Evandro Mário Lorens

Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação

Brasília

Julho de 2007

Evandro Mário Lorens

Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação

Dissertação apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre

Orientador: Prof. Dr. Mamede Lima–Marques

Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação
Departamento de Ciência da Informação e Documentação
Programa de Pós-Graduação em Ciência da Informação

Brasília

Julho de 2007

UNIVERSIDADE DE BRASÍLIA (UnB)
Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação (FACE)
Departamento de Ciência da Informação e Documentação (CID)
Programa de Pós-Graduação em Ciência da Informação (PPGCInf)

FOLHA DE APROVAÇÃO

Título: *"Aspectos Normativos da Segurança da Informação: um modelo de cadeia de regulamentação"*

Autor: *aluno Evandro Mário Lorens*

Área de concentração: *Transferência da Informação*

Linha de pesquisa: *Arquitetura da Informação*

Dissertação submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito parcial para obtenção do título de **Mestre** em Ciência da Informação.

Dissertação aprovada em: 11 de julho de 2007.

Aprovado por:

Prof. Dr. Mamede Lima-Marques
Presidente – Orientador (UnB/PPGCInf)

Prof. Dr. Jorge Henrique Cabral Fernandes
Membro Interno – (UnB/PPGCInf)

Dr. João Luiz Pereira Marciano
Membro Externo – Câmara dos Deputados

Prof. Dr. Edgard Costa Oliveira
Suplente – (UnB/PPGCInf)

Resumo

Apresentação de um modelo de cadeia de regulamentação de segurança da informação para os contextos organizacionais, apoiada na metodologia de metamodelagem e considerando os níveis de decisão estratégico, tático e operacional das organizações. Parte de uma definição social para a segurança da informação, utiliza-se das estruturas da arquitetura da informação, leva em conta a cultura e comunicação organizacionais e debruça-se sobre o planejamento estratégico organizacional para estabelecer os elementos da cadeia, ora empregando definições da literatura ajustadas à proposta, ora definindo propriamente os termos. Destaca as características epistemológicas, científicas e práticas dos elementos da cadeia proposta e contextualiza estes elementos nos ambientes informacionais organizacionais. Apresenta ainda os resultados de uma pesquisa de campo investigativa a respeito da segurança da informação e dos seus modelos normativos em organizações criteriosamente selecionadas. Propõe um modelo genérico de cadeia normativa e um modelo de cadeia normativa especializado para a segurança da informação.

Palavras-chave: segurança da informação; política de segurança da informação; cadeia normativa de segurança da informação; planejamento estratégico situacional; arquitetura da informação; diretrizes; normas; processos.

Abstract

This work presents a model for the information security regulation chain. This presentation is based on the metamodelling method, considering the organizations' strategic, tactical and operational decision methods. It starts with a socially aware definition of information security, uses the structures of information architecture, takes into account organizational culture and communication. It approaches organizational strategic planning in order to establish the chain composing elements, by using definitions of the literature, adjusted to this proposal, and by properly defining the terms themselves. It outlines the epistemological, scientific and practical features of the proposed chain elements and contextualizes these elements within the organizations' information environments. Finally, it presents the results of a field research, investigating the information security area and its normative models within selected organizations. As a result, it proposes a generic model of normative chain, plus another especifically designed model of information security normative chain.

Key-words: information security, information security policy, information security normative chain; situational strategic planning, information architecture, directives, norms, processes.

Sumário

Lista de Figuras

Lista de Tabelas

Agradecimentos

Este trabalho é resultado de um sonho, construído por muitas mãos, que seguraram as minhas e acreditaram que era possível.

Agradeço a Deus, o Criador, ser supremo, essência da sabedoria, pela minha existência.

Agradeço à Mara e à Lorena, pelo apoio incondicional, pela compreensão e pelo tempo que lhes subtraí.

Agradeço ao meu pai, Evandro Lorens, que investiu parte de sua vida na minha e que vibraria muito neste momento.

Agradeço à minha mãe, Genair Lorens e ao meu irmão, Ubirajara Lorens, pelo cuidado comigo, pelo incentivo permanente, e pelas orações.

Agradeço ao meu orientador, Professor Dr. Mamede Lima-Marques, que, além de ser um grande amigo e excelente professor, acreditou em mim.

Agradeço ao João Luiz Marciano, meu amigo, incentivador e mentor em segurança da informação.

Agradeço ao Professor Dr. Jorge Fernandes, pela disponibilidade e boa vontade em compor a conceituada banca examinadora de minha defesa.

Agradeço à Flávia Macedo, que ensinou-me disciplina e o universo da arquitetura da informação.

Agradeço às minhas primas Flávia Amorim e Lívia Rosado, pelo ânimo e pelo cuidado comigo.

Agradeço ao Beto Farias, pelo companheirismo, especialmente nos meus primeiros passos no CID.

Agradeço ao Edgard Costa, pela gentileza e apoio.

Agradeço à Elisângela Dourado, à Leila Bandeira, à Gislaine Messias, à Naiane Rodrigues, à Larissa Costa, à Silvana Carpanedo, à Gabriela Maia, à Luiza Bussolo e à Cristina Mara pelo apoio certo nas horas certas.

Agradeço ao Dinho, ao Carlos Cézar e ao Marcos Freire pela amizade verdadeira.

Agradeço aos professores Eliane Valério, Fernanda Moreno, Patricia Oliveira, Gisela Scheinpflug, Polyane Wercelens, Evandro Bervig, Nelson Filho, Alexandre Lênin e Cláudio Araújo pela força em momentos muito importantes.

Agradeço às professoras Drª Suzana Mueller e Drª Marisa Bräscher, pelas aulas riquíssimas e pela gentileza de sempre.

Agradeço ao Roberto Malheiro, à Sonia Brazil, ao Marcelo Lau, ao Kléber Leones, ao Fabiano Aguiar, à Cássia Leite, ao Eduardo Dutra, ao Marco Antônio Araújo, ao Sidnei Yokoyama e ao Gilberto Sudré, pela disponibilidade e boa vontade em colaborar.

Agradeço ao Gustavo Melgaço e à Graça Braga, pelo apoio em momentos fundamentais.

Agradeço aos colegas do CPAI, pelo tempo de orientação que deles subtraí.

Agradeço à Jucilene Gomes, à Professora Drª Sofia Baptista e ao Professor Dr. Antonio Miranda, pela consideração demonstrada para comigo.

Agradeço a muitos outros que deram-me apoio, sorrisos, abraços, conselhos, ensinamentos, momentos, compreensão, paciência, ouvidos, livros, artigos, cuidado, alegria.

A todos, muito obrigado!

"Donde, pois, vem a sabedoria, e onde está o lugar do entendimento?
...eis que o temor do Senhor é a sabedoria, e o apartar-se do mal é o entendimento."
(Bíblia Sagrada, Jó 28:20,28)

Para minha filha Lorena Lorens, por quem tudo vale a pena.

1 Introdução

A pesquisa realizada tem como objetivo investigar o arcabouço conceitual da segurança da informação, especificamente o seu contexto normativo, a fim de identificar níveis de regulamentação, discutir as definições e estruturas desses níveis, e propor um modelo de referência para a regulamentação normativa da segurança da informação nas organizações.

O modelo a ser proposto considera uma abordagem social para a segurança da informação, e é destinado a ser empregado na prática das organizações. Uma abordagem social para a segurança da informação considera o usuário como componente fundamental de sua existência.

Em geral, a prática das organizações, no que se refere aos aspectos normativos da segurança da informação, não reflete consistentemente as orientações dos seus planejamentos estratégicos. Antes, procura modelos de normas pré-estabelecidas, fundadas em consultorias, experiências alheias, ou em coletâneas de "melhores práticas de mercado", institucionalizadas por meio de padrões internacionais. A partir desses modelos, ajustam-se particularidades do contexto organizacional, advindas da própria cultura organizacional, ou da cultura organizacional considerada ideal pelas lideranças da organização.

A falta de um vínculo efetivo entre os planejamentos estratégicos e os aspectos normativos organizacionais introduz conflitos e distorções na cultura organizacional. Por conseqüência, os marcos normativos das organizações freqüentemente tornam-se letra morta ou formalismo social, cumpridos em parte pelo corpo organizacional ou cumpridas somente por parte dos membros da organização.

Percebe-se, então, a necessidade do estabelecimento de uma cadeia de regulamentação da segurança da informação com constituição interdisciplinar, metodologicamente consistente, que surja de dentro do planejamento estratégico organizacional, que esteja fundamentada nos princípios da arquitetura da informação, que entenda a segurança da informação como um fenômeno social, que seja amparado nas relações dos usuários com o contexto informacional, e que influencie e seja influenciada pela cultura e comunicação

organizacionais.

Este trabalho vem propor um modelo de cadeia com essas dimensões e traz também um retrato da realidade vivida em algumas organizações, com relação aos modelos normativos de segurança da informação praticados, permitindo um entendimento mais claro da aplicabilidade do modelo proposto.

2 Requisitos Pré-pesquisa

2.1 Objetivos

2.1.1 Objetivo geral

Propor um modelo para a cadeia de regulamentação dos aspectos normativos de segurança da informação e seus correlatos.

2.1.2 Objetivos específicos

1. Propor um referencial teórico para uma cadeia de regulamentação normativa da segurança da informação orientada a organizações;
2. Propor um modelo de integração do planejamento estratégico organizacional com o modelo da cadeia de regulamentação normativa da segurança da informação;
3. Realizar uma pesquisa de campo para identificar a abordagem das organizações e discutir a validade do modelo da cadeia de regulamentação normativa da segurança da informação proposto em contextos organizacionais reais; e,
4. Estabelecer a integração dos princípios de arquitetura da informação para o modelo proposto de cadeia de regulamentação dos aspectos normativos de segurança da informação.

2.2 Justificativa

No século XX, as organizações em todo o mundo passaram a considerar o domínio da informação como fator de sucesso para os seus negócios. Percebida como fator diferencial para a qualidade e a melhor aplicação dos recursos das organizações, a informação tornou-se um bem econômico ou ativo organizacional e as maneiras de obter, lidar e utilizar a

informação passaram a ser objeto de pesquisa visando potencializar os benefícios inerentes ao ativo organizacional.

Como ativo específico, a informação mostrou-se diferenciada dos demais bens materiais das organizações e passou a demandar tratamentos diferenciados, abrindo um imenso leque de possibilidades como campo de estudos, abordagem de problemas e métodos para manuseio, sendo considerada por Yves-François Le Coadic (2004) como: *"um produto, uma substância, uma matéria"*. Adicionalmente, a informação mostrou-se governada por leis próprias de comportamento e passível de ter o seu valor mensurado (MOODY; WALSHI, 1999).

Assim caracterizada a informação, tornou-se patente para as organizações a necessidade de sistematização do tratamento da informação no seu ciclo de vida, ou seja, nos contextos de coleta, organização, armazenamento, recuperação e disseminação, além da inquietante demanda de proteger basicamente a informação contra acesso indevido, adulteração e indisponibilidade.

A preocupação com a proteção da informação como ativo organizacional valorado deu origem ao conceito de segurança da informação, que se desdobrou em vários aspectos e conseqüentemente, em novas oportunidades para pesquisas e desenvolvimento de soluções.

Outra preocupação surgida no âmbito das organizações, a partir da definição dos conceitos em segurança da informação, foi a própria sistematização ou padronização desses conceitos, de modo a consolidar as bases para o desenvolvimento seguro e uniforme de soluções para os problemas emergentes dessas organizações. Nos últimos anos, esta preocupação tem levado à normatização internacional de vários conceitos, abordagens e práticas.

Dentre os padrões e normas mais significativos institucionalizados na última década, podemos destacar:

- **ISO/IEC 17799** - Código de prática para a gestão de segurança da informação: é uma adaptação internacional para parte 1 da norma britânica BS 7799. A versão brasileira foi oficializada pela ABNT como NBR ISO/IEC 17799;
- **ISO/IEC 27001** - Sistemas de gestão de segurança da informação - Requisitos: foi desenvolvida a partir da parte 2 da norma britânica BS 7799. A ABNT estabeleceu a equivalente brasileira que foi denominada NBR ISO/IEC 27001;
- **COBIT** - *Control Objectives for Information and related Technology*: é uma

metodologia de governança de TI que estrutura o conhecimento e boas práticas existentes em metodologias e normas correlatas e sua aplicação permite que se construa uma ponte entre as exigências do controle, questões técnicas e os riscos do negócio;

– **ITIL** - *Information Technology Infrastructure Library*: é um conjunto de melhores práticas para a gestão de serviços em TI e para o alinhamento desta área com os negócios da empresa, incluindo aspectos de segurança da informação.

A revolução informacional deflagrada também no século XX transformou o conceito original escolástico especializado de informação (do latim, *informatio*) significando "*o ato de dar ou mudar a forma de uma peça particular de matéria*", e explodiu seus campos de estudo, ao introduzir, no pós-guerra, a cibernética, a teoria geral de sistemas, a teoria da informação, a teoria dos jogos, a teoria do controle, o desenvolvimento dos computadores, o nascimento da inteligência artificial, a nova lingüística, as discussões sobre a entropia negativa, a busca pela decodificação do DNA etc. (ROBREDO, 2005).

O avanço tecnológico vivido desde a segunda metade do século passado catalisou a explosão informacional dos últimos vinte e cinco anos, contribuindo significativamente com os processos envolvidos no ciclo de vida da informação em aspectos tanto quantitativos quanto qualitativos, e mais, estabelecendo uma forte interdependência entre a tecnologia e a massa documental, em seus diferentes aspectos (MIRANDA; SIMEÃO, 2002). Em contrapartida, houve também a contribuição para automatização de mecanismos de segurança para a informação, com vistas a cobrir as novas mídias e atividades tecnológicas relacionadas à criação, produção, disseminação e descarte da informação.

Além do aspecto tecnológico, a segurança da informação surgiu também como responsável por proteger e regulamentar os aspectos comportamentais dos usuários das informações no âmbito organizacional. A observação desse fato não esteve, em princípio, refletida nas definições de segurança da informação da literatura especializada, o que evidenciou a necessidade de revisão desses conceitos e a busca por uma formulação que contemplasse também o aspecto social da segurança da informação, além das questões técnicas e associadas ao ciclo de vida da informação e seus processos.

Em sua tese de doutorado, João Luiz Marciano (2006) vem suprir essa necessidade ao apresentar uma definição para a segurança da informação em que estão contempladas as questões sociais e as questões relacionadas ao ciclo de vida da informação, considerando os recursos informacionais. Na visão de Marciano, a convergência desses aspectos

manifesta-se no comportamento do usuário ao manusear os recursos (tecnológicos ou não) no contexto dos processos do ciclo de vida da informação.

Sendo a segurança da informação uma área de conhecimento ainda em consolidação, comumente apropria-se de conceitos de outras áreas fundamentais e tenta adaptá-los para estabelecer seus próprios fundamentos, apresentando-se como um campo de estudos com a marca da interdisciplinaridade. Conceitos das áreas de ciência da informação, da ciência da computação, da engenharia, da matemática, da psicologia e da administração são freqüentemente empregados como suporte, viabilizando o delineamento dos próprios problemas de estudo da segurança da informação e a descoberta das melhores abordagens para esses problemas.

Dentre os problemas em maturação no campo da segurança da informação, encontram-se os seus aspectos normativos no âmbito das organizações. Freqüentemente, a segurança da informação aparece sem um grau apropriado de integração com os processos organizacionais e o reflexo da normatização nesses processos apresenta distorções, dificultando a aplicação mais efetiva dos conceitos e a assimilação cognitiva da importância e dos fundamentos de segurança da informação.

Diante do quadro organizacional de dificuldades para incorporar segurança da informação à sua cultura organizacional, e da percepção de que a segurança da informação deve contribuir com a estratégia de negócios, sugere-se que ela deve, como tal, integrar o planejamento estratégico da organização. Assim, as políticas da organização advindas de suas estratégias estabelecidas devem contemplar os aspectos normativos da segurança da informação e a regulamentação desses aspectos, através da representação por modelos que respondam aos níveis estratégico, tático e operacional do negócio.

2.3 Metodologia

2.3.1 Classificação da pesquisa

A presente pesquisa é constituída por duas partes. A primeira caracteriza-se como uma pesquisa descritiva analítica, construída segundo uma abordagem teórico-metodológica sobre um campo de conhecimento específico. Pode ser classificada como pesquisa bibliográfica porque tem o objetivo de conhecer, discutir e analisar as contribuições registradas acerca de um tema ou de um problema.

O método escolhido para a estruturação da primeira parte da pesquisa foi o da

meta-modelagem, proposta por van Gigch e Pipino (1986), e conhecido como M^3 porque sustenta-se em três níveis de análise incidentes sobre o objeto científico: o epistemológico, o científico e o prático.

De acordo com Antonio Gil (1999), a pesquisa descritiva "*tem como objetivo primordial a descrição de determinadas características de determinada população ou fenômeno*" e considera que a utilização de técnicas padronizadas para a coleta de dados é uma de suas características principais.

A segunda parte é uma pesquisa de campo qualitativa suportada por uma entrevista estruturada realizada com especialistas criteriosamente selecionados, objetivando captar as explicações e interpretações do que ocorre na realidade observada.

A pesquisa qualitativa é o estudo de temas em seu cenário natural, caracterizado pela busca do entendimento ou interpretação dos fenômenos em termos dos seus significados tais quais assumidos pelos indivíduos envolvidos no contexto pesquisado e pela preservação das complexidades do comportamento humano através de uma perspectiva holística (GREENHALGH; TAYLOR, 1997). Os métodos qualitativos são apropriados quando os fenômenos em estudo são complexos, de natureza social. Normalmente, são usados quando o entendimento do contexto social e cultural é um elemento importante para a pesquisa. A essência dos métodos qualitativos é o aprendizado da observação, do registro e da análise das interações reais entre pessoas, e entre pessoas e sistemas (LIEBSCHER, 1998).

