, continuaria não existindo as análises para realização dos investimentos para a Segurança da Informação nestas organizações.

Quando se busca investir em segurança, a primeira etapa é avaliar o valor da informação que se busca proteger (BOJANC e JERMAN-BLAŽIČ, 2008). No caso da CS da Saúde, claramente existe a preocupação, inclusive amparada por questões legais, conforme informado pelo Entrevistado E8, mas não há avaliação do custo para a organização ou pra cadeia se essa informação fosse

comprometida ou mesmo ficassem indisponível para os médicos ou demais profissionais da saúde por longos períodos. É importante para a administração hospitalar possuir esse tipo de valor e poder tomar ações de mitigação sobre a possibilidade dessas falhas de segurança e, principalmente, conseguir achar o denominador do valor a ser dispendido para efetuar esta segurança, pois a mesma não pode ser maior que o valor da própria segurança (HUANG *et al.*, 2014).

O Entrevistado E10 comentou durante sua entrevista que as ações para investimento em segurança são sempre reativas: primeiro ocorre o problema e então eles passam a analisar esse problema em busca da melhor forma de resolvê-lo, mitigá-lo ou impedir que se repita. Este pode ser um meio de lidar com o assunto e, como comentado também pelo o Entrevistado E9, as ações tomadas são sempre posteriores aos acontecimentos, mas se houvesse uma análise real desses problemas, poderiam ser tomadas atitudes previamente, evitando danos maiores, mas isso não ocorre por ainda não ter havido nenhum caso grave.

Estudos referentes a GCS da Saúde estão bastante atrás de outras áreas, como a industrial, por exemplo (CHEN *et al.*, 2013). Mas o mesmo não deveria ocorrer quanto à Segurança da Informação dessa área, pois trata-se de informações bastante sensíveis: informações particulares das pessoas. O impacto a ser causado no caso de falhas pode, inclusive, ser irreversível para as organizações de assistência à saúde (HEDSTRÖM *et al.*, 2011; LANDOLT *et al.*, 2012; HUANG *et al.*, 2014).

5.4 CONSOLIDAÇÃO DOS RESULTADOS

A pergunta de pesquisa questionava se as organização reconheciam suas informações mais importantes ou críticas para elas próprias e para a CS da qual fazem parte e se faziam investimentos de forma consciente em ações para proteger estas informações. Com base nos resultados, pode-se afirmar que sim, elas reconhecem as informações importantes para seus processos de prestação de assistência à saúde, mas elas não possuem processos definidos para análise e investimentos para ações para segurar estas informações. O Quadro 16

apresenta um resumo dos resultados encontrados com base nas dimensões previamente definidas.

Quadro 16 - Quadro Resumo

Dimensões	Resultados
Estrutura da CS para um melhor fluxo de informações	As organizações possuem seus processos internos bem definidos, mas o mesmo não ocorre ao longo da cadeia, onde há baixo nível de relacionamento entre as organizações parceiras e pouca integração e compartilhamento de atividades.
Informações a serem protegidas	Informações relacionadas aos pacientes são as mais críticas da CS da Saúde e as organizações possuem ações de mitigação para segurá-las.
Ameaças e ações de mitigação para a Segurança da Informação	As principais ameaças identificadas foram o vazamento e indisponibilidade de informações e ataque interno, mas as organizações procuram ter seus sistemas atualizados e possuem códigos de conduta, mesmo que não revisitados regularmente, com seus funcionários
Investimentos em Segurança da Informação	Não há análises sobre os impactos de possíveis ataques às informações, assim, as organizações não fazem investimentos específicos para segurar suas informações, o fazem através da área de TI, consequentemente, não conseguem medir a efetividade dos investimentos frente aos possíveis ataques.

