Uma visão organizacional na formulação de políticas de segurança de informações em instituições hospitalares

An organizational view on formulating information security policies in hospitals

Una visión organizacional en la formulación de políticas de seguridad de informaciones en instituciones hospitalarios

*Luis Hernan Contreras Pinochet**

RESUMO: O objetivo desta pesquisa foi compreender a participação dos gestores no processo de formulação de estratégias de uma política de segurança de informação, identificando os elementos norteadores para a elaboração de uma estrutura de análise em organizações hospitalares. O objeto desta pesquisa foi constituído por cinco organizações hospitalares, escolhidas segundo os critérios: em função da tipicidade, do seu tempo de existência e posição no mercado, e pela facilidade de acesso aos dados. Esta pesquisa utilizou um desenho de estudo de multicasos e corte transversal, de caráter contextual e processual, de cunho exploratório e descritivo, com a intenção de gerar uma classificação categórica para desenvolver uma teoria fundamentada em dados. A pesquisa conduziu o desenvolvimento de uma estrutura de análise que foi batizada com o nome de "*Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em Organizações Hospitalares*". Com esta estrutura 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 a todas as medidas de proteção que serão implementadas. Como resultado, verificou-se que as organizações hospitalares deste estudo, em suas distintas naturezas, apresentaram claras deficiências para formular uma política de segurança de informação devido à necessidade de definições claras nos papéis dos diversos grupos organizacionais, e de elementos norteadores para a percepção na tomada de decisão por parte dos gestores.

PALAVRAS-CHAVE: Tecnologia da Informação. Gestão em Saúde. Tomadores de Decisão em Saúde.

ABSTRACT: This research aimed at understanding the participation of the managers in the process of devising strategies of a policy on information security, identifying the guiding elements to make an analysis structure about hospitals. The object of this research was composed by five hospitals, chosen according to the following criteria: type, duration and position in the market, and easy access to data. This research used a multi-case and cross-section study design of a contextual and process and exploratory and descriptive nature to create a categorical classification to develop a theory based on data. This research conducted the development of an analysis structure that was named as "*Continuous Follow-up Cycle for the Development of a Policy on Information Security about Hospitals*". With this structure, it was possible to identify the duties about the information security in the different organizational levels, defining responsibilities as to the compliance, evaluation and audit verification and implementation and establishing guidelines needed for all the protection measures that will be implemented. As a result, it was observed that the studied hospitals in their different natures showed clear deficiencies to formulate a policy on information security due to the need for clear definitions in the roles of the several organizational groups and for guiding elements for the perception in the decision-making of the managers.

KEYWORDS: Information Technology. Health Management. Health Manager.

RESUMEN: El objetivo de esta investigación fue comprender la participación de los gestores en el proceso de formulación de estrategias de una política de seguridad de información, identificando los elementos orientadores para la elaboración de una estructura de análisis en organizaciones hospitalarias. El objeto de esta investigación fue constituido por cinco organizaciones hospitalarias, elegidas según los criterios: en función de la tipicidad, de su tiempo de existencia y posición en el mercado, y por la facilidad de acceso a los datos. Esta investigación utilizó un diseño de estudio de multicasos y corte transversal, de carácter contextual y procesal, de cuño exploratorio y descriptivo, con la intención de generar una clasificación categórica para desarrollar una teoría fundamentada en datos. La investigación condujo el desarrollo de una estructura de análisis que fue denominada de "*Ciclo Continuo de Acompañamiento para el Desarrollo de una Política de Seguridad de Informaciones en Organizaciones Hospitalarias*". Con esta estructura fue posible identificar las responsabilidades en relación a la seguridad de la información en los diferentes niveles organizacionales, delineando responsabilidades en relación a la implementación, verificación de la conformidad, auditoría y evaluación, estableciendo orientaciones necesarias en relación a todas las medidas de protección que serán implementadas. Como resultado, se verificó que las organizaciones hospitalarias de este estudio, en sus distintas naturalezas, presentaron claras deficiencias para formular una política de seguridad de información debido a la necesidad de definiciones claras en los papeles de los diferentes grupos organizacionales, y de elementos orientadores para la percepción en la toma de decisión por parte de los gestores.

