O Processo de Formulação de uma Política de Segurança de Informações Segundo a Percepção dos Gestores: Um Estudo em Instituições Hospitalares

Autoria: Luis Hernan Contreras Pinochet, Alberto Luiz Albertin

Resumo

O objetivo desta pesquisa foi identificar os elementos norteadores no processo de formulação de uma Política de Segurança de Informações por meio da percepção dos gestores, visando elaborar uma estrutura de análise a partir do estudo em cinco organizações hospitalares. O método utilizado nesta pesquisa foi a *Grounded Theory* que possibilitou analisar os aspectos subjetivos como as percepções e opiniões que os gestores têm quanto ao tema deste estudo. A pesquisa conduziu o desenvolvimento de uma estrutura de análise no qual foi possível identificar as responsabilidades em relação à segurança da informação nos diferentes níveis organizacionais, delineando responsabilidades em relação à implementação, verificação da conformidade, auditoria e avaliação, estabelecendo orientações necessárias em relação às ações e objetivos que poderão ser implementados. Como resultado, observou-se que as organizações hospitalares deste estudo, em suas distintas naturezas, possuíram claras deficiências para formular uma Política de Segurança de Informação devido à necessidade de definições claras nos papéis dos diversos grupos organizacionais envolvidos, e de elementos norteadores para a percepção na tomada de decisão por parte dos gestores.

1. Introdução

A área da saúde está atenta à nova realidade em adotar novos Sistemas de Informação em seus registros clínicos para transferir integralmente todos os registros dos pacientes em formato de documentos impressos e guias para o meio magnético. Dentro das instituições de saúde, o núcleo das informações está armazenado no prontuário do paciente, que pode ser considerado o coração das instituições de saúde, pois ele é o registro histórico de maior valor para o paciente, o médico, o hospital e a equipe envolvida na saúde do paciente.

A utilização da Tecnologia da Informação dentro deste tipo de organizações também direciona desafios na Gestão da Segurança dos diversos ativos (humanos, físicos, materiais e, principalmente, informacionais) porque estas organizações convivem atualmente em um mundo competitivo e altamente globalizado, no qual a informação do paciente vem sendo considerada por muitos como o mais valioso ativo das empresas.

Broderick (2001) e Scudere (2007) consideram que a informação é o recurso mais crítico no mundo dos negócios e que as empresas devem gerenciar os riscos associados a informações como uma prática padrão. Nesse sentido, faz-se necessária a formulação de uma Política de Segurança de Informações *"formal"* para as organizações hospitalares para a proteção destes ativos.

2. Referencial Teórico

2.1 O papel dos gestores na tomada de decisão em organizações hospitalares frente à adoção de Tecnologia da Informação

Na gestão hospitalar predomina a descentralização das decisões e a aproximação de todos os elementos da equipe de trabalho, oferecendo a eles oportunidades de participação efetiva na discussão e no aperfeiçoamento constante das atividades profissionais, conforme observado por Peterlini (2004).

Vasconcellos et al. (2002) destacam que o processo decisório implica assumir compromissos e que se trata de um processo de escolha, que a cada dia se torna mais difícil, dada a simultaneidade de problemas e sua complexidade, cada vez mais crescente.

Segundo Rodrigues (1996) o uso da Tecnologia de Informação por parte dos gestores de saúde tem se tornado cada vez mais importante. Este instrumento serve como fonte de

informação em relação aos indicadores do hospital, fornecendo dados importantes sobre a instituição e apoiando o processo decisório e estratégico da gestão administrativa.

Se, por um lado, a ética exige, entre outras coisas, o sigilo e a privacidade das informações sobre o paciente, por outro, o mau-uso da informática vem facilitando seu extravio e seu acesso indevido; os sistemas que utilizam redes de computadores tornam estes dados vulneráveis a acessos não autorizados; a facilidade de alteração de dados registrados eletronicamente traz perigos adicionais à vida e ao bem estar dos pacientes, além de facilitar a fraude conforme Salvador e Filho (2005).

Nesse sentido, Johanston (1993) verificou que tomando o exemplo de um hospital, podemos verificar essas relações de interdependência entre os vários subsistemas organizacionais (áreas funcionais) que buscam a segurança das informações dos prontuários dos pacientes como ativos mais valiosos.

2.2 A Gestão da Segurança e a Política de Segurança de Informações

Wilson, Turban e Zviran (1992) verificaram que os aspectos relacionados com a Segurança da Informação ganharam o mundo corporativo e, atualmente, são fatores críticos de sucesso para o negócio. Barman (2002) considera que é preciso entender o contexto atual da segurança da informação no ambiente corporativo, ou seja, o ambiente comum às empresas, composto por três aspectos básicos: pessoas, processos e tecnologia.

Segundo Nakamura e Geus (2002) e Menezes (2006) a responsabilidade da Gestão da Segurança da Informação muitas vezes é encarada como uma prática administrativa compartilhada por todos os integrantes da organização, exigindo, para a eficácia das medidas de proteção, o estabelecimento de uma estrutura organizacional capaz de planejar e implementar a segurança desejada.

Para Beal (2005) existe uma grande tendência nas organizações de se atribuir as atividades e responsabilidades de segurança à unidade de tecnologia da informação. Os obstáculos que poderão surgir no estabelecimento de uma política efetiva de segurança são, na maior parte, relacionados com fatores humanos (RAMOS; CAVALCANTE, 2005).

Peltier (2002) considera que mesmo que exista um esforço interno na unidade de Tecnologia da Informação para desenvolver também iniciativas relacionadas à proteção de ativos físicos e à conscientização de gerentes e funcionários para as questões não tecnológicas da segurança, o resultado nunca será o mesmo que o obtido com a existência de uma estrutura mais completa e integradora de todos os processos de segurança. Nesse sentido Fugini e Bellettini (2004) verificaram em suas pesquisas que a segurança da informação exige uma abordagem que envolva a cúpula estratégica da organização.

Todavia para Solms (1999) e Ramos e Cavalcante (2005), sabe-se que adotar práticas mais avançadas de segurança de informação não é trivial, devido à complexidade, ao custo e ao tempo de implantação de tais políticas. Isso se torna mais crítico em organizações de menor porte.

Peltier et al. (2003) definem que na estrutura organizacional a ser encarregada da gestão da segurança da informação, é importante levar em consideração uma série de variáveis organizacionais. Em toda organização, a forma como estão estruturadas as pessoas em termos formais e informais afeta profundamente o desempenho.

De acordo com Höner e Eloff (2002), isso indica o compromisso e o apoio da administração à segurança, definindo as regras que a segurança tem que criar para alcançar a missão da organização. Este desenvolvimento não deve ser encarado como uma atividade simples ou que mereça pouca atenção, mas como um elemento essencial para a segurança das operações e atividades do negócio (FERREIRA, 2003).