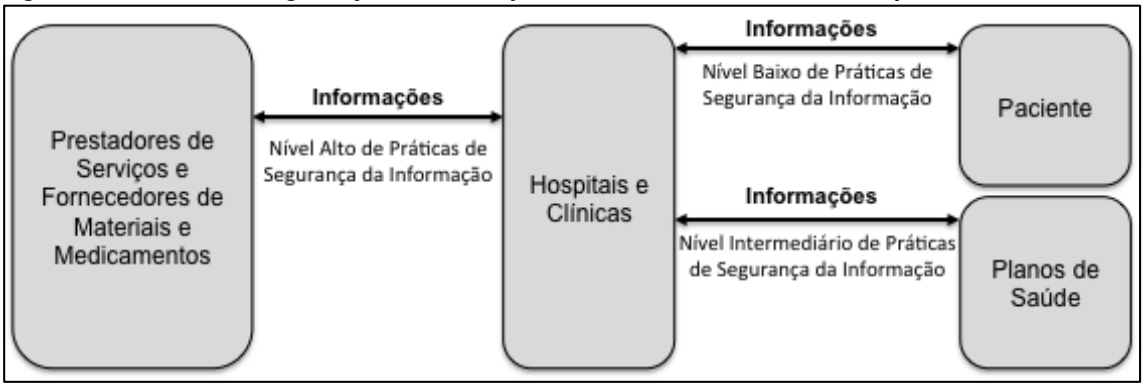
Fonte: O Autor

De maneira geral, a informação considerada mais importante é relacionada ao paciente que é atendido. Todos os entrevistados conseguem imaginar a grandeza do impacto de uma falha relacionada a essa informação, mas não há uma análise da organização para quantificar esse impacto. E isso também não é avaliado no âmbito da CS, mesmo identificando um baixo nível de relação entre as organizações, algumas informações são transacionadas e não há uma análise sobre a segurança nessas transações. A Figura 8 apresenta a percepção do Autor quanto aos níveis de Segurança da Informação entre os elos da CS da Saúde:

- Nível Alto de Práticas de Segurança da Informação: existem comunicações mais seguras, como sistemas específicos e integrações, e baixo uso de ferramentas vulneráveis, como o e-mail;
- Nível Intermediário de Práticas de Segurança da Informação: Há algumas integrações sistêmicas, mas um número maior de uso de ferramentas vulneráveis, como e-mail e papel;

- Nível Baixo de Práticas de Segurança da Informação: Uso principal de ferramentas com baixa segurança, como e-mail.

Figura 8 – Práticas de Segurança da Informação Identificadas na Cadeia de Suprimento da Saúde



Fonte: O Autor

Pelas respostas colhidas, a própria CS parece não ter muita relevância para os resultados buscados pelas organizações. Eles reconhecem a necessidade de seus fornecedores e clientes, mas não possuem uma relação próxima para se ajudarem em busca de melhor performance de todos. São relações distantes, onde alguns tentam, inclusive, esconder informações dos parceiros temendo alterações de preços ao invés de se apoiarem para que ambos atinjam melhores resultados.

Se olharmos os fluxos abordados nas entrevistas das organizações e da cadeia, vemos que conceitos de GRC não são aplicáveis às informações. Não há uma estrutura de governança e não há métricas de avaliação de riscos ou planos de mitigação. Desta tríade, a única que é contemplada é a conformidade com as leis que regulamentam o setor de saúde e isso inclui cuidados com os dados dos pacientes, principalmente envolvendo a privacidade dos mesmos (MAGNAGNAGNO *et al.*, 2015). Mas de forma alguma a tríade GRC ocorre conforme seus conceitos de agirem de forma unida nos processos organizacionais.

A pesquisa apresentou os relatos dos entrevistados e suas preocupações quanto ao acesso à informação, principalmente da equipe médica que precisa acessar o prontuário do paciente. Mas vale ressaltar que a preocupação sobre o baixo comprometimento da equipe médica sobre as informações, não é uma

novidade. Luciano *et al.* (2011) diz o seguinte sobre a privacidade de informações de pacientes: "*O aspecto que mais preocupa é o entendimento das próprias responsabilidades por parte daqueles que manuseiam estas informações, entendimento este bastante flexibilizado em termos de o que pode e o que não pode ser feito em termos de acesso e uso das informações privadas*". Esta flexibilidade citada se aproxima do relato do Entrevista E9 que informa que os médicos têm uma certa resistência ao uso exclusivo dos sistemas e quando o usam, solicitam que os mesmos estejam abertos para toda a equipe médica, o que acaba tendo uma consequência de diversos dados sigilosos de pacientes estarem disponíveis a quem não necessita ter o acesso.

Quanto ao investimento das ações de segurança, identificou-se que a maneira que as organizações planejam sua segurança, não leva em consideração o valor da informação que precisa ser protegida, nem o possível impacto causado pela falha naquela informação e, consequentemente, também não são tomadas precauções quanto a segurança das informações que permeia a CS da Saúde. O investimento em ações de segurança, são feitos de forma generalizada, com pouco foco na informação, apesar de todos os alertas e possíveis consequências que podem se abater sobre as organizações com comprometimento de suas informações.

6 CONSIDERAÇÕES FINAIS

A administração na área da saúde, cada vez mais destina esforços para manter a saúde financeira das instituições e assim continuar a prestar assistência à população e melhorar essa assistência (LEE *et al.*, 2011). Isso somado à importância das informações que circulam dentro da CS da Saúde, este trabalho buscou analisar práticas de investimentos em ações em Segurança da Informação na proteção de informações críticas na CS da Saúde e a percepção do impacto na performance financeira da cadeia.

A partir da revisão bibliográfica, foi possível a criação de um quadro de dimensões, objetivos e variáveis com base em diversos trabalhos da academia, normas e produtos de mercado. A partir da definição desse quadro, buscou-se coletar dados para suportar cada uma das variáveis identificadas em entrevistas com 11 profissionais da área da saúde e analisar o conteúdo dessas entrevistas, classificando as respostas e comentários de acordo com as variáveis. Ainda foi realizada uma análise categorial com as entrevistas transcritas e analisando estas categorias com a revisão da bibliografia.

