PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

LUIS ANTONIO JANSSEN

INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM INSTITUIÇÕES HOSPITALARES

Porto Alegre
Janeiro de 2008

LUIS ANTONIO JANSSEN

INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM INSTITUIÇÕES HOSPITALARES

Dissertação apresentada ao Curso de Mestrado em Administração e Negócios, da Faculdade de Administração, Contabilidade e Economia, da Pontifícia Universidade Católica do Rio Grande do Sul, como requisito à obtenção do título de MESTRE EM ADMINISTRAÇÃO E NEGÓCIOS.

Orientador: Prof. Leonardo Rocha de Oliveira, PhD

Porto Alegre

Janeiro de 2008

LUIS ANTONIO JANSSEN

INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM INSTITUIÇÕES HOSPITALARES

Dissertação apresentada ao Curso de Mestrado em Administração e Negócios, da Faculdade de Administração, Contabilidade e Economia, da Pontifícia Universidade Católica do Rio Grande do Sul, como requisito à obtenção do título de MESTRE EM ADMINISTRAÇÃO E NEGÓCIOS.

BANCA EXAMINADORA:

_____

Prf. Dr. Antonio Carlos Gastaud Maçada - UFRGS

_____

Prf. Dr. Mauricio Gregianin Testa - PUCRS

_____

Prfa. Dra. Edimara Mezzomo Luciano - PUCRS

Aprovada pela Banca Examinadora em 28 de Janeiro de 2008.

AGRADECIMENTOS

À Pontifícia Universidade Católica do Rio Grande do Sul, por oportunizar o meu desenvolvimento pessoal e intelectual.

Ao meu orientador e amigo, pelo apoio, estímulo e pela motivação que me guiou durante toda a realização deste estudo.

Aos colegas da YARA Brasil Fertilizantes S.A., pelo apoio e estimulo para continuar na busca constante do crescimento profissional.

Aos professores do MAN pelo carinho e acolhida que sempre me beneficiaram durante esta jornada.

A todos os profissionais e especialistas que colaboraram com o andamento deste estudo.

À minha filha pelos momentos de convívio que abdiquei para que este trabalho se realizasse.

Aos meus pais (*in memoriam)* os quais certamente estão comigo nesta conquista.

Ao meu amor pelo apoio e motivação em todos os momentos.

Finalmente, a Deus que me guia e ilumina meus pensamentos.

RESUMO

As mudanças no cenário internacional têm levado as organizações a preocuparem-se com o valor e responsabilidades em relação ao uso das informações, as quais têm reconhecido seu papel como um ativo de importância crescente. As informações estão cada vez mais disponíveis a todos os segmentos de negócios, com um papel importante no suporte à tomada de decisões em níveis operacionais e estratégicos. Este cenário também ocorre em instituições hospitalares, onde pode estar relacionada com a vida humana e todos os aspectos sociais e éticos que isto pode envolver. Este trabalho tem por objetivo propor um instrumento de avaliação da maturidade dos processos de Segurança da Informação para instituições hospitalares. Para a elaboração do instrumento foi realizada uma revisão da literatura procurando relacionar assuntos relativos a Segurança da Informação, incluindo modelos existentes e formas de avaliação de processos no contexto de instituições hospitalares. Para análise do instrumento proposto foram aplicados pré-testes com especialistas em segurança da informação. A seguir foi elaborado um estudo exploratório de natureza qualitativa com estudos de caso aplicados a profissionais de 3 instituições hospitalares. Este estudo foi elaborado com questionário semi-estruturado para posterior análise do conteúdo das entrevistas com as opiniões sobre a aplicabilidade do instrumento, estrutura lógica, clareza das questões e aderência aos objetivos propostos. Ao final, foram feitas as análises e inferências dos resultados obtidos com as percepções dos entrevistados. Como conclusão do trabalho cabe destacar a aprovação do instrumento em relação a sua utilidade para avaliar a maturidade de processos de segurança da informação em instituições hospitalares e a atual carência em relação as melhores práticas preconizadas pela literatura.

Palavras chaves: maturidade de processos, Gestão de Segurança da Informação, Informação em Instituições Hospitalares.

ABSTRACT

Changes in the international business market has taken organizations to be worried about the value and responsibilities regarding the use of information, which has been recognized as an asset of increasing importance. Information is currently available at all sectors and organizational levels, taking an important role for the decision making process for operational and strategic business activities. This scenario also occurs at hospitals, where it can be related to the human life and all the social and ethical aspects that this could involve. This work has the objective of proposing an instrument for the maturity evaluation of Information Security processes for hospitals. The instrument development was carried out based on a literature review on issues as Information Security, including existing models and processes evaluation methods, with special attention in the context of hospitals and health care institutions. For the instrument analysis were applied pre-tests with information security specialists. It has been followed by an exploratory research of qualitative nature with case studies interviewing professionals of 3 hospitals. The interviews were carried out based on a semi-structured questionnaire and the content analysis of the results have considered the instrument applicability, logical structure, questions clarity and adherence to its objectives. Conclusion taken from this work lead to the approval of the instrument regarding its application for evaluating the maturity of information security processes of hospitals and the current gap considering the best practices present in the literature reviewed.

Key words: Processes Maturity, Security Information Management, Hospital Information.

LISTA DE FIGURAS

LISTA DE TABELAS

ABREVIATURAS

ANS..... Agência Nacional de Saúde

BS……..... *British Standards*

BSI ……. *British Standards Institution*

CCSC..... *Comercial Computer Security Centre*

CCSMM……. *Community Cyber Security Maturity Model*

CFM……... Conselho Federal de Medicina

CMM..... *Capability Maturity Model*

CobiT…….. *Control Objectives for Information and Related Technology*

COSO…….. Committee of Sponsoring Organizations

HIPAA.....*Health Information Portabilit & Accountability Act*

IEC.....*International Electrotechnical Commitee*

ISACA……. *Information Systems Audit and Control Association*

ISO.....*International Standards Organization*

MS.....Ministério da Saúde

SBIS.....Sociedade Brasileira de Informática na Saúde

SI.....Segurança da Informação

SSE-CMM…….. *System Security Engineering Capability Maturity Model*

TI.....Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Este capítulo destaca a importância e a justificativa de escolha do tema avaliação de maturidade dos processos de Segurança da Informação, delimitando o escopo da dissertação e apresentando a questão de pesquisa que norteou o seu desenvolvimento, bem como a estrutura deste trabalho.

1.1 JUSTIFICATIVA E IMPORTÂNCIA DO TEMA

O mundo está passando por transformações nas esferas política, econômica, social e humana (TAPSCOTT, 2007). A globalização atinge os países e afeta a dinâmica das relações sociais, as quais incluem transformações na força de trabalho e na reorganização do mercado mundial (BOAR, 2002). Nesse ambiente, marcado cada vez mais pela complexidade, incerteza e ambigüidade, as organizações têm sido pressionadas a inovar, desenvolver processos operacionais eficientes e disponibilizar informações confiáveis para que possam não só reagir, mas também antecipar-se às inovações tecnológicas e às novas exigências e expectativas dos mercados (BEAL, 2004).

Os processos organizacionais necessitam ser suportados por informação (STUMPF, 1996). A informação auxilia na tomada de decisões e representa fonte de poder organizacional: poder de conhecer o concorrente,

poder de solucionar rapidamente um problema e poder de aprender com os seus erros mais facilmente. A ação de tornar as informações seguras e prontamente disponíveis para os integrantes de uma organização pode melhorar significativamente os resultados por ela obtidos (BEAL, 2004).

Neste sentido, a informação passa a ser um recurso estratégico, tal qual o capital financeiro e, portanto, muito cobiçada (BOAR, 2002; NIMER, 1998). Subestimar a importância da Segurança da Informação pode custar a sobrevivência da organização. Assim, a informação passa a ser preciosa e por isso desejada, precisando ser adequadamente protegida (COLTRO, 2002).

Quando bem gerenciada, a informação aumenta as possibilidades de negócio oferecidas pelos mercados, tornando as organizações mais competitivas. Com isso, possibilita que as empresas percebam que a informação pode trazer um diferencial competitivo (BEAL, 2004). Sua importância e a sua segurança passam a fazer parte da gestão do próprio negócio (BOAR, 2002).

As organizações têm tido preocupação com a segurança de informações que possam comprometer uma ação organizacional (SEMOLA, 2003). A revelação seletiva de informações é uma preocupação de extrema importância para as organizações, especialmente na elaboração de seus movimentos competitivos. Qualquer quebra do sigilo de uma informação deve ser feita apenas como parte integrante de uma estratégia e de forma intencional (BOAR, 2002).

A Segurança da Informação é um processo diretamente relacionado aos negócios de uma organização. Seu principal objetivo é garantir o funcionamento da organização frente às possibilidades de incidentes, evitando

prejuízos, aumentando a produtividade, propiciando maior qualidade aos clientes, vantagens em relação aos seus competidores e garantindo a reputação da organização (DAWEL, 2005).

Todavia, na prática é difícil prever todas as possibilidades de falhas de divulgação da informação empresarial. É comum encontrar empresas que estabelecem medidas ineficientes de segurança na tentativa de obter maior proteção da informação. Por vezes são medidas que custam caro e seus resultados são subjetivos e questionáveis (CALDER et al., 2005). A ineficiência na proteção da informação pode ser solucionada com medidas que permitam identificar e rastrear os processos relativos à sua segurança. Para isso é necessário o acompanhamento dos processos para efetiva proteção das informações, independente do processo organizacional que ela esteja inserida (EGAN, 2005).

A informação pode ser encontrada sob a forma escrita (física ou eletrônica), digital, impressa ou conhecida pelas pessoas. Pode ser transmitida por diferentes meios de comunicação como o e-mail, o correio, em filmes, de forma falada, pelo rádio, pela TV, entre outros. Seja qual for a forma de existência ou modo pelo qual ela é transmitida, armazenada ou acessada, a informação deve ser protegida (MOREIRA, 2001). Neste cenário, a Tecnologia da Informação possui um papel importante dentro das organizações para auxiliar no armazenamento, transmissão e controle da informação. Seu papel não fica apenas na condição de evitar que a informação seja roubada, mas também para garantir que ela esteja sempre disponível quando necessária, preservando a autorização para quem possa utilizá-la com agilidade e com confiabilidade (DAWEL, 2005).

Contudo, apenas a Tecnologia da Informação (TI) não é suficiente para ser o foco total das atenções em Segurança da Informação. A informação utiliza outros mecanismos de disseminação e armazenamento, que levam a necessidade de ampliar a visão da questão. Neste sentido, a gestão dos recursos envolvidos com a informação física e de políticas claras e gerenciadas de segurança permitem um controle mais amplo do processo do gerenciamento da Segurança da Informação (EGAN, 2005).

Uma das formas utilizada pelas empresas para tentar garantir a Segurança da Informação no mundo organizacional é através da análise e da avaliação da Segurança da Informação, levando a um enquadramento a normas e princípios de boas práticas adotadas por diversas empresas. As normas existentes propiciam a identificação de possíveis falhas de Segurança da Informação dentro das organizações. Por sua vez, as normativas existentes são genéricas e aplicáveis a qualquer tipo de empresa, não considerando as peculiaridades de cada segmento de negócio (EGAN, 2005).

Complementando a questão do processo de gerenciamento, Coltro (2002) afirma que a Segurança de Informação deve contemplar uma estratégia e ferramentas específicas que atendam às necessidades corporativas como um todo, propiciando a manutenção de um ambiente seguro. Além disso, essa gestão deve ser trabalhada de forma contínua e atualizada durante toda a vida da empresa.

Existe uma percepção de que alguns segmentos de negócio encontram maiores desafios na gestão dos processos de Segurança da Informação. Pode-se citar o setor bancário brasileiro, considerado como exemplo de gestão dos processos de Segurança da Informação. Provavelmente, esta percepção se

deve ao tipo de informação ao qual utilizam, o capital financeiro, e pela existência de normas específicas definidas pelo Banco Central do Brasil (FEBRABAN, 2007).

Ainda pode-se citar como exemplo os Estados Unidos, onde existem regras e políticas legais de gestão da Segurança da Informação para o segmento de saúde, através do Ato HIPAA (Health *Information Portability & Accountability Act*) (PORTER e TEISBERG, 2006; EGAN, 2005).

Entretanto, a gestão hospitalar possui um desafio frente aos órgãos reguladores da saúde em absorver a relevância desta nova cultura de administração da segurança do ativo informação. Infelizmente ainda no Brasil não existem regras ou normas específicas para a Segurança da Informação neste segmento. Porter e Teisberg (2006) enfatizam que o volume de informações e a quantidade de processos executados nas tarefas diárias de um hospital exigem controles ágeis, flexíveis e seguros, para que sejam evitadas repetições de tarefas e desperdícios pela falta de informação. Argumentam também que o processo formal de Segurança da Informação suportado por sistemas informatizados traz vantagens a médio e longo prazo, tanto com relação a custos de recuperação como a melhoria do nível da qualidade dos serviços prestados aos pacientes. Neste contexto, pode-se observar a necessidade da avaliação e acompanhamento dos processos hospitalares, identificando o estágio e as oportunidades de melhoria na Segurança da Informação.

Dentre as diferentes formas de avaliar processos, pode-se citar a avaliação através de modelos de maturidade, os quais permitem identificar um estágio atual ou a evolução de um processo em relação a uma medição

anterior, apurando quais são as oportunidades de melhoria. A maturidade "permite a avaliação de qualquer ser, coisa ou sistema, visando determinar as suas características e desempenhos, nomeadamente os seus pontos fortes e fracos em plena atividade" (ANTUNES, 2001, p. 45). Sendo a Segurança da Informação formada por um conjunto de procedimentos, percebe-se que a evolução da maturidade dos seus processos não está incluída nos quesitos dos modelos normativos existentes. Assim, este projeto contempla os temas Segurança da Informação e maturidade de processos, permitindo a proposição de um instrumento que permita uma avaliação dos processos da Segurança da Informação que esteja de acordo com as normativas internacionais e que possa adaptar-se às características do segmento das instituições hospitalares.

1.2 DELIMITAÇÃO DO TEMA E DEFINIÇÃO DO PROBLEMA

Na elaboração da estratégia empresarial a informação é crucial para servir a condução e melhoria nos processos organizacionais, na sinalização ao mercado, na comunicação de compromisso ou mesmo para a elaboração de planos ou intenções estratégicas (PORTER, 2004). Beal (2004) considera que a informação representa uma classe particular entre os ativos da organização, sendo sua gestão complexa e sujeita a desafios específicos, entre eles a proteção.

No segmento da saúde no Brasil existem algumas iniciativas de proposição de normas para a Segurança da Informação, especialmente as definidas pela Sociedade Brasileira de Informática na Saúde (SBIS), entidade vinculada ao Conselho Federal de Medicina (CFM). Entretanto, as instituições hospitalares no Brasil não estão sujeitas à estas normativas, onde o órgão

governamental o qual é responsável pelas instituições hospitalares é o Ministério da Saúde (MS).

Nos hospitais a qualidade, disponibilidade e segurança da informação são elementos diferenciadores no processo de atendimento das expectativas de seus clientes, dada o seu objetivo ético de prover serviços que aliviem ou curem o sofrimento humano (STUMPF, 1996). Segundo Minotto (2003), as informações nas instituições hospitalares são cada vez mais numerosas e reais, onde muito mais pessoas dependem da informação e da sua proteção, quer seja por motivos éticos ou operacionais, onde mantê-la em sigilo passa a ser de suma importância. Assim sendo, justifica-se um foco nas instituições hospitalares uma vez que este segmento a proteção da informação é primordial.

Segundo as orientações editadas pela SBIS, as instituições de saúde no Brasil devem manter controles que garantam a Segurança da Informação através de um padrão definido em conformidade com a norma ISO/IEC 17799 (SBIS, 2006). Por outro lado, a Agência Nacional de Saúde, órgão regulador do setor de saúde suplementar, editou um padrão para a troca de informações eletrônica entre as entidades vinculadas a ANS, incluindo normativas relativas à Segurança da Informação. Dentro deste contexto de relevância, o presente projeto irá focar na segurança das informações hospitalares e na avaliação dos processos relativos a esta.

A literatura sobre o tema Segurança da Informação em instituições hospitalares limita-se às abordagens dos conceitos de Segurança da Informação e das normativas aplicáveis ao segmento empresarial de forma

genérica, mais especificamente às recomendações baseadas nas normativas internacionais ISO/IEC 17799 e ISO/IEC 27001.

Outro ponto importante de citação refere-se aos estudos sobre os métodos de avaliação dos processos de maturidade. Existem referenciais teóricos para a avaliação de maturidade em processos em diversas áreas do conhecimento, como o alinhamento estratégico organizacional, usabilidade de *software*, desenvolvimento de *software*, qualidade, governança corporativa e de gestão de projetos (PÁDUA, 2006). Entretanto, para a avaliação de maturidade de processos de Segurança da Informação os estudos são muito escassos e fazem parte de avaliações focadas em assuntos relacionados a TI, não contemplando características e aspectos mais amplos da informação.

Este trabalho aborda os principais temas relacionados com a Segurança da Informação e com a avaliação do nível de maturidade da gestão dos respectivos processos, com foco na avaliação da maturidade dos processos da Segurança da Informação em instituições hospitalares. Neste sentido, questiona-se: Como deve ser avaliada a maturidade dos processos de Segurança da Informação em instituições hospitalares?

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é avaliar a maturidade em processos de Segurança da Informação em instituições hospitalares.

1.3.2 Objetivos Específicos

a) Identificar na literatura aspectos relativos a modelos de Segurança da Informação;

b) Propor um instrumento com dimensões de análise e itens de avaliação da maturidade dos processos em Segurança da Informação para hospitais;

c) Analisar a percepção sobre aplicação, estrutura e aderência do instrumento proposto para instituições hospitalares.

1.4 ESTRUTURA DO TRABALHO

Além deste capítulo introdutório, o qual apresenta o tema, sua justificativa, delimitação e objetivos, esta dissertação foi organizada em mais quatro capítulos conforme detalhado a seguir.

O Capítulo 2 apresenta o embasamento teórico do projeto, abordando os seguintes temas: gestão estratégica da informação e os aspectos

relacionados com a importância da informação; Segurança da Informação, contemplando as premissas existentes na literatura e as normativas internacionais e nacionais; maturidade e a sua utilização em avaliação de processos e as diretivas específicas no segmento da saúde. Foram elucidados os modelos e representações disponíveis de processos. O foco de interesse foram os aspectos dos modelos que permitem avaliações de maturidade de processos que foram descritas nesta parte do projeto para ajudarem na compreensão do cenário que foi pesquisado.

O Capítulo 3 aborda o método da pesquisa e as suas etapas de execução. O método cobre a metodologia utilizada na condução do trabalho e serviu como base para a execução da análise dos resultados.

O Capítulo 4 apresenta o estudo de caso. Mediante análise dos dados coletados, centra-se na posição atual da maturidade das empresas na gestão dos processos de Segurança da Informação e na avaliação da aplicabilidade do modelo proposto a ser aplicado nas instituições hospitalares.

O Capítulo 5 apresenta as conclusões da pesquisa e as recomendações para trabalhos futuros a serem realizados.

2 SEGURANÇA DA INFORMAÇÃO

Com o aumento da complexidade e do dinamismo do ambiente externo às organizações, estas passaram a depender de instrumentos eficazes de proteção da informação (BEAL, 2004). A descoberta dos instrumentos de suporte existentes para segurança da informação é crucial para a elaboração de uma proposição consistente. Este capítulo decorre sobre a fundamentação teórica de sustentação desta pesquisa.

2.1 O PAPEL ESTRATÉGICO DA INFORMAÇÃO

O crescimento dos mercados mundiais e suas mudanças ambientais têm impactado nos processos organizacionais, exigindo das organizações uma maior capacidade de formular e implementar estratégias (PORTER, 2004). A velocidade de ocorrência das mudanças está associada ao desenvolvimento tecnológico, à integração de mercados, ao deslocamento da concorrência para o âmbito internacional, à disponibilidade da informação, à redefinição do papel das organizações, além das mudanças no perfil demográfico e nos hábitos dos consumidores (MEIRELLES e GONÇALVES, 2001).

A formulação e a implementação de estratégias impõem vários desafios às organizações como reduzir a sua estrutura organizacional, manter sua posição de mercado de maneira defensiva ou aumentar o seu escopo de produtos e serviços. A seleção da melhor alternativa leva em conta o tempo

gasto para implementação, o custo e o controle dos processos escolhidos (PORTER, 2004). Segundo Mandarini (2004, p. 14), “a fragilidade dos processos de proteção nas organizações parece avançar na mesma proporção com que aumentam os riscos, ou seja, é a real dimensão dos perigos na segurança organizacional em nosso meio”. A ampliação dos casos de fraudes contra às organizações demonstra a real insegurança atual, onde a busca por dados, registros, informações e sistemas é intensa e preocupante (BEAL, 1994). Administrar adequadamente os processos de Segurança da Informação representa uma necessidade cada vez mais importante em qualquer tipo de negócio.

Neste sentido, percebe-se que a informação tem fundamental importância para as organizações do ponto de vista estratégico. Dispor da informação correta, no momento adequado, auxilia na tomada de decisão de forma ágil e eficiente. A informação é substrato da vantagem competitiva e deve ser administrada em seus particulares, diferenciada e salvaguardada (PORTER e TEISBERG, 2006). Ela funciona como um recurso essencial para a definição de estratégias e para a constituição de uma organização flexível e ágil para uma resposta competitiva mais eficaz.

Sendo as informações empresariais consideradas como patrimônio cada vez mais valioso e necessário para que se possa prever, compreender e responder às mudanças ambientais e alcançar ou manter uma situação favorável no mercado, a sua proteção tem relevância estratégica. A ação de tornar as informações disponíveis prontamente, de forma segura, clara, precisa, consistente e oportuna para os integrantes de uma empresa, traz para

a informação um valor significativo e um poder de tornar-se um diferencial estratégico (BEAL, 1994).

Segundo Beal (2004), as organizações precisam ter, em seus processos decisórios e operacionais, informações de qualidade, obtidas de uma boa relação custo-benefício e adaptadas às necessidades do negócio. As informações, independente do seu formato, são um ativo importante da organização e com valor estratégico e, por isso, o ambiente em que se encontram deve ser devidamente protegido (FONTES, 2006).

2.2 A PROTEÇÃO DA INFORMAÇÃO

A Segurança da Informação busca proteger a informação de um conjunto de ameaças a fim de garantir a continuidade do negócio, minimizar as perdas empresariais e maximizar o retorno dos investimentos e as oportunidades de negócios (MANDARINI, 2004).

Quando existe uma informação, ela pode estar presente em diversos meios e formatos. Ela é disponibilizada e transmitida em muitas formas. Não importa a maneira em que a informação se encontra, ou como esteja sendo compartilhada ou armazenada, ela deverá sempre estar protegida e controlada (SEMOLA, 2003). Segundo Ramakrishnan (2004), proteger uma informação consiste em preservar três elementos correlacionados, sendo expresso na Figura 1:

Confidencialidade - garantindo que a informação possa somente ser acessada por pessoas autorizadas;

Integridade - protegendo a acuracidade e a completude da informação e os caminhos em que ela é processada;

Disponibilidade - garantindo o acesso das pessoas autorizadas e associando os meios necessários para isso.

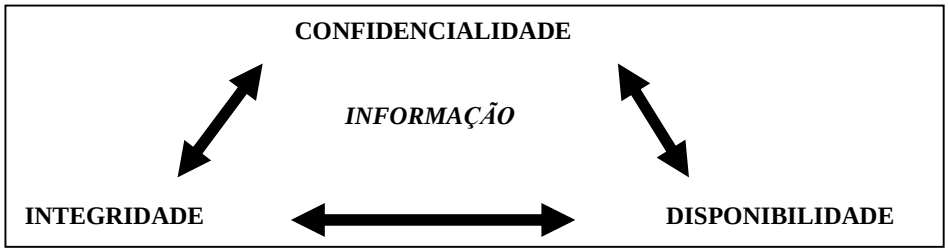

Figura 1: Correlação entre Confidencialidade, Integridade e Disponibilidade
Fonte: Adaptado de Ramakrishnan, 2004.

Proteger um bem ou ativo significa que este possui um valor para o seu proprietário(MANDARINI, 2004). Segurança é um termo que transmite conforto e tranqüilidade a quem desfruta do estado de estar seguro. Buscar uma segurança absoluta é dever e um objetivo maior de todas as organizações (SEMOLA, 2003). Portanto, implica em controlar todas as variáveis que integram esse universo, o que torna isto praticamente impossível. Carneiro (2002) e Champlain (2003) abordam especificamente a questão da Segurança da Informação, fazendo uma distinção conceitual inicial entre a segurança física e a segurança lógica, definindo as partes que as compõem. Segundo os autores, a segurança física representa os procedimentos de proteção dos meios físicos de armazenamento e de transmissão da informação.

Entende-se por segurança lógica como a forma de estabelecer os controles de acesso à informação, objetivando a integridade e a manutenção da confidencialidade da informação protegida através da definição das permissões de acesso àqueles previamente autorizados e negando o acesso daqueles que não gozem dos mesmos direitos. Buscando uma melhor clareza

conceitual, Mandarini (2004) apresenta uma subdivisão em três categorias distintas para a segurança física: (i) pessoas, (ii) equipamento e (iii) instalações.

Na categoria (i) pessoas encontram-se as possibilidades em que a componente humana seja a principal fonte de atenção e de risco em situações como o erro, falha humana, fraude ou roubo. Também se destacam particularmente as questões indiretas como os processos de seleção e recrutamento dos recursos humanos, a documentação que serve de apoio operacional (manuais, normativas internas), a sua atuação nas atividades diárias, a formação de recursos humanos, a sua sensibilização, motivação, a formalização e entendimento das políticas de segurança. Além destes aspectos, destaca-se o papel das pessoas quanto aos utilizadores (internos ou externos) dos meios que utilizam e geram a informação, da importância de que se reveste em apoiá-los e acompanhá-los no seu trabalho, de forma a promover também a segurança, mesmo quando estão se referindo aos utilizadores, que podem estar distantes da origem ou do ponto de controle (MOREIRA, 2001). Não podem ser esquecidos os trabalhadores temporários (contratados para desempenhar funções específicas) ou contratados em regime de *outsourcing*. Este tipo de profissional pode ter, por exemplo, acesso à informação privilegiada e fazer uso da mesma de forma inadequada, constituindo um potencial risco (NIMER, 1998).

Na segunda categoria da segurança física (ii) estão os equipamentos, como os computadores, servidores, equipamentos de rede, equipamentos de fornecimento de energia, sistemas de controle de acesso físico, equipamentos de detecção e combate a incêndios, controles de temperatura e umidade, de

ventilação e de picos eletromagnéticos, referindo-se alguns dos mais representativos (MOREIRA, 2001). Neste ponto, não podem ser desconsideradas as questões relativas a manutenção dos equipamentos e registros de todas as intervenções que venham a ocorrer e até questões aparentemente de pouca relevância, como a limpeza dos equipamentos e das instalações físicas.

Na terceira categoria (iii) denominada instalações, são consideradas as perspectivas do local onde estão fisicamente instalados os equipamentos que gera e armazena a informação, os locais de armazenamento e recuperação de documentos, papéis e de todos os outros tipos de registro de alguma informação de valor para a organização. Para a redução do risco e reforço da segurança são fundamentais as questões relacionadas com a sua localização, o estado de conservação predial, os riscos de inundação, de infiltrações e de acessos indevidos, a proximidade a locais muito poluídos, zonas de tumultos ou manifestações, entre outros (MOREIRA, 2001; CARNEIRO, 2002).

A segurança lógica tem por finalidade proteger as informações transmitidas ou armazenadas digitalmente. Essa proteção tem como meta impedir a alteração, divulgação ou destruição, intencional ou não, atentando para os cuidados que devem ser tomados na criação e utilização das informações. Seu uso deve ser concedido apenas às pessoas que necessitem dela para o desempenho de suas atividades. (MOREIRA, 2001). O campo de abrangência do sigilo da informação lógica envolve tanto a organização em si como também a sua rede de relações, cuja transferência de informações faz-se necessária.

Entretanto, a privacidade das informações do indivíduo é um direito do cidadão e a ele pertence, de modo que nenhuma organização deve descuidar-se de qualquer informação pessoal que lhe seja confiada (MOREIRA, 2001). Se a empresa não contar com pessoal de confiança e capaz, todas as demais medidas de segurança serão inúteis (FONTES, 1991).

As seguranças físicas e lógicas da informação possuem uma importância relevante nas organizações e, portanto, necessitam de uma forma de controle e avaliação de seus processos. Para avaliar a Segurança da Informação existem diferentes modelos na literatura. Alguns destes serão apresentados nesta pesquisa e servem para a base teórica da proposição de um modelo de avaliação de processos de Segurança da Informação, de acordo com o objetivo geral.

2.3 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Como visto anteriormente, existe uma complexidade no estabelecimento de parâmetros que sirvam de subsídios para a afirmação de que um ambiente está seguro (MANDARINI, 2006). Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. A informação é substrato dos processos organizacionais e deve ser administrada em seus particulares, diferenciada e salvaguardada. É importante a identificação das conseqüências relacionadas às vulnerabilidades do tratamento da informação, da compreensão dos diversos ambientes de contexto organizacional e da adoção de um modelo de segurança que possa eliminar tais conseqüências.

Os modelos servem como um referencial para a tomada de ação, pois representam o acúmulo de experiências em situações que podem ser repetidas e que, de alguma forma, alcançaram um objetivo satisfatório. Segundo Ferreira (2006), os modelos são estruturas simplificadas da realidade que apresenta características ou relações sob forma generalizada.

Os modelos são aproximações subjetivas, pois não incluem todas as observações e mensurações existentes, porém são valiosos instrumentos para permitir identificar aspectos fundamentais da realidade (SAYÃO, 2001). Cada modelo expressa e justifica um método de abordagem de uma realidade que, por vezes, é representado através de um instrumento de controle. Um modelo é uma representação de uma situação real que de acordo com o seu objetivo e do modo de expressão, além da sua estrutura e das suas igualdades e desigualdades em relação ao seu original, o qual tenta comunicar algo sobre o real (DINSMORE e JACOBSEN, 1985).