A política de segurança da informação segundo Trcek (2000) é um processo contínuo de estabelecer, redefinir e implementar objetivos de segurança, com relação a todos os

aspectos e níveis de recursos de sistemas de informação e que são baseados na estrutura e na missão da organização.

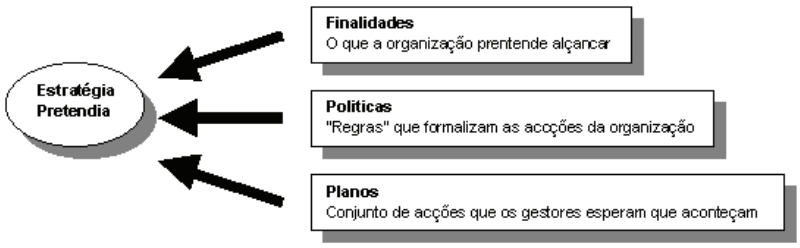
Portanto, frente a essa iniciativa de implementar as políticas de segurança, as pessoas nas organizações têm sido consideradas o componente mais importante em um programa eficaz de segurança da informação, enfocando preocupações das práticas das políticas de segurança, com atenção ao direcionado de aspectos de educação, conscientização e treinamento (WILSON, HASH, 2004; EGAN; MATHER, 2004, RAMOS; CAVALCANTE, 2005).

2.3 A Formulação da Política de Segurança como Estratégia

A concepção predominante entende a formulação estratégica como um processo que se desenvolve em uma série de etapas seqüenciais, racionais e analíticas e envolve um conjunto de critérios objetivos baseados na racionalidade econômica para auxiliar os gestores na análise das alternativas estratégicas e tomadas de decisão (LEARNED, CHRISTENSEN, ANDREWS; GUTH, 1965; ANDREWS, 1971; STEINER; MINER, 1977; HOFER; SCHENDEL, 1978; JAUCH; GLUECK, 1980).

Neste contexto de formulação estratégia, é a perspectiva introduzida por Lindbloom (1959), mas desenvolvida com Quinn (1980), com a noção de *"incrementalismo lógico"*, é a que vista a reduzir a incerteza e beneficiar a melhor informação disponível.

Segundo Mintzberg e Waters (1985) as estratégias que os gestores propõem, definem e que pretendem ver, realizadas são as estratégias pretendidas, e as que realmente se concretizam são as estratégias realizadas. Na figura a seguir são apresentadas as estratégias pretendidas:



Esquema 1- Elementos de uma estratégia pretendida
Fonte: (MINTZBERG; WATERS, 1985, pg. 57).

As estratégias pretendidas devem funcionar como linhas mestras para a forma como a organização trabalha para alcançar seus resultados. Basicamente as políticas são linhas mestras que indicam limites ou restrições sobre aquilo que se quer conseguir e os planos têm a ver com os meios que usamos para chegar a certos fins.

Em relação à política, Sloan (1963) enunciou dos princípios fundamentais relacionados com a formulação de uma política: primeiro, que o desenvolvimento ou criação de políticas avançadas e construtivas e que é de vital importância para o progresso e a estabilidade da empresa; segundo, que deve ser reconhecido através de uma especialização do desenvolvimento da política, independentemente de sua execução.

3. Trajetória Metodológica da Pesquisa

As empresas escolhidas para esta pesquisa foram selecionadas pelos seguintes critérios: em função de sua tipicidade; em função do seu tempo de existência / posição no mercado; e pela facilidade de acesso aos dados. A seguir são apresentadas, no quadro abaixo, as principais características dos cinco hospitais pesquisados.

O acesso a informações foi assegurado pela autorização formal para realizar a pesquisa, entretanto, dos cinco hospitais pesquisados, três autorizaram a publicação do seu

nome, e dois autorizaram o desenvolvimento da pesquisa, mas solicitaram que não fosse publicado o nome do hospital preservando o seu anonimato com nomes fictícios.

	Santa Casa – São José dos Campos	**Hospital e Maternidade São Camilo – Ipiranga**	**Hospital Infantil Cândido Fontoura**	**Hospital de "Alta Complexidade A"**	**Hospital de "Alta Complexidad e B"**
Natureza	Filantrópico - Privado	Filantrópico – Privado	Público – da Administração Direta (subordinado a Secretaria da Saúde).	Filantrópico - Privado	Privado
Porte (*)	Grande	Médio	Médio	Grande	Grande

Quadro 1 - Características dos hospitais pesquisados
Fonte: Primária – (*) Quanto à capacidade ou lotação (pequeno de 25 a 49 leitos; médio de 50 a 149 leitos; grande de 150 a 500 leitos; e especial ou extra acima de 500 leitos) segundo Borba (1991) e Organização Mundial de Saúde (OMS) (disponível em: http://www.who.int/en/).

A concentração desta pesquisa utilizou-se de várias fontes para a coleta dos dados em busca de evidências. As fontes para o estudo podem ser provenientes de documentos, registros de arquivos, entrevistas, observação direta ou não-participante, observação participante e artefatos. Em geral, inicia-se a coleta de dados por meio da realização de entrevistas abertas. À medida que as categorias vão emergindo dos dados, as entrevistas tornam-se semi-estruturadas (BANDEIRA-DE-MELLO; CUNHA, 2003).

Quando não foram permitidas as gravações das entrevistas, foram tomadas notas de campo. A duração média das entrevistas variou entre 2 (duas) a 3 (três) horas totalizadas aproximadamente 24 horas ou 1.440 minutos em dois momentos distintos de coletas caracterizando uma pesquisa longitudinal sempre com os mesmos gestores. As entrevistas foram gravadas, transcritas, e analisadas obedecendo às exigências do método. Cada entrevista foi precedida da apresentação do pesquisador *"entrevistador"*, uma breve explanação dos objetivos do trabalho e de uma explicação de como funcionaria o processo da entrevista.

A observação não participante foi outra fonte utilizada para a coleta de dados primários, a fim de possibilitar informações adicionais. Neste sentido, fatos e ocorrências, comportamentos e condições ambientais da realidade organizacional relacionado ao foco da pesquisa foram observados e registrados (STRAUSS, 1991).

Esta pesquisa utilizou um **design de estudo de multicasos** e **corte longitudinal** (MERRIAM, 1998), de **caráter contextual e processual** de **cunho exploratório e descritivo** com a intenção de geração de teoria, no sentido da *Grounded Theory* (STRAUSS; CORBIN, 1998).

Ao utilizar o método da *Grounded Theory* foi necessária a utilização da técnica de pesquisa qualitativa do **Estudo de Caso**, pois foram feitas descrições e análises intensivas de um grupo de gestores em relação ao tema abordado.

A lógica do tratamento de dados utilizou a **abordagem qualitativa**, porque a pesquisa teve como pressuposto a obtenção de dados a partir de entrevistas individuais e em grupo, e interativas na organização, visando compreender os fenômenos segundo as perspectivas dos sujeitos (STRAUSS, 1991).