O resultado dessa análise foi utilizado para explicar a verificação, ou não, de cada uma das quatros proposições criadas, também com base na literatura. Estas proposições estavam alinhadas com os objetivos específicos.

Vale ressaltar que a CS interna, principalmente dos hospitais, estão bem definidas e coordenadas. Eles possuem diversas práticas de segurança, como acessos individuais a sistemas e criação de perfis de acesso, como também a existência de termos de responsabilidade e manual de conduta para seus funcionários. Eles possuem sistemas de backup e alguns, inclusive, redundância em servidores. Além disso, também possuem claros os processos internos para compra de insumos, medicamentos, órteses e próteses, além de ter um rigoroso sistema de rastreabilidade de tudo que entra e circula dentro de suas instalações, possibilitando um atendimento de qualidade e segurança. Algumas dessas práticas também foram encontradas em outros hospitais brasileiros em pesquisa com foco na privacidade das informações (MAGNAGNAGNO *et al.*, 2015).

Haviam sido definidos três objetivos específicos para auxiliar a pesquisa a atingir seu objetivo geral. O primeiro era analisar a CS da Saúde e identificar o

fluxo de informações. Apesar dela não ter se demonstrado uma CS gerenciada por uma das organizações participantes, as organizações possuem alguma interação para troca de produtos, serviços e informações. A falta dessa gestão da CS implica na falta de uma coordenação das atividades para que possam buscar melhores resultados na performance de seus participantes e, também, da CS da Saúde como um todo. Cada organização busca melhorar seus resultados de maneira isolada mantendo um contato mínimo, apenas o necessário entre fornecedores ou clientes, ou ainda, manipulando ações e resultados tentando se beneficiar de alguma forma, mesmo que no outro lado tenha alguém com sugestões para que ambos saiam ganhando com uma aproximação entre as partes. Isso dá a entender que os participantes tem tanto receio de seus parceiros quando da própria concorrência do mercado. Ao invés de buscarem de forma isolada por melhores oportunidades para reduzir seus custos, poderiam se aproximar e tentar chegar em soluções de forma conjunta.

O segundo objetivo específico era identificar as informações críticas da CS da saúde e o impacto na organização em caso de um ataque bem sucedido sobre a mesma. Os entrevistados conheciam as informações críticas para suas organizações, mas pouca visibilidade sobre os impactos que poderiam ser causados na cadeia em caso de uma falha ocorrer em qualquer parte do fluxo da CS. Mesmo objetivando a identificação dessas informações internamente à organização, tinham dificuldade para mensurar o real impacto de um ataque bem sucedido ou uma falha nos sistemas internos de gestão da organização. Por mais que seja clara a necessidade de proteção, não possuem a prática de analisar a fundo as ameaças e os riscos que correm devido ao próprio meio no qual estão inseridos. Isso ocasiona um ponto cego na administração, tanto no que diz respeito ao impacto no seu dia-a-dia, para normalizar seu atendimento, como no prejuízo que isso significa para a organização, seja da imagem da mesma perante fornecedores e clientes ou financeiro. O que ainda pode ser agravado pela evasão de clientes, fornecedores ou médicos, tudo dependendo do tipo de falha ou informação comprometida dentro da organização.

O terceiro e último objetivo específico era identificar as características das definições relacionadas aos investimentos em Segurança da Informação. A conclusão deste objetivo, com uma exceção, é de que não são feitas análises

para esses investimento, mas se espera que com investimento em ações básicas de mercado sejam suficientes para protegerem suas informações. O problema é que, por não haver qualquer análise, nem é possível classificar como sendo bons investimentos ou não. São definidos orçamentos para a área de TI e ela se torna responsável por administrar esse valor da melhor forma possível, incluindo todas suas atividades e ainda a segurança das informações da organização. Isso não seria um problema, se o valor fosse definido sobre métricas específicas sobre o valor das informações mais críticas que precisam de maior proteção.

O trabalho tinha como objetivo geral analisar as práticas de ações em Segurança da Informação na proteção de informações críticas na CS da Saúde. Assim, conclui-se que as práticas adotadas para a segurança não são baseadas nas informações críticas das organizações, menos ainda com base nas relações com outras organizações participantes da CS da saúde. São realizados investimentos gerais em TI que acaba refletindo na segurança dentro das organizações, como atualizações de antivírus ou realização de *backups* e guias de comportamento para funcionários. Todas estas ações são válidas, mas não há uma análise do valor das informações para que se possa concluir que os valores investidos são compatíveis com os impactos em caso de falha nessas medidas de segurança adotadas. Isso implica também, no desconhecimento do impacto destes investimentos para a performance financeira da organização, consequentemente, no impacto na performance financeira de toda a CS.