A pesquisa qualitativa é essencialmente indutiva; nela, o pesquisador assume que a realidade é subjetiva e socialmente construída e desenvolve conceitos, idéias e entendimentos a partir de padrões encontrados nos dados coletados e dos significados atribuídos aos fenômenos pela população (fenomenologia), ao invés de coletar dados para comprovar teorias, hipóteses e modelos preconcebidos (RENEKER, 1993).

Usualmente, pesquisas de cunho qualitativo implicam a realização de entrevistas, quase sempre longas e semi-estruturadas. Nestes casos, a definição de critérios de seleção dos sujeitos que constituirão o universo de investigação é primordial, pois interfere diretamente na qualidade das informações a partir das quais será possível construir a análise e chegar à compreensão mais ampla do problema estudado. A descrição e delimitação da população base, assim como o seu grau de representatividade no grupo social em estudo são requisitos iniciais da pesquisa qualitativa baseada em entrevistas, já que o desenvolvimento do trabalho será estruturado sobre este contexto delineado.

2.4 Percurso Metodológico

2.4.1 Método da Parte I

O método escolhido para a estruturação da primeira parte da pesquisa foi o da meta-modelagem, proposta por John Van Gigch e Leo Pipino, e conhecido como M^3 porque sustenta-se em três níveis de análise incidentes sobre o objeto científico (GIGCH; PIPINO, 1986):

- **Epistemológico** – também denominado estratégico ou "de meta-modelagem" – constitui o arcabouço conceitual e metodológico de uma comunidade científica específica e objetiva investigar a origem do conhecimento da disciplina ou campo de conhecimento, justificar seus métodos de raciocínio e enunciar sua metodologia.

- **Científico** – também denominado tático ou "de modelagem" – compreende a previsão, descrição e explicação para os problemas e respectivas soluções, através do desenvolvimento de modelos e teorias.

- **Prático** – também denominado operacional ou "de aplicação" – aplicação efetiva dos modelos, teorias, técnicas e tecnologias desenvolvidos nos demais níveis para a solução dos problemas reais.

Tabela 1: Níveis de investigação

Nível de Investigação	**Insumos**	**Sistemas de Investigação**	**Produtos**
Meta-nível	Filosofia da Ciência	Epistemologia	Paradigma
Nível do objeto	Paradigmas do metanível e evidências do nível inferior	Ciência	Teorias e modelos
Nível inferior	Modelos e métodos do nível do objeto e problemas do nível inferior	Prática	Solução de problemas

(GIGCH; PIPINO, 1986)

No contexto da Ciência da Informação, a M^3 foi abordada nos trabalhos de Hebbertt Soares (2004) e Flávia Macedo (2005), para estudos no âmbito da Arquitetura da Informação.

O diagrama apresentado na figura 1, página 9, foi adaptado a partir do texto de Gigch e Pipino (1986) e representa a hierarquia de sistemas de investigação científica e as relações entre eles, conforme a M^3.

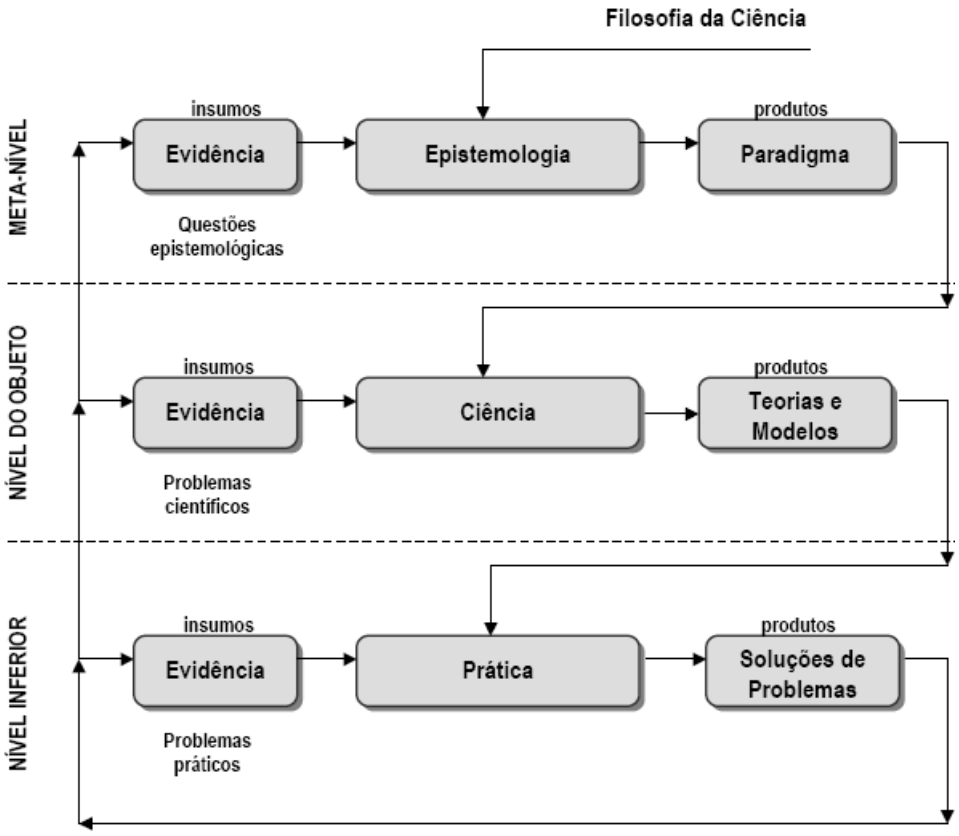

Figura 1: Metodologia de Meta-Modelagem (M^3): hierarquia de sistemas de investigação (GIGCH; PIPINO, 1986).

Nesta representação, as questões epistemológicas são formuladas tanto a partir de insumos da filosofia da ciência quanto por evidências produzidas nos níveis inferiores, o científico e o prático.

Os problemas científicos localizados no nível intermediário, por sua vez, recebem insumos através de paradigmas (originados a partir de questões epistemológicas) e através de evidências do nível inferior, o prático.

Por fim, as questões práticas recebem como insumos as teorias e modelos do nível científico e soluções de problemas do próprio nível prático.

Pela M^3, os sistemas de investigação científica podem ser classificados como:

- *conceituais*, quando tratam de questões filosóficas, epistemológicas e teóricas sobre a ciência;
- *de modelagem*, quando se referem ao desenvolvimento, formulação e validação de modelos, dos limitados aos genéricos; e

– *empíricos*, quando são utilizados para observar o relacionamento entre variáveis, testar sua invariância sob determinadas condições e inferir generalizações para contextos mais abrangentes. Nesta classe encontram-se os estudos de caso, os estudos e os testes de campo, e os estudos laboratoriais.

Notadamente, cada um dos sistemas de investigação científica relacionados remete-se a diferentes classes de problemas e serve a propósitos diferentes. No topo da hierarquia, o nível epistemológico, o propósito é construir um paradigma referencial para a ciência, posicionada no nível intermediário. No nível científico, o propósito é expandir o conhecimento e produzir modelos, relacionando-se e absorvendo métodos e conhecimento de outras ciências, se necessário. O nível prático utiliza as contribuições do nível científico para implementar o propósito de buscar soluções para os problemas das organizações.

Na visão de van Gigch e Pipino (1986), uma pesquisa pode ter como finalidade a modelagem ou a meta-modelagem. A modelagem projeta modelos inovadores e a meta-modelagem discute as questões epistemológicas e metodológicas sobre a modelagem. Assim, a modelagem ocorre no nível da ciência, o intermediário segundo a M^3, e a meta-modelagem no nível da epistemologia, o superior.

O conceito de "paradigma" utilizado na fundamentação da M^3 por van Gigch e Pipino é o de Thomas Kuhn (2001):

> *"...realizações científicas universalmente reconhecidas que, durante algum tempo, fornecem problemas e soluções modelares para uma comunidade de praticantes de uma ciência".*

Conforme o conceito de Kuhn, adotado na concepção da M^3, um paradigma representa a forma pela qual os problemas ganham conceituação no contexto de uma comunidade científica comprometida com um conjunto de determinadas abordagens, teorias, métodos e modelos.

O trabalho de van Gigch e Pipino investiga sistemas de informação enquanto uma possível ciência, analisando seu objeto de estudo e seus propósitos a partir da matriz de meta-modelagem apresentada. Para tanto, consideram que a disciplina deve definir claramente seus paradigmas, criar diretrizes viáveis de pesquisas, determinar bases para análises comparativas, e formular sólidos fundamentos de projeto para viabilizar o desenvolvimento de sistemas de informação eficientes.

Nesta dissertação, a M^3 será empregada para situar a Segurança da Informação na matriz de meta-modelagem, identificando os níveis epistemológico, científico e prático

de investigação científica. A M^3, enquanto metodologia, permite a compreensão de um objeto científico (a Segurança da Informação) em sua essência (a epistemologia), em suas abstrações (as teorias e os modelos científicos), e na aplicação dessas abstrações para a solução de problemas (a prática).

Caracterizado o objeto da Segurança da Informação, definiremos, segundo a M^3, um modelo para a cadeia de regulamentação dos aspectos normativos de Segurança da Informação, identificando suas relações e aplicações dentro do contexto da Segurança da Informação.

Yves-François Le Coadic (2004) considera que os modelos permitem o entendimento e a interpretação de fenômenos contextualizados em uma estrutura capaz de exibir os principais elementos e as relações existentes entre eles. A partir dessa concepção, pode-se afirmar que o papel dos modelos é constituído pelas funções de *explicar* (heurística), de *ordenar* (organizacional) e de *formular hipóteses* (preditiva).

2.4.1.1 Etapas da Parte I

Inicialmente foi realizado um estudo na literatura sobre a segurança da informação e os aspectos inerentes ao seu ciclo de vida, incluindo seu relacionamento com outros campos de conhecimento e a sua aplicação no âmbito das organizações. Foram também analisadas as várias concepções encontradas na literatura a respeito de conceitos chaves em segurança da informação.

Revisada a literatura, o trabalho foi direcionado à caracterização da necessidade de uma estrutura sistematizada de suporte normativo da segurança da informação que pudesse acolher, de forma organizada, a aplicação dos aspectos da segurança da informação em ambientes organizacionais.

Foram escolhidas definições apropriadas para itens específicos do modelo proposto para a cadeia, a partir de trabalhos de outros autores.

Também foram estabelecidas definições próprias para outros itens constitutivos da cadeia normativa da segurança da informação proposta, consistentes com a metodologia e inéditas.

O passo seguinte foi a elaboração efetiva e diagramação do modelo para a cadeia de regulamentação genérica das organizações e a cadeia dos aspectos normativos da segurança da informação, com foco nas instâncias de realização e decisão dessas organizações.

Um outro diagrama foi elaborado para expressar o contexto informacional em que está inserido o modelo de cadeia proposto, relacionando a metodologia aplicada, o ciclo de vida da informação e aspectos do modelo de operacionalização.

Foi construído também um diagrama para relacionar a cadeia normativa, o modelo metodológico, os instrumentos de implementação dos níveis da cadeia e os elementos da arquitetura da informação.

Por fim, foi construído um modelo de integração da cadeia de regulamentação dos aspectos normativos da segurança da informação com o planejamento estratégico situacional das organizações, visando oferecer consistência e aplicação direta do modelo proposto.

2.4.2 Método da Parte II

A segunda parte do trabalho, constituída pela pesquisa de campo, se propõe a levantar o entendimento e a prática das organizações para questões relacionadas aos aspectos de regulamentação de segurança da informação.

A partir do levantamento pretendido, será possível entender o que é concebido e praticado no dia a dia das organizações e identificar a possibilidade de aplicação do modelo teórico proposto como resultado na parte I, nas instâncias epistemológica, científica e prática.

Outro resultado a ser alcançado é o melhor entendimento e o aprofundamento da realidade específica das cadeias normativas das organizações em segurança da informação, identificando outras transformações possíveis, que contribuam para um melhor desempenho das organizações neste campo.

Como método para a pesquisa de campo, foi escolhida a entrevista semi-estruturada a ser realizada com público alvo definido, com número fixo de questões abertas.

O método *entrevista* oferece um quadro representativo para a interpretação de fenômenos relacionados ao escopo abordado e permite o acesso a um conjunto de informações pertinentes, de interesse da pesquisa, e guiadas pelas questões formuladas em busca de respostas para os problemas estudados.

Segundo Augusto Triviños (1987), a entrevista semi-estruturada, em geral, é aquela que parte de certos questionamentos básicos, apoiados em teorias e hipóteses que interessam à pesquisa, e que, em seguida, oferecem amplo campo de interrogativas, fruto de novas hipóteses que vão surgindo, à medida que recebem as respostas do informante.

Desta maneira, o informante, seguindo espontaneamente a linha de seu pensamento e de suas experiências dentro do foco principal colocado pelo investigador, começa a participar na elaboração do conteúdo da pesquisa.

No método da entrevista semi-estruturada, há um esquema pré-definido para as questões a realizar, o que possibilita a sistematização da entrevista em torno dos temas pesquisados. Em geral, as questões são abertas, o que as torna mais flexíveis, podendo ser conduzidas em forma de diálogo entre o entrevistador e o entrevistado. Este tipo de entrevista também é situacional, absorvendo naturalmente o contexto e o momento dos entrevistados. Cada especialista entrevistado tenta responder às questões recorrendo a seus próprios conceitos, à sua compreensão sobre os problemas e à visão institucional em que encontra-se inserido.

A entrevista semi-estruturada mantém a abordagem em torno do problema pesquisado de uma forma organizada e flexível. As principais vantagens deste método de coleta de dados são a possibilidade de obtenção de informações ricas e detalhadas e a liberdade dada ao entrevistado tanto para explorar sua vivência em torno dos temas abordados quanto para projetar a sua completa compreensão de procedimentos e estratégias como solução de problemas.

A escolha deste método deveu-se ao interesse em apreender a visão dos entrevistados em seu próprio contexto organizacional, obtendo informações detalhadas a partir das questões elaboradas, que permitam uma diversidade de olhares sobre o problema estudado e, conseqüentemente, a possibilidade de refletir sobre eles à luz do modelo elaborado na parte I do trabalho.

A aplicação da entrevista para um universo qualificado em torno dos assuntos da pesquisa tem o objetivo de viabilizar o aprofundamento das questões e reflexões sobre os temas, exercendo em sua essência a pesquisa qualitativa.

2.4.2.1 Etapas da Parte II

A realização da pesquisa qualitativa implementada pela entrevista semi-estruturada percorreu várias etapas. No primeiro momento, foi relevante determinar o perfil desejado para os entrevistados e selecionar os indivíduos a convocar para compor o universo pesquisado.

O segundo passo foi elaborar a estratégia de convocação, onde seriam estruturadas as razões a serem apresentadas aos candidatos com o objetivo de persuadi-los a participar

do processo, concedendo as entrevistas.

A seguir, foram elaboradas as questões, organizadas logicamente, preservando a busca pela informação mais rica e completa, e a liberdade para os candidatos discorrerem sobre os problemas abordados.

O próximo passo foi determinar a forma principal de realização da entrevista e outras formas alternativas, objetivando alcançar um quantitativo mais próximo possível do universo planejado.

Uma avaliação e a revisão das questões preparadas foram realizadas, depois de determinados os detalhes de aplicação da entrevista.

Foram feitos os contatos, aplicadas as abordagens, empregado o instrumento elaborado e analisadas as respostas produzidas.

Os resultados foram, então, avaliados globalmente sob a perspectiva do conteúdo adquirido com as entrevistas e analisados para encaminhamento das conclusões da pesquisa de campo.

3 Revisão de Literatura e Fundamentos

Neste capítulo, busca-se o entendimento dos elementos básicos para o desenvolvimento da dissertação como um todo. Em primeiro lugar, apresenta-se a Fenomenologia, sugerindo-a como referencial teórico para a compreensão do fenômeno da informação e do conhecimento. Estes fundamentos, construídos à luz da Fenomenologia, são essenciais para a Arquitetura da Informação porquanto encaminham a possibilidade de desenvolvimento de abordagens fenomenológicas também para elementos afeitos a áreas de estudo específicas, como por exemplo, a Segurança da Informação, que apresenta interesses específicos incidentes sobre a informação e o conhecimento.

Com papel preponderante no desenvolvimento da sociedade da informação, a Arquitetura da Informação compreende as questões relacionadas à integridade e à disponibilidade da informação em todo o seu ciclo de vida, bem como a utilização da informação por entidades devidamente autorizadas. Estas preocupações estão associadas à estruturação da informação e apresentam-se como aspectos da Segurança da Informação. Assim, é razoável considerar que a Segurança da Informação nasce no contexto da Arquitetura da Informação e nele é explorada desde sua perspectiva fundamental, seus princípios originários e políticas conseqüentes.

Considerando que a informação se constitui um ativo sensível e de grande importância para a existência das organizações nos tempos atuais, assume-se por premissa que a natureza das organizações e das informações organizacionais são determinantes para delineamento do escopo e do papel da Segurança da Informação nos contextos organizacionais. A natureza e os objetivos das organizações fazem-se expressar por meio dos seus princípios básicos e das suas políticas. Particularmente, os objetivos relacionados à informação fluem através de políticas de informação, que por sua vez manam políticas de segurança da informação, orientadas a determinar como será gerenciada e protegida a informação sensível do contexto organizacional. Para viabilizar o entendimento das políticas, das políticas de informação e das políticas de segurança da informação, que serão fontes dos aspectos normativos de segurança da informação, abordam-se esses conceitos

no presente capítulo.