A **amostra** foi constituída por 14 (quatorze) gestores de um dos cinco Hospitais analisados nesta pesquisa. No qual, o princípio orientador foi a saturação de dados, isto é, amostrar até o ponto em que não é obtida nenhuma informação nova e é atingida a redundância segundo Strauss e Corbin (1998).

As entrevistas foram realizadas em dois momentos distintos caracterizando duas fases de exploração dos dados em **estudos longitudinais** – este estudo exigiu que os dados fossem coletados pela mesma amostra nos dois momentos da pesquisa – isto é, os mesmos gestores participaram da pesquisa em dois momentos distintos e obedeceram aos seguintes questionamentos:

1- Como você entende o processo de evolução e o uso das tecnologias e sistemas de informação no hospital?
2- Qual é o nível de dependência da tecnologia e sistemas de informação nesta organização hospitalar?
3- Qual é a importância da segurança de informação no hospital?
4- Qual é o papel dos gestores na formulação de estratégias e na tomada de decisão em relação ao desenvolvimento de planos estratégicos no hospital?
5- Qual é o papel dos gestores na formulação de uma política de segurança de informação para o hospital?

A hipótese a seguir, é derivada dos dados após os exercícios interpretativos de análise e síntese, inerentes ao método de pesquisa:

> ***H_1:*** *As organizações hospitalares, em suas distintas naturezas, possuem claras deficiências para formular uma política de segurança de informação formal devido à falta de definições claras nos papéis dos diversos grupos organizacionais, e de elementos norteadores para a percepção na tomada de decisão por parte dos gestores.*
> **Informação pretendida:** a partir das percepções e opiniões dos gestores verificar se existe coerência na afirmação (H_1)com base na realidade das organizações pesquisadas.

As unidades de significado, categorias, e subcategorias surgiram a partir da análise das transcrições das entrevistas realizadas pelos quatorze gestores envolvidos nesta pesquisa. Os agrupamentos foram realizados com base na semelhança dos assuntos que foram abordados pelos entrevistados e também pela orientação das ferramentas analíticas do método de pesquisa.

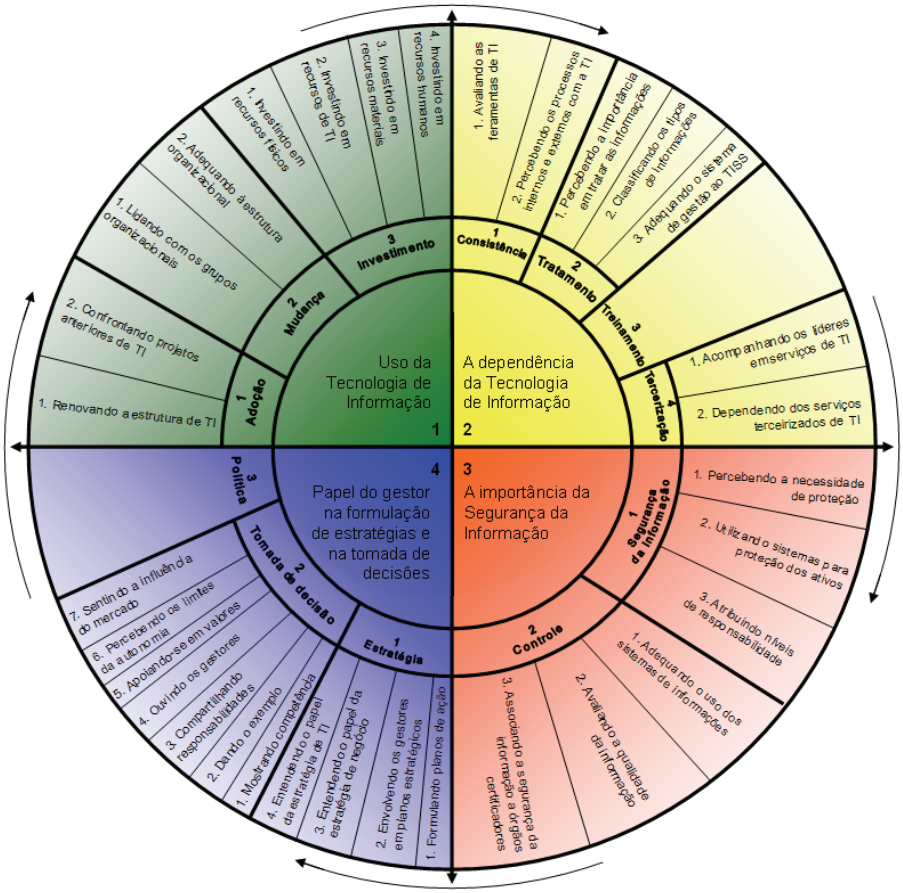
Nesse sentido, em muitos casos as subcategorias agrupadas formaram categorias que por sua vez agrupadas formaram as unidades de significados. Entretanto, nem sempre foram identificadas ocorrências de todos os hospitais e gestores em todas as categorias, seguindo o método é possível a criação de uma categoria que tenha sido apresentada por um gestor apenas ou centrada em um hospital.

4. Discussão dos Resultados

Atualmente a organização hospitalar é uma das mais complexas, não apenas pela nobreza e amplitude da sua missão, mas, sobretudo, por apresentar uma equipe multidisciplinar com elevado grau de autonomia em seu modelo estrutural.

As organizações hospitalares, públicas ou privadas, estão inseridas num ambiente complexo e singular que as condiciona a um funcionamento inadequado diante da lógica da acumulação lucrativa dos mercados. Pois, independentemente de sua natureza, ambas as condições estão subordinadas a princípios éticos e legais que normatizam o setor saúde e às políticas governamentais, que colocam os hospitais frente a uma diversidade de interesses divergentes a contemplar.

Através de um estudo foi construída uma teoria fundamentada nos dados, utilizando-se o método da *Grounded Theory*, que gerou a estrutura apresentada a seguir:



Esquema 2- Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em organizações hospitalares
Fonte: Primária.

Este tipo de pesquisa contextualista, processual, e qualitativa conseguiu captar a essência do fenômeno que ocorreu em uma área substantiva delimitada, explicando-o em seus aspectos mais relevantes para os gestores envolvidos.

Evitam-se, assim, estudos transversais que visam estabelecer correlações entre variáveis, definidas a *priori* e mensuradas quantitativamente, que não admitem diferenças entre as organizações. Tais estudos mostram-se insuficientes para explicar formulações estratégicas ou mudanças tecnológicas que devem ser tratadas como um processo político e social – e não somente como um processo analítico e racional – em face das heterogeneidades das forças e resistência que impedem a efetiva implementação das mudanças.