Acredita-se que este é um tipo de análise que ainda não se encontra em evidência dentro das organizações pesquisadas e que lidam com a assistência da saúde. Mesmo sendo dependentes de um CS, não trabalham de forma unida em busca de uma melhor performance como uma CS eficiente faria. Têm a preocupação com as informações, mas não fazem análises sobre impactos quanto a ocorrência de problemas para, a partir destas análises, ter informações qualificadas para a tomada de decisão quando a questão de novos investimentos em Segurança das Informações.

6.1 CONTRIBUIÇÕES DA PESQUISA

Conforme identificado durante o levantamento bibliográfico, pesquisas tem crescido nos últimos anos acerca da Segurança das Informações em

organizações de assistência a saúde, como também, a preocupação com a performance financeira destas organizações e da CS da qual fazem parte. Além de estudos envolvendo a Segurança da Informação nestas organizações.

Dentre as potenciais contribuições deste trabalho, podem ser citada a visão mais administrativa no que se refere à Segurança da Informação dentro de organizações da Saúde. Além da análise quanto ao gerenciamento das ações de mitigação, seja quanto aos sistemas utilizados, ou aos funcionários do quadro destas organizações. Ações estas que foram avaliadas com base na literatura referente a estas ações de mitigação.

Também pode ser considerado uma contribuição a Matrix de Dimensões (Quadro 2) desenvolvido com embasamento de uma extensa revisão bibliográfica de livros e artigos publicados em *Journals* bem conceituados. Além do próprio roteiro de pesquisa, que possibilidade a execução da pesquisa em outras regiões do país.

Outra contribuição deste trabalho, é o cruzamento da Segurança da Informação em CS da Saúde com a abordagem financeira sobre os investimentos em Segurança da Informação e seus impactos para as organizações e para a CS. Existem pesquisas realizadas na área que abordam a segurança em organizações de assistência à saúde, mas tem foco apenas na privacidade dos pacientes, como em Bragança (2010) e Magnagnagno *et al.* (2015) e analisam as organizações de forma isolada e sem abordar questões financeira quanto ao investimento nas ações de segurança.

Saúde é uma área sempre em evidência no Brasil, principalmente através da mídia, seja por problema em atendimento, ou por celebridades entrarem para uma sala de cirurgia. Esse tipo de informação sempre cativa curiosos e interesseiros. Este trabalho oferece uma análise aos praticantes da área da saúde e apresenta-lhes que ainda não há uma atenção a GCS na área da saúde, nem na avaliação de problemas com Segurança da Informação e, consequentemente, a falta de uma análise sobre investimentos em Segurança da Informação nos dados críticos que permeiam esta cadeia. O resultado deste trabalho poderia ser, inclusive, utilizado pelas pessoas diretamente ligadas à CS ou Segurança da Informação para obter apoio na busca de análises quanto aos

impactos devido à ataques ou falhas e o planejamento para futuros investimentos para proteger a organização e a CS da qual fazem parte.

6.2 LIMITAÇÕES DA PESQUISA

Um dos fatores mais limitantes da pesquisa foi o número de respondentes reduzidos. Mesmo conseguindo o contato com outros profissionais e outras instituições, não foi possível realizar algumas entrevistas devido a indisponibilidade dos mesmos.

O tipo de relação entre os participantes da CS nas organizações contatadas também foi um fator limitante, onde foi encontrado um baixo nível de integração e colaboração dentre as organizações, tanto em relação aos processos da cadeia como na busca conjunto por melhores resultados.

Outra limitação foi a obtenção de apenas um representante de organizações de operadoras de Plano de Saúde, bem como a não realização das pesquisa com pacientes.

6.3 PROPOSTAS PARA PESQUISAS FUTURAS

Algumas propostas para pesquisas futuras partindo dos resultados aqui encontrados:

- A aplicação do instrumento em outras regiões do Brasil;
- Realização de uma pesquisa quantitativa para tentar abranger um número maior de respondentes e, assim, ter uma avaliação mais abrangente da problemática e resultados estatísticos que poderia auxiliar a generalização dos dados aqui encontrados;
- Criação de um modelo integrado de governança para a Segurança da Informação em GCS da Saúde;
- Desenvolvimento de um modelo base sobre a Segurança das Informações das organizações da CS da Saúde, cruzados com os possíveis impactos e prejuízos que podem causar, sendo assim, um guia para priorização de investimentos em segurança para estas organizações.

O trabalho buscou analisar as práticas para proteção das informações críticas da Cadeia de Suprimento da Saúde. As práticas foram identificadas, mas vão de encontro à literatura onde se apresentam planos de investimentos em segurança conforme a informação que se busca proteger (GORDON e LOEB, 2002; BOJANC e JERMAN-BLAŽIČ, 2008; HUANG *et al.*, 2014). Também foi identificada a falta de práticas de segurança para a as informações que transitam na CS, também sendo um aspecto importante a ser analisado pelas organizações. Por fim, acredita-se que o trabalho tenha contribuído para chamar a atenção sobre o aspecto adotado sobre Segurança da Informação por organizações assistenciais da saúde.