A Segurança da Informação é revisada neste trabalho de forma abrangente, considerando várias linhas de entendimento sobre sua definição e alcance propostos por vários autores, incluídas as visões de normas e padrões internacionais, freqüentemente instituídas com base em *melhores práticas* das organizações ao redor do mundo. Suprindo-se da visão fenomenológica para a informação e para o conhecimento, e considerando o componente comportamental associado a aspectos normativos organizacionais, culmina este capítulo em considerar uma abordagem social para a Segurança da Informação (MARCIANO, 2006).

A seção sobre Planejamento Estratégico e a sub-seção sobre Planejamento Estratégico Situacional contribuem para o trabalho ao apresentarem elementos viabilizadores ao surgimento do fenômeno da Segurança da Informação no contexto organizacional e ao proporcionarem ambiente para a caracterização do modelo de cadeia normativa a ser proposto, em todas as instâncias administrativas das organizações, com a abrangência delimitada pelos planos resultantes dos planejamentos estratégicos.

A abordagem da Cultura Organizacional contribui com o desenvolvimento deste trabalho ao sustentar o entendimento do papel de influência recíproca entre a cultura organizacional e o conjunto dos aspectos normativos organizacionais: a cultura organizacional influenciará a existência e o relacionamento do corpo de pessoas da organização com os aspectos normativos organizacionais, e o conjunto dos aspectos normativos produzirá influência sobre a cultura organizacional ao longo do tempo. Esta relação bilateral é suportada pela comunicação organizacional que serve à cultura organizacional enquanto difunde os princípios e objetivos da organização, e consolida a cognição dos aspectos normativos junto aos membros da organização. Neste contexto, a comunicação organizacional também assume importante papel na aplicação dos aspectos normativos à realidade da organização.

No decorrer do texto, as expressões "*cadeia de regulamentação*" e "*cadeia normativa*" serão usadas equivalentemente para referir-se ao modelo de cadeia a ser proposto.

A proposta do modelo para a cadeia de regulamentação da Segurança da Informação terá sua base teórica estruturada nos conceitos apresentados neste capítulo, cada qual exercendo sua contribuição específica para o estabelecimento dos resultados.

3.1 Fenomenologia

Adota-se o referencial epistemológico da Fenomenologia como base para a compreensão das questões fundamentais sobre segurança da informação tais como a natureza do dado, da informação e do conhecimento. Portanto, serão mencionadas as idéias de seus autores mais relevantes, que servirão de base para as discussões apresentadas no decorrer da dissertação.

O termo "fenomenologia" (*phenomenologia*) é derivado do substantivo fenômeno, do latim *phaenomènon* – "*fenômeno, aparição*", ou do grego *Phainómenon* – "*coisa que aparece*", ou ainda, "*tudo o que é percebido, que aparece aos sentidos e à consciência*". Surgiu no século XVIII, nas obras do matemático e filósofo alsaciano Johann Heinrich Lambert (1728–1777) e foi difundido pelo filósofo escocês William Hamilton (1788–1856). No pensamento setecentista, era considerada como a descrição filosófica dos fenômenos, em sua natureza aparente e ilusória, manifestados na experiência aos sentidos humanos e à consciência imediata (HOUAISS, 2000).

A Fenomenologia preocupa-se em descrever de que maneira o corpo relaciona-se com a experiência, e em descobrir de que forma o ser percebe o mundo e o outro, partindo do princípio de que não há possibilidade de compreensão do mundo sem a compreensão da existência humana. Um das maiores contribuições da Fenomenologia de Husserl foi a busca permanente pela superação do subjetivismo, a partir de um ponto de vista que ressalta a relação entre o sujeito e o mundo, e se permite a autocrítica (JÚNIOR, 2003).

David Smith (2003) define a Fenomenologia como o estudo das estruturas da consciência tal qual são experimentadas do ponto de vista da primeira pessoa; ou ainda, o modo como experimentamos as coisas e o significado das coisas que temos em nossas experiências.

Johannes Hessen (1998) defende que a Fenomenologia "*é um método para descrição do fenômeno do conhecimento, que permite localizar o conhecimento, o sujeito, o mundo e as disciplinas que estudam cada elemento*".

Para João Ribeiro Júnior (2003), a Fenomenologia é uma filosofia que propõe reflexão sobre o "conhecimento do conhecimento".

Patricia Sanders (1982) propõe quatro questões sobre as quais se baseia a Fenomenologia :

– Como o fenômeno ou experiência sob investigação pode ser descrito?

– Quais são os invariantes, ou seja, os elementos comuns ou temas emergentes em tais descrições?

– Quais as possíveis reflexões acerca destes temas?

– Quais são as essências presentes nestes temas e reflexões?

Também é de Patricia Sanders (1982) o quadro comparativo registrado na tabela 2, página 18, que destaca as diferenças entre o paradigma fenomenológico e o paradigma normativo.

Tabela 2: Comparativo entre os paradigmas fenomenológico e normativo (SANDERS, 1982)

Paradigma fenomenológico	**Paradigma normativo**
1. Apreensão do mundo	
O pesquisador enxerga o mundo como indeterminado e problemático. Os fenômenos sob investigação são vistos mais diretamente como resultantes de percepções, intuição e significados pessoais.	O pesquisador vê o mundo como aproximadamente determinado e não problemático. Escolhas pessoais ainda são necessárias para decidir quais características devem ser estudadas e como devem ser avaliadas
2. Fenômenos investigados	
Considera-se a "experiência vivida" pelos indivíduos. Considera tanto as características observadas como as qualidades específicas percebidas como formas pessoais de significado.	Considera as características que são facilmente enumeráveis e empiricamente verificáveis.
3. Formulação do problema	
Inicia-se com uma atitude de *epoché*. Todos os preconceitos pessoais, crenças e afirmações sobre relações causais ou suposições são suspensas ou "colocadas entre parênteses". Questões são formuladas e as respostas são analisadas.	Inicia-se com uma hipótese de relação causal. A hipótese é verificada pela manipulação de uma ou mais variáveis independentes a fim de estudar-se o seu efeito sobre um comportamento específico (variável dependente).
4. Metodologia de pesquisa	
Dá-se ênfase à descrição do mundo pelo ponto de vista das pessoas que o vivem e o experienciam. Todos os conceitos e teorias emergem dos dados da consciência, exigindo uma abordagem cognitiva que não pode ser replicada com exatidão.	Amplas generalizações abstratas ou teorias são aplicadas de uma forma lógico-dedutiva por meio das hipóteses das definições operacionais para formar um delineamento que pode ser replicado.
5. Objetivo e inferências da pesquisa	
Chegar a essências universais puras. A lógica da inferência é a comparação direta, resultando em novos *insights* ou reclassificações.	Interpretação estatística dos dados a fim de formular categorias ou normas. A lógica da inferência é a classificação e a serialização dos resultados, levando a comparações numéricas.
6. Generalização dos resultados	
As generalizações dizem respeito apenas aos indivíduos específicos sob investigação. As conclusões servem como uma base de dados para investigações posteriores.	Generalizações são feitas com base na análise dos dados relativos a classes similares ou tendências universais que são expressas de um modo normativo (causa/conseqüência, situação/ação, correlação)

Uma das marcas da Fenomenologia é o lidar com as questões filosóficas envolvidas na geração e na aplicação do conhecimento e na análise de fenômenos sociais e humanos de

maneira apropriada e profunda.

Immanuel Kant (1729–1804) considera que o termo "*fenômeno*" designa o objeto da experiência, ou aquilo que é percebido a partir da sensibilidade e das leis do entendimento previamente estabelecidas. O fenômeno, então, define-se como "*um composto daquilo que recebemos das impressões e daquilo que nossa própria faculdade de conhecer tira de si mesma*" (JAPIASSU, 1996).

O filósofo alemão Franz Clemens Brentano (1838–1917) foi o fundador da corrente filosófica da Fenomenologia que encontra significado cognitivo em toda realização humana. Brentano classificou os fenômenos em físicos e mentais, atribuindo aos fenômenos físicos a característica de percepção direta pelos sentidos e aos fenômenos mentais a característica da intencionalidade (JÚNIOR, 2003).

3.1.1 Bases da Fenomenologia

3.1.1.1 Husserl

Edmund Husserl (1859–1938), de família israelita e nascido na Morávia foi discípulo de Franz Brentano e é considerado o fundador do movimento fenomenológico moderno. A Fenomenologia de Husserl preocupa-se com a completa caracterização do estado da mente consciente, o elemento principal do ser, e consiste em:

> "*um método filosófico que se propõe a uma descrição da experiência vivida da consciência, cujas manifestações são expurgadas de suas características reais ou empíricas e consideradas no plano da generalidade essencial*" (VERGEZ; HUISMAN, 1976).

Nesta linha, Husserl propõe a rejeição da aparente realidade do mundo formado pelas entidades físicas e perceptíveis, colocando-o "*entre parênteses*" (*epoché* fenomenológica); uma vez que o mundo e todas as suas entidades estão sempre presentes, quer sejam ou não experimentados pelo observador, não deve interferir no processo de formulação do raciocínio, o qual, por sua vez, determina a realização da consciência (LÜBCKE, 1999). Isolado o mundo estabelecido, a primeira pessoa (*self*) passa a experimentar o mundo para atribuir-lhe razão e significado através da conexão do ego transcendental (MINGERS, 2001).

O fenômeno, do ponto de vista husserliano, não significa "*a simples aparência que se opõe à verdade do ser*", como em Platão e Kant; é a aparência do objeto acessível imediatamente à consciência, a manifestação plena de sentido (JÚNIOR, 2003).

Foi Husserl o autor do termo "*intencional*", empregado para representar a relação entre o objeto e sua imagem junto à consciência que o percebe, ou seja, para expressar o seu significado para o sujeito.

No caráter intencional da consciência, a consciência é sempre consciência de algo. A "*intencionalidade*" constitui-se, portanto, na propriedade da consciência de perceber um objeto e de dar-lhe um sentido. A Fenomenologia kantiana trata da descrição da consciência e da experiência, mas abstrai-se de considerações acerca de seu conteúdo intencional (JÚNIOR, 2003).

Na visão de Husserl, a Fenomenologia interessa-se, basicamente, pela estrutura dos vários tipos de experiências do ser: percepção, pensamento, memória, imaginação, emoção, desejo e vontade de manifestação corporal, ação incorporada e atividade social, incluindo atividade lingüística, todas elas partindo de diferentes intencionalidades. Esta forma de pensar determina o direcionamento da experiência para os objetos no mundo, ou seja, é possível visar a um objeto como dado, como imaginário ou como passado (SMITH, 2003).

Ainda segundo Edmund Husserl (1996), o processo de indução fenomenológica é formado por etapas, a saber:

- A análise "intencional" da relação entre o objeto como é percebido e a sua apreensão subjetiva;
- O isolamento da realidade percebida (*epoché*); e,
- A abstração das essências a partir da consciência e/ou da experiência, superando as estruturas e padrões convencionais de pensamento e de ação com o objetivo de identificar suas raízes comuns (redução eidética).

Ao refletir sobre os objetos da consciência ao invés daqueles do mundo real, Husserl pretendia mapear as estruturas que governam a experiência. Sua conclusão foi que as informações captadas pelos sentidos são resultantes de construções da consciência e atreladas a significados. Assim, o que compõe a experiência não é a essência, mas o resultado do processo constitutivo da consciência.

Husserl (1990) também aborda fenomenologicamente a questão do "*outro*", ignorada nas teorias do conhecimento de Descartes e Kant. Ele observa que:

> "*...assim como toda consciência é consciência de alguma coisa, [...] nossa consciência reconhece a existência de outra consciência, numa experiência originária da coexistência*".

Mas, diferentemente do objeto,

> "*...o outro não é só aquele que vejo, mas aquele que me vê e é também fonte transcendental de um mundo que lhe é dado*".

Husserl considera que o conhecimento não reside no objeto observado, nem tampouco no observador, mas na imagem do objeto concebida pelo observador. Para ele, a verdade pode ser definida como a concordância perfeita entre o significado concebido pelo observador e o objeto observado, contextualizando o conhecimento como mais um dos fenômenos percebidos por meio da *epoché* (STEGMÜLLER, 1977).

Com esta formulação, Husserl (1970) influenciou significativamente pensadores como Martin Heidegger (1889–1976), Jean-Paul Sartre (1905–1980) e Maurice Merleau-Ponty (1908–1961), e a teoria moderna da consciência, desdobrando profundos reflexos em ciências como a sociologia, a psicologia e a administração. Até o fim da vida, em 1938, procurou manter uma postura crítica e equilibrada acerca da ciência, sua aplicação e desenvolvimento.

3.1.1.2 Heidegger

Martin Heidegger nasceu a 26 de setembro de 1889 em Messkirch, na Schwarzwald (Floresta Negra), Alemanha, e faleceu em 26 de maio de 1976, na mesma Messkirch, então parte da Alemanha Ocidental. Ainda jovem, demonstrou interesse pela filosofia, através da leitura do filósofo católico do final do século XIX, Franz Brentano. De seu estudo inicial de Brentano procede também seu entusiasmo pelos gregos, especialmente os pré-Socráticos. Após terminar os estudos básicos, Heidegger entrou para a ordem dos jesuítas. Como noviço, estudou a escolástica e a teologia tomista, na universidade de Freiburg.

Em sua primeira e mais conhecida obra, "*Ser e tempo*", de 1962, Heidegger aborda a Fenomenologia a partir da forma rotineira e ordinária, porém subconsciente, pela qual os indivíduos experimentam o mundo, sendo este processo o seu "modo de ser" (*way of being*) (MINGERS, 2001).

Para Heidegger (1988), o mundo é sempre formado de possibilidades e não somente de realidade, e a compreensão humana revela modos de ser em profusão. Somos o que nos tornamos ao encontrarmos a possibilidade que realmente ocorre. Isso influencia o estado da mente, o que nos leva a novas possibilidades. O estado da mente e a compreensão são inteligíveis sempre que podem ser articulados ou expressos em forma de discurso – que é parte do processo de criação de estados da mente compartilhados.

Dentre as contribuições de Heidegger para a Fenomenologia, o entendimento da cognição como uma ação engajada, a partir da visão de que o homem é auto-consciente e tem seu modo de ser caracterizado exatamente por sua forma de experimentar o mundo, diferenciou-o de Husserl, que percebia a cognição como pensamento puro. Outra preocupação denotada em "Ser e tempo" refere-se ao ser humano enquanto inserido no mundo, na coletividade, ao invés da visão individualista simples. Sobre a essência da verdade, Heidegger a defende como a liberdade de ser completo, de ser e deixar ser e sobre fenômeno, postula que "*um fenômeno é o que se mostra em si mesmo*" (MINGERS, 2001). De acordo com Vergez e Huisman (1976), Heidegger é o filósofo da ontologia, sendo o "*ser*", no sentido mais geral, mais profundo e mais oculto do termo, o tema constante de sua meditação.

As discussões de Heidegger sobre a linguagem e a comunicação levaram à formulação de vários conceitos fundamentais, tais como (MINGERS, 2001):

- A cognição e o pensamento não são funções mentais isoladas, mas se constituem em parte das atividades cotidianas, tornando-se essenciais ao ser-no-mundo;
- O conhecimento não consiste de representações de entidades objetivas independentes e concebidas nas mentes individuais; antes, cada indivíduo realiza distinções através da linguagem e no decorrer de suas interações com outros indivíduos, tendo como conseqüência a estruturação e reestruturação contínuas do mundo;
- A comunicação realizada nas interações entre indivíduos baseia-se na tradição e nas experiências pregressas, recuperadas do histórico de um complexo de agrupamentos estruturais próprios de cada indivíduo; e,
- A linguagem é a mais importante dimensão das ações do homem, mas deve ser interpretada como uma ação social através da qual o homem codifica e coordena suas realizações.

3.1.1.3 Merleau-Ponty

Maurice Merleau-Ponty, nasceu em 14 de março de 1908, em Rochefort, na França e faleceu em 4 de maio de 1961, em Paris. Estudou na Ecóle Normale Supérieure em Paris, graduando-se em filosofia em 1931. Foi professor de filosofia da Universidade de Lyon e em 1949 foi chamado a lecionar na Sorbonne, em Paris. Em 1952, ganhou a cadeira de

filosofia no *Collège de France*.

Merleau-Ponty entende a Fenomenologia como um movimento bidirecional: ao mesmo tempo que se configura como um desapegar-se do mundo, caracteriza-se como um retornar a ele. Ele preocupa-se primordialmente com a natureza da reflexão filosófica e introduz o conceito de "*embodyment*" como "*a forma real e as capacidades inatas do corpo humano*" onde a percepção consiste de ações guiadas de forma perceptiva (ou seja, a percepção de fatos anteriores influencia a percepção de fatos subseqüentes) e novas estruturas cognitivas emergem dos padrões senso-motoriais que permitem à ação ser guiada pela percepção (MERLEAU-PONTY, 1971) (MINGERS, 2001).

3.1.2 Fenomenologia e a idéia do conhecimento

A Fenomenologia é uma corrente filosófica que também estabelece uma Teoria do Conhecimento para explicar a natureza fundamental do fenômeno do conhecimento.

A figura 2, página 23, ilustra o modelo fenomenológico, destacando a correlação o entre sujeito e objeto, origem do conhecimento.