Os modelos de Segurança da Informação não se limitam à segurança das questões relativas à TI. Eles incluem um amplo conjunto de procedimentos, mecanismos, normas, diretrizes e políticas necessárias a salvaguardar a informação organizacional. Para esta pesquisa de avaliação da Segurança da Informação foram coletados alguns destes modelos.

Segundo Sayão (2001) e Dinsmore e Jacobsen (1985), os modelos podem ser classificados em 3 agrupamentos:

a) os **modelos Prescritivos** os quais não se baseiam na observação formal de um processo, pois a efetividade do modelo é garantida através da experiência do executor dos processos, em função do histórico bem sucedido. Estes modelos são utilizados para implementar algum processo específico.

Confundem-se por vezes com os modelos Normativos por terem uma estrutura direcionada do que “deve ser feito”. Entretanto, não possuem imposição e não são restritivos, como ocorre nos modelos Normativos;

a) os **modelos Normativos** tratam daquilo que pode se esperar que ocorra sob certas condições ou regras estabelecidas. Sugere um caminho ideal lógico, racional e sistematizado para a tomada de decisão. Estes modelos definem regras do que devem ser abordado e gerenciado dentro de uma organização, de forma obrigatória, através de Leis, regulamentos, normas ou procedimentos;

b) os **modelos Descritivos ou de Avaliação** tratam de uma descrição estilística da realidade, geralmente estáticos e concentram-se nos aspectos estruturais. São utilizados para descrever “como deve ser feito”, os processos devem ser executados ou avaliados em uma organização.

“Um modelo ou instrumento que se revela correto e útil em aplicações diversas, em circunstâncias distintas e sob informações diferentes, que apresenta ao mesmo tempo um amplo poder explanatório, pode ser definido como um paradigma” (SAYÃO, 2001).

Nesta pesquisa será adotada a classificação prescritivos, normativos e descritivos para os modelos que serão descritos a seguir e relacionados com a Segurança da Informação. Como modelos prescritivos que apresentam as diretivas sobre o que deve ser feito para garantir a Segurança da Informação, são apresentadas as normas BS 7799, ISO/IEC 17799 e ISO/IEC 27001. Como modelos Normativos são apresentadas a SOX e o HIPAA e, complementando, como modelos Descritivos são apresentados os modelos do COSO, PRISMA,

CCSMM, CobiT, CERT-CSO e SSE-CMM, destacando-se as questões de Segurança da Informação.

2.3.1 Modelos Prescritivos

Os caminhos que possibilitam alcançar o objetivo de tornar algo seguro resultam de esforços de diversas entidades públicas e privadas em todo o mundo, as quais estabelecem normas de conduta e recomendações para uma boa gestão da segurança (SÊMOLA, 2005). Os modelos prescritivos definem procedimentos e itens de controle para as organizações a fim de contribuir para a gestão da Segurança da Informação.

Os modelos prescritivos caracterizam-se por serem base para a tomada de decisão através de padrões que permitem uma avaliação do estado em que se encontra uma determinada situação em determinado momento. Alguns destes modelos prescritivos que serviram para a elaboração desta pesquisa serão apresentados a seguir.

2.3.1.1 Norma British Standard 7799

As entidades governamentais e privadas, preocupadas com a questão da segurança, iniciaram nos anos 80 a discutir o assunto da Segurança da Informação. Uma das entidades precursoras foi a *British Standards Institution* (BSI), na Inglaterra, a qual tem dedicado seus estudos com o propósito de definir efetivamente padrões industriais de alta qualidade em diferentes áreas organizacionais (ISACA, 2007).

A norma BS 7799 foi desenvolvida no início dos anos 90 para atender às organizações, governos e indústrias que buscavam pela criação de uma estrutura de gestão de Segurança da Informação.

Esta normativa originou de um esforço do governo britânico, que em 1987, criou o CCSC (*Comercial Computer Security Centre*), cujo objetivo era a criação de critérios para a avaliação da segurança para os usuários das informações das empresas na Grã-Bretanha. No ano de 1989 foi publicada a primeira versão do código de segurança, que na época foi denominado de PD0003 - Código de Gerenciamento de Segurança da Informação.

Em 1995 esse código foi revisado, ampliado e publicado como uma norma britânica (BS), a BS7799-1:1995 (*Information Technology - Code of pratice for information security management*). Em 1996, essa norma foi proposta a ISO para homologação, mas foi rejeitada. Neste mesmo período uma segunda parte deste documento estava sendo criada e em novembro de 1997 foi disponibilizada para consulta e avaliação das empresas. Em Abril de 1999, as duas normas (a de 1995 e a de 1998) foram publicadas, após uma revisão, com o nome de BS7799-1999 incorporando inúmeras melhorias em termos de conteúdo, abrangência e qualidade. Neste período, esta norma já estava sendo adotada por outros países como a Austrália, a África do Sul, a República Checa, a Dinamarca, a Coréia, a Suíça e a Nova Zelândia. A BS7799 foi traduzida para várias línguas das quais pode-se destacar o Francês, o Alemão e o Japonês (ISO/IEC 7799, 2007).

A normativa original BS 7799 continha duas partes: a BS 7799 Parte 1 *(Code of practice for information security management)*, ou código de práticas para o gerenciamento da Segurança da Informação, estabelecida a

partir das exigências para um programa da Segurança da Informação, dividindo o tema segurança em dez dimensões separadas por tópicos. A BS 7799-1 foi adotada como o primeiro padrão internacional para a gestão da Segurança da Informação. A BS 7799 Parte 2, intitulada *Information security management systems - Specification with guidance for us*e, ou sistema de gerenciamento de Segurança da Informação – especificação com um guia de uso, foi desenhada para permitir que uma organização iniciasse o processo de certificação através de métricas definidas na parte 1 da normativa.

Neste contexto, centenas de organizações dentro da Grã-Bretanha e Europa propiciaram à BS 7799-2 o título de certificação, tornando-a um padrão internacional. Até poucos anos atrás, se uma organização desejasse se tornar "certificada", somente poderia alcançar a certificação através do enquadramento ao padrão britânico BS 7799-2. Entretanto, os itens citados nesta normativa não contemplam pontos relevantes sobre a Segurança da Informação como a segurança física e critérios de alinhamento organizacional, ou ainda de novas tecnologias tais como assinatura digital e criptografia, as quais foram incluídas em outra norma denominada ISO/IEC 17799 apresentada a seguir (ISACA, 2005).

2.3.1.2 Norma ISO/IEC 17799 e suas Complementares

Os esforços relacionados com a busca de melhores mecanismos para gestão da Segurança da Informação culminaram com uma revisão da segunda parte da normativa BS 7799, a qual foi considerada e adaptada para a criação de uma normativa mais consistente denominada BS 17799-1. Com a criação desta norma e a posterior evolução para a nova versão BS 17799-2, esta

passou a ser padrão mundial e seguido por empresas e governos de outros países fora da Grã-Bretanha, passando a ser adotada pela ISO e pelo IEC, recebendo a denominação de ISO/IEC 17799 em 2000 (ISO/IEC 17799, 2007). Instituições em diferentes países tentam promover em nível internacional a ISO/IEC 17799, buscando mantê-la como a normativa base para gestão da Segurança da Informação (MOREIRA, 2001). A norma ISO/IEC 17799 caracteriza-se por ser um modelo contendo recomendações de boas práticas em Segurança da Informação. Todavia, a sua característica estrutural não define critérios avaliativos os quais possam ser usados para uma certificação.

A partir de 2000, a ISO iniciou a elaboração de normas específicas e complementares a ISO/IEC 17799 para a gestão da Segurança da Informação. O propósito da elaboração destas normas era de aprofundar os itens de controle em quesitos que são abordados pela ISO/IEC 17799 de forma superficial, mas com relevância para segmentos empresariais específicos.

Enquanto a ISO/IEC 17799 contém itens de controle baseado nas melhores práticas e para qualquer tipo de informação, a ISO/IEC 13335 é um manual para o gerenciamento da segurança das informações tecnológicas, sendo voltada aos aspectos técnicos do tratamento da informação eletrônica e contemplando recomendações para o gerenciamento de riscos em TI (EGAN, 2005). Como mencionado anteriormente, as diretivas da normativa ISO/IEC 13335 estão presentes de forma genérica nos itens da ISO/IEC 17799, embora não possuam o mesmo grau de especificidade.

Existe também uma forte complementaridade entre a ISO/IEC 17999 e a ISO/IEC 15408, a qual aborda de maneira mais profunda os critérios de avaliação dos produtos e sistemas de TI, definindo os níveis de defesa

necessários através de medidas de segurança. Todavia, como a norma ISO/IEC 13335, esta normativa inclui em seus itens os aspectos técnicos dos produtos e serviços, enquanto a ISO/IEC 17999 está mais focada nos aspectos organizacionais e administrativos da Segurança da Informação (EGAN, 2005).

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT), em abril de 2001 disponibilizou, através de um projeto de adaptação e tradução a norma nacional de Segurança da Informação NBR ISO/IEC 17799:2000. Esta normativa foi aprovada e homologada incluindo o Brasil no conjunto de países que adotam e apóiam o uso desta norma. Esta versão brasileira da ISO/IEC 17799 também é utilizada por outros países de língua portuguesa como é o caso de Portugal e Angola (EGAN, 2005).

Estruturalmente, a norma nacional de segurança de informação NBR ISO/IEC 17799 é dividida em 10 categorias de controle, conforme segue:

- Política de Segurança;
- Segurança Organizacional;
- Classificação e Controle dos Ativos da Informação;
- Segurança em Pessoas;
- Segurança Física e do ambiente;
- Gerenciamento de Operações e Comunicações;
- Controle de Acesso;
- Desenvolvimento e Manutenção de Sistemas;
- Gestão da Continuidade do Negócio;
- Alinhamento ou Conformidade.

Cada um destes agrupamentos é subdividido em vários outros itens, totalizando 131 controles de segurança. A relação de categorias e itens contemplados da NBR ISO/IEC 17799 apresenta as categorias e seus respectivos elementos, conforme resumido na Tabela 1 a seguir:

RELAÇÃO DE CATEGORIAS E ITENS CONTEMPLADOS DA ISO/IEC 17799

Categorias	Quantidade Elementos	Itens Contemplados
1. Política de Segurança	2	Necessidades do Negócio, Estratégia, Comprometimento, Regras e Responsabilidades, Políticas e Procedimentos.
2. Segurança Organizacional	10	Avaliação, Gestão de Riscos, Liderança do Negócio, Endereçamento e Manipulação, Estoques.
3. Classificação e Controle de Ativos	3	Inventário de ativos, classificação e manipulação de ativos
4. Segurança Pessoal	10	Demissões e Desligamentos, Regras e Responsabilidades, Treinamento, Relatórios e Revisões.
5. Segurança Física e Ambiental	13	Perímetros, Ameaças Ambientais, Gestão de Riscos, Controle de Acesso, Segurança, Destruição e Remoção de Ativos, Monitoramento, Manipulação de Incidentes, Cooperação e Premiação.
6. Comunicação e Gerenciamento de Operações	24	Padrões, Métodos de e - Comunicação, Procedimentos de Operação, Monitoramento, Backups, Administração de Exceções, Atualizações e Pacotes, Help Desk, Gestão de Mudanças, Sistemas de Criptografia, Administração de Mídias, Código Malicioso, Aceitação de Sistemas, Biblioteca de Documentação, Plano de Capacidade
7. Controle de Acesso	31	Perímetros, Gestão de Riscos, Controle de Acesso, Autenticação, Identificação, Responsabilidade de Usuários, Atualização de Acesso, Monitoramento, computação móvel, gestão de Incidentes.
8. Desenvolvimento de Sistemas e Manutenção	18	Padrões, Modelo do Ciclo de Vida, Revisões, Análise de Diferenças, Planejamento de Requerimentos, Testes de Integridade e Certificação, Repositório de Código, Lançamento de versão, Liberação.
9. Gestão de Continuidade	5	Gerenciamento de Riscos, Priorização, Backups, Continuidade do Negócio, Plano de Desastre e Recuperação, Testes, Atualizações.
10. Conformidade	15	Legal, Contratual, Propriedade Intelectual, Endereçamento e Manipulação, Retenção de Registros, Auditoria, Sanções.

Tabela 1: Relação de itens e categorias contemplados na ISO/IEC 17799
Fonte: Adaptado de ISO/IEC 17799, 2005.

Todavia, era necessário para as organizações ter um modelo de Segurança da Informação que propiciasse a alta administração das empresas identificarem os pontos de riscos ao negócio e permitisse avaliar as organizações, através de um roteiro para avaliação e certificação. Outro ponto importante é de que as organizações tinham a necessidade de incorporar em um modelo uma gestão contínua dos processos de Segurança da Informação

(MANDARINI, 2004). Estes fatos culminaram no desenvolvimento da norma ISO/IEC 27001, a qual é apresentada a seguir.

2.3.1.3 Norma ISO/IEC 27001

A ISO e a IEC publicaram em meados de 2005 a normativa ISO/IEC 27001:2005 *(Information security management systems: Requirements)*, ou sistema de gerenciamento da Segurança da Informação: requerimentos. Este documento é uma padronização e um guia de gerenciamento para a implementação de controles de Segurança da Informação descritos na ISO/IEC 17799:2005, (*Information security management systems: Code of practice)*, ou sistema de gerenciamento de Segurança da Informação: código de práticas (ISO/IEC 17799, 2005b).

A ISO/IEC 27001 é uma normativa de gerenciamento para as organizações que buscam uma certificação internacional de Segurança da Informação e um roteiro para a implementação de boas práticas. A ISO/IEC 27001 é composta por um conjunto de 133 controles sugeridos (apenas dois controles a mais do que a ISO/IEC 17799), divididos em 11 categorias de controle. A ISO/IEC 27001 requer que cada parte da organização, a qual passará a adotar a normativa, indique como será atingido um determinado item de controle (ISO/IEC 27001, 2007). Com esta abordagem, esta normativa define critérios para avaliação de entidades certificadoras autorizadas e reconhecidas internacionalmente.

A ISO/IEC 27001 é parte de um conjunto de normativas denominado grupo ISO/IEC 27000. Cada uma destas normativas tem um objetivo específico assim definido:

- ISO/IEC 27000 - Vocabulário de Gestão da Segurança da Informação (sem data prevista de publicação);
- ISO/IEC 27001 - Esta norma foi publicada em outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de Segurança da Informação;
- ISO/IEC 27002 - Esta norma substituiu em 2007 a ISO 17799:2005 (Código de Boas Práticas);
- ISO/IEC 27003 - Esta norma aborda a gestão de risco, contendo recomendações para a definição e implementação de um sistema de gestão de riscos em Segurança da Informação;
- ISO/IEC 27004 - Esta norma incide sobre os mecanismos de mediação e de relatório de um sistema de gestão de Segurança da Informação;
- ISO/IEC 27005 - Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do sistema de controles;
- ISO/IEC 27006 - Esta norma será referente à recuperação e continuidade de negócio. Este documento tem o título provisório de *(Guidelines for information and communications technology disaster recovery services)*, ou manual para serviços de recuperação de desastre da tecnologia de comunicações e informação, não estando ainda prevista a sua edição.

A ISO/IEC 27001 é uma versão internacional da norma BS 7799-2. Por ser mais completa, insere alguns pontos de outras normativas da ISO e contempla a avaliação e define critérios e indicadores de gestão e certificação (ISO/IEC 27001, 2007). O selo de certificação ISO/IEC 27001 contém um descritivo do escopo avaliado, que poderá ser parcial ou total. Esta padronização permite às organizações demonstrarem a conformidade de seus processos com a regulamentação e com uma gerência de risco eficaz do negócio, podendo iniciar o processo de certificação em algum ponto de fragilidade organizacional e expandir gradualmente para outras áreas de interesse na proteção da Segurança da Informação.

Outro ponto importante sobre a ISO/IEC 27001 foi a incorporação da especificação e recomendações para o gerenciamento da Segurança da Informação, estabelecendo uma Sistemática de Gerenciamento da Segurança da Informação, ou *Information Security Management System* (ISMS). Esta sistemática é composta por um modelo de desenho, implementação, gerenciamento e manutenção dos processos de Segurança da Informação percorrendo toda a organização (ISO/IEC 27001, 2007). Este modelo contém os seguintes capítulos: Introdução, Extensão, Referências Normativas, Condições e Definições, Sistema de Gerenciamento da Segurança da Informação, Administração de Responsabilidades, Gerenciamento das Revisões do ISMS e Melhoria Contínua no ISMS.

A norma ISO/IEC 27001 põe ênfase significante no uso do PDCA (Planejar, Fazer, Verificar e Agir), concebido por Deming (EGAN, 2005). As quatro fases são:

• Planejar: Estabeleça o ISMS

- Fazer: Instrumentalizar e operar o ISMS
- Verificar: Monitorar e revisar o ISMS
- Agir: Manter e Melhorar o ISMS

Por definição, a ISO/IEC 17799:2005 e a ISO/IEC 27001 foram desenhadas para serem utilizadas por qualquer organização em qualquer segmento. Entretanto, estes modelos, por serem genéricos, não consideram as particularidades de cada setor, o que em alguns casos não possui um caráter de completitude e uma abrangência satisfatória, fazendo com que as organizações adaptem os modelos para as suas necessidades.. Este é o caso das instituições hospitalares, as quais não possuem um modelo específico para a avaliação da Segurança da Informação. Além disso, não avaliam a maturidade em que encontra-se um processo, mas possuem uma estrutura de dimensões a qual possibilita tomar como base para a elaboração de um instrumento de avaliação de maturidade.

2.3.2 Modelos Normativos

A partir das fraudes de grandes escândalos financeiros corporativos que abalaram a confiança dos investidores do mercado de ações em várias partes do mundo, os governos adaptaram as suas legislações e regulamentações prescrevendo como as empresas devem gerir os negócios, incluindo a Segurança das Informações. O objetivo é comprometer o nível diretivo das organizações com a responsabilidade pela Governança Corporativa, incluindo-se alguns pontos relativos a Segurança da Informação,

e encorajar a todos a demonstrarem os resultados para a proteção de seus ativos (RAMAKRISHNAN, 2004).

Nos Estados Unidos, algumas Leis e Regulamentações foram criadas ou adaptadas, como a *Sarbanes-Oxley Act* de 2002 (SOX) e *o Health Insurance Portability and Accountability Act* de 1996 (HIPAA), conforme apresentado um resumo na Tabela 2 - Regulamentações nos EUA para a Segurança da Informação.

REGULAMENTAÇÕES NOS EUA PARA A SEGURANÇA DA INFORMAÇÃO				
Legislação	**Escopo**	**Atuação**	**Penalidades**	**Publicação**
Sarbanes-Oxley Act of 2002	Todas as empresas de capital aberto, sujeitas as Leis de segurança dos EUA	Controles internos e demonstrativos financeiros	Penalidades Criminal e civil	Em vigor desde 2002
Health Insurance Portability and Accountability Act (HIPAA)	Operadoras de Planos de Saúde, Instituições de Saúde e Provedores de Assistência á Saúde	Informações pessoais de Saúde em meios eletrônicos	Responsabilidade Civil e Criminal	Em vigor desde 2005

Tabela 2: Resumo Regulamentações nos EUA para a Segurança da Informação
Fonte: Adaptado de Ramakrishnan, 2004

O Ato de Lei denominada *Sarbanes-Oxley* (em homenagem aos senadores dos Estados Unidos que a elaboraram) define regulamentos relativos para as boas práticas de gestão empresarial e de ética profissional. A *Sarbanes-Oxley* (SOX) institui que diretores executivos e financeiros são responsáveis por definir, avaliar e monitorar a eficácia dos controles internos sobre relatórios financeiros e divulgação de informações.

Através destes controles internos, a organização deve definir os seus mecanismos internos capazes de livrar a instituição dos riscos empresarial e que possam ameaçar a continuidade da empresa. Estes controles devem permanecer atualizados e susceptíveis de auditoria externa e fiscalização das instituições governamentais daquele país, comprovando que os controles

internos estão sendo executados. Assim, a SOX deu um maior peso no que diz respeito às atividades de controle interno nas organizações, fazendo com que a gestão das empresas apresente seus resultados de forma clara e transparente aos acionistas e ao mercado, sem a possibilidade de esconder ou apresentar incorretamente o desempenho financeiro da organização.

A SOX consiste em 11 capítulos (numerados de 400 a 410) definindo as responsabilidades da corporação e o papel de empresas de auditoria (EGAN, 2005). Segundo Ramakrishnan (2004), os principais capítulos, no que tange aos controles da Segurança da Informação, são os artigos 404 (Controles Internos), 406 (Código de Ética) e 409 (Apuração e Publicação), os quais abordam a questão da publicidade das informações, ética nos negócios e do papel de fiscalização da SEC. Dentro dos princípios da SOX, as informações contidas nos relatórios legais devem ser disponibilizadas aos acionistas, clientes, fornecedores, governo e demais partes de relacionamento, imediatamente após a sua apuração e em algum meio oficial de publicação.

Em virtude da SOX, foi fundada a *Public Company Accounting Oversight Board* (ou Grupo de Averiguação da Contabilização de Empresas Públicas), a PCAOB. Esta comissão é supervisionada pela SEC que, em conjunto com representantes do setor privado, fiscaliza as auditorias independentes para que elas cumpram todas as premissas da SOX.

Entre os trabalhos da PCAOB, foi editado um regulamento para adaptar a conduta profissional dos advogados das empresas, os quais devem informar à comissão quaisquer irregularidades de seus clientes (empresas e seus administradores) em relação às Leis que regulam o mercado de capitais, incluindo problemas com a segurança e a transparência das informações. Cabe

aos advogados, caso o seu cliente ou os administradores não respondam a possíveis denúncias de irregularidades, comunicarem o fato ao Conselho Fiscal ou órgão competente da companhia. É provável que essa regra venha a atingir também advogados e empresas estrangeiras, incluindo departamentos jurídicos de companhias emissoras de informações (EGAN, 2005; MCCARTHY e CAMPBELL, 2001).

A SOX não define um tipo de indicador ou métrica para acompanhamento da Segurança da Informação. Entretanto, ela indica as responsabilidades e penalidades no caso de um incidente de Segurança da Informação ocorrer, oriundo da negligência ou imperícia dos gestores quanto a condução dos controles internos. A SOX impacta diretamente nas empresas brasileiras que operam nas bolsas de valores norte-americanas, pois elas devem seguir as determinações da SOX e, portanto, devem seguir as mesmas diretivas. Pela abrangência e generalização da SOX, surge a necessidade de um modelo de orientação de boas práticas para atender esta demanda, entre eles o COSO o qual é apresentado nos modelos descritivos deste trabalho.

Outra normativa relevante para esta pesquisa é o *Health Insurance Portability and Accountability Act* (Ato de Responsabilidade e Portabilidade do Seguro de Saúde). O HIPAA o qual foi promulgado em 2005 nos Estados Unidos como um Ato de Lei para proteger a informação pessoal utilizada ou informada na prestação de um serviço da área de saúde e provido por entidades que lidam com a informação pessoal em seus procedimentos diários, sejam elas instituições financeiras, provedores de serviços médicos ou seguradores. Pode-se dizer que o HIPAA é a resposta oficial para

preocupações éticas e morais da proteção da informação do indivíduo na forma de Lei nos Estados Unidos (BAUMER et al., 2000).

Quando se analisa o assunto privacidade e Segurança da Informação, verifica-se a importância e o papel no segmento da saúde, quer seja para uma organização pública ou privada. No segundo capítulo do regulamento do HIPAA, ou também denominado Simplificação Administrativa, existe a diretiva dos direitos à privacidade e à segurança de dados de saúde (MEUS, 2006).

Segundo Baumer et al. (2000), é importante na abordagem do HIPAA ter conhecimento de sua terminologia como também das diretivas específicas da Legislação. Um destes termos é Entidade Coberta, que são as instituições, organizações ou pessoas físicas susceptíveis aos critérios do HIPAA. De acordo com seus critérios, uma Entidade Coberta é definida como um plano de saúde, uma seguradora de saúde, ou uma organização provedora de cuidados médicos que transfere, aceita e transmite informação de saúde de indivíduos.

Tais transações podem contemplar o faturamento ou pagamento da prestação de serviços médicos, como também as informações pessoais dos pacientes. Estão incluídas no HIPAA as operadoras de planos de saúde, pois são entidades que provêem e/ou pagam os custos de um ato médico. Além destas, são também incluídas as companhias de seguros, clínicas, laboratórios e hospitais. Há várias organizações específicas e programas do governo dos Estados Unidos que são incluídos na definição oficial de Entidade Coberta, juntamente com um conjunto de exclusões (MEUS, 2006).

Segundo Meus (2006), as organizações do segmento da saúde que estão sujeitas a regulamentação do HIPAA, são:

- entidades que prestam serviços finais de assistência médica (entidades hospitalares ou clínicas médicas);
- profissionais da saúde ou organizações que fornecem cuidados médicos;
- organizações ligadas à prestação de serviços, como os laboratórios, centros de pesquisa e demais entidades de apoio ao ato médico;
- empresas de prestação de serviços auxiliares de serviços médicos, que fazem serviços de faturamento, reimpressão, sistemas de informação de gestão de saúde;
- organizações que adicionam valor às redes de serviços médicos em processos, ou que facilitam o processamento de dados não padronizados, recebidos de outra entidade relativo à troca de dados. .Estas empresas podem prover serviços específicos, como as empresas de cobrança de pagamento (WILSON, 2006).

A *Protected Health Information* (PHI), ou informação de saúde protegida, está no coração do HIPAA e é a base para muitas das exigências dos demais pontos do HIPAA. A PHI é qualquer informação de saúde ou informação relacionada que é criada, mantida, transferida ou recebida pela Entidade Coberta que identifica um indivíduo, ou pode ser usada indiretamente para identificar um indivíduo. A PHI está relacionada a informações passadas, presentes, ou que irão acontecer no futuro, sobre a condição física ou mental de um indivíduo, ou sobre o pagamento de um ato médico. Exemplos incluem a informação sobre uma aplicação de seguro

médico, registros médicos, números de previdência social e prontuários (WILSON, 2006).

O HIPAA é composto por duas partes principais: O ‘P’ em HIPAA representa a Portabilidade, ou seja, definindo as Entidades Cobertas. A segunda parte do HIPPA é a seção mais significativa do Ato. Esta seção é conhecida como as providências de Simplificação Administrativas. Estas se referem ao primeiro ‘A’ em HIPAA, ou seja, *Accountability*. As providências nesta seção só são aplicáveis às Entidades Cobertas, como descritas anteriormente. A segunda parte é composta por critérios de como proteger a informação de saúde, constituída de duas divisões:

a) a primeira destas divisões refere-se aos padrões para transações de saúde eletrônicas. Estas transações incluem a elegibilidade dos planos de saúde, aditivos contratuais, pagamentos da prestação de serviço médico e prêmio dos planos de saúde, *status* de uma solicitação, relatórios demonstrativos, gestão dos benefícios, e outras transações relacionadas;

b) segunda divisão requer para hospitais, médicos, enfermeiras e outros provedores de ato médico para obter um único *National Provider Identifier* (NPI) para uso em todas as transações relacionadas à prestação de serviço ou de pagamento para serviços médicos. O NPI substitui os números de identificação existentes, inclusive os demais números de identificação médica existentes nos Estados Unidos fornecidos por entidades de classe.

O HIPAA tornou-se um padrão de transações nacionais que deve ser adotado por todos os planos de saúde e prestadores de serviços médicos nos Estados Unidos. O HIPAA não possui itens de regulamentação para as entidades que usam transações não-eletrônicas e que adotam os padrões

manuais para o pagamento de serviços médicos. Porém, as transações eletrônicas são requeridas por um sistema público de informações e todos os provedores têm que adotar os padrões para estas transações. Se um provedor não adotar o padrão, terá que contratar um dos prestadores de serviços homologados para prover a transmissão dos dados e atender ao HIPAA.

Além de transações de saúde eletrônicas unificadas, o HIPAA define uma codificação padronizada, descrevendo os problemas de saúde, causas, sintomas, etc. A meta desta divisão do HIPAA é melhorar a eficiência e reduzir o erro na entrega da informação do ato médico, unificando a troca eletrônica de dados (BAUMER et al., 2000).

As Regras de Privacidade dos Direitos do Indivíduo nos Estados Unidos possibilita às pessoas questionarem as entidades cobertas que mantêm um PHI dos indivíduos, como podem assegurar que as comunicações das informações estarão sigilosas, confidenciais e seguras, ou quais são os direitos de um indivíduo de registrar as reclamações e quais as seguranças de privacidade, relacionadas segundo o formalismo do Departamento de Saúde e do Departamento de Serviços Humanos e de Direitos Civis dos Estados Unidos. Também esboça as penalizações e as responsabilidades das Entidades Cobertas (WILSON, 2006).

Observa-se que o HIPPA apresenta uma base importante para o estudo da Segurança da Informação na área da saúde, incluindo-se as entidades hospitalares. Todavia, a padronização do HIPPA referencia alguns pontos da normativa ISO/IEC 17799 vistos anteriormente, mas excluindo algumas dimensões e critérios, focalizando-se muito mais na troca e transmissão eletrônica de dados. Além disso, é aplicável aos Estados Unidos,

configurando-se um modelo normativo adequado à realidade daquele país (MEUS, 2006).

No Brasil, o Conselho Federal de Medicina (CFM), órgão de classe da área médica, fundou a Sociedade Brasileira de Informática na Saúde (SBIS) com a finalidade de elaborar normativas similares às existentes nos Estados Unidos. Entretanto, o CFM é um órgão de classe que não congrega as entidades jurídicas relacionadas ao ato médico, como os laboratórios, hospitais e clínicas. Com isso, as tentativas de criar normas iguais ao HIPPA são infactíveis. Por outro lado, o Governo do Brasil, através da agência reguladora que fiscaliza as ações destas instituições, a Agência Nacional da Saúde (ANS), não possui nenhuma ação concreta para a definição de normativas que garantam a proteção da informação dos indivíduos.

2.3.3 Análise Geral dos Modelos Prescritivos e Normativos

Como visto anteriormente, os modelos prescritivos e normativos são baseados em normas padronizadas e formuladas para serem submetidas em casos concretos, determinando o que deve ser feito. Pode-se dizer que os modelos apresentados auxiliam as organizações na medida em que impõem regras e diretivas de atuação.