PALABRAS-LLAVE: Tecnología de la Información. Gestión en Salud. Gestor de Salud.

* Doutor em Administração de Empresas pela Escola de Administração de Empresas da Fundação Getulio Vargas – EAESP/FGV. Coordenador e Professor do Curso de Graduação em Administração do Centro Universitário. E-mail: adm@saocamilo-sp.br

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, médico, hospital e equipe envolvida na saúde do paciente.

A utilização da tecnologia da informação dentro desse tipo de organizações também direciona desafios na gestão da segurança dos diversos ativos (humanos, físicos, materiais, e principalmente, informacionais) porque essas 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.

Nesse contexto, Broderick considerou 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 visando à proteção desses ativos[1].

O papel dos gestores frente à formulação de políticas de segurança de informação como estratégia pretendida

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[2].

Vasconcellos, Moraes, Cavalcante destacaram 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[3].

Segundo Rodrigues, o uso da tecnologia de informação por parte dos gestores de saúde tem se tornado cada vez mais importante. Esse 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[4].

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 esses dados vulneráveis a acessos não autorizados; a facilidade de alteração de dados registrados eletronicamente traz perigos adicionais à vida e ao bem-estar de pacientes.

Nesse sentido, Johanston 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[5].

Wilson, Turban e Zviran, verificaram que os aspectos relacionados com a Segurança da Informação ganharam o mundo corporativo e, atualmente, são fatores fundamentais de sucesso para o negócio[6].

Barman 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[7].

Nesse contexto, 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 existe uma grande tendência nas organizações de se atribuir as atividades e responsabilidades de segurança à unidade de tecnologia da informação[8]. Os obstáculos que poderão surgir no estabelecimento de uma política efetiva de segurança são, na maior parte, relacionados com fatores humanos[9].

Peltier considerou 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[10]. Nesse sentido, Fugini e Bellettini verificaram em suas pesquisas que a segurança da informação exige uma abordagem que envolva a cúpula estratégica da organização[11].

Peltier, Peltier, Blackley definiram 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[12].

De acordo com Höne, Eloff[13], 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[14].

A política de segurança da informação, segundo Trcek, 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[15].

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[16].

A concepção predominante entende a formulação estratégica como um processo que se desenvolve em uma série de etapas sequenciais, 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[17].

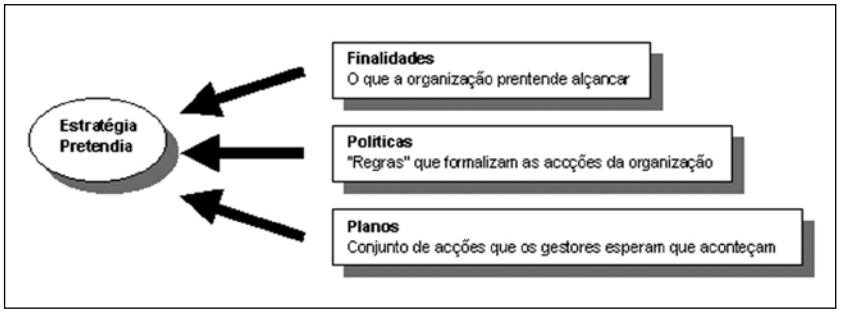
Nesse contexto de formulação estratégica, é a perspectiva introduzida por Lindblom[18], mas desenvolvida com Quinn[19], com a noção de incrementalismo lógico, que visa a reduzir a incerteza e beneficiar a melhor informação disponível.

Segundo Mintzberg e Waters[20], as estratégias que os gestores propõem, definem e pretendem ver realizadas em suas organizações são as estratégias pretendidas, e as que realmente se concretizam são as estratégias realizadas. Na Figura 1, são apresentadas as estratégias pretendidas:

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[21] enunciou os 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 por meio de uma especialização do desenvolvimento da política, independentemente de sua execução.

Figura 1. Elementos de uma estratégia pretendida



Fonte: Mintzberg, Waters (p. 57)[20].