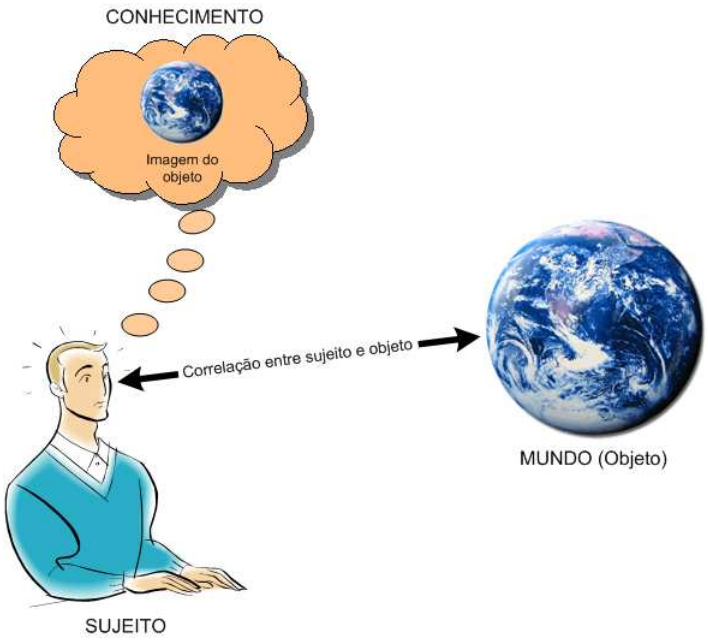

Figura 2: Modelo fenomenológico - sujeito, objeto e conhecimento (adaptado de Lima-Marques (2007))

É essencial observar e descrever com precisão aquilo a que se chama conhecimento, "*esse peculiar fenômeno de consciência*" (HESSEN, 1998).

O conhecimento surge da experiência entre o sujeito (consciência) e o objeto e

constitui-se da relação entre eles. Nesta relação, sujeito e objeto mantêm-se distintos um do outro e o dualismo "sujeito e objeto" é parte da essência do conhecimento.

Ainda segundo Hessen (1998), a relação entre sujeito e objeto é simultaneamente uma correlação. O sujeito só é sujeito para um objeto e o objeto só é objeto para um sujeito. Eles somente são o que são enquanto o são um para o outro. A função do sujeito é apreender o objeto e a função do objeto é ser apreendido pelo sujeito e assim, ser sujeito é completamente distinto de ser objeto, o que implica uma correlação não-reversível.

Pelo lado do sujeito, a apreensão do objeto é a captura das propriedades deste, que reunidas, darão origem a uma imagem do objeto. Pelo lado do objeto, o conhecimento caracteriza-se como a transferência de propriedades do objeto para o sujeito, que ocorre ao mesmo tempo em que a captura é realizada pelo sujeito. São, portanto, captura (sujeito) e transferência (objeto) de propriedades, aspectos distintos do mesmo fenômeno (HESSEN, 1998).

Pela perspectiva da Fenomenologia, o conhecimento surge, então, da relação entre sujeito e objeto e é caracterizado pelo conjunto de propriedades do objeto apreendido pelo sujeito. Sob esse enfoque, o conhecimento consiste na imagem do objeto, ou seja, no conjunto de propriedades apreendidas pelo sujeito por meio de sua consciência cognoscente.

Considerando os três elementos principais do conhecimento, o sujeito, a imagem e o objeto, Hessen (1998) indica que é caracterizado sob três aspectos de domínio: pelo sujeito, o domínio da psicologia; pela imagem, o domínio da lógica; e pelo objeto, o domínio da ontologia.

Sob a ótica de processo psicológico num sujeito, o conhecimento é objeto da psicologia. Entretanto, verifica-se que a psicologia por si não pode resolver o problema da essência do conhecimento humano porque, ao investigar os processos do pensamento, prescinde do fenômeno de uma apreensão de um objeto pelo sujeito, que consiste, segundo a Fenomenologia, no conhecimento. Antes, a psicologia direciona seus esforços para a origem e desenvolvimento dos processos psicológicos.

Através do elemento da imagem, o conhecimento toca a esfera lógica porque a imagem do objeto é uma entidade lógica, e como tal, caracteriza-se como objeto da lógica. Também verifica-se que a lógica não pode resolver o problema da essência do conhecimento porque investiga as entidades lógicas estritamente como são, a sua arquitetura própria e as suas relações respectivas. Assim, investiga a concordância do pensamento consigo mesmo e não da sua concordância para com o objeto.

Pelo terceiro elemento do conhecimento, o objeto, o conhecimento constitui referência com a ontologia e aparece diante da consciência cognoscente como algo que é, manifestando-se como um ser ideal ou como um ser real, e portanto, como um objeto da ontologia. Por sua vez, a ontologia não é capaz de resolver o problema do conhecimento humano porque não é possível eliminar nem o objeto, nem o sujeito do conhecimento, porquanto pertencem ambos ao seu conteúdo essencial, conforme estabelece a Fenomenologia.

A constatação de que nem a psicologia, nem a lógica e nem a ontologia se qualificam individualmente para resolver o problema do conhecimento sugere que a referência do pensamento humano aos objetos, e a relação do sujeito e do objeto, constituem-se na disciplina da teoria do conhecimento, o que é corroborado pelas considerações fenomenológicas (HESSEN, 1998).

3.2 Ciência da informação

A Ciência da Informação é abordada a seguir, como uma ciência social e interdisciplinar, que estuda problemas relacionados à informação e métodos para solucionar tais problemas, inclusive apoiados por ferramental da tecnologia da informação (POPPER, 1963) (SARACEVIC, 1995) (COADIC, 2004). Neste contexto, a Ciência da Informação aparece como base para estabelecer os aspectos científicos da Arquitetura da Informação, destacadamente no que se refere à questão da estruturação, que preocupa-se com a eficiência e velocidade dos acessos à informação registrada (MACEDO, 2005).

A crescente necessidade de lidar com volumes expressivos de informações (em permanente expansão), de forma organizada, pode ser considerada como a principal responsável pela concepção da Ciência da Informação. Especialmente após o fim da Segunda Guerra Mundial, a industrialização e popularização da produção gráfica catalisaram uma explosão bibliográfica sem precedentes, ainda mais se considerarmos que as preocupações com a sistematização e com o acesso à informação são muito mais antigas, remontam a China antiga e tiveram momento marcante na civilização grega antiga (FONSECA, 1991).

Ao longo da história da humanidade, várias civilizações preocuparam-se com o registro e a organização das informações com objetivos vários: torná-la acessível e preservada, viabilizar a disseminação, sistematizar a organização, dentre outros. Entretanto, apenas nas últimas décadas o foco da organização da informação passou a ser o usuário da informação, ou seja, aquele que tem a capacidade de classificar a informação segundo sua importância

para a organização e, conseqüentemente, tirar proveito do valor dessa informação para o desempenho da organização.

Em sua obra "*Conjectures and refutations: The growth of scientific knowledge*" , Karl Popper (1963) sugeriu que a Ciência da Informação não tem como objeto de estudo nenhuma disciplina específica, mas é uma ciência que estuda problemas. Concordando com ele, Tefko Saracevic (1995) defende que a Ciência da Informação é definida pelos problemas a que se dedica e pelos métodos escolhidos para solucioná-los ao longo do tempo, e que não pode ser entendida por definições léxicas ou ontologia somente.

Saracevic apresenta ainda três características gerais e fundamentais para a existência da Ciência da Informação(SARACEVIC, 1995):

1. A Ciência da Informação é interdisciplinar por natureza, mas as relações com as várias disciplinas estão mudando no tempo;

2. A Ciência da Informação está inexoravelmente conectada à tecnologia da informação; e,

3. A Ciência da Informação é um participante ativo na evolução da sociedade da informação.

Vannevar Bush (1945), numa visão além do seu tempo, em 1945, definiu o problema da explosão informacional e da necessidade de tornar os dados acessíveis e disponíveis: "*a massiva tarefa de tornar mais acessível um caótico universo de conhecimento*'. Segundo Bush, a solução para combater o problema passava pela aplicação da emergente tecnologia da informação, usando máquinas que incorporassem "*associação de idéias*" e "*processos mentais artificiais*", chamadas por Bush de "*Memex*".

Na mesma linha, Douglas Engelbart defendeu, em 1963, que o computador poderia ser uma extensão do pensamento humano em um artigo científico intitulado *"A conceptual framework"*. Em 1987, Theodore Nelson apresentou à comunidade científica o conceito de *"hipertexto"* no contexto do projeto Xanadu.

As idéias concebidas até então foram precursoras da proposta de Tim Berners-Lee, que em 1989, deu substância à *World Wide Web*, um marco na popularização do acesso à informação e responsável direta pelo aprofundamento do problema da explosão informacional e conseqüente aumento na preocupação com a sistematização e com o acesso ao conhecimento envolvendo muito mais significativamente a figura do usuário. Mais que

um conceito, a *World Wide Web* surgiu como um fenômeno revolucionário e alavancou inúmeras pesquisas que têm resultado em inovações importantes, especialmente nas áreas de organização e recuperação da informação.

Memex nunca se tornou realidade, mas muitas pesquisas têm sido desenvolvidas com o objetivo de tratar o problema do "*caótico universo de conhecimento*" (BUSH, 1945). A explosão informacional tem sido objeto de estudos da Ciência da Informação e de várias outras ciências como a Comunicação, a Ciência da Computação, a Psicologia, as ciências sociais, cada qual envidando esforços específicos sobre o problema, conforme a sua própria ótica. Essencialmente, é um problema social iniciado na ciência e propagado para todas as áreas do conhecimento humano, requerendo portanto, uma abordagem interdisciplinar no seu estudo como fenômeno. A importância estratégica da informação para a ciência e o desenvolvimento humano justifica a aplicação de esforços concentrados e recursos diversificados, incluindo largamente a tecnologia, para a tratativa do problema da explosão informacional (SARACEVIC, 1995).

Tefko Saracevic (1996) definiu a ciência da informação considerando as visões de Popper e Bush, caracterizando-a frente aos problemas que aborda, os métodos que usa para tal, a sua interdisciplinaridade e a forte conexão com a tecnologia da informação:

> "*A ciência da informação é um campo dedicado à investigação e prática profissional científicas, referenciando os problemas da efetiva comunicação e registro de conhecimento em contextos de usos sociais, institucionais e/ou individuais e de necessidades da informação. Para tanto, deve-se empregar tanto quanto possível, as modernas tecnologias da informação.*"

Rafael Capurro (2003) aponta como raízes para a Ciência da Informação: a biblioteconomia, como a ciência do estudo dos problemas relacionados com a transmissão de mensagens, e a computação, como ciência motora dos processos de produção, coleta, organização, interpretação, armazenagem, recuperação, disseminação, transformação e uso da informação .

Yves-François Le Coadic (2004) propõe que a Ciência da Informação é uma ciência social que tem por objeto o estudo das propriedades gerais da informação (natureza, gênese, efeitos), e a análise de seus processos de construção, comunicação e uso.

Sobre a recuperação da informação, Tefko Saracevic (1996) a considera como a principal atividade da Ciência da Informação e a principal fonte de relações interdisciplinares. Faz ainda uma releitura da abordagem de Clovis Mooers (1951), que sugeriu que a recuperação de informação compreende os aspectos inteligentes da descrição da informação e sua

especificação para busca, e ainda, quaisquer sistemas, técnicas ou máquinas que são empregados para esta operação. Para Saracevic, a recuperação da informação tornou-se uma atividade multi e interdisciplinar, além de um grande negócio, fonte de grande desafios e oportunidades, catalisadas pela rápida evolução dos sistemas, processos e computadores (SARACEVIC, 1996).

As questões e problemas relacionados à informação e, portanto, afeitos à Ciência da Informação, não podem ser resolvidos por uma única disciplina ou campo de estudo da ciência. O entendimento, a comunicação, a disponibilidade e a acessibilidade da informação, as manifestações, efeitos e comportamento informacional humano demandam uma diversidade de contextos e pessoas de diferentes áreas do conhecimento atuando sobre os problemas. Esta característica, que proporciona riqueza no campo de estudo, ao mesmo tempo, implica dificuldades nos processos de comunicação e educação, pela carência de unicidade nos discursos (SARACEVIC, 1995).

A Segurança da Informação, que também trata problemas específicos relacionados à informação, é um campo de estudos em desenvolvimento e tem se utilizado de ferramentas em várias áreas de conhecimento para estabelecer suas próprias definições.

A visão de João Luiz Marciano (2006) para a Segurança da Informação como um fenômeno social, mediado pela figura do usuário e caracterizado pelo equilíbrio entre o conhecimento dos recursos informacionais (incluindo aí a própria informação, seu significado e seu valor) e os riscos decorrentes da construção, comunicação e uso da informação, sugere que a Segurança da Informação pode ser estudada nos domínios da Ciência da Informação que está inserida no campo da ciência social aplicada.

3.3 Arquitetura da informação

Richard Wurman (1991) definiu, em 1975, o termo "arquitetura da informação" como a "*ciência e a arte de criar instruções para espaços organizados*". Sua visão projetava a Arquitetura da Informação como uma expansão da profissão da arquitetura aplicada a espaços informacionais. O papel do arquiteto da informação seria levantar as necessidades de informação, organizar as informações em um padrão coerente com sua natureza e interações, e projetar estruturas de informação para atender as necessidades levantadas. Assim, Wurman definiu "arquiteto da informação" como o indivíduo capaz de :

– Organizar padrões próprios aos dados, evidenciando sua complexidade;

- Criar estruturas de informações que viabilizem a busca pessoal do conhecimento para os indivíduos; e,
- Estabelecer princípios sistêmicos, estruturais e ordenados para promover a funcionalidade do acesso à informação.

Samantha Bailey (2003) define a Arquitetura da Informação como "*a arte e a ciência de estruturar e organizar sistemas de informação para ajudar pessoas a alcançarem seus objetivos*" e defende que o papel de um arquiteto da informação é organizar conteúdos e projetar sistemas de navegação para ajudar pessoas a encontrar e gerenciar a informação.

Para Iain Barker (2005), "*arquitetura da informação*" é o termo usado para descrever a estrutura de um sistema de informação, isto é, o modo como as informações são agrupadas, os métodos de navegação e a terminologia usados internamente no sistema .

Numa visão organizacional, Gilchrist e Mahon (2004) definem a Arquitetura da Informação como "*um conjunto coerente de estratégias e planos para acesso e disseminação de informações dentro de organizações, às pessoas certas e no tempo certo*" .

Sob o prisma da tecnologia da informação, Roger e Elaine Evernden definem arquitetura da informação como sendo uma visão geral sobre componentes interconectados, com relacionamentos complexos, os quais têm a finalidade de promover a organização das informações, com vistas a torná-las gerenciáveis de forma estruturada. Eles consideram como objetivo maior da Arquitetura da Informação buscar uma profunda compreensão dos princípios e dimensões que fundamentam o uso da informação (EVERNDEN; EVERNDEN, 2003).

Escrevendo especificamente sobre a construção de sítios na Web, Rosenfeld e Morville (2006) definiram a Arquitetura da Informação das seguintes maneiras:

- A combinação de organização, rotulação, e esquemas de navegação internos a um sistema de informação;
- O projeto estrutural de um espaço informacional para facilitar a realização de tarefas e o acesso intuitivo a conteúdos;
- A arte e a ciência de estruturar e classificar sítios Web e *intranets* para ajudar indivíduos a localizar e gerenciar informação; e,
- Uma disciplina e comunidade de práticas emergentes concentradas em implementar princípios de desenho e arquitetura no contexto digital.

Na visão de Fabiana Straioto (2002), a Arquitetura da Informação é o estudo dos elementos que compõem a estrutura de um sítio ou portal quanto à organização das informações, navegação, rotulagem, busca, conteúdo das informações, usabilidade e tipos de documento. Ou ainda, pode ser definida como o desenho das informações como textos, imagens e sons e a classificação dessas informações em agrupamentos de acordo com os objetivos do sítio e as necessidades dos usuários.

Segundo Flávia Macedo (2005), a significação da Arquitetura da Informação tem sido freqüentemente realizada segundo escopos limitados à Web, provavelmente por ser um ambiente que concentra grande parte dos problemas informacionais da atualidade.

Em sua dissertação de mestrado, Flávia Macedo construiu sua definição para a arquitetura da informação (MACEDO, 2005):

> "*Arquitetura da informação é uma metodologia de desenho que se aplica a qualquer ambiente informacional, sendo este compreendido como um espaço localizado em um contexto; constituído por conteúdos em fluxo; que serve a uma comunidade de usuários. A finalidade da arquitetura da informação é, portanto, viabilizar o fluxo efetivo de informações por meio do desenho de ambientes informacionais*".

Esta definição é importante porque alinha a Arquitetura da Informação aos contextos informacionais das organizações, enquanto comunidade de usuários que compartilham da mesma cultura organizacional, e sujeitas a um mesmo conjunto de princípios, origem dos aspectos normativos das organizações.

Esta característica é chave para a estruturação de um modelo normativo em cadeia, tal qual é proposto neste trabalho. A Arquitetura da Informação, enquanto viabilizadora do fluxo efetivo de informações de um ambiente, proporciona a existência de uma cadeia normativa em fluxo, que percorre todas as instâncias de decisão da organização, ou seja, os seus níveis estratégico, tático e operacional.

De modo particular, a Arquitetura da Informação também viabiliza a cadeia normativa para a segurança da informação através das instâncias de decisão da organização porque esta ocorre em fluxo, está aplicada a um contexto informacional e é constituída de conteúdos específicos de regulamentação.

Assim, a contribuição da Arquitetura da Informação para este trabalho concentra-se ao validar o modelo de conteúdos em fluxo num contexto organizacional que a cadeia normativa da segurança da informação se propõe a ser.