Os modelos prescritivos abordados por esta pesquisa são os recomendados por especialistas e difundidos pela literatura especializada sobre o tema Segurança da Informação, como guia das melhores práticas. Percebe-se uma evolução técnica das normas ISO/IEC para a Segurança da Informação, incluindo formas de gestão, uma melhor estruturação das normas

complementares e a inclusão de critérios de segurança além de aspectos tecnológicos, mantendo-se atualizada. Esta evolução das normativas trouxe um aperfeiçoamento na descrição dos processos, nos itens de controle e na forma de gerir a segurança. Foram inseridas novas dimensões de análise contemplando diferentes formas de armazenamento, transmissão e disponibilidade da informação, além de fatores externos a informação eletrônica.

Os modelos normativos ainda são genéricos e não são específicos para a Segurança da Informação, dependendo de uma adaptação a realidade de cada organização onde será aplicado. Estas adaptações para segmentos de negócio distintos por vezes são complexas e carecem de estudos e pesquisas para seguir como referencial.

Ainda no Brasil não existem Leis que possam direcionar as organizações quanto a Segurança da Informação. O que existe são iniciativas isoladas de alguns segmentos organizacionais. Na prática o que percebe-se é o uso das normas prescritivas (EGAN, 2004).

Nenhum dos modelos prescritivos ou normativos possibilita a avaliação do progresso da melhoria dos processos, pois apenas definem critérios e itens de controle os quais devem ser atendidas ou não, sem a abordagem de melhoria gradual que acontece nos controles internos com o passar do tempo. Buscando suprir esta lacuna dos modelos prescritivos e normativos alguns modelos descritivos trazem a possibilidade de uma avaliação da maturidade de processos, conforme veremos a seguir.

2.3.4 Modelos Descritivos

Existem na literatura diversos modelos descritivos que sevem para a avaliação de diversos propósitos. Os modelos descritivos servem para descrever a realidade e dar subsídios para prescrever um plano de ação que aproxima o ótimo da realidade. Entretanto, não basta descrever a realidade para saber o que fazer, pois é preciso também avaliar as diferentes opções possíveis e, para isso, faz-se necessário o uso de modelos normativos associados (SAYÃO, 2001).

Para um melhor entendimento do assunto, serão abordados neste tópico conceitos sobre medidas de avaliação e avaliação de maturidade e seus pressupostos elementares. A seguir, serão abordadas a importância das medidas de avaliação e os critérios para uma avaliação de maturidade. Na seqüência, são abordados os modelos que servem como orientação estrutural de avaliação de maturidade desta pesquisa.

2.3.4.1 Medidas de Avaliação

Segundo Chapin e Akridge (2005), as medidas ou métricas de avaliação de segurança (medidas de efetividade dos esforços ao longo do tempo da Segurança da Informação nas organizações), têm exigido um conhecimento maior da organização e seus processos. Um dos pontos importantes a ser considerado é como uma organização pode definir-se como segura e quantas vezes as medidas de segurança são realmente testadas antes que ocorra um incidente grave. Um gerenciamento adequado necessita de

algumas medidas de avaliação de como a organização encontra-se em termos de segurança, pois aquilo que não é medido não é gerenciado.

Os controles mais difíceis tendem a ser organizacionais e sua natureza, requerendo mudanças culturais (como um plano de desastre e recuperação) mais do que soluções técnicas e específicas (como um equipamento de *firewall* ou um sistema de detecção de intrusão), os quais podem ser adquiridos com pouco investimento. Elaborar e manter um processo de verificação da Segurança da Informação permite o crescimento do desenvolvimento cultural da gestão para uma correta percepção dos problemas tradicionais da Segurança da Informação.

Uma nova percepção desses problemas potenciais e com a falta de acompanhamento sistemático, possibilita o desenvolvimento de uma solução consistente para qualquer segmento organizacional (EGAN, 2005). Ainda segundo Egan (2005), esta nova percepção permite uma aproximação mais sistemática das medidas de Segurança da Informação, como:

- Gerar indicadores justificáveis de mensurações da segurança;
- Mensurar as questões de valor para a organização;
- Determinar o real progresso na postura de Segurança da Informação;
- Aplicar em larga escala o que as organizações estão utilizando, no mesmo segmento empresarial;
- Determinar em que ordem os controles de Segurança da Informação devem ser executados;
- Determinar os recursos necessários para executar os processos de Segurança da Informação;

Uma métrica ou indicador não é uma forma de mensuração, pois outros fatores relevantes como o tempo também deve ser considerados. Assim, uma métrica sozinha não é a resposta para os problemas organizacionais de segurança. Não deve-se apenas medir, mas sim agir sobre o problema. As pessoas devem pensar através deste prisma e analisar o tempo de medição de um indicador. Um ponto importante é desenvolver métricas ou indicadores que sejam simples e que possam prover a usabilidade para o gerenciamento da Segurança da Informação, conciliando com os objetivos propostos. A métrica tem que estar alinhada com a organização para demonstrar algum tipo de progresso (CHAPIN e AKRIDGE, 2005). Esta abordagem de evolução temporal na medição sustenta a avaliação por maturidade.

Certas organizações medem incidentes manipulados, como vírus ou eventos registrados. Este tipo de evento não fornece uma medida de qualidade de um programa de segurança, pois podem não mais ocorrer. Deve-se pensar na organização e em seu conhecimento organizacional e sua cultura para a elaboração de métricas realmente importantes. A evolução dos controles da Segurança da Informação é um ponto importante que demonstra evolução e deve ser sempre que possível considerada.

Uma abordagem utilizada pelas organizações de métrica clássica é o custo para o negócio relativo a um dano causado por um incidente de segurança. Presume-se inicialmente que algo ruim irá acontecer e calcula-se o valor que este possível incidente irá causar em termos financeiros. Entretanto, quando tratamos de Segurança da Informação, nem toda informação possui um valor expressivo para a organização ou irá afetar o andamento do negócio, não importando aqui o tempo que irá refletir o suposto incidente. Alguns

incidentes têm uma função de um risco residual, onde o negócio está disposto a fazer um detalhamento maior das causas; outros incidentes a relação custo-benefício para investigá-lo é maior do que não investigá-lo (CHAPIN e AKRIDGE, 2005).

Alternativamente, outros incidentes podem ser os resultados das práticas ineficientes na proteção da informação, que abrem a porta para um novo incidente. Para que se possam diferenciar os tipos de incidentes, é importante considerar que as proteções fornecem somente um determinado grau de segurança, pois através da sua forma de acompanhamento - por métricas -, haverá sempre algum risco, mas deve-se medir os seus impactos (EGAN, 2005). Segundo Mandarini (2004), a chave para um bom gerenciamento da segurança passa pela correta definição das métricas de avaliação, as quais devem:

- Ser uma medida organizacionalmente significativa de algo;
- Ser reproduzível;
- Ser objetiva e justa;
- Ao longo do tempo, deve estar apta a ser medida através de algum tipo de progressão para atingir um objetivo.

Na prática, quase todas as métricas utilizadas sobre Segurança da Informação não atendem na totalidade as características acima. As métricas tradicionais são baseadas em medidas disponíveis e relatadas e não planejadas. Esta forma de abordagem mais sistemática e planejada necessita de métricas elaboradas que possam ser direcionadas nas características mencionadas anteriormente.

2.3.4.2 Avaliação de Maturidade

Uma das formas de medição do progresso dos processos em uma organização é através do uso de um modelo de maturidade. O conceito de níveis de maturidade surgiu nos princípios do gerenciamento da qualidade. A estrutura de avaliação da maturidade através de princípios de qualidade originou-se do trabalho *Quality is Free* (CROSBY, 1999), o qual descreve cinco estágios na adoção das práticas de qualidade: Incerteza, Despertar, Esclarecimento, Sabedoria e Certeza. Cada um dos estágios é analisado por seis aspectos diferentes do gerenciamento da qualidade, formando uma matriz denominada *Quality Management Maturity Grid* ou Matriz de Maturidade do Gerenciamento da Qualidade (CROSBY, 1999).

Assim, define-se Maturidade como "a extensão em que o processo é explicitamente definido, gerenciado, medido, controlado e eficaz" (SIQUEIRA, 2005, p. 4). O conceito básico sob o termo maturidade é de que as organizações maduras fazem as coisas de modo sistemático e de que as imaturas atingem seus resultados graças aos esforços heróicos de indivíduos, usando abordagens que eles criam mais ou menos espontaneamente. Segundo Crosby (1999), a maturidade deve ser medida ao longo do tempo, além do plano de implementação, medindo não somente a qualidade do plano, mas a sua evolução e os resultados obtidos. Esta definição da maturidade tem diversas características importantes:

- Fornece o escopo para um plano de Segurança da Informação;
- Auxilia a gestão na definição da ordem de implementação;
- Conduz para o uso das melhores práticas e aderência as normas internacionais.

Em 1986, esses princípios foram adaptados pelo *Software Engineering Institute* (SEI) da *Carnegie Mellon University*, para o processo de desenvolvimento de *software* em um modelo denominado *Capability Maturity Model* (CMM) (HUMPHREY, 1987). O principal objetivo do CMM é mensurar a maturidade de uma área de desenvolvimento de *softwares*, sendo necessário ser analisado, compreendido e adaptado às características de cada organização.

O CMM descreve as etapas necessárias para que uma área desenvolvedora de *software* produza, consistentemente e previsivelmente, produtos de qualidade assegurada. O modelo possibilita analisar o quanto o processo implantado em uma organização é capaz de assegurar a qualidade dos sistemas desenvolvidos através de áreas chave do processo ou *Key Process Áreas* (KPA's).

O CMM apresenta uma estrutura em cinco níveis de maturidade para organizar as etapas evolutivas que estabelecem fundamentos sucessivos para uma contínua melhoria do processo de desenvolvimento de *software*. Esses níveis de maturidade definem uma escala ordinal para medir e avaliar a maturidade de um processo de desenvolvimento de *software* na organização, ajudando a priorizar esforços na melhoria do processo (PÁDUA, 2006).

Cada nível é um estágio evolutivo bem definido, compreendendo um conjunto de objetivos que, quando satisfeitos, estabilizam um componente importante do processo. O modelo tem como premissa a dependência dos critérios de avaliação, ou seja, segundo o CMM é necessário que todos os itens de verificação estejam em um nível de maturidade para que se possa afirmar que o processo encontra-se naquele nível. A avaliação da maturidade

dar-se-á pelo conjunto de itens de verificação e não cada um isoladamente (HUMPHREY, 1987). A análise da maturidade, neste caso, é a visão do conjunto de itens, não analisando as partes individualmente.

Alcançando cada nível da estrutura de maturidade, estabelecem-se diferentes componentes no processo de desenvolvimento de *software*, resultando em um crescimento na capacidade de processo da organização.

Segundo Humphrey (1987), o CMM identifica os níveis por meio do qual uma organização deve desenvolver-se para estabelecer uma cultura de excelência em desenvolvimento de *software*. Os níveis definidos no modelo são:

Nível 1 - Inicial: o processo de *software* é caracterizado como *ad hoc* e ocasionalmente pode ser considerado caótico. Poucos processos são definidos e o sucesso depende de esforço individual dos recursos;

Nível 2 - Repetível: os processos básicos de gestão de projeto são estabelecidos para acompanhar custo, cronograma e funcionalidade. A disciplina na execução do processo existe para repetir sucessos anteriores em projetos com aplicações similares;

Nível 3 - Definido: o processo de desenvolvimento de software para as atividades de gestão e engenharia é documentado, padronizado e integrado em um processo de software padrão para a organização. Todos os projetos utilizam uma versão aprovada do processo de desenvolvimento e manutenção de *software*;

Nível 4 - Gerenciado: medidas detalhadas do processo de desenvolvimento de software e da qualidade do produto são realizadas. O

processo e os produtos de *software* são quantitativamente compreendidos e controlados;

Nível 5 - Em Otimização: a melhoria contínua do processo é propiciada pelo *feedback* quantitativo do processo e pelas idéias e tecnologias inovadoras.

Contanto que um padrão seja utilizado, podem-se comparar os resultados obtidos de uma organização com outra ou consigo mesmo, avaliando o nível em que encontra-se.

Em 1993, outro modelo foi apresentado para a avaliação de maturidade em processos de usabilidade de *software* intitulado *Cost-Justification of Usability Engineering,* ou Justificativa de Custos da Engenharia de Usabilidade (ROHN, 1994). Ele apresenta quatro estágios de maturidade dos processos normalmente definidos para uma organização cujo negócio seja desenvolvimento de aplicações. Os quatro níveis são: cepticismo, curiosidade, aceitação e parceria (ROHN, 1994).

Outro modelo sobre maturidade em Tecnologia da Informação (TI) denomina-se *Information Technology Strategic Alignment,* ou Alinhamento Estratégico da Tecnologia da Informação (PAPP, 1998), o qual aborda a maturidade do alinhamento estratégico entre negócios e TI manifestando-se pelo nível de processo de práticas correntes nas organizações. Para tanto, ele propôs um instrumento de avaliação do nível de maturidade da TI de uma organização em relação às estratégias organizacionais. Estas práticas são agrupadas em oito grandes dimensões de análise: Comunicação, Medidas, Governança, Parcerias, Escopo, Arquitetura Tecnológica, Habilidades e Recursos Humanos (PAPP, 1998).

Também os modelos existentes de avaliação de maturidade não necessariamente direcionam os planos de Segurança da Informação para um objetivo organizacional particular, mas não abordam como devem ser os planos de implementação para uma exata Segurança da Informação. A avaliação da maturidade permite identificar pontos de melhoria em termos de segurança, propiciando a elaboração de um plano de ação consistente.

Os níveis de maturidade conduzem uma organização para um melhor entendimento do seu plano de segurança e fornecem um instrumento para avaliar o grau de confiança que pode ser colocado em informatização e na conectividade entre organizações diferentes (MOREIRA, 2001).

As organizações maduras atingem seus objetivos de qualidade, prazos e custos de forma consistente e eficiente. Organizações imaturas criam objetivos, mas com muita freqüência perdem seus objetivos por largas margens de erro. Em muitos casos, a qualidade não é a desejada e os prazos e custos podem ser maiores do que os planejados.

Organizações maduras têm processos sistematizados e métodos documentados de realizar suas atividades. Dados são sistematicamente coletados e usados para analisar, controlar, prever e planejar seu desempenho. Por outro lado, as organizações totalmente imaturas não pensam em termos de processos e seus métodos variam conforme as circunstâncias e as pessoas que executam as tarefas. Seus resultados são imprevisíveis e inconsistentes (SIQUEIRA, 2005).

O modelo de maturidade de processos é um referencial para avaliar a capacidade de processos na realização de seus objetivos, para localizar oportunidades de melhoria de produtividade, para reduzir os custos e para

planejar e monitorar as ações de melhoria contínua dos processos empresariais. Cada nível de maturidade é formado por um conjunto de atributos que caracterizam o estágio da capacidade dos processos da organização. Um modelo de maturidade de processos deve ser concebido de tal forma que a capacidade nos níveis inferiores possa prover progressivamente as bases para os estágios superiores.

Ao verificar os modelos existentes de maturidade em Segurança da Informação, o *Information Systems Audit and Control Association* (ISACA), em 2005, elaborou uma Tabela resumo, conforme apresentado na Tabela 3, contendo os principais modelos de maturidade publicados sobre Segurança da Informação e com as suas características principais. Por alguma razão não mencionada, eles apresentam igualmente cinco níveis de maturidade, definindo um padrão de quantidade de níveis. Entretanto, cada modelo aborda a sua própria visão e a sua definição de níveis de maturidade:

MODELOS DE MATURIDADE DE SEGURANÇA DA INFORMAÇÃO PUBLICADOS		
Modelo	**Níveis de Progresso de Maturidade**	**Comentários**
NIST PRISMA	1. Políticas 2. Procedimentos 3. Implementação 4. Testado 5. Integrado	Focado na direção dos níveis de documentação
Citigroup's Information Security Evaluation Model (CITI-ISEM)	1. Aderência 2. Conhecimento 3. Integração 4. Práticas Comuns 5. Melhoria Contínua	Focado na direção organizacional sem distanciamento e adaptado
CobiT Maturity Model	1. Inicial/adhoc 2. Repetitivo mas intuitivo 3. Processos Definidos 4. Gerenciado e Medido 5. Otimizado	Focado na direção de procedimentos específicos auditáveis
SSE-CMM	1. Executado Informalmente 2. Planejado e Controlado 3. Bem Definido 4. Quantitivamente Controlado 5. Melhoria Contínua	Focado na direção da engenharia de segurança e design de software
CERT/CSO Security Capability Assessment	1. Existente 2. Repetível 3. Pessoalmente Designado 4. Documentado 5. Revisado e Atualizado	Focado na direção de mensuração da qualidade relativa dos níveis de documentação

Tabela 3 : Modelos de Maturidade de Segurança da Informação
Fonte : ISACA – Information Systems Audit and Control Association, 2005.

A cada dia surgem novos estudos para a avaliação dos processos de maturidade, como o projeto SOMA (*Security Operations Maturity Architecture),* ou Arquitetura da Maturidade de Segurança das Operações, e o ISECOM ISM3 (*Information Security Management Maturity Model),* ou Modelo de Maturidade no Gerenciamento da Segurança da Informação, projetos estes em fase de conclusão. Todavia, por questões de maturidade destes modelos e sua aplicabilidade para a Segurança da Informação na saúde, estes projetos não serão abordados, mas citados apenas como iniciativas neste sentido.

Uma melhoria para um modelo de maturidade dos processos de Segurança da Informação é o focado na qualidade da execução de cada elemento planejado e pela medida da evolução dos processos de controle. Uma vantagem de adicionar uma conotação de qualidade no plano é, ao contrário da mensuração do nível de maturidade, a postura da segurança a qual se torna não estática na realização do plano de segurança e passa a ser um processo dinâmico, que pode mudar baseando-se na qualidade da execução continuada dos elementos do plano de Segurança da Informação. Isso conduz a um processo de melhoria contínua e uma evolução organizacional e requer da gestão uma postura ativa para manter o plano de segurança atualizado. A qualidade é uma medida subjetiva, e deve estar incluída na avaliação dos processos da maturidade, contribuindo significativamente para a qualidade do modelo (MOREIRA, 2001).

Quanto à quantidade de níveis necessários em um modelo, Papp (1995) sugere que para a uma avaliação consistente de evolução de um processo é necessário a elaboração de um modelo de maturidade contendo um

mínimo de três níveis (alto, médio e baixo). A prática dos modelos demonstra uma quantidade de cinco níveis para permitir uma maior identificação do processo de evolução entre uma situação para outra. Com descrições detalhadas de cada nível relativo a um item a ser mensurado, é possível obter os resultados desejados de comparação com uma situação anterior e de uma situação atual para produzir uma avaliação adequada de um enquadramento em determinado nível para cada item.

Este modelo de divisão por níveis é similar ao sugerido pelo *US National Security Agency* (Agência de Segurança Nacional) dos Estados Unidos, através do *Infosec Assessment Methodology* (Metodologia de Permissão *Infosec*), onde os itens possuem cinco níveis principais e também três níveis distintos de qualidade em detrimento da maturidade dos processos, ou seja, um modelo tridimensional. Todavia, o modelo NSA IAM contempla exclusivamente a avaliação da Segurança da Informação de dados de sistemas informatizados, desconsiderando a informação contida em outros meios de armazenamento ou transmissão.

2.3.4.3 COSO

O COSO é uma entidade nos norte-americana sem fins lucrativos, dedicada à melhoria dos processos de emissão e controle dos relatórios financeiros empresariais. Surgiu em 1975, com o nome de *Nacional Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros) para estudar as causas de fraudes em demonstrativos das empresas. Sua estrutura é composta por entidades e associações de classe vinculadas à área financeira, tais como os

representantes das empresas de investimentos, os contadores, as indústrias e a Bolsa de Valores de Nova Iorque. (GHERMAN, 2005).

O objetivo principal do COSO é definir recomendações para as empresas no que tange aos seus Controles Internos (FEBRABAN, 1999). Entende-se por Controle Interno como um conjunto de processos que preconizam, com razoável certeza, a realização dos objetivos da empresa, em algumas categorias:

a) Eficiência e efetividade operacional – cujos objetivos deste controle é o desempenho ou estratégia empresarial. Este quesito está relacionado com os objetivos básicos da organização, especialmente com os objetivos e metas de desempenho e rentabilidade, segurança e qualidade dos ativos;

b) Confiança nos registros contábeis/financeiros – cujos objetivos são de controle das informações. Esse quesito preconiza que todas as transações devem ser registradas, todos os registros devem refletir transações reais, refletindo os valores e enquadramentos corretos.

c) Conformidade – cujo objetivo é de aderência e conformidade com as Leis e normas aplicáveis à um empresa, bem como as suas entidades filiadas.

Segundo o COSO, o Controle Interno é um processo constituído de 5 elementos inter-relacionados e presentes em todos os processos: (1) Ambiente de controle; (2) Avaliação e gerenciamento dos riscos; (3) Atividade de controle; (4) Informação e comunicação e (4) Monitoramento.

Em forma de compilação de todas estas diretivas, o COSO criou em 1992 um modelo denominado *Internal* Control (Controle Interno). A estrutura

do modelo proposto pelo COSO é baseado em recomendações amplas e genéricas as quais enquadram-se em orientações de boas práticas de governança corporativa. As questões relativas a Segurança da Informação estão contidas nos Controles Internos e nos 5 componentes do modelo e não preconizam diretivas específicas sobre mensuração ou avaliação, não sendo um modelo propício para este estudo, apesar da sua relevância como direcionador para as empresas que buscam adotar boas práticas de gestão.

2.3.4.4 Modelo PRISMA

O Modelo de avaliação da Segurança da Informação do *National Institute of Standards and Technology* é baseado em métricas de avaliação por cinco níveis. As medidas de avaliação de maturidade são utilizadas para demonstrar o progresso das políticas e procedimentos de implementação e os controles individuais de segurança em uma organização.

As métricas sugeridas são definidas em termos de porcentagem constante no modelo *Program Review for Information Security Management Assistance* (PRISMA), ou Programa Revisado para a Assistência no Gerenciamento da Segurança da Informação, onde são apresentadas as políticas existentes por famílias de métricas. Segundo o modelo, aplicando os métodos de avaliação de segurança descritos no PRISMA e documentando seus resultados, obtém-se uma informação que pode ser utilizada para a identificação atual da situação que a organização se encontra em termos de Segurança da Informação e quantificar os resultados dos controles, pois inclui uma medida quantitativa no modelo (NIST, 2006).

O conceito do modelo é que as organizações precisam conhecer o estado da Segurança da Informação para suportar a compreensão das medidas (resultados) da efetividade e eficiência da implementação do controle da segurança de seu programa de segurança. Neste sentido, a implementação e desenvolvimento de métricas irão facilitar a correlação desta informação para os objetivos e metas organizacionais relacionados à estratégia e demonstrará o impacto da Segurança da Informação na implementação da estratégia como um todo.

As métricas de avaliação requerem informação que possa facilmente ser obtida dos relatórios de avaliação do controle da segurança e das medidas da performance, planos de ações e marcos, além de outras documentações e descrição das atividades do programa de controle da Segurança da Informação. Estas métricas são utilizadas para monitorar os resultados da implementação de um programa de segurança e podem requerer diversos pontos de informação, quantificando a implementação do plano de segurança e medindo o resultado da implementação (NIST, 2006).

As métricas de impacto são utilizadas para articular o impacto da Segurança da Informação na missão das organizações, normalmente através da quantificação da redução de custo produzido pelo planejamento de segurança ou através da economia alcançada pelo endereçamento dos eventos de segurança. Essas métricas combinam informação sobre os resultados da implementação dos controles de segurança com a variedade de informação sobre os recursos (CHEW et al., 2006).

As medidas podem propiciar uma visão do valor da Segurança da Informação para a organização e quais são aquelas medidas que serão

utilizadas pelos gestores. Essas medidas requerem o controle de uma variedade de informações de recursos através da organização, de forma que possa ser vinculada com as atividades de segurança. Todavia, a habilidade de gerenciamento é crítica para o sucesso deste modelo. As organizações devem limitar o número de indicadores a serem coletados entre cinco e dez para cada parte envolvida no mesmo momento (CHEW et al., 2006).

O modelo explicitamente conecta atividades da Segurança da Informação com as metas estratégicas da organização através do desenvolvimento e a conexão ao uso de indicadores de desempenho. Este modelo assume que as organizações têm diversas metas estratégicas e que apenas uma meta pode requerer múltiplos controles de segurança. Os aspectos estratégicos propostos pelo modelo são (NIST, 2006):

- Cultura e Gerenciamento da Segurança da Informação;
- Planejamento da Segurança da Informação;
- Educação, Treinamento e Recompensa pela Segurança da Informação;
- Recursos e Orçamento;
- Gerenciamento do Ciclo de Vida;
- Certificação e Acreditação;
- Infra-estrutura Crítica;
- Resposta a Incidentes.

Em cada dimensão estratégica acima citada são sugeridos aspectos técnicos que devem ser medidos e definidos pesos de relevância para o negócio organizacional, produzindo-se assim uma matriz de avaliação. Os níveis de maturidade do modelo são Políticas, Processos, Implementação,

Testes e Integração. Todavia, cada item de avaliação deve estar avaliado em cada um dos níveis de maturidade e não apenas identificando em que estágio se encontra. O modelo de desenvolvimento de métricas de desempenho propicia dois caminhos de medidas de avaliação:

- A abordagem do controle específico, onde se seleciona controles individuais como base na métrica que melhor representa toda a família de medidas e determinada pelo ambiente organizacional;
- A abordagem "atravessando" foca-se em métricas que medem o desempenho da segurança baseado em mais de um controle individual ou famílias de controle.

Enquanto ambas as abordagens irão resultar em métricas que são representativas na avaliação das organizações no suporte correspondente aos objetivos da estratégia, as métricas de "atravessando" irão prover uma visão das fronteiras do desempenho da Segurança da Informação comparada com a abordagem do controle específico. O modelo permite um alinhamento estratégico, porém, de relativa complexidade na elaboração das métricas de avaliação, pois apenas sugere as dimensões e métricas, devendo cada organização elaborar a sua matriz e seus pesos relativos em cada item de análise aderente ao negócio. O modelo PRISMA não está adaptado às necessidades das instituições hospitalares, devido as particularidades existentes neste segmento.

2.3.4.5 Modelo CCSMM

O modelo CCSMM foi proposto pelo Centro de Pesquisas da Garantia de Infraestrutura e Segurança da Universidade de San Antonio nos Estados Unidos e apresentado recentemente na Conferência Internacional das Ciências de Sistemas em 2007. Este modelo surgiu como o resultado da necessidade de melhor definir o grau de preparação das comunidades virtuais para a "era virtual" e de definir um modelo de maturidade de segurança da comunidade cibernética. Com o objetivo de avaliar muita das pendências que a comunidade enfrentava com relação à segurança do desenvolvimento das comunidades virtuais, o modelo apresenta uma formatação diferenciada.

O modelo possui cinco grupos de métricas, definidos por: medição da segurança; tecnologia necessária; ameaças que serão endereçadas; mecanismos para comunicação entre diferentes entidades da comunidade; e testes que podem ser usados juntamente com as métricas para medir o *status* atual do nível de preparação da segurança da comunidade. Em cada grupo de métricas existem diferentes itens de identificação, baseado na evolução da maturidade.

Embora uma comunidade em um local específico possa estar em um nível de maturidade, as demais entidades ou indivíduos da comunidade podem estar em outro nível de maturidade diferente. O modelo tem que ter a habilidade de diferenciar entre diferentes comunidades e seus próprios níveis de preparação. Cada um dos cinco níveis de maturidade do modelo está associado a um nome, indicando o tipo de ameaças e atividades que serão endereçadas naquele nível.

O primeiro nível é denominado “Segurança Conhecida”, a qual permite entender corretamente que o maior tema das atividades neste nível é fazer os indivíduos e as organizações terem conhecimento das ameaças, problemas e pendências relacionadas com a segurança virtual.

O Segundo nível é denominado “Desenvolvimento do Processo” e, novamente, fornece uma pista significativa de qual o tema deste nível. Os elementos do nível dois são desenhados para ajudar as comunidades a serem criadas e melhoradas em relação aos requerimentos do processo de segurança, definindo efetivamente as pendências da segurança virtual.

O terceiro nível do modelo é “Ativação da Informação” e indica que as organizações da comunidade têm conhecimento das pendências relacionadas com segurança e conhecem o processo e os mecanismos para identificar os eventos de segurança relevantes. O objetivo neste nível é melhorar através dos mecanismos de compartilhamento da informação dentro da comunidade para possibilitar à comunidade uma correlação efetiva das diferentes partes da informação coletadas por cada um dos seus participantes. Desta forma, pode-se identificar uma possível fragilidade nos métodos de segurança, permitindo uma maior vulnerabilidade.

O nível quatro do modelo é o “desenvolvimento de táticas”. Neste nível, os elementos são desenhados para desenvolver sistemas melhores e ter métodos pró-ativos para detectar e responder aos potenciais ataques. Por este nível, muitos métodos de prevenção devem estar em pauta, já desenvolvidos.

O último nível do modelo é a “Capacidade completa de segurança operacional”, a qual representa que já a comunidade deve estar preparada para quaisquer ataques, sendo as organizações consideradas operacionalmente

prontas para endereçar qualquer tipo de ameaça virtual. Isso não implica que as entidades, neste nível, estarão livres de que qualquer ataque e que tenha sucesso em caso de um ataque, mas elas terão feito tudo que podiam para preveni-lo e detectá-lo.

Além disso, comunidades no nível cinco estão em excelente preparação para responder efetivamente a um evento em um primeiro momento, mesmo que elas possam não estar prontas para prevenir que o ataque venha a ter sucesso. Organizações neste nível também estão completamente conectadas às entidades apropriadas de fora da comunidade. Com isso, esta informação do ataque pode ser compartilhada. Trabalhando cooperativamente juntas irão permitir a todas as comunidades endereçarem as ameaças da segurança virtual.

2.3.4.6 Modelo CobiT

Uma abordagem diferenciada sobre Segurança da Informação é apresentada pelo projeto do *Control Objectives for Information and Related Technology* (Objetivos de Controle para a Informação e Tecnologias Relacionadas) produzido pelo *Information Systems Audit and Control Association* (ISACA). O CobiT é supervisionado por um comitê internacional, formado por múltiplas indústrias, responsáveis por pesquisar e desenvolver o modelo do CobiT e multiplicar os grupos de trabalho (COBIT, 2004).