REFERÊNCIAS

ABNT. **ISO 28000 - Sistemas de Gestão de Segurança para a Cadeia Logística** 2013.

ATOUM, I.; OTOOM, A.; ALI, A. A. A holistic cyber security implementation framework. **Information Management & Computer Security,** v. 22, n. 3, p. 251-264, 2014. ISSN 0968-5227.

BALLOU, R. H. **Gerenciamento da Cadeia de Suprimentos/Logística Empresarial**. 5˚ ed. Porto Alegre: Bookman, 2006. 616.

BANG, Y. et al. Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. **international journal of information management,** v. 32, n. 5, p. 409-418, 2012. ISSN 0268-4012.

BARDIN, L.; RETO, L. A.; PINHEIRO, A. **Análise de conteúdo**. Edições 70, Lisboa, 1979. ISBN 9724400204.

BEAMON, B. M. Measuring supply chain performance. **International Journal of Operations & Production Management,** v. 19, n. 3, p. 275-292, 1999. ISSN 0144-3577.

BHAKOO, V.; CHAN, C. Collaborative implementation of e‐business processes within the health‐care supply chain: the Monash Pharmacy Project. **Supply Chain Management: An International Journal,** v. 16, n. 3, p. 184-193, 2011. Disponível em: < http://www.emeraldinsight.com/doi/abs/10.1108/13598541111127173 >.

BIONEXO. Solução de Gestao de Compras Hospitalares. 2015. Disponível em: < http://bionexo.com/br/solucoes/bionexo/ >. Acesso em: 01/12/2015.

BOJANC, R.; JERMAN-BLAŽIČ, B. An economic modelling approach to information security risk management. **International Journal of Information Management,** v. 28, n. 5, p. 413-422, 10// 2008. ISSN 0268-4012.

BOJANC, R.; JERMAN-BLAŽIČ, B.; TEKAVČIČ, M. Managing the investment in information security technology by use of a quantitative modeling. **Information Processing & Management,** v. 48, n. 6, p. 1031-1052, 2012. ISSN 0306-4573.

BRAGANÇA, C. E. B. D. A. Privacidade em informações de saúde: uma análise do comportamento percebido por profissionais de saúde de instituições hospitalares do Rio Grande do Sul. 2010.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. 2015. Disponível em: < http://www.cert.br/ >. Acesso em: 01/04/2015.

CHEN, D. Q.; PRESTON, D. S.; XIA, W. Enhancing hospital supply chain performance: A relational view and empirical test. **Journal of Operations Management,** v. 31, n. 6, p. 391-408, 2013. ISSN 0272-6963.

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. Cortez, 1991. ISBN 8524904445.

CHRISTOPHER, M. **Logística e Gerencimento da Cadeia de Suprimentos: Criando Redes que Agregam Valor**. 2˚ ed. São Paulo: Thomson Learning, 2007.

CROOM, S.; ROMANO, P.; GIANNAKIS, M. Supply chain management: an analytical framework for critical literature review. **Journal of Purchasing and Supply Management,** v. 6, p. 67-83, 2000.

DINI, R. C. G. A influência do contexto no comportamento responsável relativo à segurança da informação. 2014.

FLICK, U. **Desenho da pesquisa qualitativa: Coleção Pesquisa qualitativa**. Bookman, 2009. ISBN 8536321350.

FLICK, U.; NETZ, S. **Uma introdução à pesquisa qualitativa**. Bookman Porto Alegre, 2004.

FORWARD. **White Book: Emerging ICT Threats**. Seventh Framework Programme. 2010

_____. ICT-FORWARD Project. 2015. Disponível em: < http://www.ict-forward.eu >. Acesso em: 20/05/2015.

GAUNT, N. Practical approaches to creating a security culture. **International Journal of Medical Informatics,** v. 60, n. 2, p. 151-157, 2000. ISSN 1386-5056.

GIBBS, G. **Análise de dados qualitativos: coleção pesquisa qualitativa**. Bookman, 2009. ISBN 8536321334.

GIL, A. C. Métodos e Técnicas de pesquisa social. **São Paulo:**, 2010.

GIUNIPERO, L. C.; ELTANTAWY, R. A. Securing the upstream supply chain: a risk management approach. **International Journal of Physical Distribution & Logistics Management,** v. 34, n. 9, p. 698-713, 2004. ISSN 0960-0035.

GOMES, C. F. S. R., PRISCILLA C. C. **Gestão de Cadeia de Suprimentos Integrada à Tecnologia da Informação**. 2004.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. **ACM Transactions on Information and System Security,** v. 5, n. 4, p. 438-457, 2002. ISSN 1094-9224.

GORDON, L. A. et al. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. **Journal of Information Security,** v. 6, n. 1, p. 24-30, 2015. ISSN 21531234.