O método da *Grounded Theory* nesta pesquisa forneceu um conjunto de técnicas que aumentaram a credibilidade dos resultados obtidos, tornando-os passíveis de atenção das organizações hospitalares e de avaliação pela área científica acadêmica. Os principais resultados, implicações e contribuições da pesquisa são apresentadas a seguir:

- Foram identificados os elementos norteadores para a formulação estratégica de uma Política de Segurança de Informação, com base na percepção dos gestores. Estes elementos compreenderam no surgimento das unidades de significância, categorias e subcategorias que formaram a estrutura: *"Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em organizações hospitalares"* através do agrupamento dos dados que foram obtidos pelos gestores que foram os sujeitos desta pesquisa.

- Com a identificação destes elementos e da estrutura de análise foi possível nas pesquisas de profundidade com os gestores verificar como ocorre o envolvimento destes gestores em suas distintas estruturas organizacionais na formulação de estratégias de uma Política de Segurança de Informações.
- Após o entendimento de como a Política de Segurança de Informações deve ser direcionada em instituições hospitalares, foi possível compreender como seria uma política *"formal"* para este tipo de instituição e quais seriam as áreas ou grupo organizacionais que estariam alinhados neste processo em relação às percepções dos gestores.
- Considerando que o estudo teve que ser delimitado em função da redundância de dados obtidos na coleta e análise dados, verificou-se que a estrutura *"Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em organizações hospitalares"* foi capaz de relacionar os diferentes elementos norteadores para a formulação estratégica de uma Política de Segurança de Informações em organizações hospitalares.
- Também se verificou que a utilização desta estrutura de análise limita-se as organizações hospitalares: públicas ou particulares, devido a esse tipo de organização possuir especificidades características, como por exemplo, a regulamentação colocada por órgãos governamentais, tais como: a Agência Nacional de Saúde, e a Secretaria e Coordenação de Saúde. Pelas próprias certificações necessárias para as instituições hospitalares como exemplo, *Joint Comission*, Organização Nacional de Acreditação, algumas orientações da ISO específicas para processos, selos de qualidade, entre outras. Nesse sentido, esta estrutura de análise poderia servir também como um processo de avaliação para organizações hospitalares públicas e privadas.

Portanto, a estrutura do *"Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em organizações hospitalares"* surge com o propósito de auxiliar a alta gestão e os executivos que tomam decisões relacionadas com a área de Tecnologia de Informação como um *"recurso orientador"* para o desenvolvimento de uma Política de Segurança de Informações *"formal"*.

Não existiria a possibilidade de que esta estrutura de análise seja utilizada como um *check list* porque cada organização possui características, história, cultura, e gestores com direcionamentos distintos. Em uma mesma organização hospitalar poder-se-ia encontrar em um curto período de tempo diferentes formas de gestão e direcionamentos estratégicos, como foi o caso de alguns hospitais presentes nesta pesquisa.

Nesta pesquisa foram observadas 34 categorias-chave, desdobradas em 32 subcategorias, e 2 categorias que não tiveram subdivisões, que é o caso das categorias Treinamento e Política. Nestas 34 categorias-chave foram associadas à presença de contribuição dos hospitais que fizeram parte desta pesquisa e chegou-se nos seguintes resultados: o Hospital de "Alta Complexidade A" foi o que obteve a maior presença de categorias-chave, com 33 ocorrências, em segundo lugar aparece o Hospital e Maternidade São Camilo Ipiranga com 29 ocorrências, em terceiro lugar ficou o Hospital Santa Casa de São José dos Campos com 28 ocorrências, em quarto lugar aparece o Hospital Infantil Cândido Fontoura com 23 ocorrências, e por fim, ficou o Hospital de "Alta Complexidade B" com 17 ocorrências.

Estas ocorrências não pretendem relevar possíveis fraquezas ou fragilidades por parte dos gestores que foram sujeitos desta pesquisa em relação à falta de conhecimento do tema abordado nesta pesquisa ou que os gestores se reservaram ao direito de omitir possíveis informações estratégicas das organizações hospitalares, mas sim indicar o nível de

contribuição dos gestores para a geração das categorias que se tornaram representativas para esta pesquisa.

4.1 Segmentos e responsabilidades da Política de Segurança de Informações em organizações hospitalares

A política de segurança em organizações hospitalares como foi observado nesta pesquisa deve capacitar a organização com instrumentos jurídicos, normativos e processuais. Esses instrumentos devem abranger as estruturas físicas, tecnológicas e administrativas, de forma a garantir a confidencialidade, integridade e disponibilidade das informações corporativas.

Desta forma, com o propósito de fornecer orientação e apoio às ações de gestão da segurança, a política possui uma função fundamental e assume uma grande abrangência, podendo ser subdividida em três segmentos que são descritos a seguir: diretrizes, normas, e procedimentos.

Portanto, a política deve ressaltar que cada colaborador é responsável por usar os recursos tecnológicos disponíveis de forma a aumentar sua produtividade e contribuir para os resultados e a imagem pública da organização, no caso hospitalar.

Com base na estrutura que emergiu dos dados nesta pesquisa – *"Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em Organizações Hospitalares"* foi possível desenvolver um esboço do que representaria o conteúdo de uma política *"formalmente aceitável"* em organizações hospitalares. Esta política deverá ter uma abrangência ampla, mantendo seu foco nas questões de princípio, sem entrar em detalhes técnicos e de implementação adaptado a partir do modelo de Beal (2006).

Verificou-se nesta pesquisa que é aconselhável que o documento que registrará a política de segurança contenha uma declaração introdutória, inserindo o problema da segurança da informação no contexto mais amplo dos riscos do negócio e explicando a importância da informação e dos recursos computacionais e da infra-estrutura tecnológica, e a necessidade de protegê-los contra as ameaças existentes para prevenir conseqüências negativas que poderiam advir da destruição, alteração indevida ou divulgação não autorizada de informações.

A Política de Segurança de Informações deverá identificar claramente as responsabilidades em relação à segurança da informação em todos os níveis organizacionais, delineando responsabilidades em relação à implementação verificação da conformidade, auditoria e avaliação estabelecendo orientações necessárias em relação a todas as medidas de proteção que serão implementadas.

Embora o conteúdo da Política de Segurança de Informações varie de acordo com a natureza, tamanho, nível estrutural, missão, estágio de maturidade em relação ao nível de adoção tecnológica, sugere-se a partir deste estudo os seguintes aspectos para o direcionamento no desenvolvimento de uma política formalmente aplicável a organizações hospitalares e que fazendo os respectivos alinhamentos organizacionais poder-se-ia ser aplicado a outros modelos organizacionais em outros setores.