De forma a tornar mais fácil de acessar e visualizar os objetivos de controle, eles foram agrupados em 34 processos (também conhecidos como objetivos de controle de alto-nível), agrupados em quatro domínios. Cada

objetivo de controle de TI possui um detalhamento chamado “práticas de controle”, que são a extensão dos objetivos de controles. O CobiT é formado por uma classificação ampla de objetivos de negócio incluindo requerimentos que agregam valor, como qualidade, custo e entrega; requerimentos fiduciários, como efetividade e eficiência; e requerimentos de segurança, como confidencialidade, integridade e disponibilidade.

Na abordagem da Segurança da Informação, estes itens foram divididos em categorias sobrepostas, contemplando a efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade da informação. Os recursos existentes no CobiT incluem componentes como dados, aplicações, sistemas, tecnologias, facilidades e pessoas. Os dados referem-se a objetos internos e externos, estruturados e não-estruturados, gráficos, sons, ou qualquer outro tipo de dado. Sistemas aplicativos são todos os procedimentos manuais ou procedimentos informatizados. A tecnologia descreve os itens como *hardware*, sistemas operacionais, sistemas de gerenciamento de banco de dados, infra-estrutura de comunicação e multimídia. As facilidades incluem todos os recursos caseiros e os sistemas de suporte à informação. Pessoas incluem os perfis das equipes e as competências. Além disso, contempla os planejamentos de produtividade, organização, aquisição, entregas, suporte e sistemas de informação e serviços.

O CobiT também descreve a estrutura do modelo através de atividades e tarefas são combinadas para formar um processo. Estes processos então são combinados para formar um ou mais domínios. Os domínios são divididos em Planejamento e Organização (PO), Aquisição e Implementação (AI), Entrega e Suporte (DS), e Monitoramento (M). Como exemplo, as tarefas de

gerenciamento de uma senha de acesso são combinadas com outras atividades de segurança para formar um processo que garante um sistema de segurança, ou o processo DR5.

Os níveis de avaliação de maturidade propostos pelo CobiT estão divididos em seis categorias: Inexistente, Inicial/*Ad Hoc*, Repetitivo, Definido, Gerenciado e Otimizado. Para cada tópico da avaliação, a organização deve utilizar a escala de medição de seis graus, variando de 0 a 5, para definir sua posição estimada. Pode-se então, fácil e graficamente, comparar com dois pontos de referência (Média da Indústria e Meta Empresarial), conforme apresentado na Figura 2 - Níveis de Maturidade do CobiT:

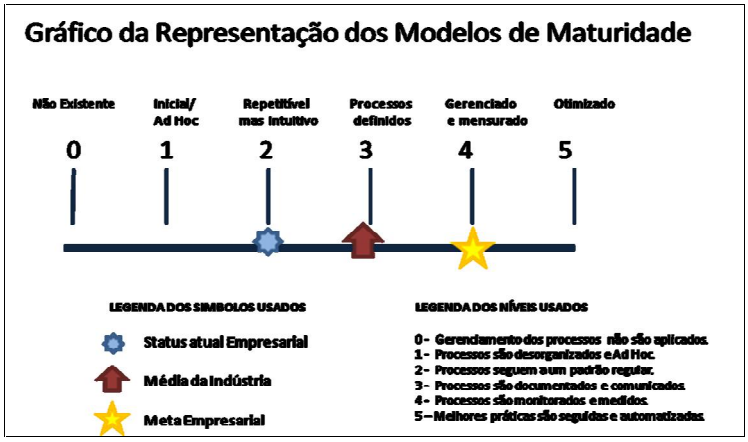

Figura 2: Níveis de Maturidade do CobiT
Fonte: Adaptado de COBIT, 2004

Segundo Chickowski (2004), o CobiT foi elaborado para trabalhar como um modelo "guarda-chuva de alto nível" e é mais eficiente quando empregado com outras metodologias. O CobiT é também compreensivo para cobrir a maioria dos requerimentos relativos à Segurança da Informação, mas genérico suficiente como outra qualquer plataforma metodológica (LAINHART, 2001). No que se refere à Segurança da Informação, o CobiT

prove instrumentos para que a TI perceba os riscos que são identificados e que permanecem expostos e não são gerenciáveis.

Segundo Hawkins, Alhajjaj, e Kelly (2003), o CobiT permite a uma organização identificar e definir suas áreas mais vulneráveis e definir um nível de controle que irá limitar as perdas das informações valiosas e garantir a continuidade dos serviços de TI. Entretanto, o modelo proposto pelo CobiT contempla a avaliação da maturidade dos processos de TI, onde parte dos processos está a Segurança da Informação. Porém, como visto em modelos anteriores, as particularidades existentes na informação hospitalar e o grau de profundidade da avaliação da maturidade dos processos pelo CobiT, não justificam a sua utilização em instituições hospitalares.

2.3.4.7 Modelo CERT-CSO

O CERT-CSO é um modelo elaborado em co-participação da *CSO Magazi*ne e pelo *CERT Coordination Center (CERT/CC)* da *Carnegie Mellon University* para auxiliar as organizações a comparar os seus processos de segurança (particularmente os pertinentes a Segurança da Informação), com os processos de outras organizações ao redor do mundo. O modelo CERT-CSO não é considerado um modelo de maturidade puro, pois não possibilita avaliar a evolução dos processos de Segurança da Informação de uma organização ao longo do tempo. Entretanto, o CERT-CSO é um modelo de avaliação que possibilita a comparação de sua maturidade indireta em relação a outras entidades. É necessário que a empresa adote controles adicionais para a gestão da evolução dos processos (ALLEN, 2005).

Também denominado de *Security Capability Assesment (CSA),* ou Avaliação de Capacidade de Segurança, o modelo foi construído e inspirado no CMM. A razão para o uso da expressão "*capability*" é relativa à capacidade de atender os quesitos propostos pelo modelo. Todavia, o termo "*maturity*" foi retirado, pois não é objetivo do modelo avaliar a maturidade na perspectiva temporal (ALBERTS e DOROFEE, 2002).

O Modelo de Capacidade de Segurança é estruturado para propiciar uma aproximação mais efetiva entre os processos de Segurança da Informação, começando a melhorar a administração de riscos, as políticas relativas e então a tecnologia associada, em lugar de manter o foco em soluções de tecnologia, como uma abordagem exclusiva. Além de outros temas de melhoria, o modelo dá ênfase à Governança de TI, especialmente da Segurança da Informação, indicando as melhores práticas e o uso de métricas e indicadores (ALLEN, 2005).

As categorias de análise são divididas em: Facilidade de Acesso, Plano de Continuidade do Negócio, Consciência dos Colaboradores e Capacitação e Verificação de Procedimentos. Os resultados indicam que a Segurança da Informação não é somente uma área voltada à TI, mas sim necessita da atenção de toda a organização.

Os níveis de aderência utilizados pelo modelo são divididos em cinco níveis: (1) Existente, (2) Repetível, (3) Pessoalmente Designado, (4) Documentado e (5) Documentos Revisados e Atualizados. A avaliação é feita na documentação dos processos referentes à Segurança da Informação, não enfocando os controles utilizados ou na forma de implementação. Pelo modelo não é possível verificar se um determinado processo está sendo executado.

CERT-CSO verifica o grau de documentação, que por vezes pode não estar refletindo a realidade da empresa.

Em termos de utilidade deste modelo para as instituições hospitalares, a mesma deixa lacunas na avaliação, pois a existe a possibilidade de um descompasso entre a documentação e a realidade prática da Segurança da Informação. Entretanto, para a avaliação do nível de maturidade dos processos de documentação da Segurança da Informação, parece ser um modelo aderente as necessidades das organizações.

2.3.4.8 Modelo SSE-CMM

O Modelo *System Security Engineering Capability Maturity Model (SSE-CMM),* ou Modelo de Maturidade da Aderência a Engenharia de Segurança, foi elaborado pelo *Department of Information Processing Science* da Universidade de Oulu (Finlândia) para a avaliação da maturidade dos processos de desenvolvimento de *software*. Segundo o modelo, existem vários graus de maturidade diferentes para cada quesito, cada um representativo da sofisticação de processos de desenvolvimento (SIPONEN, 2002).

O modelo foi baseado em diversos modelos de maturidade disponíveis como os níveis de maturidade sugeridos pelo CMM. Além deste, o modelo tem como base estrutural o Modelo de Avaliação da Maturidade da Capacidade (IA-CMM), o qual a Agência de Segurança Nacional dos Estados Unidos (NSA) usa para avaliar complacência e efetividade de organizações que desenvolvem aplicações.

Em resumo, o SSE-CMM é uma coletânea de diversos modelos de maturidade de processos de *software*, o qual define as expectativas de

processos e capacidades para cada nível dentro da área de avaliação. A cada nível mais alto na escala, o SSE-CMM torna-se menos exigente sobre um atributo de segurança específico e mais sobre o papel de segurança do desenvolvimento de aplicações dentro da organização.

O SSE-CMM adota a abordagem da Segurança da Informação no desenvolvimento de qualquer aplicativo. O modelo é extenso e complexo, o que o torna bastante rigoroso nas avaliações de maturidade para segurança do desenvolvimento de aplicações (SIPONEN, 2002). A própria descrição da maturidade completa está perto de 1.000 páginas de itens de avaliação, sendo que o processo de avaliação é formal e longo, passando por todos os pontos e fases a partir da primeira fase. Além disso, a formulação e o funcionamento do processo de avaliação são rígidos e incluem elementos burocráticos.

Por exemplo, há vários papéis organizacionais que são definidos para serem cumpridos no processo de avaliação, como facilitadores de avaliação, responsáveis por evidências, membros decisórios, os observadores (referindo-se às organizações de avaliação) e o coordenador local, executivos, porta-voz executivo, líder de projeto e demais representantes das entidades (DOBSON, 1990).

Tal burocracia possibilita avaliar detalhadamente o nível de segurança de desenvolvimento de uma grande organização, ou particularmente para organizações emergentes ou pequenas, selecionando-se os processos a serem avaliados na organização. O conjunto de processos de avaliação da maturidade proposto pelo modelo inclui 11 macro processos divididos em: Controle de Segurança Administrativa, Impacto dos Ativos, Riscos de Segurança dos Ativos, Vulnerabilidade dos Ativos, Argumentos de Garantia

de Construção, Segurança Coordenada, Postura de Segurança dos Sistemas de Monitoria, Entradas de Segurança, Necessidades Específicas de Segurança, Segurança da Verificação e Validação, Qualidade Assegurada, Gerenciamento de Configurações, Gerenciamento do Programa de Riscos, Monitoramento e Controle do Esforço Técnico, Plano do Esforço Técnico, Processo de Engenharia da Segurança da Definição Organizacional, Melhoria do Processo de Engenharia da Segurança Organizacional, Gerenciamento da Evolução do Produto de Linha, Gerenciamento Ambiental do Suporte da Engenharia de Segurança, Provimento de Conhecimento e Perfis e, finalizando, Coordenação dos Fornecedores. O SSE-CMM apresenta cinco níveis de maturidade que são: Executado Informalmente, Planejado e Controlado, Bem-Definido, Quantitativamente Controlado e Melhoria Contínua.

O SSE-CMM possibilita a liberdade de avaliação para escolher as metas particulares das avaliações em cada situação, onde as organizações podem selecionar quais processos desejam avaliar, desmembrando o modelo em partes. Entretanto, ele propõe-se a avaliar a segurança do desenvolvimento de sistemas computacionais e não a avaliação da Segurança da Informação Organizacional. Além disso, o modelo apresenta uma complexidade alta de avaliação e implementação, especialmente para instituições hospitalares, por ser adaptável a diversos contextos empresariais e abstratos em sua definição, não sendo fácil seu entendimento e adaptação.

2.3.5 Análise Geral dos Modelos Descritivos

Os modelos descritivos apresentados buscam fornecer um instrumento de avaliação da maturidade em Segurança da Informação para diversos segmentos e propósitos. Por seu aspecto restrito a propósitos específicos, os modelos descritivos apresentados concentram-se em processos definidos. Diante disso, parece que os modelos não possuem a pretensão de atender a todos os segmentos de atuação ou cobrir totalmente os critérios propostos pelos modelos normativos.

No que concerne ao segmento hospitalar, os modelos apresentados na revisão de literatura não contemplam os quesitos necessários para avaliar as instituições hospitalares, pois não incluem a adaptação para questões específicas de um negócio. Entretanto, os modelos existentes possuem uma estrutura lógica de níveis de maturidade e critérios de avaliação, os quais permitem formar um embasamento de idéias e princípios para a proposição de um instrumento focado nas instituições hospitalares.

2.4 A INFORMAÇÃO E A SAÚDE NO BRASIL

O papel da informação na saúde quer seja de origem administrativa, assistencial ou epidemiológica, tem sido apontado como crucial para auxiliar na assistência da população. Muitas são as vantagens do uso da informação em todas as áreas da atividade humana, e em especial as voltadas para o setor da saúde. Entretanto, o uso de tecnologia da informação nas instituições hospitalares, deve considerar a sua implementação considerando às questões éticas, técnicas, humanas, sociais, financeiras e legais. O uso inadequado e a

falta de gestão da tecnologia podem perturbar equilíbrios delicados na relação médico-paciente, ameaçar a privacidade da informação e simplesmente servir ao mero controle de custos em vez de significar real melhora na qualidade de atendimento. A informatização presente em hospitais trouxe, para a prática diária, agilidade, praticidade e organização que os médicos não possuem (MANDL e KOHANE, 1999).

Um dos principais meios de armazenamento da informação na área da saúde são os prontuários em papel, os quais estão sujeitos mais facilmente ao extravio, com um conteúdo por vezes ilegível, incompleto, ambíguo, que precisa ser transcrito para diversos fins. Ao mesmo tempo, o papel é facilmente carregado, possui liberdade de estilo, facilidade para burlar a sua segurança e está disponível a qualquer instante para o médico. Em uma avaliação mais ampla do assunto, ainda não existe há uma legislação específica para setor hospitalar que defina os direitos e responsabilidades para a Segurança da Informação. Todavia, tanto a sociedade, as instituições hospitalares, os órgãos do governo e os usuários da informação sabem da sua importância. Muitas questões ainda devem ser resolvidas como a classificação da informação, a sua propriedade e seus usuários e influenciadores como, por exemplo, as questões éticas envolvidas e os interesses das partes, as quais serão abordadas a seguir.

2.4.1 A Ética Médica e a Informação

A evolução tecnológica na área hospitalar e o conseqüente incremento de informações relativas ao trabalho médico têm levado a difusão do uso da informatização na prática médica. Arnodo (1993) aborda sobre a importância

da informática nos dias de hoje e dos sistemas e aplicativos específicos para a saúde, os quais são ferramentas necessárias ao gerenciamento da qualidade dos serviços médicos.

A informação médica aborda inúmeros aspectos tecnológicos que vão além do ato direto médico. Segundo Arnodo (2003), três deles são principais: os métodos diagnóstico-terapêuticos modernos através de exames subsidiários altamente especializados e informatizados; o uso da informática, principalmente Internet e sistemas de prontuário médico; e a Medicina Baseada em Evidência (MBE) para atualização médica. O uso da informação no atividade médica diária é polêmica devido ao impacto direto que causa na relação médico-paciente. Entretanto, o uso da informação e dos recursos tecnológicos na área da saúde faz emergir questões éticas, já que as boas práticas da medicina e da enfermagem são habilidades humanas que necessitam de interpretação e de segurança das informações utilizadas (LEÃO, 2003).

Um impeditivo para a adoção massiva dos sistemas de informação como suporte ao trabalho médico é a falta de critérios e regulamentações para assegurar a confidencialidade dos pacientes. Tanto os médicos quanto os pacientes não confiam que o uso da tecnologia da informação manterá as suas informações pessoais em privacidade, pois qualquer falha na Segurança da Informação estará arruinando um dos pilares da relação médico-paciente (ARNODO, 1993). Entretanto, é interessante observar que pesquisas recentes confirmam que os pacientes se sentem seguros com o uso da informática, acreditando que os prontuários manuais são passíveis de perdas, ao contrário

do prontuário eletrônico que guarda seguramente as informações (LEÃO, 2003).

Outra problemática constante em instituições hospitalares refere-se ao valor legal do prontuário eletrônico. Atualmente o Conselho Federal de Medicina (CFM) está revendo este item através da Resolução CFM nº 1.639: "Normas técnicas para o uso de sistemas informatizados para a guarda e manuseio do prontuário médico". A assinatura eletrônica já está sendo considerada válida não apenas no meio médico, mas também na sociedade em geral, como, por exemplo, na carteira de habilitação (LEÃO, 2003). A crítica que se faz é quanto à desatualização dos médicos em relação a tais recursos, uma vez que alguns utilizam prontuários eletrônicos improvisados que podem não ser considerados válidos legalmente.

Donald (1990) acredita que alguns benefícios foram determinantes para a mudança da postura do médico frente ao uso da informática, os quais destacam-se o armazenamento de fotos, filmes e exames, levantamento de seus pacientes com um banco de dados próprios, prescreverem com letra legível e com otimização do tempo, consulta a livros eletrônicos e *sites* de informação médica, prover orientações aos pacientes de forma mais legível e eficiente, além da criação de protocolos de gerenciamento de doenças.

Diferente de outros profissionais que trabalham com o perfil estatístico de produtividade e qualidade, o médico ficou aquém da organização e padronização de seus registros médicos. Sua letra caracteristicamente ilegível preenche receituários e prontuários de maneira satisfatória para a prática diária, mas pouco eficiente para um levantamento de dados ou mesmo para a busca de um exame antigo dentro de um volumoso

prontuário (ARNODO, 1993). Em contrapartida, é importante notar que alguns médicos acreditam que não há vantagem do uso da informatização, mostrando que ainda não há aceitação completa deste recurso.

As principais vantagens do uso de prontuário em formato eletrônico são os possíveis acessos simultâneos em várias partes do mundo, legibilidade, segurança de dados, flexibilidade de *layout*, integração com outro sistema de informação, captura automática de dados, assistência à pesquisa e dados atualizados (LEÃO, 2003). O prontuário do paciente é um dos principais instrumentos utilizados nas atividades diárias de um hospital pelos profissionais da saúde. A sua proteção é de extrema relevância e, portanto, deve ser controlada e fiscalizada através de regulamentos e normas específicas definidas por entidades especializadas e independentes a fim de garantir a sua segurança. Entre as entidades de destaque neste cenário está a ANS, a qual é apresentada a seguir.

2.4.2 A Agência Nacional de Saúde Suplementar (ANS)

A Agência Nacional de Saúde Suplementar (ANS) é um órgão vinculado ao Ministério da Saúde e foi criada pela Lei 9996/2000, a qual tem como finalidade promover à defesa do interesse público na assistência suplementar de saúde, regular as instituições deste setor, inclusive quanto às suas relações com prestadores e consumidores, e contribuir para o desenvolvimento das ações de saúde no Brasil.

O mercado de saúde suplementar no Brasil compreende 2.200 operadoras privadas de planos de saúde trabalhando para mais 38 milhões de beneficiários, mobilizando mais de 25 bilhões de reais em 2003, milhares de

prestadores de serviços e centenas de milhares de profissionais de saúde (BRASIL, 2007).

A saúde assistencial compreende todas as ações necessárias à prevenção da doença, à recuperação, à manutenção e à reabilitação da saúde, observados os termos da Lei. A regulamentação sobre saúde é bastante extensa, complexa e sofre constantes alterações e desdobramentos. É necessário ressaltar que existem regulamentações sobre o acesso e disponibilização das informações médicas no ambiente hospitalar e a transferência para e as operadoras privadas de planos de assistência à saúde através de um padrão de comunicação denominado TISS (Troca Eletrônica de Informações para a Saúde Suplementar (BRASIL, 2007).

A Lei que cria a ANS estabelece, entre as suas competências: expedir normas e padrões para o envio de informações de natureza econômico-financeira; proceder à integração de informações com os bancos de dados do Sistema Único de Saúde (SUS); monitorar a evolução dos preços de planos de assistência à saúde, seus prestadores de serviços (onde estão inseridos os hospitais), e respectivos componentes e insumos; requisitar o fornecimento de informações às operadoras de planos privados de assistência à saúde, bem como da rede hospitalar e aos demais prestadores de serviços médicos; articular-se com os órgãos de defesa do consumidor visando a eficácia da proteção e defesa do consumidor de serviços assistência à saúde.

A Lei nº 8.078/90 define que recusa, omissão, falsidade ou retardamento injustificado de informações ou documentos solicitados pela ANS constitui infração punível com multa diária para garantir a sua eficácia (LIMA, 2005). Além desta, a ANS aprovou uma resolução que cria normas

para o fornecimento de informações dos pacientes dos hospitais e beneficiários das operadoras privadas de planos de assistência suplementar à saúde. A resolução determina que os dados cadastrais dos beneficiários das operadoras devem ser feitos através de arquivo magnético para o departamento de informática do Ministério da Saúde. Entretanto, nenhum dispositivo legal referente a segurança destas informações é mencionada (BRASIL, 2007).

Através do cruzamento destas informações do Ministério da Saúde (MS) é possível identificar os atendimentos realizados pelos hospitais que podem gerar diversos benefícios ao controle de saúde no país. O cadastro de pacientes e atendimentos realizados possibilita, por exemplo, estudos de demografia com comparações das freqüências, base para estudos e pesquisas epidemiológicas, com verificação da freqüência de eventos vitais através dos sistemas de notificação de nascidos vivos, de notificação compulsória de agravos e de informações de mortalidade do Sistema Único de Saúde (SUS) (LIMA, 2005).

Entretanto, há um conflito de definições entre os diferentes órgãos reguladores do segmento de saúde. Por um lado o CFM, o qual determina normativas para a proibição aos médicos da divulgação e disponibilização das informações relativas ao ato médico; por outro lado a ANS e o MS, que determinam a prestação de informações dos pacientes. Sabe-se que a fonte de informação, neste contexto, é oriunda dos médicos e dos pacientes. Esta questão gera uma grande discussão no setor de saúde no Brasil em relação ao fornecimento e proteção das informações o qual ainda não encontra uma solução definitiva.

Buscando minimizar esta questão, uma resolução da ANS estabelece que as informações médicas relativas à assistência prestada aos pacientes e das instituições hospitalares deve ficar sob a responsabilidade de um profissional médico dentro das instituições hospitalares e dentro das operadoras de planos de saúde. Estas regras foram definidas na Lei nº 9.656/98, com a finalidade de preservar o sigilo da informação dos indivíduos (ANS, 2007). O profissional responsável pela segurança dessas informações é denominado Coordenador Médico de Informações em Saúde. A resolução adverte que, resguardando as prerrogativas e obrigações profissionais do Coordenador Médico de Informações em Saúde com relação ao sigilo médico, as entidades permanecem responsáveis pelo envio das informações relativas aos beneficiários de planos de assistência à saúde respondendo pela omissão ou incorreção dos dados (LIMA, 2005).

Outra resolução importante é a RN nº 88, que atualiza o Sistema de Informações de Beneficiários (SIB) e define normas para o envio de informações dos indivíduos à ANS. Esta resolução estabelece a sistemática de geração, transmissão e de controle da segurança das informações da totalidade dos beneficiários existentes na carteira das operadoras de planos privados de assistência à saúde. A proposta desta normativa tem o objetivo de estabelecer um padrão essencial obrigatório para as informações trocadas entre operadoras e prestadores de serviços de saúde, definindo inclusive alguns mecanismos de Segurança da Informação, denominado TISS (ANS, 2007).

A ANS reconhece o estabelecimento de um padrão essencial de troca e Segurança da Informação como necessário para o aprimoramento da qualidade da prestação da assistência, para o aperfeiçoamento das informações sobre o

setor e para a otimização dos recursos utilizados na troca de informações entre operadoras e prestadores, incluindo-se as instituições hospitalares. Entretanto, são iniciativas válidas para um setor que carece de regulamentações sobre a Segurança da Informação e que necessita encontrar um alinhamento entre os diversos órgãos reguladores e as instituições de saúde no Brasil.

2.4.3 A Informação e as Instituições Hospitalares

Desde o ano de 2003, o governo brasileiro através do MS lançou um programa para discutir com a sociedade uma Política Nacional de Informação e Informática em Saúde (PNIIS), que preconiza a adoção de normas e padrões para a gestão da informação em instituições de saúde, onde estão inseridos os hospitais brasileiros (BRASIL, 2004). Ela sugere a adoção do Prontuário Eletrônico do Paciente (PEP) como módulo básico de coleta e armazenamento de informações. A Proposta é a interligação destes sistemas em todo o Brasil, formando assim um Sistema Único de Informação em Saúde, o qual permitiria o conhecimento da realidade da Saúde no país, a gestão das informações com qualidade e segurança e, com isso, a formulação de gestão de saúde mais condizentes (LIMA, 2007).

A formulação da PNIIS faz parte das diretrizes do Ministério da Saúde (MS), que busca integrar o Brasil ao contexto internacional, onde políticas e estratégias setoriais em comunicação e informação em saúde estão tornando-se prioridade. O foco dessa política está no uso e na disseminação da Tecnologia da Informação entre os profissionais de saúde, visando à interoperabilidade dos sistemas, o que consiste na compatibilização, interface

e modernização dos sistemas de informação e da criação de uma Política Nacional de Segurança da Informação para a Saúde (CUNHA e MENDES, 2004).

Os sistemas de informação dos hospitais brasileiros são estruturados para atender às necessidades de gestão ou geração de informações dos pacientes e doenças relacionadas para estatísticas dos órgãos competentes do Governo, as quais propõem iniciativas fragmentadas e que não aperfeiçoam ações concretas para uma gestão de saúde. Apesar de esses sistemas terem seu significado, na prática ainda não responde às demandas dos profissionais das áreas hospitalares e profissionais da área de TI (LEÃO, 2003).

Outro ponto importante é que existem diversas soluções tecnológicas implementadas nas instituições hospitalares o qual resulta num conjunto de informações distribuídas em diversas áreas e aplicativos que não integram os dados entre os diferentes serviços hospitalares e nem alimentam automaticamente os sistemas de informação internos. Destacam-se as informações em equipamentos e dispositivos eletrônicos de diagnose, análise e monitoramento, com diferentes níveis de complexidade e tecnologias embarcadas e que expõe a fragilidade dentro de um hospital. (CUNHA e MENDES, 2004).

Os desafios são constantes, para a identificação, integração, armazenamento e disponibilização das informações hospitalares, o que significa definir como efetivar a operabilidade entre os diversos sistemas, com segurança (LEÃO, 2003).

Uma das ações adotadas é a padronização do registro eletrônico dos prontuários e a integração e centralização do registro dos eventos dos

pacientes, seja esses individuais ou coletivos, além da capacitação e conscientização permanente de trabalhadores, gestores e prestadores de serviços hospitalares. O objetivo maior dessa ação é a melhoria da qualidade e a eficiência dos processos hospitalares, uma vez que as informações dos prontuários serão alimentadas automaticamente, o que eliminará instrumentos paralelos de coleta, otimizando a ação dos profissionais que realizam esses serviços dentro dos hospitais. Neste contexto, o fator humano é crucial para a Segurança da Informação. A inexistência de políticas e normas internas nos hospitais que direcionem os esforços neste sentido torna-se um fator crítico. Como visto anteriormente, cabe aos Coordenadores Médicos de Informações em Saúde exigirem da gestão da instituição hospitalar e da área de TI dos hospitais, regras e controles que garantam a Segurança da Informação.

Neste sentido, um conjunto de diretrizes está sendo proposta, através do PNIIS. Segundo BRASIL (2004), estas diretrizes contemplam:

- Organizar e desenvolver as áreas de Informação e Informática, articulando a integração dos diferentes sistemas informatizados, capacitando as categorias de profissionais da saúde e dotando os ambientes organizacionais hospitalares nas premissas de uma padronização informacional;
- Reforçar a democratização da informação e da comunicação em todos os aspectos no ambiente (focando a disseminação da informação);
- Definir recursos, fontes de financiamento, prazos, cronogramas e critérios para a implantação do Cartão Nacional de Saúde em todo o país, por meio do amplo debate com gestores e incluindo

os pré-requisitos de informatização e infra-estrutura tecnológica, capacitação de gestores e profissionais de saúde e implantação da rede de informações (promovendo o uso de produtos e serviços de informação);

- Fomentar investimentos em telecomunicações, viabilizando a interoperabilidade entre os serviços de saúde e as instâncias governamentais (viabilizando investimentos em serviços de informação);
- Estabelecer os registros únicos de saúde do indivíduo, possibilitando que esses registros sejam disponibilizados aos profissionais de assistência em qualquer lugar que esse indivíduo procure o acolhimento assistencial (organizando, armazenando e disseminando informação);
- Padronizar a representação da informação em saúde (vocabulários, conteúdos e formatos de mensagens) por meio de um processo participativo, a fim de garantir o intercâmbio entre os sistemas de informação (classificando/organizando a informação);
- Dotar o segmento de saúde de instrumentos jurídicos, normativos e organizacionais, com a finalidade de assegurar a confidencialidade, a privacidade e a disponibilidade dos dados e das informações em saúde, garantindo a sua autenticidade e integridade, por meio de certificação digital (promovendo a adoção de padrões de Segurança da Informação).

A elaboração de um prontuário eletrônico único implica a adoção de padrões na representação da informação (vocabulário), dos meios de armazenamento (*hardwares* e *softwares*), bem como ao que se refere às telecomunicações (transmissão e acesso) e padrões de Segurança da Informação em saúde, os quais deverão ser adotados pelas instituições hospitalares. O uso de padrões viabiliza a troca de dados e de textos livres, possibilitando a automação de processos como o assistencial, administrativo, de pesquisa, ensino e da gestão de um sistema de saúde (LEÃO, 2003).

Essas abordagens apontam novos horizontes aos hospitais e, por conseguinte, a toda a rede de saúde, caso efetivem o uso de informação como base de suas atividades. Nessa lógica, a organização hospitalar passará a ter maior ênfase como recurso estratégico a informação. A adoção dos processos de gestão da informação e de diretrizes de segurança é essencial para que a informação propicie os resultados na qualidade dos serviços hospitalares almejados pela sociedade. Todavia, são iniciativas válidas, mas ainda sem um caráter concreto para a solução de um tema importante quanto a Segurança da Informação hospitalar.