3.4 Políticas e políticas de informação

A grafia *politikê*, da raiz etimológica do termo "*política*" tem o significado de "*ciência dos negócios do Estado; a administração pública*". Nos dias atuais, o termo é empregado em diversos sentidos, navegando do significado original a variações como "*astúcia, capacidade de relacionar-se para obtenção de resultados*", passando por "*cortesia e urbanidade*" (HOUAISS, 2000).

No contexto de "*arte ou ciência de governar*", encontramos o termo política aplicado a "*orientação ou método político*", significando o conjunto dos comportamentos voltados a atingir fins específicos em uma determinada área administrativa. Neste sentido, não se limita mais à figura do Estado, antes, assume livremente um lugar no âmbito organizacional e passa a designar os comportamentos das áreas específicas, como por exemplo, política de inclusão social, política de recursos humanos, política de tecnologia, dentre outras "*políticas*".

Ainda nesta linha, as políticas situam-se no contexto decisório coletivo das instituições, figurando entre os níveis constitucional e operacional ou individual (KAY, 2005).

No ciclo de vida das políticas, têm papel preponderante as redes políticas, que descrevem a sistemática de atuação dos agentes políticos, complexa especialmente por não estar contida em um método bem controlado, nem tampouco produzir modelos estáticos ou inspirar confiavelmente outras políticas. Assim, as redes políticas permitem a análise de formas de interação não-hierárquica entre os atores públicos e privados na construção das políticas (BÖORZEL, 1998), permitindo inclusive a análise de alguns tipos de relações humanas (CASTELLS, 2003).

Apesar de as interações entre os atores políticos apresentarem-se vinculadas à formulação de políticas, parece ser ambígua a relação de causalidade, podendo as interações aparecerem como causadoras das políticas, ao mesmo tempo em que se pode entender que as interações entre os atores políticos são ocasionadas pela existência das políticas (MARCIANO, 2006).

A relevância do papel dos atores no fenômeno social das políticas indica a adoção da definição de Marciano (2006):

> "*Uma política é uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido. Nestes termos, é um fenômeno eminentemente social e como tal deve ser compreendido*".

Para Theodor Lowi (1964), a política pode ser classificada e deve assumir um dos quatro tipos básicos:

- **políticas distributivas** – basicamente são decisões tomadas pelo governo, que desconsideram a limitação de recursos e produzem impactos localizados ao privilegiar determinados grupos sociais ou regiões, em detrimento do todo;
- **políticas regulatórias** – visam à regulamentação e controle de atividades e envolvem burocracia, políticos e grupos de interesse, requerendo alta especialização para sua formulação e implementação. Os benefícios deste tipo de política demonstram-se mais lentamente;
- **políticas redistributivas** – afetam um número maior de indivíduos, proporcionando expectativa de ganhos para certos grupos sociais e perdas concretas e imediatas para outros grupos, visando à modificação da distribuição de recursos existentes; e,
- **políticas constitutivas** – lidam com procedimentos e são destinadas ao tratamento de bens comuns e não renováveis.

Dentre as possibilidades de políticas, as políticas de informação podem ser destacadas pela importância do contexto da sociedade da informação. Adequadas abordagens para a coleta, armazenamento, disseminação, tratamento e descarte da informação são considerados diferenciais enquanto permeiam as demais políticas e mesmo as relações sociais, conferindo-lhes visibilidade, compreensão, capacidade de penetração, viabilidade de discussão e maturação no seio dos ambientes em que são aplicadas. É importante observar o vigor que somente a informação pode proporcionar às políticas em termos de comunicação, o que confirma a relevância das políticas de informação.

De acordo com Rubens Ferreira, no campo das políticas públicas, no qual a informação tem papel essencial, cabe aos governos de todos os níveis desenvolver as políticas de informação. De natureza peculiar, as políticas de informação referem-se às diretrizes e ações estratégicas capazes de orientar o uso eficaz desse recurso no campo da cultura, da política e da economia na sociedade da informação de acordo com os novos paradigmas, tais como a descentralização de processos, otimização de custos, participação social direta nas decisões políticas e gestão dos serviços públicos, bem como o livre acesso do cidadão à informação pública (FERREIRA, 2003).

Segundo Marciano (2006) e Lima-Marques (2006), uma definição razoável para "*política de informação*" é a seguinte:

> "*Uma política de informação é uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido voltada à caracterização, ao delineamento e à definição de condutas orientadas à utilização da informação como ativo transformador da sociedade*".

Das políticas de informação são derivadas as políticas de segurança da informação que serão tratadas na sessão própria sobre segurança da informação neste trabalho.

3.5 Segurança da informação

Desde que a informação passou a ser considerada um ativo com significado de negócio e valor mensurável para as organizações, o conceito de segurança da informação tornou-se importante, comumente relacionado às ações de preservação e proteção do bem informação contra ameaças de roubo, destruição, adulteração, acesso e uso indevido, e indisponibilidade.

Segundo a norma NBR ISO/IEC 17799 (*Código de prática para a gestão da segurança da informação*) (ABNT, 2000):

> "*A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e conseqüentemente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio*" .

Nos primórdios da sociedade que percebeu o valor da informação e que desenvolveu mecanismos para manuseá-la, também se desenvolveram técnicas de segurança pontuais para a informação, aplicadas à medida do seu significado em cada contexto, atendendo a demandas isoladas e específicas.

O estudo sistemático da informação, a Ciência da Informação, é fruto da história de formação das instituições, dos conhecimentos científicos, do desenvolvimento de técnicas e desenvolvimento dos indivíduos, do advento da teoria da informação e da história da documentação e da própria informação. Diferentemente das ciências mais antigas que amadureceram ao longo de centenas e milhares de anos, a Ciência da Informação venceu sua pré-história e tornou-se adulta em cerca de trinta anos (COADIC, 2004). Pode-se

dizer que a Ciência da Informação começou a tomar forma a partir da década de 1930 e que alcançou o patamar de ciência na segunda metade do século passado. Mais que isso, pode-se afirmar que a Ciência da Informação é uma ciência em permanente evolução, movida pela explosão informacional prevista por Bush e pela sociedade da informação e do conhecimento.

Com a Ciência da Informação, foi possível estruturar a maneira de estudar a informação, seu ciclo de vida, as técnicas para manuseio e sustentação do ciclo informacional. Foram abertas as possibilidades para o desenvolvimento organizado de várias disciplinas laterais, como a Comunicação e a Segurança da Informação.

A Segurança da Informação, como disciplina estruturada, é recente, está em consolidação, e freqüentemente ainda é vista como um conjunto de técnicas associadas a suportes tecnológicos. Este paradigma costuma ofuscar uma concepção mais holística, mais social, mais fenomenológica para a Segurança da Informação e desagua em um desenvolvimento relativamente desordenado da disciplina: muito se pesquisa e se investe em ferramentas e técnicas aplicadas de segurança da informação e pouco se fala nas raízes e nos aspectos humanos deste fenômeno.

A despeito desse desequilíbrio, tem-se percebido muitas contribuições importantes para a Segurança da Informação, em um grande esforço por sistematizar o conhecimento deste campo, organizar as idéias e torná-las acessíveis aos atores envolvidos nos processos informacionais, quais sejam as pessoas que produzem, manipulam, recebem, disseminam e utilizam a informação.

Confirmando a hipótese acima, podem ser encontradas muitas abordagens para a Segurança da Informação na literatura e grande parte delas se restringe a contemplar os aspectos técnicos ou tecnológicos da segurança da informação, ignorando ou omitindo-se de tratá-la como um fenômeno social.

Rita Summers (1997), num contexto essencialmente tecnológico, vê a Segurança da Informação como uma componente conjugada ao uso de computadores e considera que a segurança da informação é uma meta a ser atingida – proteger os sistemas computacionais contra ameaças à confidencialidade, à integridade e à disponibilidade.

Marcos Sêmola (2003) define a Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, contra alterações indevidas ou contra sua indisponibilidade. Apesar de entender a Segurança da Informação como "*área do conhecimento*", restringe seu objeto à proteção de ativos infor-

macionais, ou seja, da própria informação e dos instrumentos de suporte à informação, não contemplando as relações sociais envolvidas nos fenômenos informacionais.

Cláudia Dias (2000) propõe a segurança da informação como:

> "*...a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança*".

Basicamente na mesma linha que Sêmola, Dias já inclui componentes humanos em sua definição, representados por expressões tais como "*serviços*", "*erros*", "*manipulação não autorizada*", mas limita-se aos aspectos interativos voltados à produção e uso da informação, reduzindo o componente humano a uma proposta normativa.

A visão de José Carlos Martins (2003), ao tratar da gestão de projetos em segurança da informação, é que esta se sustenta em três pilares: a integridade, a confidencialidade e a disponibilidade da informação. Contudo, não apresenta uma definição objetiva para o termo "*segurança da informação*" e deixa abertas as possibilidades de entendimento do conceito, sem uma linha de orientação claramente definida.

De acordo com Tom Peltier (2001), a Segurança da Informação compreende o uso de controles de acesso físicos e lógicos para os dados, de modo a garantir o uso apropriado desses dados e impedir modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou acesso aos registros e arquivos manual ou automaticamente, bem como perdas, danos ou mau uso dos ativos informacionais.

Para George McDaniel (1994), a Segurança da Informação é o conjunto de conceitos, técnicas, medidas técnicas e administrativas usadas para proteger os ativos informacionais contra obtenção, dano, revelação, manipulação, modificação, perda ou uso não autorizados, deliberada ou inadvertidamente.

A norma NBR ISO/IEC 17799 define a Segurança da Informação em três vertentes: "*o que ela faz*", "*o que a caracteriza*" e "*o que deve ser feito para obtê-la*", conforme abaixo em ABNT (2000):

- ***O que a segurança da informação faz*** – "A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio";
- ***O que caracteriza a segurança da informação*** – "A segurança da informação é aqui caracterizada pela preservação de: a) confidencialidade: garan-

tia de que a informação é acessível somente por pessoas autorizadas a terem acesso; b) integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento; c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário"; e,

– ***O que deve ser feito para obter a segurança da informação*** – "Segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software".

Roger Clarke (2001), do *Australian Defence Signals Directorate* (DSD), define a Segurança da Informação como a combinação de segurança em comunicações, segurança computacional e segurança de irradiação (emissões realizadas por dispositivos como monitores e impressoras).

Um ponto comum das definições anteriormente apresentadas é que são abrangentes, englobam várias atividades que eventualmente colaboram com a Segurança da Informação, mas que não parecem refletir a sua essência. Em geral, relacionam atividades que a Segurança da Informação objetivamente realiza, mas não dão significado a o que a Segurança da Informação efetivamente é.

Numa visão ontológica de John Searle (1995), "*objetivo*" e "*subjetivo*" aparecem como predicados de entidades e tipos de entidades, e a elas associam modos de existência. A partir de seu raciocínio, implementações em segurança da informação relacionadas aos suportes tecnológicos, por exemplo, podem ser consideradas ontologicamente objetivas porque seu modo de existência é independente de qualquer percepção ou estado mental. Em contrapartida, os significados e valores das informações a serem protegidas, assumem um papel ontologicamente subjetivo porque o seu modo de existência depende de ser percebido pelos sujeitos.

A percepção de que a Segurança da Informação não pode ser reduzida a um contexto objetivo, ou ainda, que não pode ser definida como um conjunto de funções, tem conduzido o tema à reflexão, à busca por uma definição em melhor concordância com a realidade social proposta pelo advento da sociedade da informação.

James Anderson (2003), em seu artigo "*Why we need a new definition of information security*", sugere que o equilíbrio entre riscos (subjetivos) e controles (objetivos), percebido através de uma convicção bem fundamentada de segurança (subjetiva) é uma definição

razoável para a Segurança da Informação. Esta visão é uma resposta aos clamores por uma definição melhor equilibrada para a Segurança da Informação e uma evolução significativa no entendimento da sua abrangência, introduzindo definitivamente o componente humano na definição de segurança da informação.

João Luiz Marciano (2006), também defendendo equilíbrio entre as visões objetiva e subjetiva da Segurança da Informação, propôs uma definição social para a Segurança da Informação, em que traz para o nível cognitivo dos usuários da informação a concepção do fenômeno da segurança, relacionando a este usuário a capacidade de uso dos recursos informacionais (incluídos aí a própria informação e os suportes):

> "*Segurança da informação é um fenômeno social no qual os usuários dos recursos informacionais têm razoável conhecimento sobre o uso destes recursos, incluindo os ônus decorrentes, bem como sobre os papéis que devem desempenhar no exercício deste uso*".

Para o desenvolvimento deste trabalho, serão consideradas as definições de Anderson e Marciano, sendo esta última fundamental para as definições a serem propostas.

3.5.1 Políticas de segurança da informação

Não é comum encontrar definições elaboradas para políticas de segurança da informação. Normalmente, as políticas de segurança são associadas um arcabouço de regulamentação orientado a subsidiar decisões cotidianas que envolvem a segurança das informações nas organizações.

O homem, razão de ser das políticas de segurança, normalmente não aparece nas definições correntes ou, eventualmente, figura como mero cumpridor das regras estabelecidas, sem nenhuma relação de experiência que seja capaz de afetar ou colaborar com a segurança da informação. As definições a seguir confirmam esta assertiva.

Segundo Dias (2000):

> "*A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos*".

Martins (2003) subsidia-se na obra "*Writing Information Security Policies*", de Scott Barman, para definir política de segurança da informação como:

> "*...um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade*".

Para Summers (1997), uma política de segurança da informação é um conjunto de leis, regras e práticas que regulamentam como a organização gerencia, protege e distribui a informação para atingir seus objetivos de segurança.

Fonseca (1991) define política de segurança da informação como o conjunto de diretrizes que deve expressar o pensamento da alta administração da organização em relação ao uso da informação por todos aqueles que têm acesso a esse bem.

Alguns autores, ao definir as políticas de segurança da informação, consideram os usuários como parte de um processo de construção de políticas, ou ainda, como uma entidade a quem se atribuem responsabilidades bem definidas no contexto das políticas.

Na visão de Sêmola (2003), a política de segurança é o dispositivo que estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida, pela e para a empresa. Ele ainda compara o grau de importância da política de segurança de uma organização ao grau de importância da Carta Magna para uma nação.

Tom Peltier (1998) descreve a política de segurança como um conjunto de diretivas originadas da alta gerência, que propõem a criação de um programa de segurança da informação, o estabelecimento de suas metas, métricas e alvos, e a associação de responsabilidades.

Várias dificuldades na implementação e cumprimento de políticas de segurança da informação organizacionais sugerem que seus modelos conceituais não são tão ajustados quanto precisariam ser. Percebe-se que pelo menos uma parte deste problema pode ser atribuída à conceituação e visão da segurança da informação e das políticas de segurança da informação adotadas nessas organizações.

Um papel mais efetivo para o usuário também tem sido reclamado na construção de novas definições para a política de segurança da informação, e cada vez mais é questionado o significado de uma política de segurança da informação que não considere os usuários de informação como protagonistas.

Marciano (2006) define assim a política de segurança da informação:

> "*Política de segurança da informação é um conjunto de regras, dispostas como diretrizes, normas e procedimentos que regulam como a informação*

> *sensível, assim classificada pela organização, bem como os recursos e usuários que com ela interagem, devem ser gerenciados e protegidos. Todo o ciclo de vida da informação deve ser objeto da política*" .

A definição de Marciano introduz vários componentes à política de segurança da informação, usualmente não contemplados nas definições tradicionais. Considera, por exemplo, que além da informação propriamente dita, a política deve se preocupar com todo o ciclo informacional, colocando os recursos e usuários que interagem com a informação como atores e objetos a serem gerenciados e protegidos.

A inclusão do usuário na definição de política de segurança da informação, em um nível de importância mais próximo da própria informação e os recursos de interação, inova e traz várias implicações sociais para a segurança da informação. Comportamento, interatividade, interesses, questões éticas e culturais, dentre outras componentes, passam a contribuir ou influenciar as políticas de segurança da informação das organizações.

Neste trabalho, consideraremos esta última definição como base para o desenvolvimento das contribuições.

3.5.2 Normas e padrões internacionais

3.5.2.1 NBR ISO / IEC 17799 - Código de prática para a gestão de segurança da informação

A norma NBR ISO / IEC 17799 é a tradução brasileira para a norma internacional ISO / IEC 17799, elaborada como uma adaptação da primeira parte da norma britânica BS 7799. Basicamente, a norma define um conjunto de boas práticas para a gestão de segurança da informação.

Em sua parte inicial, a NBR ISO / IEC 17799 versa sobre conceitos básicos como "Segurança da Informação", defendendo a sua importância para os negócios, e tece considerações sobre a avaliação de riscos e controles de segurança.

A norma NBR ISO/IEC 17799 considera que a regulamentação dos aspectos da segurança da informação dá-se através da política de segurança da informação, a qual define um documento que expressa orientações para prover à direção uma orientação e apoio para a segurança da informação (ABNT, 2000).

A norma também relaciona uma série de fatores de sucesso para a implementação de segurança da informação nas organizações e atribui a lista à "*experiência*" adquirida ao longo do tempo na vivência organizacional. Os fatores relacionados são os seguintes

(ABNT, 2000):

- política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;
- um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;
- comprometimento e apoio visível da direção;
- um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;
- divulgação eficiente da segurança para todos os gestores e funcionários;
- distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;
- proporcionar educação e treinamento adequados;
- um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

Devem ser destacados os itens referentes a políticas de segurança da informação, cultura organizacional e diretrizes e normas, que serão abordados neste trabalho. Tal destaque se deve à contribuição desses elementos na construção deste trabalho, especificamente no desenvolvimento da cadeia normativa.