Tabela 1 - Conteúdo de uma Política de Segurança de Informações

Aspectos	Definições e Orientações	Forma de Apresentação
Organização da segurança	- **Diretrizes** que definem sobre a estrutura de gestão adotada para administrar as questões de segurança da informação, com indicação de quem é responsável e presta contas pela segurança em todos os níveis da organização e quais as linhas hierárquicas existentes entre as funções de segurança.	**Ações e Objetivos**
Classificação e controle dos ativos de	- **Diretrizes** que orientam sobre realização de inventário dos ativos informacionais, formas de classificação da informação,	

informação	responsabilidades pela manutenção dos controles necessários para protegê-los.	
Aspectos humanos da segurança	- **Diretrizes** que definem a política de segurança de pessoal (processos de admissão e demissão, requisitos de segurança aplicáveis a funcionários e prestadores de serviço, treinamento em segurança). - **Diretrizes** do comportamento esperado em relação ao uso dos diversos tipos de recursos computacionais disponíveis (tais como e-mail, Internet, Intranet, sistemas de informação, entre outros) e em caso de ocorrência de uma quebra de segurança.	
Segurança do ambiente físico	- **Diretrizes** para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis do negócio contra acesso não autorizado, dano ou interferência.	
Segurança do ambiente lógico	- **Diretrizes** para garantir a operação correta e segura dos recursos computacionais e proteger a integridade dos serviços.	
Segurança das comunicações	- **Diretrizes** para a proteção de dados e informações durante o processo de comunicação.	
Prevenção e tratamento de incidentes	- **Diretrizes** para a prevenção, detecção, notificação, investigação e tratamento de incidentes de segurança, bem como, para a emissão de relatórios a eles relacionados.	
Desenvolvimento / aquisição, implantação e manutenção de sistemas	- **Diretrizes** para o uso de controles de segurança em todas as etapas do ciclo de vida dos sistemas, incluindo o padrão mínimo de segurança a ser aplicado a todos os sistemas corporativos, e orientações a respeito do uso da avaliação de risco para a identificação dos sistemas que irão merecer medidas extras de proteção.	
Gestão da continuidade do negócio	- **Diretrizes** de recomendações para que a organização se prepare para neutralizar as interrupções às atividades organizacionais e proteja os processos críticos na ocorrência de uma falha ou desastre.	
Conformidade	- **Diretrizes** para a preservação da conformidade com requisitos legais (exemplo: privacidade das informações), com as **normas** internas (incluindo o tratamento de informação proprietária) e com os requisitos técnicos de segurança. - **Procedimentos** a serem adotados em caso de violação da política de segurança, e descrição das punições a que estão sujeitos os infratores (podendo ir de u ma simples advertência a demissão e ação judicial).	

Fonte: Primária - adaptado de Beal (2005) para Organizações Hospitalares com base na Estrutura – *"Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em Organizações Hospitalares"*.

A tabela apresentada anteriormente mostra um *"modelo"* de como poderia ser tratada uma Política de Segurança de Informações, sendo que o seu desdobramento em aspectos, definições e orientações, e ação e objetivos é uma forma prática e formal de identificar as necessidades de uma organização na adoção de uma Política de Segurança de Informações.

Os aspectos apresentados indicam uma seqüência lógica de passos para a montagem da política, as definições e orientações apresentam os diferentes níveis de responsabilidades: diretrizes (estratégico), normas (tático), e procedimentos (operacional) em relação aos pilares de sustentação para a formulação dessas políticas, e as ações e objetivos seriam a forma mais conveniente para a explicação do detalhamento das definições e orientações. Nesse sentido, o conjunto de todos estes elementos poderá constituir em uma política de fácil compreensão e com forte apoio e presença da alta gestão.

A política, preferencialmente, deverá ser criada antes da ocorrência de problemas com segurança de informação para evitar reincidências. Ela é uma ferramenta que possui a finalidade tanto de prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade.

A organização hospitalar se caracteriza por ser uma burocracia profissional do ponto de vista estrutural no qual o setor operacional tem importância nas atividades principais, e é onde se concentra o *"poder"* na organização. O seu mecanismo de controle dá-se por padronização de habilidades realizadas por órgãos fiscalizadores externos das diversas categorias profissionais. Isto lhe confere autonomia e independência da gerência estratégica, pois suas habilidades profissionais são definidas fora da organização em cursos profissionalizantes, ou seja, o estado da arte é um atributo das próprias corporações que desenvolvem seu trabalho no hospital. Tal condição enfraquece a vinculação com a organização e confere dificuldades adicionais como alta resistência às mudanças.

Portanto, verificou-se nesta pesquisa com base nos resultados obtidos que os gestores atribuíram responsabilidades departamentais e funções de segurança de informação a serem exercidas pelos seus integrantes, para a elaboração de uma política de segurança de informação em suas organizações, que foram associadas a cada um dos principais grupos organizacionais: cúpula estratégica, núcleo operacional, linha intermediária, tecnoestrutura e assessoria de apoio, e parcerias externas.

Tabela 2 - Responsabilidades atribuídas pelos grupos organizacionais envolvidos na elaboração de uma política de segurança de informação em organizações hospitalares

Grupo organizacional envolvido	Departamentos Envolvidos nas Organizações Hospitalares	Responsabilidades atribuídas
Cúpula estratégica	- Executivos (diretores e gerentes responsáveis) - O Comitê de Segurança deve envolver representantes das áreas de Tecnologia de Informação, Comercial, Jurídica, Negócio, Financeira, Auditoria, entre outras.	- Responsável por endossar todas as políticas e os planos de Sistemas de Informação. - Decisões de investimento. - Comitê de Segurança de Informação (mandatos ou nomeados pelo conselho gestor). Devem ser desenvolvidas atas documentando o conteúdo das reuniões e distribuídas aos demais participantes. - Análise crítica e aprovação das políticas. - Iniciativas de segurança e treinamento dos usuários. - A figura do *Security Officer* (Gerente de Tecnologia de Informação).
Tecnoestrutura	Área de Recursos Humanos que estabelece sanções e penalidades a serem aplicadas nas situações em que a política for desrespeitada. RH deve atuar em conjunto com TI. Assessoria de Qualidade e Auditoria.	- Analistas que não fazem parte do trabalho operacional, atuam na organização e no planejamento desse trabalho e no treinamento das pessoas que o executam. - Padronização, planejamento e controle, tais como organização e métodos, controle da produção e contabilidade. - Deve obter a assinatura dos termos de responsabilidade de segurança da informação, sendo que o documento deve formalizar o conhecimento e a concordância do funcionário sobre as políticas estabelecidas para o uso adequado da informação e também das penalidades da organização e da lei.
Linha intermediária	São representadas pelos *"proprietários das informações"* que são os responsáveis pela autorização do acesso as informações. São todas as áreas de supervisão, chefias, e gestores departamentais.	- Supervisão direta. - Requisitos de segurança para os ativos de informação. - Definição das regras de acesso. - Limitação dos privilégios dos usuários e dos sistemas de processamento. - Responsáveis finais pelo processo. Coordenação, planejamento, execução e avaliação da implementação da segurança.
Assessoria de apoio	Área de Tecnologia de Informação e Empresas	- Reavaliar riscos associados às mudanças no ambiente de SI e TI, tais como: expansão da conectividade de rede, alterações na

	Terceirizadas.	infra-estrutura de TI, introdução de novas tecnologias. Possuem a função de consultoria especializada em segurança da informação (consultor interno ou externo).
Núcleo operacional	- Equipe médica envolvida no processo de atendimento ao paciente. - Enfermeiros.	- Fabricação dos produtos e/ou à prestação dos serviços na organização. - Responsáveis em alimentar os sistemas de processamento de transações. - Cumprem os procedimentos e rotinas de segurança derivados da política de segurança e dos planos de continuidade do negócio. - Usuários das informações devem entender e seguir a política assegurando que os procedimentos de segurança sejam respeitados e cumpridos.
Parcerias externas	- ONA, órgãos certificadores. - Provedores de serviços de telecomunicações. - Empresas terceirizadas em serviços de gestão de TI (exemplo: sistemas de integração).	- Autoridades legais e certificadoras. - Organismos reguladores. - Provedores de serviços de informação. - Operadoras de telecomunicações.