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. No Quadro 1, são apresentadas, as principais características dos cinco hospitais pesquisados.

O acesso a informações foi assegurado pela autorização formal para realizar a pesquisa. Dos cinco hospitais pesquisados, três autorizaram a publicação do seu nome, e dois autorizaram o desenvolvimento da pesquisa, mas solicitaram que não fosse publicado seu nome, preservando o seu anonimato com nomes fictícios.

A concentração desta pesquisa utilizou-se de várias fontes para a coleta dos dados em busca de evidências. As fontes para o estudo são 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 semiestruturadas[24].

A observação não participante foi outra fonte utilizada para a coleta de dados primários, a fim de possibilitar informações adicionais. Nesse sentido, fatos e ocorrências, comportamentos e condições ambientais da realidade organizacional relacionado ao foco da pesquisa foram observados e registrados[25].

Esta pesquisa utilizou um *design* de estudo de multicasos e corte transversal[26], de caráter contextual e processual de cunho exploratório e descritivo com a intenção de geração de teoria, no sentido da *Grounded Theory*[27].

Quadro 1. Características dos hospitais

	Hospital A	Hospital B	Hospital C	Hospital D	Hospital E
Natureza	Filantrópico – Privado	Filantrópico – Privado	Público – da Administração Direta (subordinado a secretaria da saúde)	Filantrópico – Privado	Privado
Porte (*)	Grande	Médio	Médio	Grande	Grande
Localização	Cidade: São José dos Campos – Estado de SP	Região Centro – Sul de SP	Zona Leste – Cidade de SP	Zona Sul – Cidade de SP	Centro – Cidade de SP
Características	Hospital Geral. Instalações clínico-hospitalares de alto padrão, tecnologia superior em equipamentos médicos e um serviço completo de hotelaria	Hospital Geral. Centro de Diagnóstico Especializado Moderno Centro Cirúrgico Aprimoramento do Equipamento Constante Multiprofissional	Hospital Infantil (neonatal até adolescentes)	Hospital Geral. Todos os serviços de diagnósticos e terapêuticos. Posicionamento de mercado para as classes A e B	Hospital Geral, com ênfase em pacientes cirúrgicos, dispondo de todos os serviços diagnósticos e terapêuticos. Posicionamento de mercado voltado para as classes B e C+
Colaboradores	863	532	700	5.000	1.500
Leitos	215	98	140	470	280
Acreditação	Acreditado pela ONA nível 1	Prepara-se para o processo de acreditação	Acreditação pela secretaria da saúde – nível 2 (modelo da ONA, mas aplicado pela secretaria da saúde).	Primeiro Hospital fora dos Estados Unidos a obter *Joint Comission International* (selo de qualidade)	Acreditado pela ONA nível 2

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[22] e Organização Mundial de Saúde (OMS)[23].

Ao utilizar o método da *Grounded Theory*, foi adotada a 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 a compreender os fenômenos segundo as perspectivas dos sujeitos[25].

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[26].

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 –, ou seja, 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?

O pressuposto metodológico fundamental (PMF_1) foi derivado dos dados após os exercícios interpretativos de análise e síntese, inerentes ao método de pesquisa: 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 orien-

tação 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.

Discussão dos Resultados

Atualmente, a organização hospitalar é uma das mais complexas, não apenas pela nobreza e amplitude de 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, uma vez que, 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.

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. Esses 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" por meio do agrupamento dos dados obtidos pelos gestores que foram os sujeitos desta pesquisa.

Com a identificação desses elementos e da estrutura de análise, foi possível, nas pesquisas de profundidade com os gestores, verificar como ocorre o envolvimento desses 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 esse tipo de instituição e quais seriam as áreas ou grupos organizacionais que estariam alinhados nesse 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 de 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 dessa estrutura de análise limita-se às 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, essa estrutura de análise poderia servir também como um processo de avaliação para organizações hospitalares públicas e privadas.