GORDON, L. A.; LOEB, M. P.; SOHAIL, T. Market value of voluntary disclosures concerning information security. **MIS quarterly,** v. 34, n. 3, p. 567-594, 2010. ISSN 0276-7783.

GUNASEKARAN, A.; NGAI, E. W. T. Information systems in supply chain integration and management. **European Journal of Operational Research,** v. 159, n. 2, p. 269-295, 2004. ISSN 03772217.

GUNASEKARAN, A.; PATEL, C.; MCGAUGHEY, R. E. A framework for supply chain performance measurement. **International journal of production economics,** v. 87, n. 3, p. 333-347, 2004. ISSN 0925-5273.

GUNASEKARAN, A.; PATEL, C.; TIRTIROGLU, E. Performance measures and metrics in a supply chain environment. **International Journal of Operations & Production Management,** v. 21, n. 1, p. 71-87, 2001. ISSN 0144-3577.

GUPTA, M. et al. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. **Decision Support Systems,** v. 41, n. 3, p. 592-603, 2006. ISSN 0167-9236.

GUTTMAN, B.; ROBACK, E. A. **An introduction to computer security: the NIST handbook**. Journal of Research of the National Institute of Standards and Technology, 1995. ISBN 0788128302.

HASSINI, E.; SURTI, C.; SEARCY, C. A literature review and a case study of sustainable supply chains with a focus on metrics. **International Journal of Production Economics,** v. 140, n. 1, p. 69-82, 2012. ISSN 0925-5273.

HEDSTRÖM, K. et al. Value conflicts for information security management. **The Journal of Strategic Information Systems,** v. 20, n. 4, p. 373-384, 2011. ISSN 0963-8687.

HUANG, C. D.; BEHARA, R. S.; GOO, J. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. **Decision Support Systems,** v. 61, p. 1-11, 2014. ISSN 0167-9236.

IDS. IDS - Saúde. 2015. Disponível em: < http://www.ids.inf.br >. Acesso em: 05/12/2015.

ISO-IEC. **ISO 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary** 2014.

ITPCG. The financial benefits of spend on security. 2013. Disponível em: < http://www.wellingtonresearch.com >. Acesso em: 07/01/2016.

KAZEMZADEH, R. B.; SEPEHRI, M. M.; JAHANTIGH, F. F. Design and analysis of a health care supply chain management. Advanced Materials Research, 2012, Trans Tech Publ. p.2128-2134.

KERLINGER, F. N. Metodologia da pesquisa em ciências sociais: um tratamento conceitual. In: (Ed.). **Metodologia da pesquisa em ciências sociais: um tratamento conceitual**: Editora Pedagógica e Universitária, 2009.

KETCHEN, D. J.; HULT, G. T. M. Bridging organization theory and supply chain management: The case of best value supply chains. **Journal of Operations Management,** v. 25, n. 2, p. 573-580, 2007. ISSN 02726963.

KRAEMER, S.; CARAYON, P. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. **Applied ergonomics,** v. 38, n. 2, p. 143-154, 2007. ISSN 0003-6870.

LANDOLT, S. et al. Assessing and comparing information security in swiss hospitals. **Interactive journal of medical research,** v. 1, n. 2, 2012.

LAVASTRE, O.; GUNASEKARAN, A.; SPALANZANI, A. Supply chain risk management in French companies. **Decision Support Systems,** v. 52, n. 4, p. 828-838, 2012. ISSN 0167-9236.

LEE, S. M.; LEE, D.; SCHNIEDERJANS, M. J. Supply chain innovation and organizational performance in the healthcare industry. **International Journal of Operations & Production Management,** v. 31, n. 11, p. 1193-1214, 2011. ISSN 0144-3577.

LI, L.; SU, Q.; CHEN, X. Ensuring supply chain quality performance through applying the SCOR model. **International Journal of Production Research,** v. 49, n. 1, p. 33-57, 2011. ISSN 0020-7543.

LIANG, H.; XUE, Y. Avoidance of information technology threats: a theoretical perspective. **MIS quarterly**, p. 71-90, 2009. ISSN 0276-7783.

LOCKAMY III, A.; MCCORMACK, K. Linking SCOR planning practices to supply chain performance: An exploratory study. **International Journal of Operations & Production Management,** v. 24, n. 12, p. 1192-1218, 2004. ISSN 0144-3577.

LOSSES, N. Estimating the Global Cost of Cybercrime. **McAfee, Centre for Strategic & International Studies**, 2014.

LUCIANO, E. M.; BRAGANÇA, C. E. B.; TESTA, M. G. Privacidade de informações de pacientes de instituiçoes de saúde: a percepção de profissionais da área de saúde. **REUNA,** v. 16, n. 2, 2011. ISSN 2179-8834.

LUCIANO, E. M.; MAÇADA, A. C. G.; MAHMOOD, A. The influence of human factors on vulnerability to information security breaches. AMCIS, 2010. p.351.