As colocações dispostas pela norma NBR ISO / IEC 17799, embora dissociadas umas das outras, sugerem que existe a percepção, em nível de melhores práticas normatizadas internacionalmente, sobre a importância desses elementos para a segurança da informação, ainda que, pela norma, a Segurança da Informação não seja considerada um fenômeno social.

O objetivo da norma NBR ISO / IEC 17799, descrito em seu corpo é (ABNT, 2000):

> "*prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações*".

Com base nesse espírito, a norma referida enuncia, ao longo de seus capítulos, recomendações sobre "*o que*" deve ser considerado na realização de segurança da informação, sem entretanto detalhar o percurso de implementação para cada um dos itens. Em linhas gerais, norma NBR ISO / IEC 17799 versa recomendações sobre os seguintes temas:

- Política de segurança da informação;
- Segurança organizacional;
- Classificação e controle dos ativos de informação;
- Segurança em pessoas;
- Segurança física e do ambiente;
- Gerenciamento das operações e comunicações;
- Controle de acesso;
- Desenvolvimento e manutenção de sistemas;
- Gestão da continuidade do negócio;
- Conformidade.

A principal contribuição da norma NBR ISO / IEC 17799 para as organizações é apontar uma série de aspectos que devem ser tratados em termos de segurança, sobre a informação e os recursos informacionais. A partir dessa indicação, foi possível às organizações, dar um primeiro passo e alinhar sua visão sobre o que é importante proteger em termos de recursos de informação.

A norma NBR ISO / IEC 17799 tem sido usada extensivamente pelas organizações, através de trabalhos de consultoria externa ou interna, para iniciar seus programas de segurança da informação, apoiar programas existentes, ou ainda redirecionar os princípios das organizações relacionados à proteção da informação.

Apesar deste benefício proporcionado, a norma em tela enfrenta resistências em muitas organizações, porquanto postula recomendações gerais, e não refletem a cultura de segurança da informação existente nessas organizações, nem tampouco o nível cultural informacional que a organização pretende alcançar a partir da execução de seus planejamentos estratégicos, estes sim, teoricamente comprometidos com a realidade existencial

da organização. Mesmo assim, ao se prestar ao papel de referencial para a segurança da informação das organizações, a norma NBR ISO / IEC 17799 tem representado um avanço para a Segurança da Informação e tem despertado a intenção e a realização de novas pesquisas para construção dos conceitos da área.

A norma NBR ISO / IEC 17799 tem sido usada freqüentemente em conjunto com outros padrões e normas internacionais para o estabelecimento de governança em tecnologia da informação (TI) e apoio às práticas gerenciais no que concerne à Segurança da Informação (CALDER; WATKINS, 2006).

3.5.2.2 NBR ISO / IEC 27001 - Requisitos para um sistema de gerenciamento de segurança da informação

A norma NBR ISO 27001:2005 é a tradução brasileira da norma internacional ISO/IEC 27001, que por sua vez, é uma adaptação revisada da norma britânica BS7799-2:2002, que trata da definição de requisitos para um sistema de gestão de segurança da informação. Na adaptação, o padrão foi incorporado pela *The International Organization for Standardization (ISO)*, que cuida do estabelecimento de padrões internacionais de certificação em diversas áreas (ABNT, 2005).

As mudanças mais relevantes na migração para norma ISO/IEC 27001 ocorreram na estrutura do sistema de gestão de segurança da informação (SGSI), quando são destacados aspectos de auditoria interna e indicadores de desempenho do sistema de gestão de segurança e passou a incluir uma seção sobre gestão de incidentes de segurança da informação.

ISO 27001 é o padrão formal para o qual as organizações podem buscar certificação independente de seus sistemas de gerenciamento de segurança da informação, que deverão conter estruturas para projetar, implementar, gerenciar, manter e implantar processos de segurança da informação e controles sistemáticos e consistentes nas organizações (CALDER; WATKINS, 2006).

Os termos do padrão oferecem cobertura a todos os tipos de organizações. Ele especifica os requerimentos para o estabelecimento, implementação, operação, monitoração, revisão manutenção e aperfeiçoamento de um sistema de gerenciamento de segurança da informação, documentado em um contexto dos processos genéricos de gerenciamento de riscos da organização. Especifica requerimentos para a implementação de controles de segurança ajustáveis para as necessidades individuais de cada organização (ISO27001, 2006).

ISO 27001 provê um modelo de sistema de gerenciamento de segurança da informação para adequar e proporcionar controles de segurança que protejam os ativos de segurança e inspirem confiança para as partes interessadas.

Segundo o sítio ISO 27001 Security, o comitê SC27 da ISO responsável pela família 27000 dos padrões ISO/IEC considera que a norma ISO 27001 "*é direcionada a ser apropriada para várias finalidades de uso*", tais quais (ISO27001, 2006):

- Formulação de requerimentos de segurança e objetivos;
- Garantia de que os riscos de segurança estão gerenciados em termos de custos efetivos;
- Garantia de aderência a leis e regulamentações oficiais;
- Estrutura para implementação de processos e gerenciamento de controles para garantir que os objetivos de segurança específicos de uma organização estejam alinhados;
- Definição de novos processos de gerenciamento de segurança da informação;
- Identificação e compreensão de processos existentes de gerenciamento de segurança da informação;
- Determinação do nível das atividades de gerenciamento de segurança da informação da organização;
- Demonstração para auditorias internas e externas das políticas de segurança, diretrizes e padrões adotados pela organização e determinação do grau de aderência da organização àquelas políticas, diretrizes e padrões;
- Provimento de informações relevantes sobre as políticas de segurança, diretrizes, padrões e procedimentos de parceiros de negócio e outras organizações que interagem com a organização por razões operacionais ou comerciais;
- Implementação de segurança da informação para viabilização de negócios; e,
- Provimento de informações relevantes sobre a segurança da informação para os clientes.

3.5.2.3 COBIT - Control objectives for information and related technology

Control Objectives for Information and Related Technology (COBIT) é uma metodologia de governança de tecnologia da informação (TI) que estrutura o conhecimento e boas práticas existentes em metodologias e normas correlatas, e sua aplicação permite que se construa uma ponte entre as exigências do controle, questões técnicas e os riscos do negócio.

Segundo Weill e Ross (2004), é preciso primeiramente entender a maneira como a organização decide as suas questões estratégicas de TI, e somente então implementar ou adaptar os objetivos de controle de COBIT. Assim, estes objetivos poderão auxiliar o entendimento de como está a maturidade dos processos que suportam o planejamento e a organização de TI, e permitirão avaliar a efetividade dos controles existentes.

COBIT pode ser considerado um padrão aberto de controles de tecnologia da informação (TI) e segurança, e consiste de seis componentes: sumário executivo, linhas de conduta de gerenciamento, objetivos de controle, arcabouço COBIT (*framework*), linhas de conduta de auditoria e conjunto de ferramentas de implementação. A proposta de COBIT é ser, ao mesmo tempo, pragmático e compreensivo frente às necessidades dos negócios, mantendo-se dissociado de plataformas de TI adotadas pelas organizações (MICROSOFT, 2005).

Segundo o *COBIT Steering Committee*, a missão de COBIT é pesquisar, desenvolver, publicar e promover um conjunto internacional, confiável e atualizado de objetivos de controle sobre tecnologia da informação geralmente aceitos para uso cotidiano de gestores e auditores (COBIT, 2000).

Um dos princípios de concepção de COBIT é conviver com outros padrões na área de controles para sistemas de informação e apoiar-se neles para a construção de seus próprios controles. Dentre os padrões identificados como inspiradores para COBIT, podem ser relacionados (COBIT, 2000):

- Padrões técnicos ISO (*International Organization for Standardization*), EDIFACT (*Eletronic Data Interchange For Administration, Commerce and Transport*), etc.;
- Códigos de conduta publicados pelo Council of Europe, OECD (*Organisation for Economic Co-operation and Development*), ISACA (*Information Systems Audit and Control Association*), etc.;

- Critérios de qualificação para sistemas e processos de TI: ITSEC (*Information Technology Security Evaluation Criteria*), TCSEC (*Trusted Computer System Evaluation Criteria*), ISO 9000, SPICE (*Software Process Improvement and Capability dEtermination* - ISO 15504), TickIT, *Common Criteria*, etc.;
- Padrões profissionais para controle interno e auditoria: COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), IFAC (*The International Federation of Accountants*), AICPA (*American Institute of Certified Public Accountants*), CICA (*Chartered Accountants of Canada*), IIA (*The Institute of Internal Auditors*), PCIE (*President's Council on Integrity and Efficiency*), GAO (*Government Auditing Standards*), etc.;
- Práticas da indústria e requerimentos de fóruns da indústria (ESF-14) e plataformas patrocinadas por governos (IBAG, NIST, DTI); e,
- Requerimentos específicos da indústria para bancos, comércio eletrônico e fabricantes em TI.

Uma premissa básica de COBIT é que, para prover as informações que a organização necessita para atingir seus objetivos, os recursos de TI precisam ser gerenciados por um conjunto de processos naturalmente agrupados.

COBIT é estruturado em quatro domínios de TI, trinta e quatro objetivos de controle gerais (e respectivos processos) e trezentos e dezoito objetivos de controle específicos, estruturados de forma consistente e integrada, cujo desdobramento é executado de forma gradual no contexto da organização (ROVAI, 2007). O mapeamento desses objetivos de controle supostamente permite realizar um sistema de controle adequado para o ambiente de TI.

Os objetivos de controle gerais de COBIT (um para cada um dos principais processos de TI) são agrupados nos quatro domínios principais, quais sejam: planejamento e organização, aquisição e implementação, distribuição (ou entrega de serviços) e suporte, e monitoração.

Os domínios de COBIT compreendem os seguintes objetivos de controle (ROVAI, 2007):

Planejamento e organização

- Plano estratégico
- Arquitetura de informação

- Organização de TI
- Investimento em TI
- Administração de recursos humanos
- Avaliação de riscos
- Administração de projetos e de qualidade

Aquisição e implementação

- Identificação de soluções
- Aquisição e manutenção de software e arquitetura de tecnologia
- Desenvolvimento e manutenção de procedimentos de TI
- Administração de mudanças

Distribuição e Suporte

- Administração de serviços próprios e de terceiros
- Serviço contínuo
- Segurança de sistemas
- Educação e treinamento de usuários
- Administração de configuração e dados
- Gerenciamento de incidentes

Monitoramento

- Monitoramento de processos e de controle interno
- Auditoria independente

Em COBIT, a conexão entre os processos e recursos de TI, a informação e os objetivos e estratégias da organização é provida por uma estrutura denominada governança de TI (*IT governance*) que tem por finalidade habilitar a organização a tirar proveito da sua informação, buscando vantagem competitiva (ISACA, 2007).

Uma evolução na cultura de gestão de TI tem sido percebida nos últimos anos com o surgimento de metodologias estruturadas que propõem a combinação de ferramentas com técnicas avançadas de gestão. A governança de TI mede a eficácia, os padrões de serviços e os níveis de riscos e, sobretudo, sugere uma nova abordagem que destaca o papel estratégico de TI na geração de valor para o negócio (WEILL; ROSS, 2004). Segundo o *IT Governance Institute*, a governança de TI trata basicamente de alinhamento e agregação de valor por parte da área de TI para o negócio, correta alocação e medição dos recursos envolvidos e mitigação de riscos em TI.

O papel estratégico da governança de TI está associado tanto às definições estruturais quanto às melhores práticas de planejamento, organização, aquisição, desenvolvimento, implantação, manutenção, suporte e administração permanente do desempenho de TI, na coordenação de projetos, processos, competências, recursos materiais e informacionais (WEILL; ROSS, 2004).

A principal estrutura de sustentação dos processos da governança de TI é COBIT, que contempla a aplicação de diversos tipos de ferramentas e técnicas avançadas em um modelo de gestão compreensivo, para atender de forma integrada às múltiplas necessidades da gestão de TI, provendo suporte aos riscos do negócio, necessidades de controle e requisitos tecnológicos (WEILL; ROSS, 2004).

Para viabilizar a auditoria dos objetivos de controle gerais, COBIT implementa o conjunto recomendado de trezentos e dezoito objetivos de controle detalhados, que servirão para certificar a organização e apontar situações que ensejem melhorias. A este conjunto dá-se o nome de guia de auditoria (*Audit guideline*) (MICROSOFT, 2005).

O guia de gerenciamento (*Management guidelines*), outra ferramenta provida por COBIT, é constituído por ações gerais e orientadas para a direção da organização, no sentido de melhorar a efetividade no controle das informações e dos processos relacionados ao negócio, monitorar a busca pelas metas organizacionais e produzir padrões de avaliação e comparação (*benchmarking*) para a organização (MICROSOFT, 2005).

Os modelos de maturidade (*Maturity models*) de COBIT têm por objetivo apoiar a gerência da organização no mapeamento indicativo sobre o estágio atual da organização,

sobre a sua posição em relação aos líderes do seu ramo de atuação e em relação aos padrões internacionais, e, sobre onde a organização quer chegar (MICROSOFT, 2005).

Os fatores críticos de sucesso (*Critical sucess factors*) definem as mais importantes linhas de conduta gerenciais a serem implementadas para obtenção de controle sobre os processos de TI e os indicadores de metas chaves (*Key goal indicators*) definem medidas que permitem verificar se um processo de TI está alcançando as requisições do negócio. Por fim, há também os indicadores de performance chaves (*Key performace indicators*) que permitem avaliar o desempenho dos processos de TI na busca dos objetivos da organização (MICROSOFT, 2005).

COBIT também disponibiliza um conjunto de ferramentas de implementação (*Implementation Tool Set*) que apresenta lições aprendidas das organizações que aplicaram COBIT com sucesso e rapidamente em seus ambientes.

A figura 3, página 49, de Cobit (2000) ilustra os domínios de COBIT e seus processos associados.

3.5.2.4 ITIL - Information technology infrastructure library

ITIL - *Information technology infrastructure library* é um conjunto de melhores práticas para a gestão de serviços em TI e para o alinhamento desta área com os negócios da organização, incluindo aspectos de segurança da informação.

ITIL era originalmente um conjunto de cerca de sessenta livros produzidos no final da década de 1980 pela companhia governamental britânica CCTA (*Central Communications and Telecom Agency*), como um conjunto de melhores práticas para tecnologia da informação (TI).

Muitos dos conceitos da disciplina gerenciamento de serviços de ITIL não se originaram do projeto inicial da agência CCTA para o desenvolvimento de ITIL. A IBM reclama que seus "*Livros amarelos*" (*Yellow books – A Management System for the Information Business*) foram os precursores de ITIL (IBM, 2003).

Desde o início, ITIL foi disponibilizado publicamente, o que fez com que fosse usado por um grande número de organizações de todos os tamanhos, tais como governos, instituições financeiras, companhias energéticas, de utilidade pública, comércio e indústria, tornando-o um padrão de fato aceito mundialmente, aprovado pela prática nas organizações.

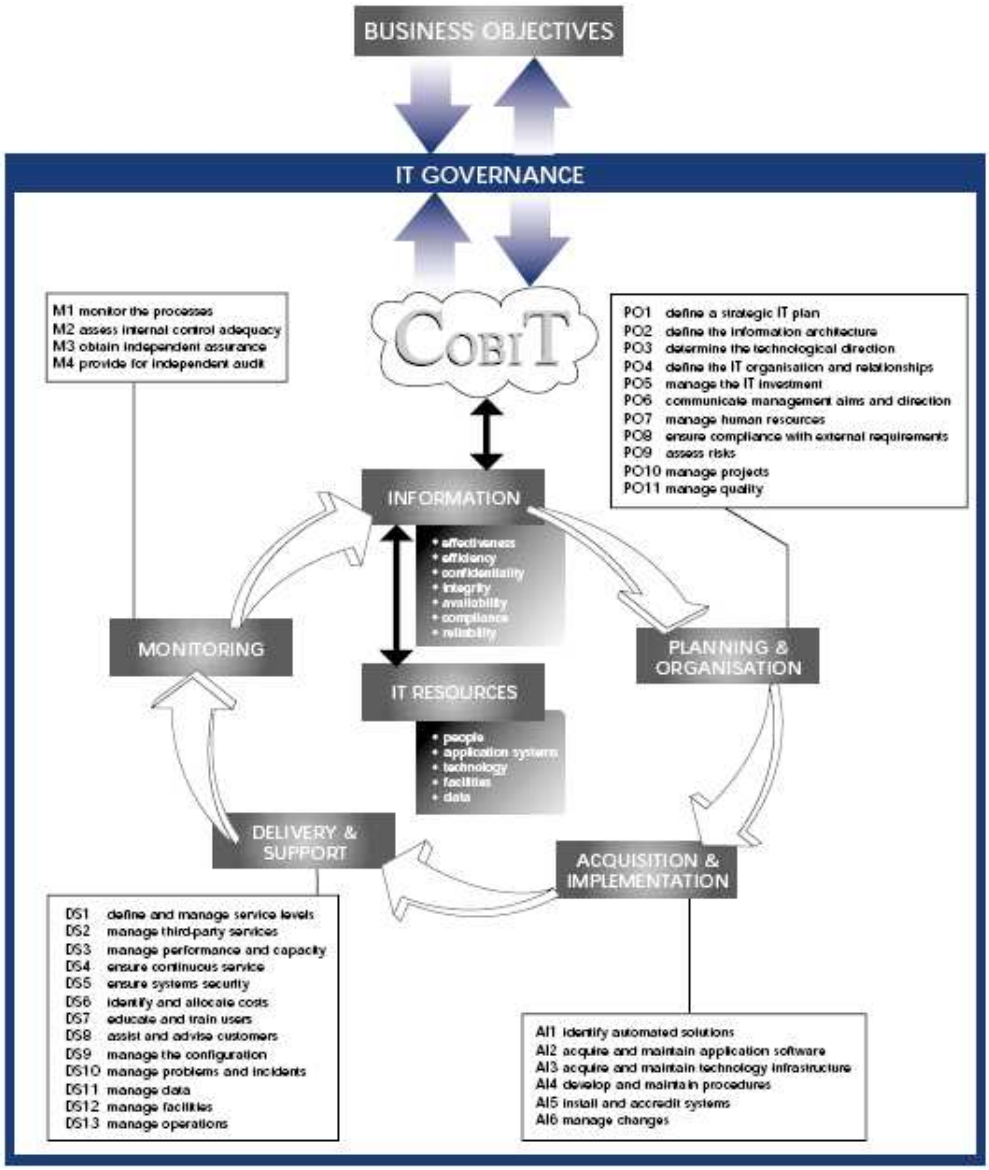

Figura 3: Domínios COBIT e seus processos (COBIT, 2000).