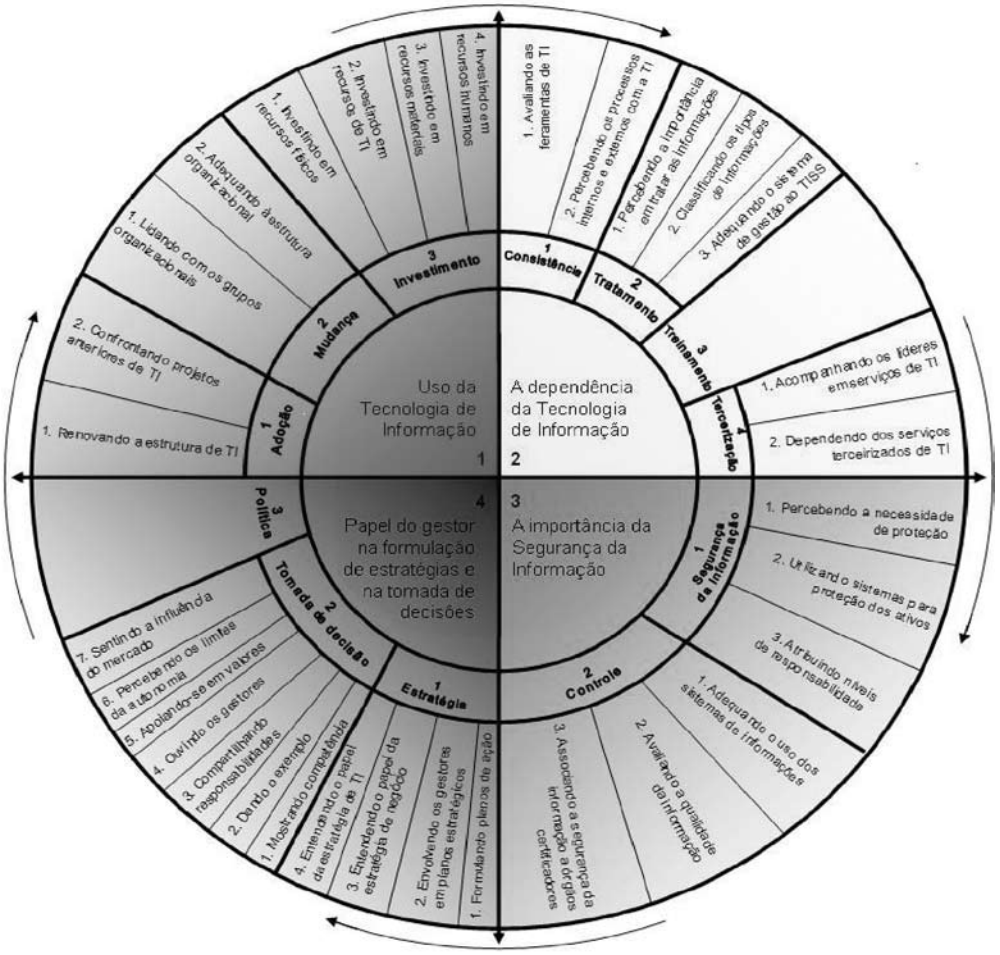
Com base em um estudo, foi construída uma teoria fundamentada nos dados, utilizando-se o método da *Grounded Theory*, que gerou a estrutura apresentada na Figura 2.

Portanto, a estrutura "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 essa estrutura de análise fosse 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. Nessas 34 categorias-chave, foram associa-

Figura 2. Ciclo contínuo de acompanhamento para o desenvolvimento de uma Política de Segurança de Informações em Organizações Hospitalares



Fonte: Primária.

das à presença de contribuição dos hospitais que fizeram parte desta pesquisa e chegou-se nos seguintes resultados: o Hospital A foi o que obteve a maior presença de categorias-chave, com 33 ocorrências; em segundo lugar, aparece o Hospital B, com 29 ocorrências; em terceiro lugar, ficou o Hospital C, com 28 ocorrências; em quarto lugar, aparece o Hospital D, com 23 ocorrências; e, em quinto lugar, ficou o Hospital E, com 17 ocorrências.

Essas ocorrências não pretendem revelar possíveis fraquezas ou fragilidades por parte dos gestores que foram sujeitos desta pesquisa em relação à falta de conhecimento do tema abordado neste estudo, 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.