Fonte: Primária.

4.2 Validação da hipótese fundamental

Durante a condução da análise de dados após emergirem as unidades de significado, categorias e subcategorias foram percebidas algumas proposições que validaram totalmente ou parcialmente a hipótese fundamental deste estudo. Estas proposições foram percebidas com base no relacionamento dos elementos da teoria que foram explicitados pelos gestores e que foram fundamentais para revelar as condições que compuseram o esquema teórico.

Tabela 3 - Associação das proposições identificadas nos hospitais pesquisados em relação à validação da H_1

Hipótese Fundamental		***H_1:*** *As organizações hospitalares, em suas distintas naturezas, possuem claras deficiências para formular uma política de segurança de informação formal devido à falta de definições claras dos papéis nos diversos grupos organizacionais, e de elementos norteadores para a percepção na tomada de decisão por parte dos gestores.* **Informação pretendida:** a partir das percepções e opiniões dos gestores verificar se existe coerência na afirmação (H_1) com base na realidade das organizações pesquisadas.
Proposições	HSJC	P_1: apesar desta organização hospital estar preparada em diversas instâncias relacionadas a gestão da segurança da informação ficou claro que a atribuição e a responsabilidade da gestão da segurança é exclusiva da área de tecnologia de informação. P_2: apesar de existir um modelo preliminar formalizado de segurança digital (segurança da informação) instaurado no hospital para os colaboradores, o documento aborda em suma aspectos técnicos e não de gestão. P_3: a construção do modelo preliminar formalizado de segurança digital do hospital foi tratada de forma centralizada pela área de Tecnologia de Informação. P_4: procura-se desenvolver um modelo único de política de segurança de informação que atenda duas empresas do mesmo grupo organizacional, mas com realidades e estruturas diferentes de negócio, uma é o hospital e a outra um plano de saúde.
	HMSC–I	P_1: o hospital possui deficiência em desenvolver uma política de segurança de informações devida à estrutura centralizadora em nível de decisão da mantenedora, oferecendo limitações nas decisões que envolvam investimentos em tecnologia de informação e desenvolvimentos de planos de ação, entre eles o de política de segurança de informação. P_2: não existe uma padronização de sistemas de informação em nível de gestão na rede em que este hospital está inserido, inviabilizando, portanto, um documento que fosse padronizado para todas as unidades devido que estas unidades operam com sistemas tecnológicos de gestão distintos. P_3: os gestores atribuem a falta de formalização de uma política de segurança de

		informação pela falta de um sistema de integração de dados confiável para o hospital. P_4: a área de tecnologia de informação não é considerada como estratégica no hospital, mas como operacional dentro do aspecto de processo produtivo e operacional, apesar de estar ligada diretamente a diretoria geral. P_5: os gestores em sua maioria consideram que falta conhecimento de como mapear as necessidades para se desenvolver uma política segurança de informação formal e um plano diretor de informática. P_6: a cultura em desenvolver planos estratégicos é muito recente, portanto, ainda não existe um envolvimento dos diferentes grupos que permita uma sinergia maior com a área de TI e a direção geral para o desenvolvimento de uma política de segurança de informação que envolva todo o hospital.
	HICF	P_1: o hospital possui claras deficiências em desenvolver uma política de segurança de informação devido à falta de orientação da secretaria e do conselho de saúde. P_2: o hospital pretende atribuir a responsabilidade em desenvolver uma política de segurança de informação para terceiros visto que não existem funcionários internos ao hospital que possuam o *know how* para desenvolvê-la ou que fiquem alocados no cargo por muito tempo em função da rotatividade do funcionalismo público. P_3: não existe uma continuidade nos planos estratégicos que envolvam a gestão de Tecnologia de Informação no hospital dada a sua natureza pública e a constante mudança de normatizações de governos e novos direcionamentos no mesmo governo.
	HAC–A	P_1: apesar de haver indícios de que existe uma política de segurança de informação formal a mesma parece ficar restrita a área de Tecnologia de Informação, sendo que nem todos os gestores das diferentes áreas da organização participam desse processo. P_2: os gestores e seus subordinados por área são monitorados a partir de sistemas de informação em suas estações de trabalho em relação ao conteúdo e acesso a informações, entretanto, não há uma formalização das regras de conduta ou referentes à necessidade da segurança da informação.
	HAC-B	P_1: o hospital passou por uma forte mudança de gestão familiar para uma profissional nos últimos cinco anos no qual ocorreram novos direcionamentos estratégicos do uso da TI no hospital. P_2: apesar de haver indícios que exista uma área específica para a gestão da Segurança da Informação, a de Gestão de Riscos, atuando em conjunto com a área de Tecnologia de Informação parece não haver a necessidade de uma política formal de segurança de informação pela preocupação nos aspectos legais.

Legenda: HSJC – Hospital São José dos Campos; HMSC-I – Hospital e Maternidade São Camilo – Ipiranga; HICF – Hospital Infantil Cândido Fontoura; HAC-A – Hospital de "Alta Complexidade A"; e HAC-B - Hospital de "Alta Complexidade B".
Fonte: Primária.

As proposições acima resumem o que análise dos casos das organizações hospitalares pode revelar sobre a formulação de uma política de segurança de informações e, portanto, validar a hipótese fundamental. Apesar de constituir-se em um estudo de caso com apenas cinco organizações do mesmo setor sendo que uma pública e quatro particulares, a tipicidade das organizações e a comparação entre elas aumentam o potencial de generalização da teoria e do seu poder explicativo. Entretanto, os dados poderão sofrer alterações devido ao fator de periodicidade em que os dados forem coletados e também pelas percepções únicas que os gestores poderão fazer das afirmações, estas informações poderão variar caso exista uma nova pesquisa.

Porém, é importante salientar que os dados obtidos referem-se especificamente ao fenômeno pesquisado na área substantiva: a formulação de uma política de segurança de informações nas organizações hospitalares. Generalizações para outros setores podem ser feitas, criteriosamente, desde que o contexto da área específica seja semelhante.