ITIL implementa um guia de melhores práticas da indústria. Sendo um conjunto de ferramentas e técnicas, descreve os contornos de organização do gerenciamento de serviços. O modelo apresenta as metas, as atividades gerais e as entradas e saídas de vários processos que podem integrar as organizações de TI, mas não especifica cada uma das ações que deve ser executada no cotidiano porque este aspecto diferirá de organização para organização. Assim, o foco principal de ITIL é descrever os processos necessários para gerenciar a infra-estrutura de TI eficientemente, objetivando garantir os níveis de serviços acordados com os clientes.

Embora tenha sido desenvolvido durante a década de 1980, ITIL não foi amplamente

empregado até meados dos anos 1990. Desde então, tem se destacado como um instrumento amplamente reconhecido para o suporte aos negócios de TI.

A larga adoção nos dias atuais tem levado à elaboração de vários outros padrões internacionais cobrindo partes significativas de ITIL. ITIL tem sido considerado em vários conjuntos de melhores práticas e tem sido associado fortemente com a governança de TI. É comum encontrar abordagens e metodologias para a estruturação de processos ou segurança em TI apoiadas em ITIL, COBIT e normas ISO simultaneamente (SCHAIK, 2006).

Em maio de 2007 tornou-se disponível a versão 3 de ITIL que inclui cinco contextos centrais denominados (OGC, 2005):

1. Estratégia de serviço (*Service strategy*)
2. Desenho de serviço (*Service design*)
3. Transição de serviço (*Service transition*)
4. Operação de serviço (*Service operation*)
5. Melhoria de serviço continuada (*Continual service improvement*)

A figura 4, da página 51, ilustra a estrutura da versão 3 de ITIL e seus relacionamentos com outros padrões voltados à governança em TI, tais quais as famílias ISO 17799 e 27000 e COBIT, considerados neste trabalho (OGC, 2005).

ITIL surgiu como uma coleção de livros, cada um deles cobrindo uma prática específica do Gerenciamento de serviços de TI. Depois da publicação inicial, o número de livros rapidamente cresceu para mais de trinta volumes. Com o objetivo de tornar ITIL mais acessível e economicamente viável para aqueles que desejavam explorá-lo, a versão 2 de ITIL tratou de consolidar as publicações em conjuntos lógicos que agrupavam linhas de conduta de processos inter-relacionados em diferentes aspectos do gerenciamento de TI, aplicações e serviços (WIKIPEDIA, 2006).

A versão 2 de ITIL, cujas disciplinas aparecem em integração, ilustradas pela figura 5, página 52, é composta pelos seguintes livros (OGC, 2005):

Os conjuntos de gerenciamento de serviços de TI

- Disponibilização de serviço (*Service Delivery*)

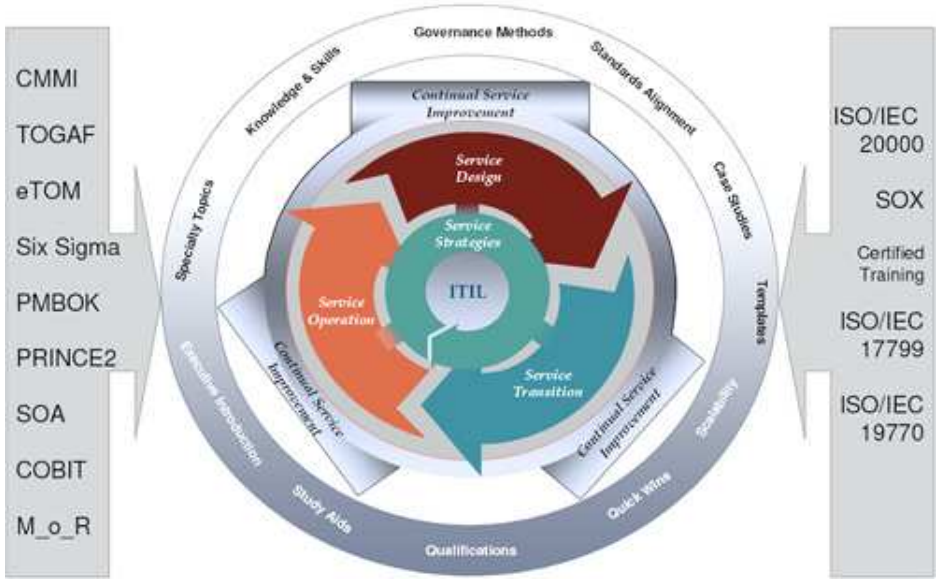

Figura 4: Versão 3 de ITIL e seus relacionamentos com outros padrões. (OGC, 2005)

– Suporte ao serviço (*Service support*)

Outros guias operacionais

– Gerenciamento de infra-estrutura de TIC (*ICT Infrastructure Management*)

– Gerenciamento de segurança (*Security Management*)

– A perspectiva do negócio (*The Business Perspective*)

– Gerenciamento de aplicação (*Application Management*)

– Gerenciamento de ativos de *software* (*Software Asset Management*).

Para acompanhar a implementação das práticas de ITIL, um livro adicional foi publicado para orientação dos processos de implementação, especialmente do gerenciamento de serviços:

– Planejamento para implementar Gerenciamento de serviços (*Planning to Implement Service Management*).

E, mais recentemente, um outro conjunto de linhas de conduta para pequenas unidades de TI foi agregado ao conjunto original de livros da versão 2:

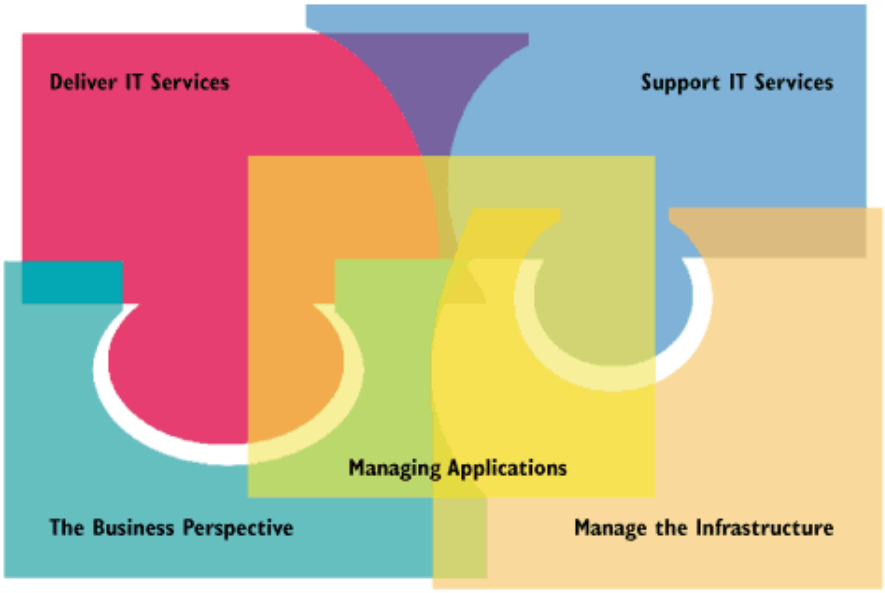

Figura 5: Disciplinas ITIL - versão 2 (OGC, 2005)

– Implementação de ITIL em pequena escala (*ITIL Small-Scale Implementation*).

Um dos principais benefícios agregados pela proposta de ITIL para a comunidade de TI foi a elaboração de um vocabulário comum para a área, suportado por um glossário de termos bem definidos e amplamente utilizados. Para a versão 3 de ITIL, um glossário novo e ampliado está sendo disponibilizado, e aparece como um recurso chave da nova versão (OGC, 2005).

Uma característica importante da biblioteca é poder ser usada sem restrições por organizações que já possuem implementados seus próprios métodos e atividades de gerenciamento de serviços, sem exigir mudanças radicais na maneira de pensar e agir da organização. Os métodos e atividades legadas precisarão apenas serem colocados em um contexto estruturado.

Outros pontos fortes de ITIL são a ênfase na relação entre processos, que permite eliminar ou pelo menos minimizar qualquer falha de comunicação e cooperação entre várias funções de TI, e o método de planejamento de processos, regras e atividades comuns, que prevê o devido referenciamento e detalha como a comunicação deve existir entre eles.

A abordagem de ITIL presta-se bem a suportar a complexidade das estruturas de TI contemporâneas à luz dos objetivos do negócio. O conjunto ITIL é composto pelos livros ITIL (núcleo), certificação, consultoria e serviços, ferramentas e *software* de suporte,

treinamento e comunidades de usuários.

Basicamente, ITIL inclui um conjunto de módulos com papéis bem definidos. Dentre os principais módulos, podem ser citados (OGC, 2005):

1. Gerenciamento de nível de serviço de TI (*IT Service Continuity Management*)
2. Gerenciamento financeiro (*Financial Management*)
3. Gerenciamento de capacidade (*Capacity Management*)
4. Gerenciamento de disponibilidade (*Availability Management*)
5. Gerenciamento de incidentes (*Incident Management*)
6. Gerenciamento de problemas (*Problem Management*)
7. Gerenciamento de configuração (*Configuration Management*)
8. Gerenciamento de mudanças (*Change Management*)
9. Gerenciamento de liberações (*Release Management*).

3.6 Planejamento estratégico

A preocupação com retorno sobre investimentos nos negócios já esteve orientada para a gestão dos ativos, para a gestão financeira e orçamentária, para a gestão dos processos, para a gestão dos clientes, e hoje, pode-se dizer que aponta para a gestão da informação. Em um futuro não muito distante, este foco poderá direcionar-se para a gestão do conhecimento, obviamente, assim que as ameaças ao retorno sobre o capital investido estiverem claramente associadas ao fluxo do conhecimento (HAVE et al., 2003).

No âmbito da administração, as definições a respeito de níveis de regulamentação das organizações na constituição dos processos administrativos não têm modelos universalmente aceitos e consolidados, sendo comumente vistos como particularidades inerentes a cada organização.

As referências pesquisadas sugerem que não existe nos processos administrativos, de forma bem definida, a divisão hierárquica ou formal entre níveis de regulamentação dos aspectos da segurança da informação, ou seja, não há uma relação de ordem, relevância ou nível de atuação consolidada entre, por exemplo, políticas, diretrizes, normas, procedimentos e regras relacionadas com segurança da informação nas organizações.

David Hampton (1990) reconhece o uso variado e inconsistente desses termos, destacando que as distinções de sua aplicação não são relevantes, mas o é o seu papel em fornecer informação orientadora de ação, expressa ou implicitada, que ajudem as pessoas na organização a se comportarem para servir à missão, aos objetivos e às estratégias da organização.

No seu texto, Hampton (1990) apresenta definições apenas para os termos "*políticas*", "*procedimentos*" e "*regras*" no escopo dos processos administrativos. Define políticas como orientações para tomada de decisão:

> "*Uma política reflete um objetivo e orienta os gerentes e funcionários em direção a esse objetivo em situações que requeiram discrição e julgamento. A função de uma política é aumentar as chances de os diferentes gerentes e funcionários fazerem escolhas semelhantes ao enfrentar, independentemente, situações similares*".

Procedimentos, ainda na visão de Hampton (1990), são métodos de se executar atividades, e regra é a simples proibição declarada de um ato ou um requisito a ser obedecido.

3.6.1 Planejamento estratégico tradicional

O planejamento estratégico é um método de organização do raciocínio próprio para subsidiar ou viabilizar os processos de tomada de decisões. Em ambientes de gestão, é freqüentemente empregado como método pelo qual a organização define a mobilização de seus recursos para alcançar determinados objetivos propostos. Nestes casos, o planejamento estratégico permite que se estabeleça um direcionamento a ser seguido pela organização, com o objetivo de se obter uma otimização na relação entre a empresa e seu ambiente.

Para Matus (1993), o ato de planejar precede e dirige a ação porque é um cálculo realizado no passado, que orienta as opções e ações no presente e que incidirá no futuro. O cálculo estratégico supõe uma relação com o outro, o que traz para o contexto do planejamento questões complexas de ordem psicológica, ética e política.

Conforme Oliveira (2005), o planejamento pode ser conceituado como um processo estruturado e desenvolvido, que tem por objetivo o alcance de uma situação futura desejada, de um modo mais eficiente, eficaz e efetivo, com a melhor concentração de esforços e recursos pela organização.

O planejamento estratégico corresponde ao estabelecimento de um conjunto de providências a serem tomadas pelo executivo para a situação em que o futuro tende a ser diferente do passado e a um exercício mental executado pela empresa independentemente de vontade específica de seus executivos.

Ainda segundo Oliveira (2005), o planejamento estratégico pressupõe a necessidade de um instituto decisório que ocorrerá antes, durante e depois de sua elaboração e implementação na organização, permeando e encaminhando cada passo desse planejamento. Para o autor, o exercício sistemático do planejamento tende a reduzir as incertezas nas decisões e provocar o aumento das chances de sucesso no alcance de objetivos, desafios e metas da organização.

Frente a esta consideração e refletindo no grande número de variáveis e condicionantes organizacionais que influenciam na operacionalização do planejamento estratégico, e também na mutabilidade e relações de interdependência próprias do ambiente das organizações, é razoável admitir que o planejamento estratégico apresenta-se como um processo complexo, que não se estabelece linearmente. Antes, tem no contexto de cada organização o conjunto de fatores determinantes para sua realização, distribuídos em graus variáveis e decorrentes das pressões internas e externas que recaem sobre a organização.

Outras considerações importantes sobre o planejamento estratégico refletem e reforçam o aspecto da complexidade abordado acima (OLIVEIRA, 2005):

- O planejamento não é um ato isolado, mas é um conjunto de ações inter-relacionadas e interdependentes, em busca de objetivos previamente estabelecidos;
- O planejamento refere-se a decisões presentes que implicarão em conseqüências no futuro; e,
- O planejamento é mais importante que o plano resultado do planejamento porque o plano depende da abordagem utilizada no planejamento.

O planejamento estratégico relaciona-se com objetivos de longo prazo e com estratégias e ações para alcançá-los que afetam a organização como um todo, diferentemente de outros planejamentos, como tático e operacional, que podem focar objetivos de curto prazo e envolver apenas uma parte ou algumas partes da organização. Em geral, pode-se ilustrar a relação entre os tipos de planejamento de uma organização e os níveis de decisão através do gráfico da figura 6, da página 56 (OLIVEIRA, 2005).

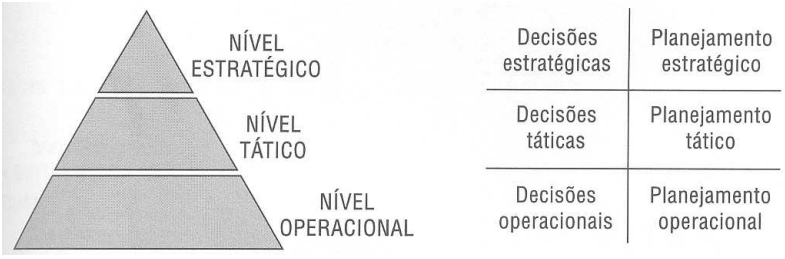

Figura 6: Níveis de decisão e tipos de planejamento (OLIVEIRA, 2005)

Considerando o planejamento estratégico como um processo administrativo que proporciona sustentação metodológica para o estabelecimento da direção a ser seguida, deve ser realizado nos níveis superiores da hierarquia funcional da organização, apontando para a formulação de objetivos e para a seleção dos cursos de ação a serem seguidos para a consecução desses objetivos, respeitando as características singulares e premissas da organização.

A relevância do planejamento estratégico para a organização está sustentada basicamente sobre as expectativas lançadas sobre ele. Este conjunto de expectativas pode ser sintetizado pelos seguintes itens (OLIVEIRA, 2005):

- Conhecer e utilizar racionalmente seus pontos fortes;
- Conhecer e mitigar seus pontos fracos;
- Conhecer e usufruir as oportunidades externas;
- Conhecer e evitar as ameaças externas;
- Ter um efetivo plano de trabalho que estabeleça as premissas básicas da organização, as expectativas de cenário objetivadas, os caminhos para alcançar os resultados esperados, a situação de cada um dos planos de ação e os critérios de alocação de recursos.

A elaboração e implementação podem ser estruturadas em quatro fases básicas: diagnóstico estratégico, missão da empresa, instrumentos prescritivos e quantitativos, e controle e avaliação, conforme o esquema da figura 7, da página 57, de Oliveira (2005).