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.

Dessa 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. Essa 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[8].

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 infraestrutura tecnológica, e a necessidade de protegê-los contra as ameaças existentes para prevenir consequências 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.

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. Isso 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.

Validação do pressuposto metodológico 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 o pressuposto metodológico fundamental deste estudo. Essas 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.

As proposições acima resumem o que a análise dos casos das organizações hospitalares pode revelar sobre a formulação de uma política de segurança de informações e, portanto, validar o pressuposto metodológico 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; essas informações poderão variar caso exista uma nova pesquisa.

É importante salientar que os dados obtidos referem-se especificamente ao fenômeno pesquisado na área substantiva: a formulação

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

Grupo organizacional	Departamentos	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 às 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 Terceirizadas.	- Reavaliar riscos associados às mudanças no ambiente de SI e TI, tais como: expansão da conectividade de rede, alterações na infraestrutura 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 a 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.

Quadro 3. Associação das proposições identificadas nos hospitais pesquisados em relação à validação da PMF_1

Pressuposto Metodológico Fundamental	PMF_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 (PMF_1) com base na realidade das organizações pesquisadas.	
Proposições	Hospital A	P_1: apesar dessa organização, o hospital está preparado em diversas instâncias relacionadas à 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 de segurança digital preliminarmente formalizado (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 de segurança digital preliminarmente formalizado 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.
	Hospital B	P_1: o hospital possui deficiência em desenvolver uma política de segurança de informações, devido 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 esse hospital está inserido, inviabilizando, portanto, um documento que fosse padronizado para todas as unidades, considerando que essas unidades operam com, sistemas tecnológicos de gestão distintos. P_3: os gestores atribuem a falta de formalização de uma política de segurança de informação à 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 à diretoria geral. P_5: os gestores, em sua maioria, consideram que falta conhecimento de como mapear as necessidades, para se desenvolver uma política de 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.
	Hospital C	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.
	Hospital D	P_1: apesar de haver indícios de que existe uma política de segurança de informação formal, ela parece ficar restrita à 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.
	Hospital E	P_1: o hospital passou por uma forte mudança, de gestão familiar para uma profissional, nos últimos cinco anos, durante os quais 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.

Fonte: Primária.

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.

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 das organizações hospitalares, bem como as de tecnologia de informação, envolveram mudanças nas práticas de trabalho, ou estão sendo levadas a essas 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; isso 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 em quais grupos organizacionais deveria haver liberdade para a ação independente.

Assim, o estabelecimento de uma política de segurança de informação, bem como os procedimentos operacionais, ajuda 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 a 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 executada 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 frequentes, é a pedra fundamental da estratégia eficaz. Segundo Eisenhardt[28], 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 a união de recursos humanos e de 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.

Contribuições da pesquisa para as organizações

Uma gestão estratégica da segurança da informação poderá contribuir com o 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 (diretrizes, normas, procedimentos e instruções) de segurança da informação, as pessoas nas organizações poderão ser consideradas como o componente mais importante em um programa eficaz de segurança da informação. Estas orientações nas práticas de políticas de segurança no componente "pessoas" deverá estar alinhado a 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 dessas 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 dessa à estratégia de negócio. Esse e outros aspectos vêm exigindo dos executivos e dos responsáveis pela área de segurança da informação mais do que o conhecimento técnico e, por isso, organizações investem em suas carreiras, tornando-os cada vez mais capacitados e com percepções alinhadas às estratégias da empresa.

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, que 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, fazem-se necessárias, em primeira instância, a vontade e a disposição dos principais executivos e do envolvimento dos outros níveis da organização.

REFERÊNCIAS

1. Broderick JS. Information security management – when should it be managed? Information Security Technical Report. 2001;6(3):12-8.

2. Peterlini OLG. Cuidado gerencial e gerência do cuidado na interface da utilização do sistema de informação em saúde pelo enfermeiro [dissertação]. Curitiba (PR): Universidade Federal do Paraná; 2004. (Mestrado em Ciências da Saúde)

3. Vasconcellos MM, Moraes IHS, Cavalcante MTL. Política de saúde e potencialidade de uso das tecnologias de informação. Saúde Debate. 2002 Mai/Ago;26(61):219-35.