4.3 Condução na formulação estratégica e na tomada de decisão de uma Política de Segurança de Informações nas organizações hospitalares pesquisadas

As constantes mudanças nas estratégias da organização hospitalares, bem como as de tecnologia de informação envolveram mudanças nas práticas de trabalho, ou estão sendo levadas a estas mudanças nas práticas de trabalho e na maneira com que as operações internas serão conduzidas.

A solicitação para que as pessoas modifiquem seus procedimentos e comportamentos arraigados sempre poderão *"perturbar a ordem"* interna da organização. A resistência e ansiedade dos funcionários sobre como serão afetados pelas mudanças tecnológicas são respostas normais; isto é especialmente verdadeiro quando as mudanças trazem em seu bojo a potencialidade de eliminação de postos de trabalho. Provavelmente ocorram também perguntas sobre o que precisa ser feito de maneira comum e onde precisa haver liberdade para a ação independente.

Assim, o estabelecimento de uma política de segurança de informação, bem como os procedimentos operacionais ajudam na tarefa da implementação da estratégia de várias maneiras:

- A política nova ou revisada recentemente proporciona orientação para os gerentes operacionais, pessoal de supervisão e empregados em termos de como certas coisas precisam ser feitas daqui para frente e o comportamento a ser esperado, estabelecendo assim algum grau de regularidade, estabilidade e confiança sobre a maneira com que o gestor decidiu executar a estratégia e operar o negócio diariamente.
- A política ajuda a alinhar as ações e o comportamento com a estratégia na organização, colocando limites para ações independentes e canalizando esforços individuais e em grupos para a implementação. A política reage às tendências de alguma ou algumas partes da organização resistir ou rejeitar as abordagens comuns – as pessoas em sua maioria deixam de ignorar práticas estabelecidas ou violar as políticas da empresa sem antes obter esclarecimentos ou mesmo ter uma forte justificação.
- A política padrão estabelece e ajuda a reforçar a firmeza com que as atividades críticas para a estratégia são executas auxiliando o pessoal interno sobre como fazer o seu trabalho.
- Os gestores podem usar o processo de mudança de política como uma alavanca poderosa para mudar a cultura corporativa para produzir um melhor alinhamento com a nova estratégia.

Portanto, de uma perspectiva de implementação de estratégia, os gestores precisam ser inventivos para criar uma política que possa fornecer suporte vital para a execução efetiva da estratégia.

Neste estudo foi observado que a capacidade de tomar decisões estratégicas rápidas, com amplo suporte e alta qualidade em bases freqüentes, é a *"pedra"* fundamental da estratégia eficaz. Segundo Eisenhardt (1999) para se usar a linguagem do pensamento estratégico contemporâneo considerando a grande competitividade no mercado é necessário que a tomada de decisão estratégica seja uma aptidão dinâmica nas organizações da saúde.

Na gestão dos hospitais verificou-se que a união de recursos humanos e procedimentos muito diversificados. Portanto, a alta direção tem o importantíssimo papel de facilitar, propiciar e conduzir as transformações.

Nesse sentido, os tomadores de decisão eficazes nas organizações hospitalares pesquisadas deveriam desenvolver estratégias seguindo algumas orientações:

- Construir intuição coletiva que aumenta a capacidade da diretoria de ver ameaças e oportunidades mais cedo e mais acuradamente.
- Estimular o conflito rápido para melhorar a qualidade do pensamento estratégico sem sacrificar muito tempo.

- Manter um ritmo disciplinado que conduza o processo de decisão a uma conclusão *"mais"* precisa.
- Enfraquecer o *"comportamento político"* que cria conflito improdutivo e perda de tempo.

Dentre as principais abordagens do processo decisório foi verificado que para o desenvolvimento de uma política de segurança de informações a abordagem do **incrementalismo lógico** é a que melhor define os aspectos racionais e político-lógico no papel dos dirigentes que foram entrevistados nesta pesquisa.

5. Contribuições da pesquisa para as organizações

Uma gestão estratégica da Segurança da Informação poderá contribuir com que as diversas áreas têm a oferecer à organização, servindo como linha orientadora à integração dos esforços desenvolvidos pelos vários especialistas, dispersos pela organização.

Um adequado desempenho na segurança da informação depende de interdependências complexas e multidimensionais, que decorrem da complexidade tecnológica e organizacional que atualmente permeia a atividade empresarial e – de forma equivalente – a administração pública também. Longe de ser simples problema técnico, envolve todo o processo de gestão da organização.

Frente à adoção de políticas, os padrões e os procedimentos de segurança da informação, as pessoas nas organizações poderão ser consideradas como o componente mais importante em um programa eficaz de segurança da informação, enfocando preocupações nas práticas de políticas de segurança, com enfoque direcionado aos aspectos de educação, conscientização e treinamento.

Desenvolver uma visão de portfólio de projetos está intrinsecamente relacionado ao aculturamento dos colaboradores que prestarão suporte a essa visão. O mesmo vale para a segurança da informação. Quando falamos da necessidade de uma visão holística para tratar, de forma adequada, das questões de segurança da informação, estamos nos referindo a três aspectos principais: processos, tecnologia e pessoas.

Quando os esforços são direcionados para tratar das pessoas e da influência destas sobre o nível e/ou maturidade de segurança da informação de uma organização, o desafio é grande. Partindo do princípio de que não adianta ter a melhor tecnologia e os processos desenhados da melhor forma se as pessoas (usuários, funcionários, entre outros) que usam a tecnologia e suportam os processos não estão comprometidas com os objetos estratégicos e de segurança da informação, conclui-se que a questão cultural é de suma importância.

A conscientização dos usuários pode ser desenvolvida de várias formas, mas deve ter como *"pano de fundo"* e como suporte legal a Política de Segurança da Informação, que deve ser corporativa e aprovada pelo principal executivo da empresa, depois de ser desenvolvida por um grupo multidisciplinar, ou seja, não somente pela área de segurança da informação, mas com a participação das áreas de negócio, Recursos Humanos, Jurídica, entre outras e de TI durante a construção da política de segurança. Depois dessa etapa, esse grupo deve constituir um comitê que irá zelar pelo cumprimento, divulgação, atualização e conscientização da política de segurança da informação.

À medida que o ambiente corporativo e de negócios fica dependente da tecnologia e dos processos automatizados, ganham importância a prática adequada da segurança da informação e a aderência desta à estratégia de negócio.

Esses e outros aspectos vêm exigindo dos executivos de segurança da informação mais do que o conhecimento técnico e, por isso, esses profissionais vêm investindo em suas carreiras e tornando-se cada vez versáteis e completos.

A busca pela segurança da informação deve ser um ato contínuo no contexto empresarial, suportando as iniciativas de governança corporativa e de Tecnologia da Informação e buscando a conscientização dos usuários das informações, os quais devem entender que, mais que um ato, a segurança da informação precisa tornar-se um hábito. Portanto, todos os funcionários de uma organização são responsáveis pela segurança da informação.