3 MÉTODO

O método de pesquisa descreve os procedimentos necessários para a realização deste trabalho e apresenta as etapas de execução. Esta seção foi estruturada através da definição do método de investigação, da estratégia de pesquisa, do desenho de pesquisa, da coleta dos dados, da elaboração do instrumento proposto e da forma de avaliação do instrumento e do pré-teste, descritas a seguir.

3.1 MÉTODO DE INVESTIGAÇÃO

O método de investigação constitui o caminho lógico entre os dados a serem coletados e as conclusões de um estudo (YIN, 2005). Segundo Cooper e Schindler (2003), cada pesquisa possui uma natureza que conduz seus procedimentos racionais e sistemáticos buscando propiciar as respostas aos problemas que são propostos.

Uma pesquisa pode ser de natureza exploratória, descritiva, causal ou explicativa (MALHOTRA, 2001). Enquanto a pesquisa descritiva procura observar, registrar, analisar, classificar e interpretar os fatos ou fenômenos, sem que o pesquisador interfira no fenômeno ou os manipule, a pesquisa explicativa, além de registrar, analisar e interpretar os fenômenos estudados tem como preocupação primordial identificar fatores que determinam ou que

contribuem para a ocorrência dos fenômenos, isto é, suas causas (FACHIN, 2002). Além destas, a pesquisa causal busca determinar as relações de causa e efeito de um fenômeno com a finalidade de compreender quais as variáveis é a causa (variáveis independentes) e quais são os efeitos (variáveis dependentes) e a sua correlação (MALHOTRA, 2001). Os métodos de pesquisa acima descritos não enquadram-se dentre os quais permitem explorar o assunto de maturidade em segurança da informação.

A pesquisa exploratória caracteriza-se por ser "a estratégia de pesquisa que visa prover o pesquisador de um maior conhecimento sobre o tema ou problema de pesquisa em perspectiva" (MATTAR, 1997, p.23). Face ao objetivo desta pesquisa, a natureza exploratória foi adotada para esta pesquisa uma vez que a compreensão dos assuntos Segurança da Informação, avaliação da maturidade de processos e as características da informação hospitalar, são poucos ou inexistentes por parte do pesquisador.

Dentre as diferentes estratégias possíveis, uma pesquisa exploratória pode ser realizada por métodos característicos, onde se destacam a pesquisa-ação, estudo etnográfico ou pelo estudo de caso (YIN, 2005).

A pesquisa-ação é uma estratégia que aproveita os sentidos de percepção, análise e explicação do pesquisador que tem convívio constante com a prática e, a partir desta vivência, poderá criar inferências teóricas sobre o fato estudado (MALHOTRA, 2001). O estudo etnográfico envolve um longo período de estudo onde o pesquisador fixa residência em uma comunidade e passa a usar a técnica de observação, tendo contato direto e participando das atividades da comunidade (FACHIN, 2002; YIN, 2005).

O estudo de caso é caracterizado como um estudo intensivo, onde são considerados, principalmente, os assuntos a serem investigados, sendo um estudo limitado a poucas unidades, caracterizando-se como uma pesquisa detalhista e profunda (MAANEN, 1979). O estudo de caso representa "uma maneira de se investigar um tópico empírico seguindo-se um conjunto de procedimentos pré-estabelecidos" (YIN, 2005, p.5). Evidencia-se ainda mais o uso do estudo de caso, quando a estratégia de pesquisa contempla questões do tipo "como" e "por que" (YIN, 2005).

Complementando, o estudo de caso é uma forma de pesquisa que busca examinar um fenômeno contemporâneo dentro de seu contexto (MALHOTRA, 2001). Assim, a escolha pelo estudo de caso nesta pesquisa deve-se ao fato de que o objetivo desta pesquisa é a proposição de um instrumento e para tanto a questão "como" é latente, sendo a Segurança da Informação um assunto atual e presente na realidade das organizações.

Como pressuposto, a definição da unidade de análise é primordial para a correta coleta de dados. A unidade de análise relaciona-se com o problema fundamental da pesquisa, ou seja, o "caso". Segundo Yin (2005), o "caso" pode ser algum evento ou entidade que é definida como unidade em que ocorre o fato objeto da pesquisa.

A definição da unidade de análise está relacionada à maneira como os objetivos da pesquisa foram definidos ou sobre o que a pesquisa é dirigida. Corroborando com esta posição, Gil (1995) apresenta que a análise de algumas unidades de determinado universo irá possibilitar a compreensão dos mesmos ou irá estabelecer uma base para um estudo posterior, mais sistêmico e preciso. Tendo em vista o objetivo propostos, a unidade de análise desta

pesquisa são os processos de Segurança da Informação das instituições hospitalares.

A unidade de análise de um estudo de caso pode ser única, múltipla ou comparativa (YIN, 2005; FACHIN, 2002). O estudo de caso único volta-se para uma compreensão de um caso particular que contém em si mesmo o interesse da investigação. Já o estudo de caso comparativo caracteriza-se por fornecer a introspecção sobre um assunto, esclarecer uma teoria, proporcionar conhecimento sobre algo que não é exclusivamente o caso em si, ou seja, o estudo do caso funciona como um instrumento para compreender outros fenômenos.

Por fim, o estudo de caso múltiplo contempla vários casos aplicados a um único critério de pesquisa, possibilitando, pela comparação, um conhecimento mais profundo sobre o fenômeno, população ou condição (MATTAR, 1997). O objeto do estudo de caso é a unidade de análise. No entender de Godoy (1995, p.25), “o estudo de caso visa ao exame detalhado de um ambiente, de um sujeito ou de uma situação em particular”.

A abordagem dita única é indicada diante da pesquisa de casos únicos, extremos ou revelatórios (YIN, 1984). O foco deste estudo claramente não se enquadra nessa descrição, uma vez que há grande quantidade de instituições hospitalares com interesse pelo enfoque da Segurança da Informação, não se evidencia a existência de um caso extremo e tampouco não se configura como revelatório devido à literatura presente, apesar de escassa.

Neste contexto, o estudo de caso múltiplo permite um maior entendimento do tema desta pesquisa a qual aponta para uma variedade de processos de gestão da Segurança da Informação. A quantidade e a definição

das instituições hospitalares que fizeram parte da pesquisa deram-se em virtude da representatividade no seu segmento, pelo seu porte mensurado através do número de leitos superior a 100, expressão no contexto nacional e pelo interesse destas instituições no foco da pesquisa, além das dificuldades em obter maior número de hospitais que forneçam informações pertinentes sobre o tema Segurança da Informação para pesquisas acadêmicas.

Sendo assim, foram selecionadas 3 instituições hospitalares para a avaliação do instrumento proposto e 1 hospital como caso piloto para a avaliação da maturidade dos processos de Segurança da Informação.

Cada pesquisa possui uma abordagem distinta que pode ser qualitativa, quantitativa ou ambas (GODOY, 1995). Enquanto as pesquisas quantitativas geralmente procuram seguir com rigor um plano previamente estabelecido e baseado em hipóteses claramente indicadas e variáveis que são objeto de definição operacional, a pesquisa qualitativa é direcionada ao entendimento de uma situação específica e da forma que ela ocorre. Além disso, as pesquisas qualitativas não buscam enumerar ou medir eventos e, geralmente, não emprega instrumental estatístico para análise dos dados, pois seu foco de interesse é o entendimento aprofundado de um fato (YIN, 2005). Este método de investigação de pesquisa é apropriado quando trata de melhorar a efetividade de um processo.

No método de pesquisa qualitativo deve-se direcionar uma quantidade de pessoas específicas e participantes de um grupo que estejam associadas às atividades em questão. Nas pesquisas quantitativas, os participantes podem ou não estar associados diretamente com a atividade em questão (YIN, 2005).

Nas pesquisas qualitativas é freqüente que o pesquisador procure entender os fenômenos, segundo a perspectiva dos participantes da situação estudada e, a partir daí, situe sua interpretação (YIN, 2005). A pesquisa qualitativa pode considerar um conjunto de diferentes técnicas interpretativas que visam a descrever e decodificar os componentes de um tema complexo com quantidade de pesquisas anteriores limitadas e com possibilidade de múltiplas interpretações, onde o assunto Segurança da Informação está inserida. Tem por objetivo traduzir e expressar o sentido dos fenômenos do mundo social e trata de reduzir a distância entre a teoria e a realidade dos dados ou entre um contexto e uma ação (MAANEN, 1979), porém, o melhor método é aquele que melhor se adequar aos objetivos de buscar respostas para uma questão de pesquisa (MIGUELES, 2003). De acordo com a natureza desta pesquisa e do objetivo proposto, o método qualitativo proporciona um entendimento mais amplo sobre o assunto Segurança da Informação e avaliação de maturidade.

3.2 ESTRATÉGIA DE PESQUISA

Além de conhecer a variedade de paradigmas e perspectivas teóricas disponíveis que embasam as investigações, é necessário conhecer as estratégias de condução e os seus delineamentos. Trata-se, portanto, do lado prático das direções teóricas contidas no estudo de caso, representado pelo seu desenho de pesquisa, o qual é apresentado na Figura 3 a seguir.

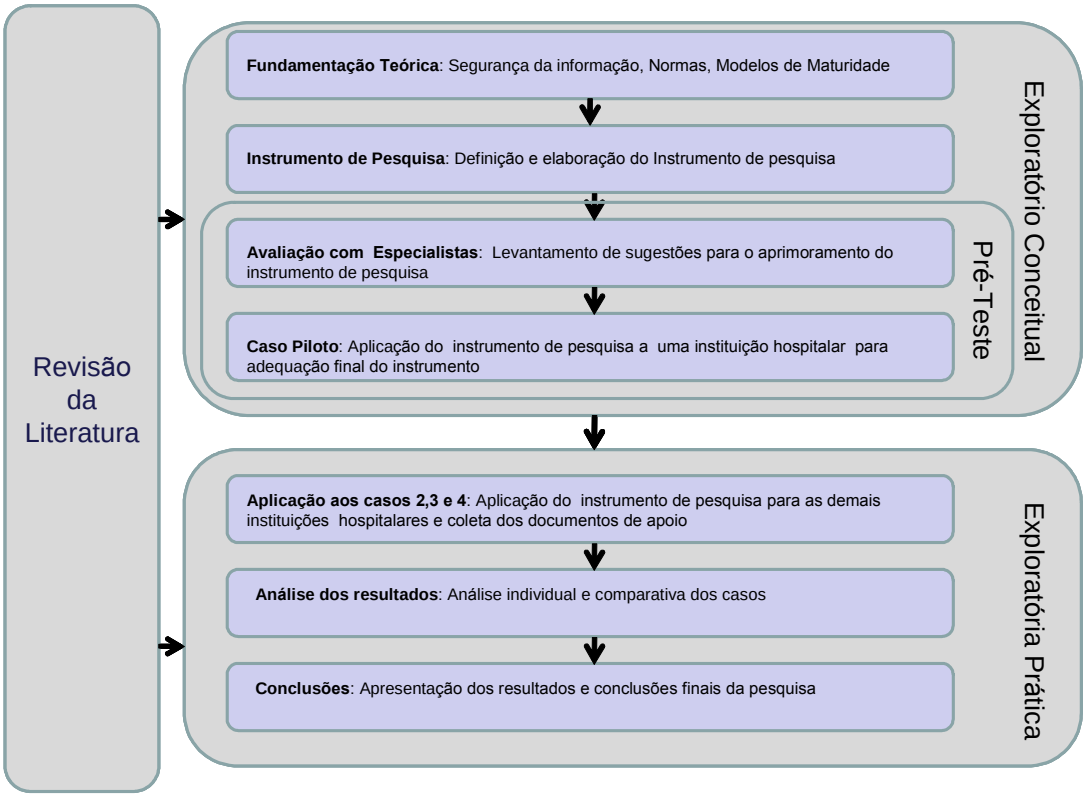

Figura 3: Desenho de Pesquisa
Fonte: Elaborado pelo Autor

Na primeira etapa da pesquisa, de cunho conceitual, foram identificados na literatura os modelos e métricas de avaliação de maturidade, normativas e regulação da Segurança da Informação, como também da situação das instituições hospitalares no contexto nacional. A revisão da literatura caracteriza-se como composição fundamental para o amadurecimento e aprofundamento do problema de pesquisa (MATTAR, 1997), sendo utilizada durante todas as fases deste estudo de caso. A base teórica sustenta o estudo de caso que, por sua vez, serve como guia de análise do conjunto de questões da pesquisa e das novas interpretações que possam surgir (YIN, 2005).

Na segunda etapa da pesquisa foi elaborada uma proposição inicial do instrumento de avaliação da maturidade em Segurança da Informação, composto pelas dimensões, questões de avaliação e níveis de maturidade sugeridos pela literatura, especialmente com base no modelo normativo ISO/IEC 27001.

Segundo Bardin (1977), a escolha do tipo de pergunta é essencial tanto para a estruturação lógica do instrumento quanto para o custo de resposta exigido dos sujeitos. As perguntas abertas são essenciais numa pesquisa exploratória quando se quer verificar a abrangência das respostas, apesar de exigirem maior esforço, alto custo do respondente, principalmente em questionários auto-aplicados, o que pode diminuir a probabilidade do respondente completar a tarefa.

As perguntas fechadas, por sua vez, são indicadas para investigar temas mais pesquisados e também conhecidos pelos sujeitos, principalmente quando os respondentes são muitos e dispõe-se de pouco tempo (FOWLER, 1998). O desafio era de elaborar um instrumento de avaliação capaz de captar as respostas mais adequadas ou convenientes para a avaliação da maturidade dos processos. Neste contexto, o instrumento proposto foi estruturado com questões fechadas, de escolha única e independente, sem correlação entre os itens de avaliação. Entretanto, o roteiro das entrevistas foi elaborado através de um questionário com questões abertas, objetivando captar a abrangência da percepção na avaliação dos respondentes.

Quanto mais ajustado à realidade, mais o instrumento é capaz de relatar com precisão as melhores respostas. Assim, o problema de elaborar um bom instrumento de avaliação se transfere para a busca de um melhor

conhecimento do universo de respostas, que no caso desta pesquisa foi baseada em uma ampla revisão de literatura (GUNTHER, 1999).

Na terceira etapa da pesquisa, foram efetuados os pré-testes com especialistas em Segurança da Informação e com um gestor de TI de um hospital piloto. O objetivo desta fase foi de capacitar o pesquisador para a execução das entrevistas, revisando a estrutura e o conteúdo do instrumento proposto, verificando a quantidade de questões, a coerência e relevância das perguntas, a facilidade de resposta e seu conteúdo relacionado ao assunto da pesquisa (COOLICAN, 1999). Assim, o conteúdo das questões foi avaliado pelos especialistas para verificar se a pergunta deveria ser feita, se o escopo era apropriado, se o respondente poderia e se iria responder adequadamente e se o vocabulário está adaptado a realidade dos hospitais.

Para auxiliar na condução das entrevistas, foi elaborado um questionário semi-estruturado contendo um roteiro de perguntas buscando otimizar a condução das entrevistas e análise posterior dos resultados. Este questionário foi utilizado tanto na fase de pré-teste quanto na condução dos estudos de casos. Segundo Coolican (1999) e Günther (1999) um bom questionário é aquele formado por itens que possibilita ao sujeito compreendê-lo em vários aspectos relevantes (conceito, linguagem e expectativa de resposta) para que o respondente possa preenchê-lo com disposição e veracidade, evitando aqueles que possibilitem interpretações com viés ou ambigüidade. Desta forma, cada item deve ser específico, breve, claro, objetivo e redigido com vocabulário correto, preciso, apropriado a pesquisa (termos técnicos).

Segundo Cooper e Schindler (2003) um pré-teste pode ocorrer de duas formas:

a) pré-teste do pesquisador: onde o pré-teste acontece de maneira informal e se busca obter sugestões de melhoria;

b) pré-teste do respondente: onde o instrumento é testado por respondentes substitutos, ou seja, pessoas como o mesmo perfil dos respondentes finais.

O pré-teste do pesquisador foi aplicado à quatro especialistas no tema Segurança da Informação, selecionados pela suas experiências no assunto e formação acadêmica. “A partir de um problema de pesquisa, obter outras interpretações e avaliações, constitui-se de grande utilidade no fornecimento de informações práticas na condução e de teorias de suporte de uma pesquisa específica” (BARDIN, 1977, p. 45).

A seguir, foi efetuado um pré-teste de respondente, através de um caso piloto em uma instituição hospitalar selecionada por conveniência e manifestação tácita desta instituição em participar como caso piloto.

Por fim, foi efetuada a pesquisa exploratória, com a aplicação do instrumento proposto às instituições hospitalares e a avaliação por parte dos entrevistados quanto a sua percepção do instrumento proposto.

A pesquisa exploratória, da maneira proposta nesta pesquisa, apóia-se em princípios difundidos, como o fato de que “a teorização deve estar alinhada com a prática, deve-se buscar sempre ampliar o conhecimento e esperar respostas racionais pressupõe formulação de perguntas também racionais, através de perguntas congruentes com o conhecimento estruturado” (BRADLEY, 1993, p. 72). Segundo esse entendimento, se coadunarem com a

estruturação dos conhecimentos contidos na forma de questões estruturadas, as respostas estarão em conformidade com a "realidade" (BABBIE, 1986).

As entrevistas são consideradas uma das mais importantes fontes de informações para um estudo de caso; outro ponto importante caracteriza-se por apresentar ao entrevistado a relevância da pesquisa, uma vez que as respostas obtidas poderão afetar a qualidade dos dados (BRADLEY, 1993). Esta qualidade dos dados está intimamente relacionada à forma que os mesmos são coletados, a qual é exposta a seguir.

3.3 COLETA E ANÁLISE DE DADOS

A coleta de dados é a etapa da pesquisa que fornece os subsídios para uma correta análise e a elaboração das conclusões, visando atingir o objetivo proposto. Existem diferentes formas de coletar os dados para um estudo de caso. A coleta dos dados é composta por métodos e procedimentos claros e adaptados para cada caso específico, onde a preparação pode ser uma atividade complexa e difícil. Por isso, a habilidade do pesquisador é primordial (YIN, 2005).

As entrevistas foram conduzidas aos gestores responsáveis pela Segurança da Informação nas instituições hospitalares foram realizadas no mês de novembro de 2007 nos próprios hospitais de forma individual para não haver influência entre as respostas.

Os entrevistados da pesquisa foram os responsáveis pela Segurança da Informação de cada instituição, totalizando três profissionais. O perfil dos entrevistados está relacionado ao conhecimento tecnológico em Segurança da

Informação e sobre a temática da pesquisa, além da importância que a Segurança da Informação representa para a sua atividade profissional dentro das suas instituições.

A análise dos dados levantados foi realizada com base nos procedimentos de análise de conteúdo e proposições teóricas, buscando-se conceituar, codificar e interpretar os conteúdos obtidos através das pesquisas resultantes da etapa de execução (BARDIN, 1977). “A análise dos dados consiste em examinar, categorizar, classificar em Tabelas, ou, do contrário, recombinar as evidências tendo em vista proposições iniciais de um estudo" (YIN, 2005, p.31).

A estratégia de análise baseada em proposições teóricas, que refletem um conjunto de questões realizadas através das revisões feitas na literatura sobre o assunto de pesquisa (BARDIN, 1977). Neste caso, compreende-se que estas propostas de preposições teóricas tornam-se guias na evolução desta pesquisa.

As análises das informações das entrevistas foram realizadas confrontando os objetivos da pesquisa, o conteúdo das respostas e a convergência com o referencial teórico. Inicialmente foram transcritas as gravações das entrevistas e analisados os resultados das respostas dos questionários semi-estruturados. Para apoiar a análise das respostas foram levantadas evidências dos meios adotados de gestão da Segurança da Informação pelas respostas fornecidas no instrumento de avaliação de maturidade proposto. Os dados e apontamentos foram relacionados com as propostas mencionadas pelos autores da fundamentação teórica, buscando uma interpretação substancial dos mesmos. Ao final, foram elaboradas inferências

com base na interpretação dos resultados e relacionando-se aos objetivos propostos pelo estudo. Estas inferências também foram apoiadas por referencial teórico e tomaram como base a relação entre as avaliações e a estrutura do instrumento proposto (BARDIN, 1977), o qual é descrito a seguir.

3.4 ELABORAÇÃO DO INSTRUMENTO PROPOSTO

A elaboração do instrumento proposto foi realizada contemplando as diferentes dimensões de avaliação da normativa ISO/IEC 27001, consolidados por adaptação e complementação, garantindo questões pertinentes aos objetivos da pesquisa. Como primeira definição, a norma ISO/IEC 27001 foi considerada como base estrutural do instrumento proposto por possuir dimensões de avaliação que são estruturados em diferentes perspectivas sobre o tema Segurança da Informação e que permite uma adaptação às particularidades das instituições hospitalares. Além deste fato, a norma ISO/IEC 27001 é um instrumento atualizado frente as inovações tecnológicas e com um grau de completitude que possibilita a elaboração de um instrumento de avaliação de processos adequado aos objetivos da pesquisa. Os demais modelos e normas encontrados na revisão da literatura, ou possuem uma visão específica de algum ponto do tema Segurança da Informação, ou o assunto Segurança da Informação é tratado superficialmente, como um sub-item em outra norma mais ampla.

Como visto na revisão de literatura, a norma possui 133 itens de verificação distribuídos em 39 categorias e 11 dimensões estruturais.

Inicialmente o pesquisador analisou a possibilidade de criar um instrumento mais amplo, contendo um item de avaliação de maturidade para cada um dos 133 itens de avaliação de processos. Entretanto, considerando o escasso tempo dos respondentes, além desta pesquisa possuir um cunho exploratório, optou-se pela elaboração do instrumento proposto baseado nas 39 categorias e nas 11 dimensões de análise para uma proposição inicial do instrumento. Esta decisão pretendeu evitar viés em sua aplicabilidade. Entretanto, uma das categorias da norma exigiu a abertura em dois itens, a fim de cobrir itens de avaliação de maturidade de processos significativos para as instituições hospitalares. As 11 dimensões permaneceram como elenco agrupador dos itens do instrumento, sendo utilizadas também nas análises dos resultados. O instrumento proposto de pesquisa encontra-se no Apêndice A.

Como base para a estruturação, o instrumento foi elaborado a partir dos 3 tipos de mensuração citados por Schindler e Cooper (2003), os quais são também utilizados como alicerce para instrumentos gerais de pesquisas nas áreas sociais. Segundo os autores, os instrumentos devem considerar os seguintes pontos de mensuração: (i) gerencial, (ii) de classificação e (iii) de direcionamento. A estrutura do instrumento em relação ao tipo de mensuração é apresentada na Tabela 04 de tipos de mensuração para o instrumento proposto.

Mensuração gerencial	
Objetivos	identificar o respondente, o local e as condições da entrevista e traçar o perfil da organização, procurando minimizar possíveis fontes de erro e promover uma aproximação entre o pesquisador e a unidade de análise
Número de questões	5 questões
Tipo de questões	Abertas
Forma de mensuração	Descritiva
Mensuração de classificação	
Objetivo	identificar a forma de controle relativos a Segurança da Informação
Número de questões	40 questões
Tipo de questões	Fechadas
Forma de mensuração	qualitativa
Mensuração de direcionamento	
Objetivo	investigar a forma de controle: aplica-se apenas para os níveis de maturidade Gerenciado e Otimizado, pela identificação dos controles aplicados
Número de questões	uma para cada item de controle
Tipos de questões	Abertas
Forma de mensuração	Descritiva

Tabela 04: Tipos de Mensuração do Instrumento Proposto
Fonte: Elaborado pelo Autor

Seguindo as recomendações de Cooper e Schindler (2003), a elaboração do instrumento buscou utilizar um vocabulário comum, com significado único, alternativas adequadas, evitando suposições enganosas e redação com viés.

Não há correlação direta ou dependência entre cada uma das questões, ou seja, cada item de controle pode estar em um nível de maturidade distinto do outro. A análise do resultado é independente por item, como a estruturação da ISO/IEC 27001. O objetivo do agrupamento em dimensões de análise é de proporcionar maior facilidade na interpretação e comparação dos resultados das entrevistas. Conforme ISO/IEC 27001 (2007), cada dimensão da ISO/IEC 27001 possui um determinado objetivo, como segue:

D1 – Política de Segurança: Avalia se o hospital possui uma política organizacional para a Segurança da Informação, formal e conhecida pelos seus colaboradores diretos e indiretos;

D2 –Organizacional: Avalia as responsabilidades e comprometimento dos colaboradores e terceiros com a Segurança da Informação hospitalar,

verificando as autorizações e relacionamentos pela manipulação das informações;

D3 – Ativos: Avalia a identificação e o controle da utilização dos ativos computacionais e equipamentos de geração, armazenamento e transmissão da informação;

D4 – Recursos Humanos: Avalia os aspectos humanos relativos à proteção da informação, incluindo a admissão, responsabilização e rescisão de contratos de trabalho;

D5 – Segurança Física: Avalia o acesso às áreas físicas e instalações hospitalares e a segurança dos equipamentos de geração e armazenamento de informações;

D6 – Procedimentos e Responsabilidades: Avalia os procedimentos operacionais e a responsabilidade na geração, armazenamento, transmissão e disponibilização de informações hospitalares, segregação das funções e administração dos papéis e funções dos envolvidos;

D7 – Controle de Acesso: Avalia as questões pertinentes com o acesso à informação, gerenciamento dos acessos aos diferentes ambientes e tecnologias do ambiente hospitalar;

D8 – Exigências de Segurança: Avalia a validação dos dados de entrada, segurança das bases de dados e arquivamento, segurança dos processos de desenvolvimento e vulnerabilidade técnica de TI;

D9 – Comunicação: avalia os processos de comunicação de eventos de quebra de segurança e as respectivas responsabilizações;

D10 – Continuidade: Avalia os processos relativos aos impactos da segurança e da sua relação com a continuidade empresarial, através da existência de planos e responsabilidades;

D11 – Alinhamento: Avalia o alinhamento dos processos de segurança com os requisitos legais e com os processos de auditoria.

Para compor os níveis de maturidade dos processos foram analisados e compilados os modelos de maturidade resultantes da revisão de literatura. Os níveis de maturidade são utilizados no instrumento proposto para avaliar a situação em que encontra-se a Segurança da Informação. A idéia principal da grade de maturidade é descrever em uma frase, o comportamento típico exibido por uma instituição entre os vários níveis de maturidade, para cada um dos itens de avaliação. Nesta pesquisa optou-se por adotar 5 níveis de maturidade, conforme (CROSBY, 1999). Isto permite classificar o que está adequado, o que está inadequado e ainda aqueles pontos que encontram-se em um estágio intermediário ou em transição, conforme descritos a seguir:

N1 – Inexistente: Não existe nenhum processo relativo ao item;

N2 – Informal : Existe um processo dentro do hospital, porém não existe a formalização do processo, porém os envolvidos demonstram conhecer o processo;

N3 – Organizado: Existe a formalização do processo e este é conhecido e disponibilizado a todos os envolvidos no processo;

N4 – Gerenciado: Existe um processo formal e conhecido por todos os envolvidos. Além disso, o processo é controlado por indicadores de avaliação;

N5 – Otimizado: Existe um processo formal e com indicadores de acompanhamento. Além disso, o processo é submetido periodicamente à reavaliação para melhoria contínua;

Os níveis N4 (Gerenciado) e N5 (Otimizado) do instrumento apresentam um alto grau de maturidade e, portanto, foi incluído no instrumento um elemento não-estruturado explicativo para justificar e detalhar a forma de controle dos indicadores. Os aspectos e as características relativas ao segmento hospitalar foram extraídos da revisão de literatura e adaptados no instrumento, buscando maior enfoque a realidade do segmento. Na Tabela 5 estão descritos os principais referenciais teóricos avaliados e considerados na estruturação do instrumento proposto.

REFERENCIAL CONSIDERADO PARA ELABORAÇÃO DO INSTRUMENTO PROPOSTO	
Estrutura do Instrumento	**Referencial Teórico**
Dimensões de Análise	CALDER &WATKINS, 2003; ISO/IEC 27001, 2007;
Questões de Análise	CALDER &WATKINS, 2003; ISO/IEC 27001, 2007; MOREIRA, 2001; RAMAKRISHNAN, 2004. SEMOLA, 2003;
Níveis de Maturidade	CHEW et.al., 2006; NIST, 2006; PÁDUA, 2006; PAPP, 1998;
Particularidades da Informação Hospitalar	LEÃO, 2003; MANDL e KOHANE, 1999; MEUS, 2006; MINOTTO, 2002; SBIS, 2006.

Tabela 5: Referencial de considerações avaliado para a elaboração do instrumento proposto
Fonte: Elaborado pelo autor

Para apoiar às entrevistas de avaliação do instrumento proposto foi elaborado um questionário de avaliação descrito a seguir.

3.5 QUESTIONÁRIO DE AVALIAÇÃO DO INSTRUMENTO

Para a condução das entrevistas de avaliação do instrumento proposto foi elaborado um questionário semi-estruturado, o qual consta no Apêndice B deste trabalho, composto por questões abertas e com base nas quatro categorias propostas por Günter (1999) para avaliação de instrumentos de pesquisa: (i) a aplicabilidade do instrumento, (ii) a sua estrutura lógica, (iii) a clareza das perguntas e (iv) a aderência aos objetivos propostos, conforme resumido na Tabela 5.

Segundo Günther (1999), uma estrutura bem elaborada contribui significativamente para reduzir o esforço físico e mental do respondente, além de assegurar que todos os temas de interesse do pesquisador sejam tratados numa ordem que sugira uma 'conversa com objetivo', mantendo o interesse do respondente em continuar. "Pode-se definir uma boa questão como aquela que gera respostas fidedignas e válidas. Apresenta cinco características básicas: (a) a pergunta precisa ser compreendida consistentemente; (b) a pergunta precisa ser comunicada consistentemente; (c) as expectativas quanto à resposta adequada precisam ser claras para o respondente; (d) a menos que se esteja verificando conhecimento, os respondentes devem ter toda informação necessária; e (e) os respondentes precisam estar dispostos a responder. Para assegurar tais atributos, cada pergunta deve ser específica, breve, clara, além de escrita em vocabulário apropriado e correto" (GUNTHER apud. FOWLER, 1999, p.15)

É importante focalizar-se nos objetivos do questionário e no conteúdo das perguntas que o pesquisador busca respostas, sabendo claramente por que está incluindo cada item no questionário. No pré-teste é relevante haver a

possibilidade de ajustes no questionário, isto é, para incluir, excluir ou alterar itens sobre os quais o pesquisador não tem certeza se estão adequados (Günther, 1999).