MAGNAGNAGNO, O. A. Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde. 2015.

MAGNAGNAGNO, O. A.; LUCIANO, E. M.; BRITTO-DA-SILVA, V. R. Mecanismos para Proteção da Privacidade das Informações do Prontuário Eletrônico de Pacientes de Instituições de Saúde. **Anais do XXXIX ENANPAD, 2015, Brasil.**, 2015.

MARUCHECK, A. et al. Product safety and security in the global supply chain: Issues, challenges and research opportunities. **Journal of Operations Management,** v. 29, n. 7, p. 707-720, 2011. ISSN 0272-6963.

MIN, H.; ZHOU, G. Supply chain modeling: past, present and future. **Computers & industrial engineering,** v. 43, n. 1, p. 231-249, 2002. ISSN 0360-8352.

MONTESDIOCA, G. P. Z.; MAÇADA, A. C. G. Measuring user satisfaction with information security practices. **Computers & Security,** v. 48, p. 267-280, 2015. ISSN 0167-4048.

MUSTAFFA, N. H.; POTTER, A. Healthcare supply chain management in Malaysia: a case study. **Supply Chain Management: An International Journal,** v. 14, n. 3, p. 234-243, 2009. Disponível em: < http://www.emeraldinsight.com/doi/abs/10.1108/13598540910954575 >.

MV. Solução - Hospitalar. 2015. Disponível em: < http://www.mv.com.br/pt/solucoes/hospitalar >. Acesso em: 01/12/2015.

NAGURNEY, A.; NAGURNEY, L. S. A game theory model of cybersecurity investments with information asymmetry. **NETNOMICS: Economic Research and Electronic Networking**, p. 1-22, 2015. ISSN 1385-9587.

OCEG. **OCEG Red Book - GRC Capability Model**. oceg.org 2012.

_____. GCR. 2015. Disponível em: < http://www.oceg.org >. Acesso em: 12/04/2015.

ÖĞÜTÇÜ, G.; TESTIK, Ö. M.; CHOUSEINOGLOU, O. Analysis of personal information security behavior and awareness. **Computers & Security,** v. 56, p. 83-93, 2016. ISSN 0167-4048.

PATEL, S. C.; GRAHAM, J. H.; RALSTON, P. A. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. **International Journal of Information Management,** v. 28, n. 6, p. 483-491, 2008. ISSN 0268-4012.

PHILIPS. Philips Tasy - Sistema de Gestão em Saúde. 2015. Disponível em: < http://www.cilatam.philips.com.br/solucoes/13/tasy-prestador/ >. Acesso em: 03/12/2015.

RACZ, N.; WEIPPL, E.; SEUFERT, A. A frame of reference for research of integrated governance, risk and compliance (GRC). Communications and Multimedia Security, 2010, Springer. p.106-117.

RIVARD-ROYER, H.; LANDRY, S.; BEAULIEU, M. Hybrid stockless: A case study: Lessons for health-care supply chain integration. **International Journal of Operations & Production Management,** v. 22, n. 4, p. 412-424, 2002. ISSN 0144-3577.

SAFA, N. S.; VON SOLMS, R.; FURNELL, S. Information security policy compliance model in organizations. **computers & security,** v. 56, p. 70-82, 2016. ISSN 0167-4048.

SAMPIERI, R. H. et al. **Metodologia de pesquisa**. 5 ed. Porto Alegre: Penso, 2013. ISBN 8586804932.

SAMY, G. N.; AHMAD, R.; ISMAIL, Z. Security threats categories in healthcare information systems. **Health informatics journal,** v. 16, n. 3, p. 201-209, 2010. ISSN 1460-4582.

SCC. **Supply Chain Operations Reference (SCOR) model** 2010.

SCHLEGEL, G. L.; TRENT, R. J. **Supply Chain Risk Management: An Emerging Discipline**. Crc Press, 2014. ISBN 1482205971.

SPDATA. Sistema de Gestão Hospitalar. 2015. Disponível em: < http://www.spdata.com.br >. Acesso em: 05/12/2015.

TEN, C.-W.; LIU, C.-C.; MANIMARAN, G. Vulnerability assessment of cybersecurity for SCADA systems. **Power Systems, IEEE Transactions on,** v. 23, n. 4, p. 1836-1846, 2008. ISSN 0885-8950.

WARREN, M.; HUTCHINSON, W. Cyber attacks against supply chain management systems: a short note. **International Journal of Physical Distribution & Logistics Management,** v. 30, n. 7/8, p. 710-716, 2000.

APÊNDICE A – ROTEIRO DE ENTREVISTA

Roteiro de Entrevista

Estrutura da CS para melhor performance financeira

1. Qual é o fluxo das informações da empresa? Desde a chegada de um item ou serviço do fornecedor até a entrega/prestação do mesmo ao seu cliente?
2. Quais atividades podem ser consideradas essenciais neste fluxo?
3. Qual sua percepção quanto ao papel da empresa na CS?
4. Existe uma relação integrada com os parceiros e o conhecimento de como eles lidam com as informações compartilhadas?
5. Quem são seus principais fornecedores com os quais compartilham informações?
6. Quem são seus principais clientes com os quais compartilham informações?