A gestão da segurança da informação deveria ser implementada como uma prática de gestão estratégica, considerando-se as proporções e necessidades, em grandes, médias e também pequenas empresas. Ao pensar em adotá-la, faz-se necessário em primeira instância, à vontade e a disposição dos principais executivos e do envolvimento dos outros níveis da organização.

Referencias Bibliográficas

ABNT. NBR ISO/IEC 17799: *Tecnologia da informação – código de práticas para a gestão da segurança da informação*, Associação Brasileira de Normas Técnicas, 2001.

ANDREWS, K. *The concept of corporate strategy.* Dow Jones Irwin, 1971.

BANDEIRA-DE-MELLO, Rodrigo; CUNHA, Cristiano J. Castro de Almeida. *Operacionalizando o método da Grounded Theory nas pesquisas em estratégia:* técnicas e procedimentos de análise com o apoio do software ATLAS.TI. In: EnANPAD - Encontro de Estudos em Estratégia, 1., 2003, Curitiba. Anais... Curitiba: ANPAD, 2003.

BARMAN, Scott. *Writing Information Security Policies*. New Riders Publishing, 2002.

BEAL, Adriana. *Segurança da Informação. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações.* São Paulo: Atlas, 2005.

BORBA, Valdir Ribeiro. *Administração Hospitalar*. Princípios Básicos. 3ª Edição. CEDAS – Centro São Camilo de Desenvolvimento em Administração da Saúde – Faculdade São Camilo de Administração Hospitalar, 1991.

BRODERICK, J. S. *Information security management – when should it be managed?* Information Security Technical Report, n. 3, 2001. p. 12-18 6v.

EGAN, Mark; MATHER, Tim. *The Executive Guide to Information Security:* Threats, Challenges, and Solutions. Addison-Wesley Professional, 2004.

EISENHARDT, Kathleen M. *Strategy as Strategic Decision Making*. MIT Sloan Management Review, primavera 1999, pp. 65-72.

FERREIRA, F. N. F. *Segurança da Informação.* Rio de Janeiro: Ciência Moderna Ltda., 2003.

FUGINI, Mariagrazia; BELLETTINI, Carlo. *Information Security, Policies and Actions in Modern Integrated Systems*. Idea Group Inc, 2004.

HOFER, Charles E. e SCHENDEL, Dan. *Strategy formulation. Analytical concepts*. St. Paul, West Publishing Company, 1978.

HÖNE, Karin.; ELOFF, J. H. P. *Information security policy:* what do international information security standards say? Computer and Security, n. 5, 2002, p. 402-409. 21v.

JAUCH, L. R.; GLUECK, W. F. *Business Policy and Strategic Management*. 5ed. McGraw-Hill, 1980.

JOHANSTON, H. *Sistemas de informação hospitalar: Presente e future*, Revista Informédica, v. 1, n. 2, p. 5-9, 1993.

LEARNED, E. P.; CHRISTENSEN, C. R.; ANDREWS, K. R.; GUTH, W. D. *Business Policy, Test and Cases.* Richard D. Irwin, 1965.

LINDBLOM, C. *The science of Muddling-Through*. Public Administration Review, Cambridge (MA), BLackwell Publishing, nº 1, 1959. 19v.

MENEZES, J. C. *Gestão da segurança da informação*. Leme : Mizuno, 2006.

MINTZBERG, Henry.; WATERS, J. A. *Of Strategies, Deliberate and Emergent.* Strategic Management Journal, 1985.

NAKAMURA, Tissato; GEUS, Paulo Lício de. *Segurança de redes em ambientes cooperativos*. São Paulo: Berkeley, 2002.
PELTIER, Thomas. *Information Security, Policies, Procedures, and Standards. Guidelines for Effective Information Security Management*. Auerbach Publications – CRC Press LLC, 2002.
PELTIER, Thomas R; PELTIER, Justin; BLACKLEY, John A. *Managing a Network Vulnerability Assessment.* Auerbach Publications – CRC Press LLC, 2003.
PETERLINI, O. L. G. Cuidado gerencial e gerência do cuidado na interface da utilização do sistema de informação em saúde pelo enfermeiro. 2004. 142p. *Dissertação (Mestrado em Ciências da Saúde)* – Universidade Federal do Paraná, Curitiba, 2004.
QUINN, J. *Strategies for change.* Homewood Illinois: Irwin, 1980.
RAMOS, Anatália Saraiva Martins.; CAVALCANTE, Sayonara de Medeiros. *Práticas de Conscientização e Treinamento em Segurança da Informação no Correio Eletrônico – Um Estudo de Caso*, Congresso Anual de Tecnologia da Informação – CATI 2005, FGV-EAESP, 2005.
RODRIGUES, R. *Manual de pautas para el establecimiento de sistemas locales de información*. OPAS – Organização Panamericana da Saúde, 1996.
SALVADOR, Valéria Farinazo Martins; FILHO, Flávio Guilherme Vaz de Almeida. *Aspectos Éticos e de Segurança do Prontuário Eletrônico do Paciente.* II Jornada do Conhecimento e da Tecnologia, UNIVEM, Marilia, SP, 2005.
SCUDERE, Leonardo. *Risco Digital.* Como a tecnologia pode agregar valor aos negócios, criar novas oportunidades e reduzir as fraudes. Rio de Janeiro: Campus, 2007.
SLOAN, A. P. *My Years With General Motors*. Londres: Sedgewick & Jackson, 1963.
SOLMS, Rossouw von. *Information security management:* why standards are important. Information Management & Computer Security, n.1, 1999, p. 50-57. 7v.
STEINER, G. A.; MINER, J. B. *Management policy and strategy – Text, Readings and Cases.* McMillan Publishers Inc., New York, 1977.
STRAUSS, A.; CORBIN, J. *Basics of qualitative research:* techniques and procedures for developing grounded theory. 2. ed. Thousand Oaks: Sage, 1998.
STRAUSS, A. *Une Perspective en Termes de Monde Social*. In La Trame de la Négociation – Sociologie Qualitative et Interaccionisme vol. (eds. I. Baszanger), Paris, L'Harmattan, 1991.
TRCEK, D. *Security policy conceptual modeling and formalization for networked information systems.* Computer Communications, n. 17, 2000, p. 1716-1723. 23v.
VASCONCELLOS, M. et al. *Política de saúde e potencialidade de uso das tecnologias* de informação. Saúde em Debate, Rio de Janeiro, n.61, maio/ago. 2002. p. 219-235. 26v.
WILSON, J.; TURBAN, E.; ZVIRAN, M. *Information systems security:* a managerial perspective. International Journal of Information Management. n.2, 1992, p. 105-119. 12v.
WILSON, Mark; HASH, Joan. *Information Technology Security Awareness, Training, Education, and Certification.* Computer Security Division, National Institute of Standards and Technology, 2004.