CATEGORIAS	OBJETIVO	QUESTÕES
1. Dados de Identificação	Identificar o respondente, seu perfil e características relevantes à pesquisa.	Nome Tempo de experiência na área de TI Idade Tempo na função no hospital
1. Aplicabilidade	Identificar se o instrumento possibilitará uma aplicação prática resultando em valor ao respondente	O conteúdo está de acordo com a normativa ISO/IEC 27001? Você estima que o tempo de uma hora para o preenchimento do instrumento é adequado? Porquê? É de fácil utilização? Os níveis de maturidade propostos são adequados? Por quê?
2. Estrutura do Instrumento	Identificar se o instrumento possui uma estrutura funcional adequada	A estrutura das alternativas de respostas está clara? Por quê? A estrutura das alternativas de respostas é objetiva? Por quê? A ordem das questões é adequada? Por quê? O formato do instrumento é adequado? Por quê? O instrumento é funcional? Por quê? O Instrumento é prático? Por quê?
3. Clareza das Questões	Identificar se as perguntas estão claras e objetivas	A redação é clara? A redação é objetiva? As orientações para o preenchimento do instrumento são claras? Cite quais as perguntas que você julga serem desnecessárias e a sua justificativa.
4. Aderência aos Objetivos Propostos	Identificar se o instrumento está aderente ao que ele se propõe avaliar	Você acredita que o instrumento atenderá as expectativas? Por quê? As questões abordadas permitirão avaliar a maturidade da Segurança da Informação? De que forma? Descreva sua opinião geral sobre o instrumento, comentando críticas, impressões pessoais e sugestões de melhorias.

Tabela 6: Questões do Questionário de Entrevistas
Fonte: o autor

É importante destacar que o papel do entrevistador é fundamental para alcançar os objetivos propostos, pois o roteiro serve apenas como um guia durante uma entrevista, mas as percepções adjacentes às perguntas do questionário, por vezes revelam fatos relevantes ao contexto da pesquisa.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

A apresentação dos dados referentes aos resultados da pesquisa é dividida nas fases em que estas ocorreram. Faz-se inicialmente a apresentação dos pré-testes dos especialistas e do caso piloto, a análise dos estudos de casos e, por fim, as considerações finais sobre esta pesquisa.

Para os estudos de casos, os dados obtidos nas entrevistas são apresentados e analisados a partir das quatro categorias propostas por Günter (1999). Cada categoria é apresentada e analisada individualmente, com as falas alusivas dos respondentes visando enriquecer ou justificar os dados encontrados, permitindo assim, maior entendimento dos resultados obtidos. Para melhor compreensão, a análise é apresentada cronologicamente conforme estas ocorreram.

4.1 PRÉ-TESTE DO ESPECIALISTA E1

O primeiro especialista a avaliar o instrumento foi um Administrador de Empresas e Mestre pela Universidade Federal do Rio Grande do Sul (UFRGS). Seu trabalho de pesquisa foi relacionado a Gestão de Segurança da Informação e a implementação da norma BS7799-2:2002 em uma instituição financeira. Possui mais de 20 anos de experiência na área de TI e atualmente

é Diretor Administrativo e de Tecnologia da Informação do Banco Matone S.A.

A duração da entrevista individual foi de aproximadamente uma hora e gravada com autorização do entrevistado. Em princípio, foi apresentado o instrumento de avaliação de maturidade de Segurança da Informação inicialmente proposto, o qual continha 133 questões de avaliação.

A primeira consideração do entrevistado foi que as questões de identificação estão apropriadas e objetivas, não havendo qualquer consideração. Após, o entrevistado destacou a correta e procedente divisão do instrumento nas 11 dimensões de análise, relacionadas com a norma ISO/IEC 27001, salientando a importância da aderência a uma norma atualizada.

A seguir, o especialista avaliou a estrutura do instrumento e recomendou a redução do número de questões. Na sua percepção, um instrumento de avaliação contendo um número elevado de questões, não será prático e aplicável a qualquer organização, pelo fato de que os entrevistados não teriam disponibilidade de tempo e possibilitaria respostas evasivas ou viés. Segundo Coolican (1999), a quantidade de questões de um instrumento de pesquisa deve ser adequada ao tempo em que o respondente irá dispor e que não se torne atrativo e não cansativo, evitando respostas evasivas.

Esta consideração foi importante para a aplicabilidade prática do instrumento e continuidade na busca de resultados consistentes da pesquisa. Por proposição do entrevistado e consideração do pesquisador, as questões foram reescritas e agrupadas em 39 questões. Entretanto, uma categoria da ISO/IEC 27001 foi desmembrada em 2 questões (relativos ao alinhamento com os requisitos legais - itens 37 e 38 do instrumento), a fim de abranger pontos

relevantes para o segmento hospitalar. A final, o novo instrumento proposto possui 40 itens de verificação. Este novo instrumento foi reapresentado ao especialista E1.

A partir da readequação do instrumento, o entrevistado considerou a nova estrutura do instrumento correta e objetiva. O entrevistado expôs que a ordem das questões está em compasso com a norma, além do fato de que a ordem das questões parte de um item de controle mais elementar (como a existência de uma política de segurança), até em questões mais complexas no que tange a Segurança da Informação (como a continuidade de negócios ou o alinhamento organizacional com a segurança), conforme relato a seguir:

> "Achei muito boa a divisão do instrumento em dimensões e categorias de análise iguais as propostas pela norma 27001. As questões vão de itens de controle elementares até os mais sensíveis para a segurança, como determina a norma. Também existe um padrão o que irá permitir avaliar o estágio atual e comparar com o de outros hospitais iguais." (E1)

O tempo para resposta proposto de 1 hora, segundo opinião do entrevistado, irá depender do nível de gestão da Segurança da Informação que o hospital encontra-se, pois segundo ele, "quanto maior o nível de maturidade, maior será o tempo de resposta".

Na avaliação do especialista as questões estão claras e objetivas. O entrevistado apenas fez referência a algumas questões que foram adequadas a terminologia para o segmento hospitalar e que não são do seu conhecimento. O entrevistado sugeriu a correção da redação de duas questões, procurando deixar mais claro a questão e a definição do termo "alinhamento", sugerindo o termo "conformidade".

Quanto aos propósitos do instrumento, o entrevistado destaca que a aplicabilidade deve ser diretamente proporcional ao interesse da gestão do hospital na gestão da Segurança da Informação. Ele avalia que um bom instrumento de avaliação da maturidade dos processos de Segurança da Informação servirá para as instituições hospitalares que preocupam-se com o tema e que, por conseguinte, o nível de maturidade da maioria dos itens não deverá ser classificada como inicial.

Finalizando a entrevista, o especialista solicitou uma cópia do modelo para adaptá-lo ao segmento financeiro e utilizá-lo como guia na organização em que atua. Este fato demonstrou ao pesquisador o interesse por parte do entrevistado pelo assunto e a possibilidade do modelo ampliar o seu escopo para outros segmentos de negócio.

4.2 PRÉ-TESTE DO ESPECIALISTA E2

O segundo especialista é Bacharel em Ciência da Computação e Mestrando da Universidade Federal do Rio Grande do Sul (UFRGS), tendo como área de pesquisa a Segurança da Informação em instituições bancárias. Possui mais de 20 anos de experiência na área de TI e atualmente é exerce atividade profissional na área de Segurança da Informação no Banco Regional de Desenvolvimento do Extremo Sul.

Inicialmente foi apresentado o instrumento proposto ao entrevistado que, como o primeiro especialista, avaliou todas as questões do instrumento. Logo após foi efetuada a entrevista gravada e autorizada pelo entrevistado de forma tácita. O tempo de duração da entrevista foi de 45 minutos, um pouco menor do que o tempo do primeiro especialista. Entretanto, as suas

contribuições foram relevantes para a pesquisa e aos objetivos do trabalho, pois confirmaram algumas observações do primeiro especialista.

Na visão do entrevistado, o instrumento está corretamente estruturado, com aderência tanto com a normativa ISO/IEC 27001 quanto as especificidades para o segmento hospitalar. A avaliação do especialista nesta questão foi confirmada através dos relatados a seguir:

> "Em minha percepção, o instrumento está contemplando todos os aspectos relevantes da norma 27001. Além disso, têm uma adaptação para os hospitais que me parece estar muito bem elaborada. Desconheço em detalhe as necessidades dos hospitais, mas percebo que os itens estão adaptados e bem estruturados. A linguagem é simples e direta, não deixando dúvidas quanto a sua interpretação" (E2).

Quanto à questão sobre a facilidade na utilização do instrumento proposto, o especialista considerou ser um instrumento de fácil utilização, não tendo nenhuma ressalva ao seu formato. Quando questionado sobre a estruturação dos níveis de maturidade em cinco níveis, julgou apropriado, bastante claro e de fácil entendimento, mesmo por um profissional que não conhece o assunto, conforme relato:

> "A divisão no instrumento nestes cinco níveis de maturidade é fácil de entender por qualquer um. Dá para perceber que há um padrão de evolução e crescimento entre os níveis e de que existe uma coerência em cada nível com o que se está avaliando." (E2)

Outro aspecto importante foi a percepção de adequação das questões do instrumento ao segmento hospitalar. Na percepção do especialista, as questões estão bem transcritas para a linguagem do respondente. Isso facilita o entendimento e, conseqüentemente, reduz as chances de erro nas respostas.

Segundo Coolican (1999), as questões de um questionário estruturado deverão utilizar a terminologia que o respondente esteja habituado, a fim de evitar erros de interpretação da questão.

Na avaliação do especialista, o tempo definido de 1 hora é adequado face ao número de questões do instrumento e da complexidade das questões. Aqui cabe salientar que todos especialistas já possuem o conhecimento prévio dos itens de avaliação da norma ISO/IEC 27001 e, portanto, acreditam que seu tempo é menor ao responder o instrumento. Mesmo assim, afirma que uma hora para preenchimento por profissional da área de Segurança da Informação é adequado, conforme relatos a seguir:

> "Uma hora é tempo suficiente para respondê-lo. Ele é muito objetivo e não requer uma interpretação das questões: apenas é olhar como se encontra a segurança na empresa e responder." (E2)

Finalizando, o especialista foi unânime na sua percepção de que o instrumento atenderá as expectativas e que as questões abordadas permitirão avaliar a maturidade da Segurança da Informação das instituições hospitalares. Aqui também é importante destacar que todos os especialistas manifestaram que não são especialistas na área hospitalar, mas acreditam que o instrumento está bem elaborado.

4.3 PRÉ-TESTE DO ESPECIALISTA E3

O terceiro especialista foi é Bacharel em Ciências da Computação pela Universidade do Vale dos Sinos (UNISINOS), com mais de 20 anos na área de Tecnologia da Informação, sendo responsável pela área de infra-

estrutura e segurança da informação da YARA Brasil Fertilizantes S.A. e anteriormente desenvolveu carreira em mais de 18 anos em instituições hospitalares.

Na avaliação do especialista existe a percepção de que o instrumento está bem ordenado, cujo formato é adequado para a avaliação da maturidade em Segurança da Informação. A ordem das questões, na visão do dele, é bem estruturada, seguindo a mesma ordem em que a normativa ISO/IEC 27001 apresenta seus itens.

> "...está muito bom mesmo. Eu não me recordo de todos os itens da norma 27001 de cabeça, mas pelo que me lembro todos os itens estão sendo contemplados aqui. Além disso, pela minha experiência na área de hospitalar, o instrumento está muito bem adaptado para os hospitais, com questões atuais como a transferência de dados pelo padrão TISS e outros..." (E3)

Segundo o especialista, o agrupamento dos itens em dimensões e categorias de análise, permite uma avaliação consolidada em níveis da maturidade dos processos de Segurança da Informação. Este ponto facilita a comparação entre as organizações sem expor o nível de maturidade de um processo específico, conforme relato a seguir:

> "A estrutura do instrumento em níveis de maturidade e em itens de avaliação, consolidados por dimensões vão auxiliar certamente às organizações hospitalares na gestão da Segurança da Informação. Posso afirmar pela minha experiência que o instrumento será aplicado constantemente para verificar a evolução dentro do hospital, servindo como um guia de boas práticas, simples e direto." (E3)

Pelo seu formato simples e direto, o especialista considera que o instrumento é funcional e prático. As questões estão dispostas de forma

estrutural simples e objetiva, possibilitando o seu preenchimento sem dificuldade. Entretanto, o campo para apor a forma de controle foi questionado pelo especialista que considera desnecessário, conforme relato a seguir:

> "Não sei se os entrevistados irão preencher o campo de forma de controle. Para mim, o importante é saber o nível de maturidade dos processos em que as instituições estão, e não justificar como é feitoo controle. Acho desnecessário este campo". (E3)

4.4 PRÉ-TESTE DO ESPECIALISTA E4

O quarto especialista é Administrador de Empresas e pós-graduado em Governança e Estratégia de Tecnologia pela Pontifícia Universidade do Rio Grande do Sul (PUCRS). Possui mais de 15 anos de experiência na área de Tecnologia da Informação e atualmente exerce a função de Coordenador de Segurança da Informação, Riscos Operacionais e Segurança no SICREDI (Sistema de Crédito Cooperativo).

A entrevista ocorreu na PUCRS e teve a duração de aproximadamente 1 hora e da mesma forma que os demais especialistas, o instrumento foi apresentado e avaliado para, então, ser conduzida a entrevista. O primeiro aspecto questionado ao especialista foi relativo a estrutura do instrumento e a sua aderência à norma ISO/IEC 27001. O entrevistado salientou que na sua análise as 11 dimensões e os 39 itens da norma estão contemplados. O entrevistado reparou que haviam 40 questões e não 39 itens de verificação sugeridos pela norma. Foi esclarecido ao especialista que o instrumento proposto é baseado na norma ISO/IEC 27001 e adaptado para a realidade dos

hospitais, não sendo uma transcrição literal da norma. Günter (1999) destaca a importância de adaptar o instrumento aos objetivos propostos de uma pesquisa, buscando estar aderente a realidade do respondente.

Durante a avaliação do especialista foram identificadas duas células em que havia erros de redação as quais foram corrigidas, buscando evitar dúvidas quanto ao seu preenchimento. A objetividade das questões deve contemplar o seu conteúdo e ser de fácil entendimento, mesmo que o respondente não seja um especialista no assunto, mas que pelo entendimento da questão possa respondê-la (COOLICAN, 1999). A avaliação do especialista foi de que as questões estão bem formuladas e não deixam dúvidas quanto ao que se propõem avaliar.

Quanto às orientações de preenchimento do instrumento e ao formato do instrumento, o especialista destacou a clareza e objetividade das instruções, conforme relato a seguir:

> "As instruções para preenchimento do instrumento no cabeçalho são bem claras, não há dúvida. Além disso, o próprio formato e conteúdo do instrumento já são bastante alto-explicativo, e não precisa de explicações de como preencher." (E4)

Quando questionado sobre quais perguntas são desnecessárias, o especialista enfatizou que nenhuma das questões deve ser eliminada, uma vez que o instrumento está embasado em uma normativa consolidada e que abrange os principais aspectos referentes à Segurança da Informação, tendo o risco de ficar incompleta a avaliação.

4.5 PRÉ-TESTE DE RESPONDENTE

O Caso piloto buscou aprofundar a aplicabilidade e avaliação prática do instrumento proposto. O hospital em questão é uma instituição privada localizada em Porto Alegre, no Estado do Rio Grande do Sul, com 165 leitos, divididos em 3 unidades de internação, um centro cirúrgico, um centro de diagnose por imagem e um centro de quimioterapia. O hospital é mantido por uma instituição religiosa e hoje é referência nacional em redução da infecção hospitalar através de um forte programa de qualidade. Sua área de TI é formada por 7 profissionais divididos na área de desenvolvimento e infra-estrutura. Não existe um profissional específico responsável pela segurança, cabendo esta tarefa ao gestor da área de TI.

O gestor de TI do hospital possui 8 anos de experiência em instituições hospitalares e mais de 15 anos na área de TI. Têm formação superior em Ciência da Computação pela UNISINOS e não possui especialização em Segurança da Informação.

Da mesma forma que a condução com os especialistas, o instrumento proposto foi apresentado e respondido pelo entrevistado. Após, foi conduzida a entrevista com o questionário semi-estruturado buscando as sua percepções sobre o instrumento. O tempo de resposta do instrumento foi de 21 minutos, menor do que o tempo de resposta dos especialistas. Provavelmente porque os especialistas possuem maior experiência sobre Segurança da Informação e tinham uma preocupação analítica em profundidade na avaliação do instrumento, ou pelo fato de que o nível de maturidade dos processos de Segurança da Informação ainda é baixo. Este aspecto é confirmado pela análise superficial das respostas do instrumento proposto, que os itens de

avaliação do hospital estavam entre N1 (Inexistente) e N2 (Informal). Buscar fatos complementares adjacentes às entrevistas permitem uma análise e interpretação mais apurada dos fatos (MALHOTRA, 2001), apesar desta pesquisa não se propor analisar a maturidade dos processos de Segurança da Informação. Além disso, o entrevistado salienta que a gestão da Segurança da Informação e mesmo da TI no hospital está em um nível baixo de maturidade, especialmente por limitações financeiras da instituição e pela cultura organizacional da organização mantenedora.

4.5.1 Aplicabilidade

Na avaliação do entrevistado, a conformidade dos itens de avaliação do instrumento proposto frente a normativa ISO/IEC 27001 foi avaliada como aderente, apesar de que a instituição hospitalar não possuir controles adequados sobre a Segurança da Informação, conforme relato a seguir:

> "Não conheço muito bem esta norma mas acho que está ok. Aqui no hospital nós não temos uma maneira estruturada de cuidar da Segurança da Informação, apesar ser importante para qualquer hospital. As informações circulam muito aqui e passam por muitas pessoas através de muitos processos. O risco é grande de haver problemas e nós (TI) sabemos disso." (H1)

Há uma percepção clara da importância e relevância do tema Segurança da Informação segundo a avaliação do entrevistado. Quando questionado do motivo que leva a instituição ter níveis de maturidade entre Inexistente ou Informal, o entrevistado justifica que a gestão hospitalar

naquela instituição é formada por religiosos e médicos, os quais não valorizam a importância da Segurança da Informação.

> "Nosso hospital não cuida da Segurança da Informação porque não temos a cultura e a preocupação quanto a isso. Sei que o MS está cobrando isso de nós (hospital), mas a não é fácil investir nisso. Aqui a direção prefere comprar um novo equipamento do que se preocupar com a segurança por achar que nunca irá acontecer algo. Até o dia que acontece e ai saímos correndo para apagar o incêndio." (H1)

Nota-se uma preocupação por parte do entrevistado que, aparentemente, não é a preocupação dos membros da alta direção. Isso é destacado durante o decorrer da entrevista em outros momentos.

Quando questionado sobre o tempo de 1 hora para responder o instrumento proposto, o entrevistado respondeu que dependerá do conhecimento do respondente sobre os processos de Segurança da Informação do hospital. Segundo ele, os profissionais de TI normalmente é quem são encarregados de cuidar da proteção da informação, pois tratam das informações eletrônicas em sua maioria. O tempo para um hospital organizado pode ser maior do que isso, caso tenha que informar a forma de controle para os níveis de maturidade gerenciado e otimizado do instrumento proposto. Destaca também que será um desafio para ele e para toda a organização chegar no nível de maturidade otimizado, pois terão que elaborar um plano de ação para cada item de verificação, mas acredita que o instrumento servirá como um guia.

Na avaliação do entrevistado, o instrumento será útil para a avaliação da atual situação da instituição e irá auxiliar o responsável pela Segurança da Informação (no caso o entrevistado) a demonstrar para a alta administração a

relevância do tema em questão. O entrevistado acredita que a aplicabilidade do instrumento é total e em todas as áreas onde haja informações. Percebe-se o entendimento do entrevistado na amplitude do instrumento proposto indo além da informática.

A estruturação em níveis, segundo o entrevistado, permite melhor identificar a situação em que se encontra o hospital. Contudo, o entrevistado salienta que não acredita que algum hospital esteja em nível Otimizado. Na sua percepção ainda é necessário criar uma cultura de gestão por indicadores na administração da Segurança da Informação hospitalar, conforme relato a seguir:

> "O nível otimizado é bastante audacioso. Nosso hospital precisa evoluir em termos de controle de indicadores. Este aspecto não é fácil de implementar pois não é algo do nosso dia-a-dia. Mas acho muito importante pensar isso. Talvez motive a gestão do hospital a pensar melhor" (H1)

Refletindo sobre esta questão, a cultura organizacional sobre a relevância do tema é difusa. Por um lado, a gestão responsável acredita ser importante o gerenciamento da Segurança da Informação; por outro lado, parece que não existem procedimentos ou controles relativos ao tema. Para Cunha e Mendes (2004) este ponto é importante pois existe a necessidade das instituições de saúde no Brasil atentar para a gestão da Segurança da Informação, através do uso de medidas de avaliação e indicadores, uma vez que este tema possui uma importância e relevância para a garantia da continuidade das suas operações. Isso é enfatizado pelo respondente, conforme relato a seguir:

> "Fiquei agora imaginando se um computador do centro de tratamento intensivo venha a parar por problema de vírus. Hoje eles estão conectados em nossa rede local e integrado com nossos sistemas. Isso é um perigo! Poderia impactar na vida de uma pessoa." (H1)

4.5.2 Estrutura Lógica do Instrumento

Segundo o entrevistado, a estruturação é bastante lógica e coerente. O instrumento possui uma estruturação das alternativas clara e objetiva. A ordem das questões é lógica e adequada, motivando a sua utilização. O formato é simples, mas eficiente, sendo funcional e prático.. Segundo o entrevistado:

> "Não sei dos outros hospitais, mas todas as perguntas são muito claras e objetivas. Não é para ser respondido por um médico, mas por alguém da área de TI não haverá problemas para completar. Achei a disposição das questões bem elaborada" (H1)

4.5.3 Clareza das Questões

Segundo o entrevistado, o instrumento é claro e objetivo. Não há questão em que houve alguma dúvida quanto à redação e clareza. Sua utilização é prática especialmente na estrutura distribuída em questões e a descrição de cada nível em cada célula do instrumento. As instruções de preenchimento são diretas, não deixando dúvidas quanto ao seu preenchimento.

Na visão do entrevistado, o campo para informar o meio de controle para os níveis gerenciado e otimizado faz o respondente refletir sobre se realmente existem indicadores e estes são gerenciados, como relato a seguir:

> "Esta parte onde se coloca a forma de controle ajuda a pensar no como iremos controlar os indicadores aqui dentro. Como já disse, nosso nível é inicial na maioria das questões, mas pretendemos evoluir. Já devemos pensar como montar indicadores de acompanhamento dos processos." (H1)

Esta visão corrobora para a avaliação da maturidade dos processos, uma vez que o respondente necessita ter indicadores claros e gerenciados, não bastando colocar a sua percepção. Além deste ponto, o entrevistado acredita que o hospital será muito beneficiado se criar uma política de avaliação periódica do nível de maturidade de seus processos, pois como isso terá uma diretriz para a gestão da sua segurança.

Quando questionado sobre quais questões o entrevistado acredita não serem necessárias, nenhuma questão foi mencionada. Na percepção do entrevistado, a quantidade de itens a ser observados é completa e muito bem focada nas necessidades de um hospital, não havendo nenhum ponto a não ser considerado.

4.5.4 Aderência aos Objetivos Propostos

Segundo o entrevistado, o instrumento irá contribuir com a gestão do hospital e com a área de TI, através de uma melhoria do nível de gestão do responsável da Segurança da Informação. Segundo o entrevistado, ele não acredita que nos hospitais brasileiros exista uma cultura sobre o tema

Segurança da Informação em uso, mas que o instrumento pode contribuir com o aprimoramento de boas práticas.

Ao final, o respondente solicitou a autorização para iniciar o uso do instrumento na medição e acompanhamento da maturidade dos processos de Segurança da Informação.

4.6 ESTUDO DE CASO 1

O hospital do estudo de caso 1 está localizado em Porto Alegre, no Estado do Rio Grande do Sul, com 260 leitos e conta com 1737 colaboradores diretos e mais de 3700 médicos credenciados, com 12 salas no centro cirúrgico. Possui certificação internacional de acreditação hospitalar da JCI (*Joint Commission International*), sendo referencia nacional pela qualidade.

A área de Segurança da Informação está vinculada a área de TI do Hospital que atualmente conta com 22 colaboradores nas funções de suporte e desenvolvimento de sistemas. Não existe um profissional dedicado exclusivamente para a gestão da Segurança da Informação, sendo esta função de responsabilidade do gestor da área de TI. O hospital possui certificação na norma ISO 9002.

O tempo da entrevista foi de 45 minutos. Após a aplicação do instrumento, foi efetuada a entrevista com o roteiro semi-estruturado, cuja análise dos resultados é apresentada a seguir.

4.6.1 Aplicabilidade

Segundo percepção do entrevistado, o instrumento está aderente a normativa ISO/IEC 27001 e da sua predecessora ISO 17799, que é utilizada como diretriz no hospital para a Segurança da Informação. Todavia, o hospital não possui nenhuma certificação específica neste sentido, conforme relato a seguir.

> "Seguimos aqui no hospital as diretivas da ISO 17799. Analisamos os nossos processos e tentamos segui-la. Porém esta avaliação por maturidade pode nos ajudar a ver como chegaremos noutro patamar de gestão. Vai ser bem útil." (H2)

Segundo o entrevistado, a avaliação dos processos de Segurança da Informação através de nível de maturidade permite uma visão do estágio em que se encontra o hospital em relação às melhores práticas e permitirá fazer comparações entre entidades do mesmo porte. Além disso, serve como fonte de orientação para elaboração de um plano de ação. Pelo conteúdo avaliado, o instrumento está bastante objetivo e é de fácil utilização.

Foi questionado ao entrevistado se o tempo de 1 hora seria suficiente para o preenchimento do instrumento proposto. Em sua percepção, dependerá do nível em que se encontram os controles do hospital, conforme observação a seguir:

> "Quanto maior o nível de maturidade dos processos de um hospital, onde existam diversos quesitos como gerenciados e otimizados, maior será o tempo de resposta, pois o preenchimento das evidências exige certo tempo. Se retirar esta parte de informar a forma de controle ou deixar opcional ficará mais simples e terá o mesmo resultado." (H2)

Esta observação parece ser bastante pertinente, devendo ser avaliada a necessidade de manter esta determinação de obrigatoriedade para os níveis “Gerenciados” e “Otimizados”.

4.6.2 Estrutura Lógica do Instrumento

Na percepção do respondente, a estruturação do instrumento em alternativas objetivas e adequadas. Entretanto, em algumas questões o entrevistado acredita que devem ser mais claras, citando exemplos práticos, para melhor entendimento da questão, conforme observação a seguir:

> “Nesta parte de informar de saber se uma alternativa tem documentação ou não é difícil responder se a gente não tem um exemplo do que seja um documento. Serve um pedaço de papel?” (H2)

A questão aqui parece ser o entendimento do que seja um procedimento documentado, e não da redação da questão em si. Na avaliação do entrevistado, a documentação de um procedimento é muito individual, variando de hospital para hospital e a sugestão do respondente é de criar um modelo de documentação de procedimentos e de indicadores padronizados para cada item de avaliação. Entretanto, foi esclarecido que este aspecto não faz parte do escopo desta pesquisa e, portanto, deve ser fonte para estudos futuros.

Quanto ao formato, a funcionalidade, a praticidade e a ordem das questões, o entrevistado salienta que os itens estão adequados aos seus objetivos.

4.6.3 Clareza das Questões

O entrevistado observa que a clareza das questões quanto a redação e objetividade é adequada. Segundo o respondente, as orientações de preenchimento são bem simples e fáceis de entender. Quando questionado se haveria alguma questão que na sua avaliação são desnecessárias, o entrevistado salientou que não há nenhuma questão que deva ser eliminada, pois todas estão aderentes a uma normativa e, por conseguinte, estão aderentes as melhores práticas de gestão da Segurança da Informação.

4.6.4 Aderência aos Objetivos Propostos

O entrevistado observa que o instrumento irá atender plenamente as expectativas, sendo que esta iniciativa no segmento hospitalar irá contribuir na melhoria prática da gestão dos processos de Segurança da Informação. Além disso, o instrumento será muito útil para avaliar a Segurança da Informação da instituição, indo além da abrangência da informática, mas sim contemplando os processos de negócio, auxiliando a entender e agir naquilo que impacta no hospital.

Em uma análise do caso, percebe-se nesta instituição hospitalar um grau de preocupação com o tema Segurança da Informação e uma maturidade elevada do gestor e, conseqüentemente, da gestão dos processos de TI. Talvez isso se deva pela experiência que esta instituição possui em processos de certificação como o da normativa ISO 9002 ou pelo fato de estarem

periodicamente sujeitos a uma avaliação internacional de seus processos internos.

4.7 ESTUDO DE CASO 2

A instituição hospitalar do estudo de caso 2 é um complexo localizado em Porto Alegre, no Estado do Rio Grande do Sul, com uma estrutura de 400 leitos, mantido por uma congregação religiosa. Conta com mais de 1700 funcionários distribuídos em um centro clínico com 58 consultórios e 130 médicos, um centro de saúde integrada e um instituto para tratamento de doenças do câncer. A área de TI do hospital é composta por 19 funcionários, e não possui um profissional específico para a gestão da Segurança da Informação, sendo esta função exercida pelo gestor da área.

A aplicação do instrumento proposto deu-se nas instalações do hospital e em seguida foi efetuada a entrevista através do questionário semi-estruturado. O tempo de avaliação da maturidade dos processos de Segurança da Informação do hospital foi de trinta e quatro minutos. Houve uma questão em que o entrevistado detalhou a forma de controle, o que levou o tempo de dois minutos para o detalhamento, pois segundo a sua percepção, o nível de maturidade deste processo é “Gerenciado” e, portanto, necessário descrever a forma de controle.