Informações a serem protegidas

7. Que tipo de informação são mais críticas de serem protegidas?
8. Qual a principal preocupação quanto à Segurança da Informação na CS quanto a relação com o fornecedor, internamente e no relacionamento com o cliente?
9. Existe a definição e controle de acesso das pessoas que podem acessar os sistemas e realizar ações no fluxo de informações da CS?
    a. Que tipo de segurança existe para controlar essas iterações?
10. Como se dá a comunicação com fornecedores e clientes? Existem sistemas para realizar esta comunicação?

Ameaças e ações de mitigação para a Segurança da Informação

11. A empresa reconhece a existência de ameaças à Segurança das Informações?
    a. Podes descrever quais os possíveis impactos? (ex.: imagem, operação, financeira)
    b. Que tipo de ações são realizadas para mitigá-las?
    c. Existe alguma ação de mitigação especial envolvendo a CS? Explique.
12. A empresa possui políticas formais de Segurança da Informação, tais como regras e políticas de comportamento?
    a. São realizados treinamentos aos funcionários para conscientização sobre Segurança da Informação? Explique.
13. A maior parte dos sistemas utilizados são adquiridos no mercado ou desenvolvidos internamente?
14. São utilizados sistemas compartilhados com os parceiros da CS?
15. Existe algum tipo de monitoramento constante sobre os servidores e sistemas quanto a possíveis ataques? Explique.

Investimentos em Segurança da Informação

16. Existe na empresa alguma avaliação formal dos possíveis prejuízos que podem ser causados por ataques à informação?
    a. É utilizado algum tipo de métrica na empresa para medir estes impactos?
17. Existe a definição de orçamento específico para o investimento em ações de segurança?
    a. Este orçamento é baseado em que tipo de critério?
18. Você consegue estabelecer uma relação custo benefício entre investimentos em Segurança da Informação em relação a possíveis prejuízos causados por ataques bem sucedidos?
    a. Este assunto já foi abordado alguma vez na empresa? Como?
19. A empresa possui ou já considerou a contratação de seguros para informações?

Encerramento

20. Tens algum comentário geral ou observação sobre aspectos de Segurança da Informação em sua CS?
21. Tens algum comentário geral ou observação sobre a pesquisa?

Dados Pessoais e Organizacionais dos entrevistados

22. Qual sua idade? Gênero: M( ) F( )
23. Qual sua área de formação?
24. Qual seu tempo de atuação profissional?
25. Qual sua atual função na empresa?
    a. Há quanto tempo está nesta função na empresa?
    b. Como ela se relaciona com CS e/ou Segurança da Informação?
26. Quantos profissionais atuam na empresa?

APÊNDICE B – CARTA DE APRESENTAÇÃO

Pontifícia Universidade Católica do Rio Grande do Sul
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
PÓS-GRADUAÇÃO

Coleta de Dados para Dissertação de Mestrado

Prezado(a),

Venho por meio desta, solicitar sua participação em uma pesquisa para minha Dissertação sobre investimentos em segurança de informação. Sou estudante de Mestrado em Administração da PUC RS e orientado pela Profa. Dra. Edimara Mezzomo Luciano.

A pesquisa se trata sobre investimentos em Segurança da Informação em Cadeias de Suprimento da Saúde. Ela tem por objetivo compreender como os participantes da cadeia percebem e decidem sobre os gastos com equipamentos, sistemas e treinamentos de seus funcionários para proteger suas informações dentro da empresa e no relacionamento com as demais empresas da cadeia.

Para que se consiga atingir o objetivo citado, busca-se entrevistar pessoas que efetivamente participem das decisões sobre os investimentos de TI. Dois perfis principais foram identificados:

1. **Profissional de TI**. Gerentes, diretores ou CIO. Que provêm as informações e suas análises aos demais participantes da administração para que as decisões sejam tomadas.
2. **Profissional da área administrativa ou financeira**. Gerentes, diretores ou CEO. Que tenham uma visão abrangente do negócio e que possam avaliar os impactos financeiros sobre ações de Segurança da Informação.

Não serão publicadas quaisquer informações que possa identificar diretamente a empresa ou o entrevistado. Após a conclusão da pesquisa, a mesma poderá encaminhada para seu conhecimento.

A expectativa é de que a entrevista não dure mais do que 40 minutos.

Atenciosamente,

Tiago M Furlanetto

tiagomf@gmail.com

PUCRS
Campus Central
Av. Ipiranga, 6681 – P. 50 – CEP: 90619-900
Fone: (51) 3320-3524 – Fax (51) 3320-3624
E-mail: man@pucrs.br
www.pucrs.br