4. Rodrigues R. Manual de pautas para el establecimiento de sistemas locales de información. Washington: OPAS; 1996.

5. Johanston H. Sistemas de informação hospitalar: presente e futuro. Rev Informédica. 1993;1(2):5-9.

6. Wilson J, Turban E, Zviran M. Information systems security: a managerial perspective. Intern J Inform Manag. 1992;12(2):105-19.

7. Barman S. Writing information security policies. USA: Sams Publishing; 2001.

8. Beal A. Segurança da informação. Princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas; 2005.

9. Ramos ASM, Cavalcante SM. Práticas de conscientização e treinamento em segurança da informação no correio eletrônico – um estudo de caso. Congresso Anual de Tecnologia da Informação – CATI FGV-EAESP; Jun 2005.

10. Peltier T. Information security, policies, procedures, and standards: guidelines for effective information security management. Michigan: Auerbach Publications – CRC Press LLC; 2001.

11. Fugini M, Bellettini C. Information security, policies and actions in modern integrated systems. IGI Publishing; 2004.

12. Peltier TR, Peltier J, Blackley JA. Managing a network vulnerability assessment. Michigan: Auerbach Publications – CRC Press LLC; 2003.

13. Höne K, Eloff JHP. Information security policy: what do international information security standards say? Computer Security. 2002;21(5):402-9.

14. Ferreira FNF. Segurança da informação. Rio de Janeiro: Ciência Moderna Ltda; 2003.

15. Trcek D. Security policy conceptual modeling and formalization for networked information systems. Computer Communications. 2000;23(17):1716-23.

16. Egan M, Mather T. The executive guide to information security: threats, challenges, and solutions. Addison: Wesley Professional; 2004.

17. Andrews KR. The concept of corporate strategy. Homewood: Dow Jones Irwin, Inc; 1971.

18. Lindblom C. The science of Muddling-Through. Public Admin Rev. 1959;19(2):79-88.

19. Quinn J. Strategies for change: logical incremetalism. Homewood: Richard D. Irwin; 1980.

20. Mintzberg H, Waters JA. Of strategies, deliberate and emergent. Strateg Manag J. 1985;19(3):257-72.

21. Sloan AP Jr. My years with General Motors. New York: Currency Book; 1963.

22. Borba VR. Administração Hospitalar: princípios básicos. 3a ed. São Paulo: Cedas, 1991.

23. World Health Organization (WHO). [cited Ago 2011]. Available from: http://www.who.int/ent

24. Mello BR, Cunha CJCA. Operacionalizando o método da Grounded Theory nas pesquisas em estratégia: técnicas e procedimentos de análise com o apoio do software ATLAS.TI. Anais do Encontro de Estudos em Estratégia, Curitiba (PR); Brasil, 2; Set 2003.

25. Merriam SB. Qualitative research and case study applications in education: revised and expanded from case study research in education. San Francisco: Jossey-Bass Publishers; 1998.

26. Strauss A. Une perspective en termes de Monde Social. In La Trame de la Négociation – Sociologie Qualitative et Interaccionisme. Paris: L'Harmattan; vol.1. 1991.

27. Strauss A, Corbin J. Basics of qualitative research: techniques and procedures for developing grounded theory. 2nd ed. Thousand Oaks: Sage Publications, Inc; 1998.

28. Eisenhardt KM. Strategy as strategic decision making. MIT Sloan Management Review, 1999;65-72. [cited July 25 2007]. Available from: http://sloanreview.mit.edu/the-magazine/articles/1999/spring/4036/strategy-as-strategic-decision-making/

BIBLIOGRAFIA CONSULTADA

Abnt. Nbr Iso/Iec 17799. Tecnologia da informação – código de práticas para a gestão da segurança da informação [Manual]. Associação Brasileira de Normas Técnicas; 2001.

Recebido em *11 de abril de 2011*
Aprovado em *30 de maio de 2011*