4.7.1 Aplicabilidade

Segundo percepção do entrevistado, o instrumento é adequado e está em conformidade com a norma ISO/IEC 27001. Os níveis de maturidade em cinco níveis do instrumento proposto foram comparados com outros modelos de maturidade, sendo considerado adequado pelo entrevistado. Como sugestão de conteúdo, o entrevistado acredita ser necessária a alteração do formato do instrumento para aumentar a coluna para informar a forma de controle, pois segundo o mesmo, ela é pequena para um detalhamento. Aqui cabe uma consideração de que o instrumento foi apresentado em papel e não em meio eletrônico, o que solucionaria esta questão.

O instrumento, segundo o entrevistado, servirá para medir o nível de segurança da empresa em relação a sua aplicação, podendo dar subsídios à gestão para planejar futuras ações de melhorias. Em sua avaliação, o instrumento é de fácil uso é um subsídio não apenas para avaliar os processos de gestão da Segurança da Informação, mas também auxilia no monitoramento em um possível plano de implementação. Isso se deve, segundo o entrevistado, pelo seu conteúdo ser completo, contemplando todos os pontos de observância em termos de Segurança da Informação que uma instituição hospitalar deve ater.

O entrevistado enfatiza a questão de que desconhece algum instrumento semelhante e que a Segurança da Informação em hospitais ainda é precária e considerada um custo e não um investimento para a redução de riscos. Além disso, segundo o mesmo, geralmente a direção das instituições hospitalares no Brasil são exercidas por médicos, os quais têm apenas a preocupação na estrutura física do hospital e pouco na informação. Segundo o

entrevistado, talvez isso se deva ao fato de que o médico possui uma formação profissional em tratar, normalmente, de algum mal físico, o qual é tratado e prevenido, diferentemente da Segurança da Informação que é abstrata e nem sempre sua relevância e importância é percebida.

4.7.2 Estrutura Lógica do Instrumento

Na avaliação do entrevistado, o instrumento possui uma lógica estruturada das questões que encaminha o respondente em um raciocínio lógico e estruturado, conforme relato a seguir:

> "O estrutura das questões em dimensões e categorias facilita o raciocínio das questões pois me explica do que se trata a questão,antes mesmo de avaliar o item. Não tenho dúvida que os itens tem a ver um com o outro e que seguem uma seqüência dentro de seu tópico." (H3)

Além deste ponto, o entrevistado destaca que o instrumento é funcional e prático, com uma redação bem objetiva, o que facilita e motiva ao seu preenchimento.

4.7.3 Clareza das Questões

Na avaliação do entrevistado, as questões do instrumento proposto estão bem descritas e com um conteúdo abrangente de avaliação da maturidade de processos para a Segurança da Informação. Todavia, o entrevistado salienta que em sua percepção, algumas categorias de análise não

permitem ser mensuradas e, portanto, não podem ter indicadores associados. Analisando esta questão levantada pelo entrevistado, Chew et. al. (2006) aborda a questão de que a definição de indicadores é um processo complexo, não sendo construído de uma relação direta entre o que quer se medir e uma unidade de medida, mas em alguns casos necessita de um grau de abstração por parte de quem o define.

O entrevistado não definiu nenhuma questão para ser eliminada ou reescrita, considerando adequado aos seus objetivos. Quanto a questão das instruções para o preenchimento do instrumento, ele acredita que estão muito claras as orientações.

4.7.4 Aderência aos Objetivos Propostos

A percepção quanto ao tempo para preenchimento do instrumento proposto, segundo o entrevistado, deve ser em torno de trinta minutos e, portanto, não é um ponto que possa impactar na avaliação, conforme a seguir:

> " O tempo de uma hora é muito! Não precisa de tudo isso. Eu conseguir preencher em trinta minutos e ainda pensei como responder a forma de controle. Mesmo que eu tivesse todos os itens gerenciados e tivesse que descrever a forma de controle, não levaria uma hora." (H3)

O entrevistado acredita que o instrumento irá atender as expectativas de qualquer gestor da Segurança da Informação e que o instrumento auxiliará a gestão dos processos de Segurança da Informação, além de avaliar a maturidade dos processos relativos. Em uma análise deste ponto, se confirma a importância da utilização da normativa ISO/IEC 27001 como base da

estrutura e de conteúdo do instrumento, pois esta já está sedimentada como ferramenta de gestão da Segurança da Informação.

4.8 ESTUDO DE CASO 3

O hospital do estudo de caso 3 é uma instituição hospitalar localizada em Porto Alegre, no Estado do Rio Grande do Sul, com uma estrutura de 749 leitos, com função de hospital escola da Universidade Federal do Rio Grande do Sul, mantida pelo Ministério da Educação e Cultura. Conta como 164 consultórios ambulatoriais e 19 centros cirúrgicos em diversas especialidades, e com mais de 4070 funcionários, 279 professores e 314 médicos residentes.

Com 2000 computadores em sua rede local, a área de TI do hospital é compostos por 87 funcionários, divididos nas áreas de desenvolvimento de sistemas, serviços de suporte a rede e serviços de atendimento ao usuário, não possuindo um profissional específico para a gestão da Segurança da Informação, sendo esta função exercida pelo gestor da área de suporte a rede e serviços.

A aplicação do instrumento proposto deu-se nas instalações do hospital e em seguida foi efetuada a entrevista através do questionário semi-estruturado. O tempo de avaliação da maturidade dos processos de Segurança da Informação do hospital foi de 25 minutos. Não houve nenhuma questão em houvesse dúvida por parte do entrevistado.

4.8.1 Aplicabilidade

Quando questionado sobre a aderência do instrumento à normativa ISO/IEC 27001, o entrevistado afirmou que na sua percepção ele está totalmente aderente. Além disso, o entrevistado acredita que a proposição em cinco níveis de maturidade irá possibilitar uma avaliação dos processos por critério e permitir traçar planos de ação baseado nos resultados, pois auxilia a identificar em que estágio encontra-se a organização e o que deve ser feito. Além disso, a sua estrutura por ter um padrão entre os níveis de maturidade e as questões de avaliação, permite comparar com outras instituições e analisar as oportunidades de melhoria.

Segundo o entrevistado, ele é de fácil utilização, quando comparado com outros instrumentos, ou até mesmo com a norma ISO/IEC 27001. O instrumento proposto sugere em um maior nível de maturidade a utilização de indicadores e de melhoria contínua, enquanto a norma é descritiva e não traz a questão dos indicadores, o que o entrevistado acredita ser importante para uma gestão adequada da Segurança da Informação, conforme relato a seguir:

> "Esta parte do instrumento em que temos indicadores como um maior nível de maturidade é bem legal! Aquilo que se quer gerenciar deve ser medido e por isso os indicadores são bem importantes. Alguns processos de Segurança da Informação já mantêm o controle por indicadores." (H4)

Outro ponto destacado durante a entrevista foi a adaptação ao segmento hospitalar. Segundo o entrevistado, um instrumento aderente ao negócio facilita a interpretação e o enquadramento na realidade do hospital. Também permite verificar outras questões que não são percebidas em um modelo genérico. Ele salienta a avaliação dos processos de Segurança da

Informação dos equipamentos médicos computadorizados, os quais geralmente não são considerados pelos gestores da Segurança da Informação e que possuem alta relevância para o negócio. Segundo o entrevistado, os riscos associados a falta de gestão dos processos da Segurança da Informação em qualquer instituição hospitalar é grande, conforme transcrição de seu relato a seguir:

> " Em todos os hospitais diariamente circulam muitas pessoas, entre funcionários, médicos, prestadores de serviços, enfermeiros e outros. A informação que está disponível a todos como um prontuário de um paciente ou um laudo de um exame, pode expor um paciente ou mesmo o hospital a um escândalo na mídia e na comunidade. Vivemos de credibilidade e isso poderia impactar diretamente no negócio." (H4)

4.8.2 Estrutura Lógica do Instrumento

Na avaliação do entrevistado, as questões estão dispostas em uma estrutura adequada. Além disso, percebe-se uma lógica entre as questões, seus agrupamentos e nos níveis de maturidade dos processos. No que concernem as questões e a estrutura do instrumento, o entrevistado julga adequado o seu formato, enfatizando a característica em que em cada questão existe um detalhamento da questão em um nível específico, não tendo apenas uma escala de pontos ou valores de peso. Segundo o entrevistado, esta formatação contendo um claro detalhamento do nível em cada questão elimina possíveis erros de interpretação e de falso julgamento do nível de maturidade de um processo específico, conforme relato a seguir:

> "O formato do instrumento contendo a explicação de cada célula de maturidade não deixa dúvida quanto ao que é cada questão. Em outros instrumentos de avaliação de maturidade onde apenas tem-se uma escala de pontos, às vezes é difícil de encaixar exatamente a percepção da maturidade. Neste instrumento não se tem este problema." (H4)

No que tange a funcionalidade do instrumento, o entrevistado destaca que ele é prático, especialmente por ser em colunas e linhas, como em uma planilha do MS-Excel. Isso permitirá um acompanhamento das versões de avaliação periódicas e manter um vínculo com os indicadores a serem definidos. Neste ponto da entrevista, ele sugere que seria interessante em uma pesquisa complementar buscando indicadores padronizados para acompanhamento de cada processo.

4.8.3 Clareza das Questões

No aspecto de clareza das questões, fica a avaliação do entrevistado de que todas as questões estão bem redigidas e claras, tanto em termos de conteúdo quanto em termos de adaptação a realidade do negócio. A percepção do entrevistado, entretanto, é de que às definições e termos utilizados nas questões do modelo serão fonte de suporte para a área de TI das instituições hospitalares, e não para as áreas médicas do hospital. A sua observação é de que a terminologia utilizada é técnica e, portanto, não pode ser aplicada em instituições em que o gestor de TI não seja um profissional com formação adequada. Segundo o entrevistado, muitas instituições hospitalares no Brasil não possuem uma área de TI, utilizando um terceiro ou mesmo o corpo médico assumindo esta função.

A objetividade dos itens, segundo o entrevistado, está adequada, não deixando qualquer dúvida quanto ao seu conteúdo e a forma de preenchimento. Observa que as redações são bem dirigidas aos pontos necessários de avaliação, conforme o relato a seguir:

> "Os itens são bem objetivos e expressam os pontos necessários a uma boa gestão da segurança das informações hospitalares. As respostas de cada entrevistado são a percepção do responsável quanto aos controles que possui no seu hospital. Quando se pensa em maturidade de um processo fica claro que o que deve ser respondido." (H4)

Ao ser questionado sobre as possíveis questões que deveriam ser eliminadas, o entrevistado acredita que o modelo é completo e que todos os aspectos e dimensões abordadas são muito coerentes em um hospital, não devendo ser excluída nenhuma questão. Também ele salienta que as orientações de preenchimento são bastante óbvias e que responder ao questionário é muito simples.

4.8.4 Aderência aos Objetivos Propostos

O entrevistado salienta que, em sua avaliação, este modelo servirá não somente para hospitais, mas também para outras instituições de saúde, como os laboratórios, as clínicas médicas e pronto-atendimentos, que igualmente possuem a necessidade de manter um nível adequado de Segurança da Informação. Pelo fato de que esta instituição hospitalar ser a maior em termos de infra-estrutura de TI, o entrevistado observa que o instrumento proposto pode ser aplicado em alguns processos ou áreas do hospital, a fim de se obter um processo evolutivo de amadurecimento dos conceitos, conforme relato:

> "Em um hospital grande como o nosso, a implementação de indicadores, controles e processos é mais fácil quando se aborda por áreas. Temos tido sucesso com esta estratégia em outros controles. Como o modelo proposto é bem flexível e bem estruturado, acredito que teremos mais facilidade na implementação por áreas. Vamos definir uma área e iniciar por lá. Acho que assim criaremos esta cultura na organização." (H4)

Complementando a avaliação quanto aos objetivos propostos, o entrevistado achou válida a iniciativa e a proposição de um instrumento para auxiliar na gestão da Segurança da Informação. Além disso, o entrevistado acredita que o instrumento estará aderente as novas exigências do Ministério da Saúde sobre a Segurança da Informação, especialmente as diretivas da TISS as quais são baseadas na mesma normativa. Observa-se aqui que o gestor desta instituição percebeu que o instrumento proposto poderá auxiliar a adequação dos processos de Segurança da Informação aos modelos exigidos pelos órgãos reguladores. Também, o entrevistado observou a possibilidade da adequação dos processos internos do hospital visando uma futura certificação na ISO/IEC 27001 utilizando o instrumento proposto como direcionador.

4.9 RESULTADO GERAL DAS ANÁLISES

As análises foram realizadas a partir dos dados das entrevistas e com base na fundamentação teórica. Esta abordagem possibilitou avaliar aspectos relevantes apontados pelos gestores especialistas da área em relação a Segurança da Informação. Como o pesquisador possui experiência profissional na área de TI em instituições de saúde, a linguagem utilizada

pelos entrevistados foi de fácil compreensão, bem como a percepção de aspectos influenciadores na contextualização do ambiente hospitalar. É relevante uma reflexão sobre alguns pontos relatados pelos entrevistados e pelo preenchimento do instrumento proposto, os quais contribuem para uma análise mais aprofundada relativo a forma de gestão da Segurança da Informação, segundo a percepção dos gestores responsáveis.

Uma análise generalista dos resultados das entrevistas demonstra que não houve qualquer restrição quanto a aplicabilidade do instrumento em todos os hospitais pesquisados. Na percepção dos gestores poderá ser bastante útil como ferramenta de suporte a gestão de seus processos de Segurança da Informação. Com base nas respostas em relação ao nível de maturidade apresentados no instrumento foi possível notar um baixo grau em praticamente todos os itens nos hospitais avaliados. Isso comprova que estas instituições realmente carecem de um instrumento de apoio como este, pois mesmo o conhecimento sobre a norma ISO/IEC 27001 não era presente.

Os profissionais que ocupam cargos de gerenciamento da área de TI exercem a função de responsável pela Segurança da Informação. Nenhuma das instituições observadas possuía profissionais com conhecimento especializado sobre o assunto, ou mesmo um departamento específico para esta função.

Comparando-se os dados através das dimensões de análises do instrumento, percebe-se que a aderência aos objetivos propostos e a aplicabilidade, em todos os casos analisados, estão adequados segundo todos os respondentes. Na dimensão referente a clareza das questões foram identificadas algumas adaptações e ajustes no instrumento. Na dimensão estrutura, após a reavaliação do instrumento do número de questões, o

instrumento não recebeu qualquer consideração quanto a sua organização, seqüência de questões e tempo para preenchimento.

A análise dos dados sugere alguns fatores que, na percepção dos gestores, podem influenciar nos resultados. Entre esses fatores destacam-se a cultura organizacional e a importância do tema Segurança da Informação para a alta administração. Em algumas questões específicas, com o caso da dimensão de continuidade e análise de riscos, houve a percepção unânime por parte dos entrevistados de que, em suas instituições por parte da alta administração, não existe um entendimento da necessidade e da importância de um plano de continuidade.

5 CONSIDERAÇÕES FINAIS

Este trabalho procurou contribuir com demais estudos sobre a Segurança da Informação em instituições hospitalares, mais especificamente sobre a maturidade dos processos de gestão, através da proposição de um instrumento de avaliação. As considerações finais obtidas deste trabalho foram estruturadas em conclusões sobre a pesquisa, nas limitações do estudo e nas sugestões para pesquisas futuras apresentados a seguir.

5.1 CONCLUSÕES

Como constatado durante o desenvolvimento desta pesquisa, a proposição de um instrumento de avaliação que identifique o estágio da maturidade da Segurança da Informação é relevante para qualquer organização, onde estão inseridas as instituições hospitalares, especialmente em virtude da natureza da informação que está utiliza. Este instrumento proposto, além de avaliar o atual estágio de maturidade, visa também apoiar na identificação de oportunidades de melhoria dos processos de gestão da Segurança da Informação, uma vez que está baseado em uma normativa sedimentada e completa. Aliado ao isso, é crescente a exigência por parte dos órgãos reguladores, clientes e médicos, para que os hospitais, tanto privados quanto públicos, organizem-se de modo a responder às exigências de Segurança da Informação. Pesquisadores e profissionais da área de TI têm sido unânimes em relatar a complexidade envolvida na tarefa de administrar

os sistemas hospitalares e demais aspectos envolvidos na Segurança da Informação. É claro que ainda não há uma percepção clara da relevância por parte dos dirigentes hospitalares sobre o tema, quando considerados os hospitais desta pesquisa. Existe ainda a necessidade de uma pesquisa mais profunda em um número maior de instituições buscando confirmar ou identificar novos fatores que possam explicar o baixo nível de maturidade atual destas instituições.

As formas de controle e proteção da informação devem ser aprimoradas em todos os níveis das instituições hospitalares, através da elaboração de planos de ação e de um cuidado mais efetivo da informação (MINOTTO, 2002). Cabe aqui salientar que as instituições hospitalares, em sua maioria, tem diversas prestadores de serviços terceiros que possuem de alguma forma acesso a informação, sendo uma ameaça constante caso não exista uma boa gestão da Segurança da Informação.

Considerando os objetivos propostos para esta pesquisa, pode-se afirmar que a revisão de literatura sobre os temas que sustentam este trabalho, foram amplos e suficientes para auxiliar na elaboração do instrumento. Foram identificados e analisados os conceitos de diversos autores, especialmente norma ISO/IEC 27001, buscando subsídios para as definições das dimensões de análise e os itens de avaliação.

No objetivo de elaboração do instrumento, houve uma evolução do instrumento proposto inicialmente, até alcançar o instrumento de avaliação final desta pesquisa. As opiniões dos especialistas contribuíram com a ampliação da visão sobre características de praticidade e qualidade do instrumento, especialmente ao focado na estrutura. No objetivo de avaliação

do instrumento proposto, parece unânime a opinião entre os entrevistados de que o instrumento atingiu os objetivos propostos e a sua estrutura, aplicação e aderência ao que se propõe está adequada. Quanto às percepções que mais se destacaram pelas entrevistas foi que a avaliação do instrumento proposto deve ser ampliada para outros hospitais, buscando um aprimoramento na sua estrutura, itens de verificação e níveis de maturidade.

Neste sentido, destaca-se que os gestores entrevistados responsáveis pela informação hospitalar, em sua maioria, parecem ter pouca familiaridade e preocupação com a confidencialidade, integridade e disponibilidade de informações que não as diretamente relacionadas aos sistemas de informação. Entretanto, não percebem a importância da informação escrita ou falada existente dentro das diversas áreas e processos hospitalares. Assim, o quadro geral traçado a partir das entrevistas revela um desconhecimento da amplitude sobre a Segurança da Informação hospitalar, verificando-se, no entanto, exceções.

Em geral, os gestores concordam que a Segurança da Informação não é realizada de acordo com as prioridades dos hospitais, mas com o que é solicitado pelos órgãos reguladores. Ou ainda, simplesmente assumem controles básicos sem nenhum indicador ou critério claro de gestão da Segurança da Informação. É comum a percepção desses gestores de que o instrumento proposto possibilitará um acompanhamento periódico e irá auxiliar como ferramenta de gestão dos processos de segurança nos hospitais, pois acreditam ser este um dos motivadores para que viabilize a percepção da alta gestão hospitalar sobre a importância do assunto.

Embora boa parte das instituições ainda não compare seus indicadores com os de hospitais similares, esta é uma prática que desejam. Alguns gestores hospitalares referiram não realizar esta comparação por impossibilidade de acesso às informações de outros hospitais, sugerindo a apresentação do modelo a um órgão regulador ou associação de classe.

Parece existir pouco investimento na Segurança da Informação hospitalar e, apesar do consenso existente na literatura sobre a necessidade de profissionais capacitados para avaliar, em conjunto com os gestores, as informações e os aplicativos de TI (SEMOLA, 2003). Não foi identificado nas entrevistas um profissional responsável pela gestão de informação com formação específica e função exclusiva dentro dos hospitais, inclusive, em alguns casos, os entrevistados manifestaram desconhecimento do Coordenador Médico de Informações em Saúde. Os métodos de gestão da Segurança da Informação nos hospitais estudados revelaram-se insuficientes por referência ao proposto na literatura, ou que enfatiza a relevância do instrumento proposto (MANDARINI, 2006).

Com base no objetivo geral deste trabalho e nos resultados dos estudos de casos, a proposição do modelo de avaliação dos processos de Segurança da Informação através de níveis de maturidade irá possibilitar uma melhor gestão da informação nos hospitais. Todos os gestores entrevistados (e mesmo os especialistas) foram unânimes em afirmar que o instrumento proposto atingiu os seus objetivos, especialmente por estar adaptado às terminologias específicas dos hospitais e por considerar aspectos da gestão da informação.

Por fim, o presente estudo pôde contribuir com as instituições hospitalares que participaram desta pesquisa e que, segundo seus gestores de forma unânime, irão utilizar o instrumento na gestão de seus processos.

Em termos acadêmicos, o estudo propiciou uma compilação de diversos pontos sobre o tema Segurança da Informação, que poderão servir como base inicial para novos estudos e pesquisas. Ao pesquisador, a grata experiência e a possibilidade do aprofundamento do conhecimento em um assunto relevante e importante para o seu desenvolvimento acadêmico e profissional.

5.2 LIMITAÇÕES DO ESTUDO

Inerente a qualquer pesquisa, as limitações estarão presentes. Estas limitações podem ser de cunho teórico, metodológico ou prático.

Neste estudo, como limitação teórica pode-se citar a análise dos principais modelos e normas existentes. Este estudo tomou como base os modelos utilizados e disseminados na literatura e no meio empresarial, não abrangendo a totalidade dos modelos existentes pelo fato de que os novos modelos estão em um estágio inicial de desenvolvimento e não existirem referencial teórico sobre estes modelos, ou pela referencia teórica utilizada nesta pesquisa estar suficiente para embasar a proposição do instrumento objeto desta pesquisa.

Quanto ao aspecto metodológico, o presente estudo de caso, limitou-se a um estudo exploratório em três instituições hospitalares. Entretanto, características regionais e culturais podem influenciar nos resultados obtidos, o que sugere um aprofundamento neste sentido.

Outro aspecto da limitação deste estudo deve-se ao cunho prático. A ausência de profissionais de Segurança da Informação com conhecimento profundo sobre informações hospitalares, influenciou na percepção da relevância do instrumento para os respectivos hospitais. Outro fator importante é a constatação da baixa importância que os hospitais dão ao tema Segurança da Informação, especialmente por parte dos gestores destas instituições.

Também, por questões de limitação prática, a pesquisa limitou-se a propor um instrumento de avaliação e não efetuar a análise dos resultados de sua aplicação, apenas deteve-se nas percepções e inferências sobre o instrumento proposto, o que é sugerido para pesquisas futuras a seguir.

5.3 SUGESTÕES PARA PESQUISAS FUTURAS

Como sugestão para pesquisas futuras, existe a possibilidade da continuidade dos estudos sobre maturidade em Segurança da Informação e um aprofundamento na aplicação do instrumento proposto focado em instituições hospitalares e ampliando para outros segmentos. Dentre as opções de desenvolvimento de trabalhos, destacamos:

a) aplicar o instrumento em outras instituições hospitalares a fim de obter uma pesquisa quantitativa sobre a maturidade dos processos em outros hospitais. Exemplificando, pode-se identificar o nível de maturidade dos processos de Segurança da Informação das instituições hospitalares no Brasil.

Nesse caso, utilizar-se-ia a análise dos resultados da aplicação do instrumento proposto através de outra forma de coleta de dados e de estratégia de pesquisa;

b) adaptar o conteúdo do instrumento proposto para outros segmentos e avaliar a percepção, podendo comparar os resultados entre os diferentes segmentos. Nessa opção exigirá do pesquisador um tempo maior de análise e comparação;

c) Aprofundar o entendimento dos níveis de maturidade resultantes da aplicação do instrumento, buscando identificar outros fatores que são influenciadores, tal como as questões culturais que impactam na implementação de controles de gestão da Segurança da Informação nas entidades hospitalares.

REFERÊNCIAS

ALLEN, J. **Governing for Enterprise Security**. Pittsburgh, PA: Carnegie Mellon University. Networked Systems Survivability Program, 2005.

ALBERTS, C.; DOROFEE, A. **Managing Information Security Risks: The OCTAVESM Approach.** Boston, MA: Addison-Wesley, 2002.

ANTUNES, Ilídio. A Problemática da Avaliação e da Maturidade nos Processos de Desenvolvimento de Aplicações Informáticas. **Revista do Instituto Nacional de Pesquisas Econômicas**, n. 26, p. 46-47, 2001.

ARNODO, L. **Sistemas de informação hospitalar**: a importância do serviço de arquivo médico e estatística. São Paulo: Escola de Administração de Empresas de São Paulo, 1993. Dissertação (Mestrado em Administração), Programa de Pós-graduação da Escola de Administração de Empresas de São Paulo, 1993.

BABBIE, E. **The Practice of Social Research.** 4th. Wadsworth: Ed. Belmont, 1986.

BARDIN, L. **Análisis de Contenido**. Madrid: Editora Akal, 1975.

BAUMER, D.; EARP, J.; PAYTON, F. **Privacy of Medical Records:** IT Implications of HIPPA. Nova Iorque: ACM Press, 2000.

BEAL, A. **Gestão Estratégica da Informação.** São Paulo: Editora Atlas, 2004.

BOAR, B. **Tecnología da Informação:** A Arte do Planejamento Estratégico. 2. ed. São Paulo: Berkeley, 2002.

BRADLEY, Jana. Methodological issues and practices in qualitative research. **Library Quarterly,** Tucson, AZ, School of Information Resources and Library Science The University of Arizona v.63, n. 4, oct. 1993.

BRAILER, D. **Interoperability: The Key To The Future Health Care System.** Washington: U.S. Department of Health and Human Services Journal, 2005.

BRASIL. Ministério da Saúde**. PNIIS - Política Nacional de Informação e Informática em Saúde**; proposta versão 2.0; inclui deliberações da 12ª Conferência Nacional de Saúde. Brasília, 2004. Disponível em:

<w3.datasus.gov.br/APRESENTACAO/PoliticaInformacaoSaude29_03_2004.pdf> Acesso em: 20 jul. 2007.

CALDER, A.; WATKINS, S. **IT Governance, Data Security & BS 7799/ISO 17799**: A Manager's Guide to Effective Information Security. London: Kogan Page, 2003.

CARNEIRO, A. **Introdução a Segurança dos Sistemas de informação**. Lisboa: FCA Editores, 2002.

CHAMPLAIN, J. **Auditing Information Systems**, 2. ed. New Jersey: Jon Wiley & Sons, 2003.

CHAPIN, D.; AKRIDGE, S. **How Can Security Be Measured?** Information System Control Journal. Salem: ISACA, 2005. v. 2.

CHEW, E.; CLAY, A.; HASH, J.; BARTOL, N.; BROWN, A. **Guide for Developing Metrics for Information Security**. Gaithersburg: National Institute of Standards and Technology, 2006.

CHICKOWSKI, Ericka. Models Of IT Governance: Is It Time To Evaluate Your Decision-Making Process?, In: **Cover Focus Articles,** v. 26, p. 6, 9 abr., 2004. Disponível em: <http://www.processor.com/editorial/article.asp?article=articles%2Fp2615%2F21p15%2F21p15%2Easp&guid=1E38C072E2374E3A96BDF7BD7A612047>. Acesso em: 20 jul. 2007.

COBIT. **COBIT Security Baseline: An Information Security Survival Kit**. Rolling Meadows, IL: Information Systems Audit and Control Association, 2004.

COLTRO, Renata. Segurança: prioridade coorporativa. **Revista Computerworld,** São Paulo: IDG Brasil, n. 359, p. 26, 13 mar 2002.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.638/2002.** CFM: Brasília, 2002. Disponível em: <http://www.cfm.org.br/ResolNormat/Numerico/1638_2002.htm> Acesso em 18 mar. 2007.

COOLICAN, H. **Research Methods and Statistics in Psychology.** London: Hodder, Stoughton Educational, 1999.

COOPER, D.R.; SCHINDLER, P.S. **Métodos de Pesquisa em Administração.** 7ª. ed. Porto Alegre: Bookman, 2003.

CRESSON, C. **Information Security Policies Made Easy**. Houston, TX: Information Shield, Inc. 2005.

_____Information Security Roles and Responsibilities, Made Easy. Houston, TX: Information Shield, Inc. 2005.

CROSBY, P. **Quality is Free: the Art of Making Quality Certain**. New York: McGraw Hill,1978.

CROSBY, P. B. **Qualidade é Investimento**. Rio de Janeiro: José Olympio, 1999.

CUNHA, Francisco J. A. Pedroza; MENDES, Vera L. P. S. A política nacional de informação e informática: uma base para a implantação da gestão da informação nos serviços de saúde. In: Encontro Nacional de Ciência da Informação, 2004, Salvador. **Anais**. Salvador: ICI/ UFBA, 2004. p. 137-145.

CURTIS, M. B.; WU, F. H. The components of a comprehensive framework of internal control. **The CPA Journal**, n.70, p.64-66, 2000.

DAWEL, G. **A Segurança da Informação nas Empresas -** Ampliando Horizontes além da Tecnologia. Rio de Janeiro: Ed. Ciência Moderna, 2005.

DISMORE, P.; JACOBSEN, P. **Prosolve Processo Decisório: da Criatividade a Sistematização**. São Paulo: Ed. Cop, 1985.

DOBSON, J. **A Methodology for analysing human and computer related issues in secure systems.** Finland, Espoo: Proceedings of the Sixth IFIP International Conference on Computer Security and Information Integrity, 1990.

DONALD, J. **The consulting room computer - friend or foe?** The Practitioner. London: British Medical Journal, 1990.

EGAN, M. **The Executive Guide to Information Security.** New Jersey: Symantec Corporation, 2005.

EHRLICH, K.; ROHN, J. A. Cost Justification of Usability Engineering: A Vendor's Perspective. In: BIAS, R.; MAYHEW, D (eds.). **Cost-Justifying Usability.** Boston: Academic Press, 1994.

FACHIN, O. **Fundamentos de Metodologia.** São Paulo: Saraiva, 2002.

FEBRABAN – Federação Brasileira de Bancos. **Evolução da Norma BS 17799**. 2006. Disponível em: <www.febraban.org.br/Palestras.> Acesso em 2 Mai. 2007.

_____ **Novas Metodologias**. São Paulo: Subcomissão de Auditoria Interna da Febraban, 1999.

FERREIRA, A. **Novo Dicionário Aurélio da Língua Portuguesa.** 3. ed. São Paulo: Editora Positivo, 2006.

FONTES, Edison. **Segurança da Informação. O usuário faz a diferença**. Rio de Janeiro: Editora Saraiva, 2006.

FOWLER, F. **Design and evaluation of surve questions**. Thousand Oaks, CA: Sage, 1998.

FREITAS, H., OLIVEIRA, M., SACCOL, A.Z.; MOSCAROLA, J. O Método de Pesquisa Survey. São Paulo: **Revista de Administração da USP, RAUSP**, v.35, n.3, p.105-112, jul/set. 2000.

GHERMAN, M. **Controles Internos - Buscando a solução adequada - Parte II**. Rio de Janeiro: Módulo Security, 2005.
GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 4. ed. São Paulo: Atlas, 1995.

GODOY, Arilda S. Pesquisa qualitativa - tipos fundamentais. **Revista de Administração de Empresas**, São Paulo: FGV-EAESP, v.35, n.3, p. 23, mai.-jun. 1995.

GÜNTHER, H. **Como Elaborar um Questionário.** Série Planejamento de Pesquisas nas Ciências Sociais, no. 1, Brasilia: UnB, Laboratório de Psicologia Ambiental, 2003.

HAWKINS, K.; ALHAJJAJ, S.; KELLEY, S. **Using CobiT to secure information assets.** Alexandria, VA: The Journal of Government Financial Management Summer 52, 2003.

HUMPHREY, W. **Characterizing the software process**: a maturity framework. Pittsburgh: Software Engineering Institute, 1987.

ISACA - Information Systems Audit and Control Association. **Mapping ISO/IES 17799:2005 with COBIT 4.0**. 2005. Disponível em: <http://www.isaca.org>. Acesso em: 18 fev. 2007.

ISO/IEC 17799:2005a. **Code of practice for information security management**. International Standards Organization e British Standards Institute. Disponível em: <http://www.iso.org/> Acesso em 15 fev. 2007.

ISO/IEC 17799:2005b. **Information technology – Security techniques – Code of practice for informaton security management**. International Standards Organization. Disponível em: <[http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html]> Acesso em: 15 fev. 2007.

ISO/IEC TR 13335-3. **Guidelines for the Management of IT Security:** Techniques for the Management of IT Security. International Standards Organization. Disponível em: <http://www.iso.org/> Acesso em: 15 fev. 2007.

ISO/IEC 27001. **Information security management systems — Requirements**. International Standards Organization. Disponível em: http://www.iso.org/ Acesso em 15 fev. 2007.

KIILYNICH, J.; KORN, D. **The new HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: help or hindrance for clinical research?** Journal of the American Heart Association, 2003.

LEÃO, Beatriz de Faria. A infra-estrutura brasileira para a construção do registro eletrônico de saúde. In: MARIN, Heimar de F. et al. (org.). **O prontuário eletrônico do paciente na assistência, informação e conhecimento médico**. São Paulo: H. de F. Marin, 2003.

LAINHART, J.W**. COBIT – an update and look into the future.** ISACA. p. 6, 2001.Disponível em: <http://www.isaca.org/Content/ContentGroups/CoBIT2/Articles/C_small_OBI_small_T_An_Update_and_Look_into_the_Future.htm >. Acesso em: 18 jul. 2007.

LIMA, Clóvis. **Informação, Assimetria de Informações e Regulação do Mercado de Saúde Suplementar.** Artigo disponível em: <http://www.encontros-bibli.ufsc.br/bibesp/esp_03/910_GT5_lima.pdf> Acesso em: 20 jul. 2007.

LOURENÇO, Alexandre F. M. Do médico ou do paciente? Informe ABRANGE em **Medicina Social de Grupo.** São Paulo, v. 15, n 172, p. 01-03, mar/abr. 2001.

MAANEN, John Van. Reclaiming qualitative methods for organizational research: a preface. **Administrative Science Quarterly,** NY, The Johnson School at Cornell University Ithaca, v. 24, n. 4, p. 520-526, Dec. 1979 a.

_____ The fact of fiction in organizational ethnography. **Administrative Science Quarterly** , NY, The Johnson School at Cornell University Ithaca, v. 24, n. 4, p. 539-550, dec. 1979 b.

MALHOTRA, Naresh K. **Pesquisa em Marketing:Uma Orientação Aplicada**. Porto Alegre: Bookman, 2001.

MANDL, K.D.; KOHANE, I.S. **HealthConnect: Clinical grade patient-physician communication**. Cambridge: Journal of the American Medical Informatics Association, 1999.

MANDARINI, M. **Segurança Corporativa Estratégica**. São Paulo: Manole, 2004.

MATTAR, Fauze Najib. **Pesquisa de Marketing**: Metodologia, planejamento. 4. ed., São Paulo: Atlas, 1997.

MCCARTHY, M.; CAMPBELL, S. **Security Transformation – Digital Defense Strategies.** New York: McGraw-Hill, 2001.

MEIRELES, A.; GONÇALVES, C. A. **Administração estratégica: múltiplos enfoques para o sucesso empresarial.** Belo Horizonte: UFMG/CEPEAD, 2001.

MEUS, K. **Security and Privacity in the Healthcare Industry: A survey of industry practices and trends relatin to HIPAA.** Portland: Oregonian Business Center, 2006.

MIGUELES, C. **Por que os administradores precisam entender disto?** Porto Alegre: Nova Harmonia, 2003.

MINOTTO, Ricardo. **A Estratégia em Organizações Hospitalares.** Porto Alegre: EDIPUCRS, 2002.

MOREIRA, S. Nilton. **Segurança Mínima:** Uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

NIMER, Fernando. Segurança da Informação em Ambientes Distribuídos. **Developers Magazine,** Rio de Janeiro, v. 24,, Ago. 1998.

NIST - National Institute of Standards and Technology. **Recommended Security Controls for Federal Information Systems.** Washington, D.C.: Computer Security Resource Center, September, 2006.

PÁDUA, Claríndo I.P.S.. **Modelos de avaliação de maturidade em usabilidade.** Belo Horizonte: Synergia-Gestus, 2006.

PAPP, Raymound G. **Alignment of Business and Information Technology Strategy: How and Why?** New Jersey: Information Management Jornal, 1998. v. 11.

_____ **Determinants of Strategically Aligned Organizations: A Multiindustry, Multi-Perspective Analysis**. Hoboken, NJ: Stevens Institute of Technology, 1995.

PORTER, Michael E. **Estratégia Competitiva.** Rio de Janeiro: Campus, 2004.

PORTER, Michael E.; TEISBERG, Elizabeth O. **Redefining Health Care:** Creating Value-Based Competition on Results. Boston: Harvard Business School Press, 2006.

RAMAKRISHNAN, Prasanna. Information Security Management Systems. **The CISSP and SSCP Open Study Guides Website**, Canada, Quebec: CISSP and SSCP, p. 21, 2004.

ROESCH, Sylvia M.A. **Projetos de Estágio e de Pesquisa em Administração**. 2. ed. São Paulo: Atlas, 1999.

ROHN, E. **Cost-Justification of Usability Engineering : A Vendor's Perspective.** Boston: Academic Press, 1994.

SAYAO, L. **Modelos Teóricos em Ciência da Informação -** abstração e método científico. *Ci. Inf.* [online]., Brasília v. 30, n. 1 , p. 82-91, 2001.

SBIS – Sociedade Brasileira de Informática na Saúde. **Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES).** Disponível em: <www.sbis.org.br> Acesso em 02 out. 2006.

SEMOLA, M. **Gestão de Segurança da Informação** – uma visão executiva. Rio de Janeiro: Editora Campus, 2003.

SIPONEN, M. **Designing Secure Information Systems and Software: Critical evaluation of the existing approaches and a new paradigm.** Oulu, Finlândia: Oulu University Press, 2002.

SIQUEIRA, J. **Nucleando Qualidade**. Instituto Brasileiro da Qualidade Nuclear. Rio de Janeiro, n. 45, p. 4, ano XI, 2005.

STUMPF, Mariza Klück. **A gestão da informação em um hospital universitário: o processo de definição do** *patient core Record*, Porto Alegre: UFRGS, 1996. Dissertação (Mestrado em Administração), Faculdade de Administração, Universidade Federal do Rio Grande do Sul, 1996.

TAPSCOTT, D. **Wikinomics: como a colaboração em massa pode mudar o seu negócio**. Rio de Janeiro: Nova Fronteira, 2007.

WILSON, J. Health Insurance Portability and Accountabillity Act Privacy rules causes ongoing concerns among clinicians and researchers**. Annual Internal Medical 145,** USA, Washington – DC: National Library of Medicine, ago., 2006.

YIN, Robert K. **Estudo de Caso: planejamento e métodos**. 3. ed. Porto Alegre: Bookman, 2005.

_____ **Case Study Research.**. California, USA: Sage Publication Inc, 1984.

APENDICE A

INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO HOSPITALAR

Pontifícia Universidade Católica do Rio Grande do Sul - Faculdade de Administração, Contabilidade e Economia
Mestrado em Administração e Negócios - MAN

AVALIAÇÃO DE MATURIDADE DOS PROCESSOS DE SEGURANÇA DA INFORMAÇÃO HOSPITALAR

Data: _____/_____/_____

Instituição Hospitalar : _____ Respondente: _____

Instruções: Este instrumento de pesquisa visa a identificação do nível de maturidade dos processos da segurança da informação do hospital.
por favor, preencha APENAS uma opção em cada linha com a sua percepção referente aos itens de avaliação dispostos na tabela (‖ **X** ‖).
Em caso do nível de maturidade ser Gerenciado ou Otimizado, favor informar no campo especificação da forma de controle como é atendido o critério selecionado.

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Política	Política de segurança da informação	1	**Documentação da política de segurança da informação**	Não existe nenhuma política de segurança da informação ‖ ‖	Existe uma política de segurança da informação informal ‖ ‖	Existe uma política de segurança da informação formalizada ‖ ‖	Existe uma politica de segurança da informação formal e revisada com indicadores de acompanhamento de sua implementação ‖ ‖	Com base nos indicadores são implementadas melhorias contínuas na política de segurança da informação ‖ ‖	
Organizacional	Responsabilidade Organizacional	2	**Responsabilidade organizacional quanto a segurança da informação**	Não existe a responsabilidade organizacional dentro da segurança da informação ‖ ‖	Existe uma responsabilização organizacional informal pela segurança da informação ‖ ‖	A distribuição na organização das responsabilidades pela segurança da informação é formal ‖ ‖	Existe um processo formal com indicadores para a distribuição na organização das responsabilidades da segurança da informação ‖ ‖	Com base nos indicadores são implementadas melhorias contínuas na distribuição organizacional da responsabilidade na segurança da informação ‖ ‖	
	Relacionamento com Terceiros	3	**Critérios de segurança para a disponilibização de informações à terceiros**	Não existem critérios de segurança para a disponibilização de informações à terceiros ‖ ‖	Existem critérios informais de segurança para a disponibilização de informações à terceiros ‖ ‖	Existem critérios documentados de segurança para a disponibilização de informações à terceiros ‖ ‖	Existem critérios documentados de segurança para a disponibilização de informações à terceiros, revisados periodicamente e acompanhados por indicadores ‖ ‖	Com base nos indicadores são implementadas melhorias contínuas nos critérios de segurança para a disponilibização de informações à terceiros ‖ ‖	
Ativos	Gerenciamento de Ativos	4	**Inventário e alocação de ativos**	Não existe controle de inventário e alocação dos ativos ‖ ‖	Existe um controle informal de inventário e alocação dos ativos ‖ ‖	Existe um controle documentado de inventário e alocação dos ativos ‖ ‖	Existe um controle documentado de inventário e alocação dos ativos com revisão periódica e com indicadores de acompanhamento ‖ ‖	Com base nos indicadores são implementadas melhorias contínuas no inventário e alocação dos ativos ‖ ‖	
	Classificação da Informação	5	**Diretrizes da Classificação da Informação**	Não existem diretrizes de classificação da informação ‖ ‖	Existem diretrizes informais de classificação da informação ‖ ‖	Existem diretrizes formalizadas de classificação da informação ‖ ‖	Existe um processo de definição de diretrizes de classificação da informação e com indicadores de acompanhamento ‖ ‖	Com base nos indicadores são implementadas melhorias contínuas nas diretrizes da classificação da informação ‖ ‖	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Recursos Humanos	Processo Admissional	6	**Processos Admissionais**	Não existe na admissão ou contratação um esclarecimento quanto aos direitos e responsabilidades na segurança da informação do hospital	Existe na admissão ou contratação um esclarecimento informal quanto aos direitos e responsabilidades da segurança da informação do hospital	Existe na admissão ou contratação um documento de esclarecimento dos direitos e responsabilidades quanto a segurança da informação do hospital	Existe na admissão ou contratação um processo formal de esclarecimento dos direitos e responsabilidades da segurança da informação do hospital e com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nos processos de admissão ou contratação para esclarecimento dos direitos e responsabilidades da segurança da informação do hospital	
	Execução das atividades profissionais	7	**Concientização, educação e treinamento da segurança da informação**	Não existe uma concientização, educação ou treinamento da segurança da informação	Existe informalmente uma concientização, educação ou treinamento da segurança da informação	Existe documentos para a concientização, educação ou treinamento da segurança da informação	Existe processos formais para a concientização, educação ou treinamento da segurança da informação e com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na concientização, educação e treinamento da segurança da informação	
	Demissão ou mudança de relação de trabalho	8	**Responsabilidade na demissão ou alteração da relação de trabalho**	Não existe uma definição de responsabilidade na demissão ou mudança na relação de trabalho quanto a segurança da informação (remoção de privilégios, retorno de ativos,...)	Existe uma definição informal de responsabilidade na demissão ou mudança na relação de trabalho quanto a segurança da informação (remoção de privilégios, retorno de ativos,...)	Existe uma definição documentada de responsabilidade na demissão ou mudança na relação de trabalho quanto a segurança da informação (remoção de privilégios, retorno de ativos,...)	Existe um processo formal de definição de responsabilidade na demissão ou mudança na relação de trabalho quanto a segurança da informação (remoção de privilégios, retorno de ativos,...) e com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na responsabilidade em demissão ou alteração da relação de trabalho quanto a segurnaça da informação (remoção de privilégios, retorno de ativos,...)	
Segurança Física	Áreas Seguras	9	**Controle de acesso físico dos colaboradores (médicos, empregados, prestadores de serviços, terceiros,...)**	Não existem regras quanto ao controle de acesso físico dos colaboradores	Existem regras informais quanto ao controle de acesso físico dos colaboradores	Existem regras documentadas quanto ao controle de acesso físico dos colaboradores	Existe um processo documentado de definição quanto ao controle de acesso físico dos colaboradores e com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no controle de acesso físico dos colaboradores (médicos, empregados, prestadores de serviços, terceiros,...)	
	Segurança dos Equipamentos	10	**Controle da informação contida nos equipamentos (computadores, equipamentos de diagnose, telemetria, monitoramento,...)**	Não existem procedimentos para a segurança da informação contida nos equipamentos	Existem procedimentos informais para a segurança da informação contida nos equipamentos	Existem procedimentos documentados para a segurança da informação contida nos equipamentos	Existe um processo formal para a definição dos procedimentos de segurança da informação contida nos equipamentos com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no controle da informação contida nos equipamentos	
	Procedimentos Operacionais e Responsabilidades	11	**Procedimentos operacionais de controle de alterações e segregação das funções**	Não existem procedimentos operacionais documentados ou controlados para o controle de alterações e segregação das funções	Existe informalmente procedimentos operacionais para o controle de alterações e segregação das funções	Existem procedimentos operacionais documentados para o controle de alterações e segregação das funções	Existe um processo de definição dos procedimentos operacionais de controle das alterações e segregação das funções, com indicadores de acompanhamento e controle	Com base nos indicadores são implementadas melhorias contínuas nos procedimentos operacionais documentados de controle de alterações e segregação das funções	
	Administração dos serviços de terceiros	12	**Gestão dos serviços contratados**	Não existe a gestão dos contratos de serviços de terceiros	Existe informalmente a gestão dos contratos de serviços de terceiros	Existe um controle formal da gestão dos contratos de serviços de terceiros	Existe um processo formal de definição da gestão dos contratos de serviços de terceiros e com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na gestão dos serviços contratados de terceiros	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Procedimentos e Responsabilidades	Procedimento de aceitação de sistemas	13	**Aceitação de sistemas**	Não existe um procedimento de aceitação de sistemas	Existe um procedimento informal de aceitação de sistemas	Existe um procedimento documentado de aceitação de sistemas	Existe um processo formal de definição dos procedimentos de aceitação de sistemas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nos processos de aceitação de sistemas	
	Proteção contra códigos maliciosos (virus, spam, phishing, ...)	14	**Controle contra códigos maliciosos (virus, spam, phishing, ...)**	Não existe um procedimento de tratamento de códigos maliciosos	Existe um procedimento informal de tratamento de códigos maliciosos	Existe um procedimento documentado de tratamento de códigos maliciosos	Existe um processo formal de definição de controle de códigos maliciosos com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no controle contra códigos maliciosos	
	Backups	15	**Backup das informações**	Não existem procedimentos de backups das informações	Existem procedimentos informais de backups das informações	Existem procedimentos documentados de backups das informações	Existe um processo formal de definição de controle de backups das informações com indicadores de controle	Com base nos indicadores são implementadas melhorias contínuas nos processos de backup das informações	
	Transmissão de dados na rede	16	**Segurança das redes de comunicação de dados e voz**	Não existem procedimentos de segurnaça das redes de comunicação de dados e voz	Existem procedimentos informais de segurança das redes de comunicação de dados e voz	Existem procedimentos documentados de segurança das redes de comunicação de dados e voz	Existe um processo de definição de controle de segurança das redes de comunicação de dados e voz com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na segurança das redes de comunicação de dados e voz	
	Manipulação de mídia	17	**Administração de armanzenamento das mídias digitais**	Não existem procedimentos de segurança no armazenamento ou eliminação das mídias digitais	Existem procedimentos informais de segurança no armazenamento ou eliminação das mídias digitais	Existem procedimentos documentados de segurança no armazenamento ou eliminação das mídias digitais	Existe um processo formal de segurança de controle do armazenamento e eliminação das mídias digitais com indicadores de acompanhamento	Com base em indicadores são implementadas melhorias contínuas na segurança no armazenamento e eliminação das mídias digitais	
	Troca de Informações	18	**Procedimentos de troca de informações eletrônicas (TISS, CIAP,...)**	Não existem procedimentos de segurança para a troca de informações	Existem procedimentos informais de segurança para a troca de informações	Existem procedimentos documentados de segurança para a troca de informações	Existe um processo formal de definição dos procedimentos de segurança para a troca de informações com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nos procedimentos de troca de informações	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Controle de Acesso	Portais e Transações on-line	19	**Portais corporativos e transações on-line**	Não existem procedimentos para segurança dos portais corporativos e transações on-line	Existem procedimentos informais para segurança dos portais corporativos e transações on-line	Existem procedimentos documentados para segurança dos portais corporativos e transações on-line	Existe um processo formal de controle da segurança dos portais corporativos e transações on-line com indicadores de desempenho	Com base nos indicadores são implementadas melhorias contínuas nos processos de segurança dos portais corporativos e transações on-line	
	Monitoramento de sistemas	20	**Monitoramento e Auditoria de transações dos sistemas**	Não existem procedimentos de monitoramento e auditoria das transações de sistemas	Existem procedimentos informais de monitoramento e auditoria das transações dos sistemas	Existem procedimentos documentados de monitoramento e auditoria de segurança das transações dos sistemas	Existe um processo formal de monitoramento e auditoria de segurança das transações dos sistemas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no monitoramento e na auditoria de segurança de transações dos sistemas	
	Exigência empresarial de controle de acesso	21	**política de controle de acesso**	Não existe uma política definida pela alta direção de acesso aos sistemas	Existe uma política informal definida pela alta direção de acesso aos sistemas	Existe uma política documentada definida pela alta direção de acesso aos sistemas	Existe um processo formal de definição da alta direção de acesso aos sistemas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na política da alta direção de controle de acesso	
	Gerenciamento de acesso dos usuários	22	**Gerenciamento de usuários (acessos, privilégios, senhas)**	Não existem procedimentos de gerenciamento de usuários	Existem procedimentos informais de gerenciamento de usuários	Existem procedimentos documentados de gerenciamento de usuários	Existe um processo formal de controle do gerenciamento de usuários com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no gerenciamento de usuários	
	Responsabilidades dos usuários	23	**Responsabilidade no uso dos equipamentos e mesa limpa**	Não existem procedimentos de responsabilização dos usuários quanto a manter mesas limpas e ao uso de equipamentos	Existem procedimentos informais de responsabilização dos usuários quanto a manter mesas limpas e ao uso dos equipamentos	Existem procedimentos documentados de responsabilização dos usuários quanto a manter mesas limpas e ao uso dos equipamentos	Existe um processo formal de controle de responsabilização dos usuários quanto a mesas limpas e do uso dos equipamentos, com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na responsabilidade no uso equipamentos e mesas limpas	
	Controle de acessos para transmissão em redes	24	**Gestão dos serviços de redes (autenticação de usuários, equipamentos conectados, controle de tráfego, segregação de redes)**	Não existem procedimentos quanto aos serviços de rede	Existem procedimentos informais quanto aos serviços de rede	Existem procedimentos documentados quanto aos serviços de rede	Existe um processo formal de controle quanto aos serviços de rede com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na gestão dos serviços de rede	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
	Controle de acessos ao sistema operacional	25	**Procedimento para controle de acesso ao sistema operacional**	Não existem procedimentos para o controle de acesso ao sistema operacional	Existem procedimentos informais para o controle de acesso ao sistema operacional	Existem procedimentos documentados de controle de acesso ao sistema operacional	Existe um processos formal de definição dos controles de acesso ao sistema operacional com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no procedimento para controle de acesso ao sistema operacional	
	Aplicação e informação do controle de acesso	26	**Restrição ao acesso da informação**	Não existem procedimentos para restrição ao acesso da informação	Existem procedimentos informais para restrição ao acesso da informação	Existem procedimentos documentados para restrição ao acesso da informação	Existe um processo formal para controle de restrição ao acesso da informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na restrição ao acesso da informação	
Exigências de Segurança	Computação móvel	27	**Computação móvel e comunicações**	Não existem procedimentos para computação móvel e comunicações remotas	Existem procedimentos informais para segurança da computação móvel e comunicações remotas	Existem procedimentos documentados para segurança da computação móvel e comunicações remotas	Existe um processo formal de controle da segurança da computação móvel e comunicações remotas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na segurança da computação móvel e comunicações	
	Exigências de segurança dos sistemas de informação	28	**Análise de especificação e exigências de segurança**	Não existem procedimentos para análise de especificação e exigências de segurança	Existem procedimentos informais para análise de especificação e exigências de segurança	Existem procedimentos documentados para análise de especificação e exigências de segurança	Existe um processo formal de controle da análise de especificação e exigências de segurança com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na análise de especificação e exigências de segurança	
	Processo de valiadação de dados em aplicações	29	**Validadação da entrada, processamento e saida de dados**	Não existem procedimentos para validação da entrada, processamento e saída de dados	Existem procedimentos informais para validação da entrada, processamento e saída de dados	Existem procedimentos documentados para validação da entrada, processamento e saída de dados	Existe um processo formal de controle da validação da entrada, processamento e saída de dados com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na validadação da entrada, processamento e saída de dados	
	Controles criptográficos	30	**Politica de uso de criptografia**	Não existem uma política de uso de criptografia	Existe uma política informal de uso de criptografia	Existe uma política documentada de uso de criptografia	Existe um processo formal de controle do uso de criptografia com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na politica de uso de criptografia	
	Segurança de arquivos dos sistemas	31	**Controle das bases de dados dos sistemas aplicativos (ambiente de desenvolvimento, testes e produção)**	Não existe controle de segurança das bases de dados dos sistemas aplicativos	Existe controle informal de segurança das bases de dados dos sistemas aplicativos	Existe controle documentado de segurança das bases de dados dos sistemas aplicativos	Existe um processo formal de controle de segurança das bases de dados dos sistemas aplicativos com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no controle de segurança das bases de dados dos sistemas aplicativos	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
	Segurança em desenvolvimento e processos de apoio	32	**Procedimentos de controle de desenvolvimento e alterações nos sistemas**	Não existe controle de de desenvolvimento e alterações nos sistemas	Existe uma verificação informal da segurança do desenvolvimento e das alterações nos sistemas	Existe uma documentação de controle da segurança do desenvolvimento e das alterações nos sistemas	Existe um processo de controle de segurança do desenvolvimento e das alterações nos sistemas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nos procedimentos de controle de segurança do desenvolvimento e alterações nos sistemas	
	Administração de vulnerabilidade técnica	33	**Controle de vulnerabilidade técnica dos sistemas**	Não existe controle quanto a vulnerabilidade técnica dos sistemas	Existe uma verificação informal quanto a vulnerabilidade técnica dos sistemas	Existe uma verificação documentada quanto a vulnerabilidade técnica dos sistemas	Existe um processo de controle da verificação da vulnerabilidade técnica dos sistemas com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no controle de vulnerabilidade técnica dos sistemas	
Comunicação	Comunicação dos eventos e deficiências na segurança da informação	34	**Comunicação dos eventos e deficiências de segurança da informação**	Não existem procedimentos para a comunicação dos eventos e deficiências de segurança da informação	Existem procedimentos informais para a comunicação dos eventos e deficiências de segurança da informação	Existem procedimentos documentados para a comunicação dos eventos e deficiências de segurança da informação	Existe um processo formal de controle da comunicação dos eventos e deficiências de segurança da informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na comunicação dos eventos e deficiências de segurança da informação	
Continuidade	Administração de incidentes e melhorias	35	**Responsabilidades e procedimentos**	Não existem procedimentos para a responsabilização e administração de incidentes de segurança da informação	Existem procedimentos informais para a responsabilização e administração de incidentes da segurança da informação	Existem procedimentos documentados para a responsabilização e administração de incidentes da segurança da informação	Existe um processo formal de controle e responsabilização de incidentes da segurança da informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nas responsabilidades e procedimentos	
	Relevância da continuidade na segurança da informação	36	**Processo de garantia da continuidade na segurança da informação (riscos, plano de continuidade)**	Não existem procedimentos para continuidade na segurança da informação	Existem procedimentos informais para continuidade na segurança da informação	Existem procedimentos documentados para continuidade na segurança da informação	Existe um processo formal de gestão da continuidade na segurança da informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no processo de continuidade na segurança da informação	
ento	Alinhamento com requisitos legais	37	**Identificação da legislação aplicável**	Não existem procedimentos para identificação da legislação de segurança da informação hospitalar	Existem procedimentos informais para identificação da legislação de segurança da informação hospitalar	Existem procedimentos documentados para identificação da legislação de segurança da informação hospitalar	Existe um processo formal de identificação da legislação de segurança da informação hospitalar com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na identificação da legislação aplicável	
		38	**Proteção dos registros com base nas politicas da instituição hospitalar**	Não existem procedimentos para a proteção dos registros hospitalares	Existem procedimentos informais para a proteção dos registros hospitalares	Existem procedimentos idocumentados para a proteção dos registros hospitalares	Existe um processo formal de controle de proteção dos registros hospitalares com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas na proteção dos registros hospitalares	

Dimensão de Análise ISO/IEC 27001	Categoria de Análise	Nr	Critério	Inexistente	Informal	Organizado	Gerenciado	Otimizado	Especificação da forma de controle
Alinham	Alinhamento com as políticas de segurança	39	**Alinhamento com as políticas de segurança da informação**	Não existem alinhamentos das operações diárias com as políticas de segurança da informação	Existem alinhamentos informais das operações diárias com as políticas de segurança da informação	Existem um documento de alinhamento das operações com as políticas de segurança da informação	Existe um processo formal de controle do alinhamento das operações com as políticas de segurança da informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas no alinhamento entre as operações diárias com as políticas de segurança da informação	
	Auditoria em sistemas de informação	40	**Procedimentos de auditoria nos sistemas de informação**	Não existem procedimentos de auditoria nos sistemas de informação	Existem procedimentos informais de auditoria nos sistemas de informação	Existem procedimentos documentados de auditoria nos sistemas de informação	Existe um processo formal de controle da auditoria nos sistemas de informação com indicadores de acompanhamento	Com base nos indicadores são implementadas melhorias contínuas nos procedimentos de auditoria nos sistemas de informação	

APENDICE B

QUESTIONÁRIO DE AVALIAÇÃO DO INSTRUMENTO PROPOSTO

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
MESTRADO EM ADMINISTRAÇÃO E NEGOCIOS

Mestrando : Luis Antonio Janssen

FORMULÁRIO DE AVALIAÇÃO DO INSTRUMENTO DE AVALIAÇÃO DE DIRETRIZES ESTRATÉGICAS DE SUCESSÃO EMPRESARIAL

Com o objetivo de avaliar o instrumento de pesquisa apresentado, favor dar a sua opinião sobre os tópicos apresentados a seguir. Sua avaliação deve ser baseada na sua visão em relação a aplicabilidade e eficiência do Instrumento em avaliar a Maturidade da Segurança da Informação em Instituições Hospitalares

Nome do Entrevistado:
Cargo:
Entidade Hospitalar:

Em relação à formulação das questões...

1) o conteúdo está de acordo com a Normativa ISO/IEC 27001?

2) a redação está clara?

3) a redação está objetiva?

4) as orientações de preenchimento do instrumento são claras?

5) a estrutura das alternativas de respostas está clara?

6) a estrutura das alternativas de respostas é objetiva?

7) a ordem é adequada?

8) o formato do intrumento é adequado?

9) você estima que o tempo de uma hora para o preenchimento do instrumento é adequado?

10) Cite quais as perguntas que você julga serem desnecessárias e a sua justificativa

Em relação ao instrumento...

11) é de fácil utilização?

12) é funcional?

13) é prático?

Você acredita que o instrumento atenderá as expectativas?

☐ Sim ☐ Não

Os pontos de avaliação constantes no instrumento motivam o preenchimento do início ao fim?

☐ Sim ☐ Não

As questões abordadas permitiram avaliar a Maturidade da Segurança da Informação?

☐ Sim ☐ Não

Descreva sua opinião geral sobre o instrumento, comentando críticas, impressões pessoais e sugestão de melhorias.