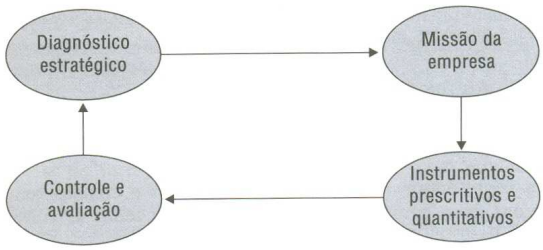

Figura 7: Fases do planejamento estratégico (OLIVEIRA, 2005)

3.6.1.1 Diagnóstico estratégico

Esta fase é caracterizada pela determinação da realidade do estado atual da organização dos pontos de vista interno e externo e pode ser dividida em cinco etapas básicas: identificação da visão, identificação dos valores, análise externa, análise interna e análise dos concorrentes.

Na identificação da visão, levantam-se quais são as expectativas dos gestores, dos conselheiros, dos acionistas, dos patrocinadores e empreendedores em relação à própria organização.

Segundo Oliveira (2005) a "*visão*", pode ser entendida como o que a organização pretende ser no futuro próximo ou distante. É delimitada pelo alcance da visão dos principais responsáveis pela organização e será a base do delineamento do planejamento estratégico a ser desenvolvido e implementado.

Na etapa de identificação de valores, identifica-se o conjunto de princípios e crenças fundamentais incorporados na cultura organizacional que sustentam as principais decisões que orientam a condução da organização.

O mapeamento adequado dos valores propriamente ditos e o entendimento de como esses valores permeiam o ambiente da organização tem peso significativo na qualidade do planejamento estratégico a ser elaborado.

A análise externa objetiva identificar as oportunidades e ameaças associadas ao ambiente em que está inserida a organização e indicar as maneiras de usufruir ou evitar esses elementos externos, que podem ser sociais, econômicos, políticos, culturais, legais, ecológicos, tecnológicos, geográficos, infra-estruturais, dentre outros.

A análise interna apura os pontos fortes, fracos e neutros da organização. Os objetivos são: convergir as estratégias de atuação às áreas em que a organização se destaca positi-

vamente, colocar sob observação os pontos de atuação considerados neutros, e desenvolver as competências necessárias para reverter os pontos fracos detectados.

Apesar de poder ser considerado um caso particular da análise externa, a análise dos concorrentes deve concentrar-se na identificação das vantagens competitivas dos concorrentes em comparação com aquelas da própria organização. Para que esta avaliação seja feita adequadamente, é importante que se faça uma análise interna e externa dos principais concorrentes, primando pela qualidade das informações a serem obtidas.

3.6.1.2 Missão da empresa

Esta fase caracteriza-se pelo estabelecimento da razão de ser da organização e do seu viés estratégico. Para tanto, além do estabelecimento propriamente dito da missão da organização, são realizados o estabelecimento dos propósitos atuais e potenciais, a estruturação e debate dos cenários futuros, o estabelecimento da postura estratégica da organização frente ao seu ambiente delineado pelo diagnóstico estratégico, e o estabelecimento das macroestratégias e macropolíticas (OLIVEIRA, 2005).

Por macroestratégias, entendem-se as grandes ações a serem adotados pela organização para interagir e produzir vantagens competitivas com o seu ambiente. Macropolíticas são as orientações corporativas que sustentarão as decisões principais que a organização precisará tomar ao interagir com seu ambiente.

3.6.1.3 Instrumentos prescritivos e quantitativos

Os instrumentos prescritivos determinam o que deve ser feito pela organização para que se oriente no rumo da sua missão, dotado da postura estratégica estabelecida, em conformidade com as macropolíticas e em consonância com as macroestratégias. A definição de instrumentos prescritivos inclui o estabelecimento de objetivos, desafios e metas, de estratégias e políticas funcionais, e de projetos e planos de ação.

Os instrumentos quantitativos realizam o balizamento econômico e financeiro dos planos de ação e projetos frente ao planejamento orçamentário da organização. São considerados e mensurados aqui os recursos necessários para execução e as expectativas de retorno para cada investimento e acomodados à realidade orçamentária da organização (OLIVEIRA, 2005).

3.6.1.4 Controle e avaliação

Nesta fase, verifica-se o andamento das ações planejadas e o que precisa ser encaminhado para que tudo corra conforme planejado em termos de objetivos, desafios, metas, projetos ações e estratégias.

Para realizar controle e avaliação, são aplicados indicadores e avaliação de desempenho, análise comparativa do planejado frente ao realizado, análise de desvios e alterações necessárias no planejamento. É também nesta fase que são elaboradas, aplicadas e avaliadas as ações corretivas para saneamento de possíveis desvios detectados pela avaliação e controle (OLIVEIRA, 2005).

3.6.2 Planejamento estratégico situacional

Planejamento estratégico situacional é o cálculo permanente que precede, preside e segue a ação orientada à solução de problemas e a obter êxito na busca de um objetivo pretendido.

A implementação de planejamento estratégico situacional envolve, além de fatores econômicos, questões relacionadas ao poder, e por isso, inclui a necessidade de formular estratégias para viabilizar os fatores necessários à ação, de forma dinâmica e flexível.

O planejamento estratégico situacional é estratégico por admitir opositores, o que requer a formulação de estratégias para conseguir o apoio necessário para sua viabilização e é situacional porque centraliza sua análise, propostas e ação, preponderantemente na situação, baseado na certeza de que para alterar a projeção do futuro indesejável, tem que se atuar no presente.

Dentre as características essenciais do planejamento estratégico situacional, destacam-se a possibilidade de acesso fácil a todas as suas etapas porquanto pressupõe a existência de registro dessas etapas, e a possibilidade de participação e contribuição dos colaboradores no planejamento, o que os torna co-responsáveis pela execução (MATUS, 1993).

O planejamento estratégico situacional é constituído por três características principais: o subjetivismo, a elaboração de planos-proposta a partir de problemas e a incerteza do futuro.

O subjetivismo tem por objetivo identificar e analisar os problemas e tem foco nos atores envolvidos, nos seus conceitos e percepções. É um pressuposto que cada ator é único, com seu conjunto particular de competências, e que sua visão sobre os problemas

é diretamente dependente de seus conhecimentos, experiências, crenças, posição no jogo social.

Considerando que as ações dos atores surgem do significado atribuído a cada situação, a maneira de agir também é variável porque o significado dado a cada situação muda de indivíduo para indivíduo. O planejamento estratégico situacional, então, defende que não se pode planejar como se o planejador fosse o único ator, não se pode desconsiderar os demais envolvidos ou predeterminar seus comportamentos futuros (MATUS, 1993).

Como segunda característica do planejamento estratégico situacional tem-se a elaboração de planos-proposta realizada a partir do mapeamento de problemas, que se denotam como as barreiras existentes entre a realidade atual do jogo social e a situação desejada, conscientemente alcançável pelo planejador.

O planejamento estratégico situacional também assume que o futuro não é previsível, e não compartilha de uma visão determinista do mundo. Antes, enumera as possibilidades e capacita os atores para enfrentá-las, objetivando que o futuro seja efetivamente influenciado. Segundo Carlos Matus (1993):

> "*O planejamento estratégico situacional é, na verdade, uma ferramenta de liberdade, pois, ao não se basear na capacidade de predição, mas na de previsão, se constitui em um cálculo que precede e preside a ação para criar o futuro, dependendo, portanto, das possibilidades de os atores serem capazes de imaginar e descobrir e da qualidade dos planos desenvolvidos*".

Ao considerar a subjetividade e a incerteza sobre o futuro, o planejamento estratégico situacional aumenta a complexidade para o tratamento de problemas e do planejamento, mas as diferentes perspectivas e o alto nível de detalhamento que passam a compor cada problemática passam a ser fundamentais para o sua abordagem e solução (MATUS, 1997).

Carlos Matus (1993) tece dez considerações chaves para o planejamento estratégico situacional, que delineiam as suas principais características, quais sejam:

1. "*Planeja quem governa*" - o planejamento é um comportamento vinculado à condição de execução dos planos, quaisquer que sejam as alçadas de governança;

2. "*A planificação refere-se ao presente*" - tudo que se planeja tem como base a situação atual, incluídas aí todas as condições cognitivas dos atores envolvidos;

3. "*A planificação exige um cálculo situacional*";

4. "*A planificação refere-se a oportunidades e problemas reais*";
5. "*A planificação é inseparável da gerência*";
6. "*A planificação situacional é, por definição, necessariamente política*";
7. "*A planificação nunca está referida à adivinhação do futuro*";
8. "*O plano é modular*";
9. "*A planificação não é monopólio pessoal*"; e,
10. "*A planificação não domina o tempo e nem se deixa enrijecer por ele*".

Carlos Matus também elabora três advertências para os realizadores do planejamento estratégico situacional (MATUS, 1993):

1. "*Cada âmbito problemático requer um desenho particular da planificação situacional*";
2. "*Devemos entender a planificação como uma dinâmica de cálculo que precede e preside a ação, que não cessa nunca, como processo contínuo que acompanha a realidade mutável*"; e,
3. "*Não dispomos de uma ciência social suficientemente sólida para acertar na análise causal das conseqüências das decisões que tomamos*".

3.6.2.1 Cálculo situacional

De acordo com Carlos Matus (1993), "*O planejamento é uma organização para a ação; o planejamento situacional baseia-se em idéias, porém, se concretiza em soluções*".

O planejamento estratégico situacional é o resultado de uma mediação entre o conhecimento e a ação, onde em três momentos importa a acumulação de conhecimentos antes da ação: identificação e seleção de problemas, sua explicação situacional, planos por problemas com cenários, planos de contingência, análise de confiabilidade do plano e análise estratégica.

Ainda segundo Matus (1993):

> "*O conceito de momento indica instância, ocasião, circunstância ou conjuntura pela qual passa um processo contínuo, ou em cadeia, que não tem*

> *começo nem fim definidos. A passagem do processo de planejamento por um momento determinado é apenas o domínio transitório deste momento sobre os outros, que sempre estão presentes. No caso do processo de planejamento, os momentos encadeiam-se e formam circuitos repetitivos para ajudarem-se mutuamente e passar sempre a um momento distinto*" .

A figura 8, página 62, ilustra a relação entre os momentos do cálculo situacional.

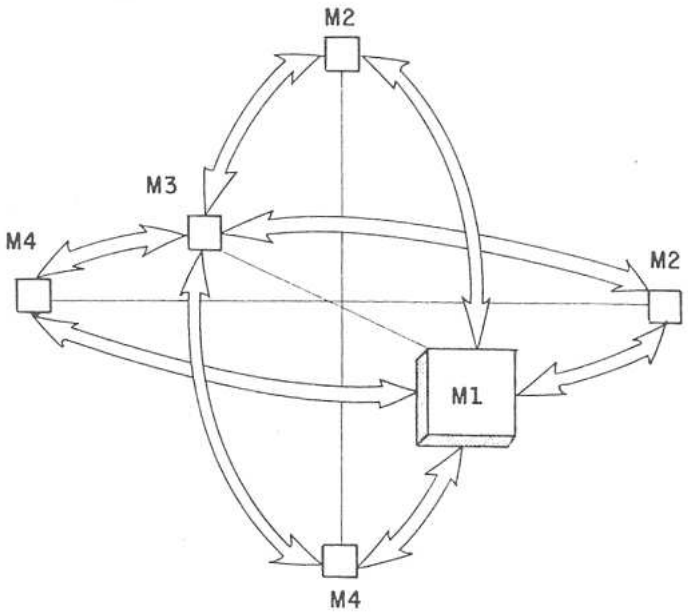

Figura 8: Momentos do cálculo situacional (MATUS, 1993)

3.6.2.2 O momento explicativo (M1)

Trata de compreender e explicar a realidade identificando os problemas que envolvem os atores sociais. Está situado nas seguintes questões: "*como foi*", "*como é*", "*como chegamos a esta situação*" e "*como tende a ser*". Realiza o diagnóstico da situação inicial, a análise situacional, o levantamento dos problemas existentes e de suas causas e priorização dos problemas a serem abordados. Começa com a enumeração e seleção dos problemas, a análise do problema em nível macro, a identificação dos atores relevantes e termina com a explicação sistêmica de cada problema pelo diagrama situacional. A partir desta análise, constrói-se a árvore explicativa e selecionam-se os nós críticos de cada problema (MATUS, 1993) (MATUS, 1997) (RIEG; FILHO, 2002).

3.6.2.3 O momento normativo (M2)

Trata do modo como se formula o plano ou o saber esboçar as propostas. Aborda essencialmente a questão "*como deve ser*". Realiza o desenho do "*deve ser*", permite a retirada ou a redefinição de soluções em caso de mudanças de cenário e dimensiona soluções conforme as variáveis previsíveis, apropriando mais ou menos recursos segundo as exigências de cada situação.

Neste momento baseia-se a grande aposta do plano e todas as apostas parciais por problema e por nós críticos ou subproblemas. Começa com o desenho prévio das operações e a avaliação prévia das variantes, invariantes e surpresas próprias do plano global e de cada problema, a formulação de cenários e planos de contingência e orçamentação das operações exigidas em recursos econômicos (MATUS, 1993) (MATUS, 1997) (RIEG; FILHO, 2002).

3.6.2.4 O momento estratégico (M3)

Trata do modo de examinar e do processo de construção da viabilidade política do plano. Aborda a questão "*como pode ser*". Realiza a análise de viabilidade do planejamento, em dimensões administrativa, financeira, técnica, política, econômica, etc. e determina as restrições para o cumprimento do planejamento. Seu propósito é formular propostas estratégicas para tratar as operações como um processo de produção política em parte cooperativa e em parte conflitiva.

Passando pelos três momentos, apenas foi alterado o conhecimento que os atores têm sobre o problema e a realidade continua à espera da ação. Daí a importância da mediação entre o conhecimento que se acumula nos três momentos mencionados e o quarto momento da ação (MATUS, 1993) (MATUS, 1997) (RIEG; FILHO, 2002).

3.6.2.5 O momento tático/operacional (M4)

Trata da ação com o suporte do plano. Aborda essencialmente a questão "*o que fazer*" e realiza o "*saber fazer*". Tem a finalidade de criar um processo contínuo, sem rupturas, entre os três momentos anteriores e a ação diária. Trata também de recalcular o plano e de aprimorá-lo de acordo com as circunstâncias do momento da ação e do detalhe operacional que a prática exige.

As idéias do plano não se executam até que se complete o seu processamento técnico

e político, com o detalhamento operacional exigido pelo sistema administrativo. Mas nem esse detalhamento produz-se espontaneamente, tampouco os gerentes estão num vazio de ação à espera dos planos. O espaço da ação está usualmente ocupado pelas rotinas, pelas urgências e pela improvisação. Assim, é necessário que exista uma demanda real por planejamento.

O drama do momento 4 é esse: não há demanda por planejamento, ninguém cobra desempenho em função dos planos, gerentes não têm tempo de planejar porque os processos de gestão pública são tão deficientes que tudo o que deveria ser normal tem que ser tocado como se fosse emergência. Nesse caso, a ação dissocia-se do planejamento. Planeja-se o que não se faz e faz-se o que não se planeja. O resultado é evidente: a acumulação angustiante de problemas e a incapacidade dos governos para manejar seu balanço de gestão pública (MATUS, 1993) (MATUS, 1997) (RIEG; FILHO, 2002).

3.7 A cultura e a comunicação organizacionais

3.7.1 Cultura organizacional

Cada organização tem um conjunto próprio de comportamentos, conhecimentos e domínio técnico refletido nas pessoas que a compõem. Estes valores, característicos de um grupo humano, são chamados por alguns autores de cultura organizacional.

Pode-se admitir que tal conjunto de valores é adquirido por meio de um processo de aprendizagem e transmitido ao conjunto de seus membros necessariamente através de processos de comunicação. Por isso, a comunicação deve ser básica entre os grupos humanos da organização para que se estabeleça e maximize a coordenação, a cooperação e se desenvolva a cultura organizacional.

Para Edgar Schein (2001), cultura organizacional é o conjunto de pressupostos básicos que um grupo inventou, descobriu ou desenvolveu ao aprender como lidar com os problemas de adaptação externa ou integração interna e que funcionaram bem o suficiente para serem considerados válidos e ensinados a novos membros como a forma correta de perceber, pensar e sentir, em relação a esses problemas.

Maria Tereza Fleury (1987) define cultura organizacional a partir da mesma concepção de Schein, mas incorpora a dimensão política inerente a este fenômeno:

> *"...um conjunto de valores e pressupostos básicos expressos em elementos simbólicos, que em sua capacidade de ordenar, atribuir significações,*

> *construir a identidade organizacional, tanto agem como elemento de comunicação e consenso, como ocultam e instrumentalizam as relações de dominação".*

Pela visão de Robert Srour (1998), a cultura organizacional é algo mais sentido e percebido, do que efetivamente declarado, assumido, comprovado. Para este autor, a cultura organizacional, por ser abstrata, só pode ser decodificada com a vivência cotidiana da organização; a cultura organizacional é a representação do imaginário simbólico; é abstrata, mas não é invisível, pois ao refletir-se no comportamento dos indivíduos, é claramente observável.

Um ponto de vista bastante aceito atualmente é o de que a cultura organizacional não é resultado exclusivo da estrutura formal da organização, mas também de uma rede informal entremeada aos aspectos convencionais e formais. Gaudêncio Torquato (1991), por exemplo, a define como:

> "*...o somatório dos inputs técnicos, administrativos, políticos, estratégicos, táticos, misturados às cargas psicossociais, que justapõem fatores humanos individuais, relacionamentos grupais, intergrupais e informais*" .

Ainda de acordo com Maria Tereza Fleury e Rosa Maria Fischer, a cultura de uma organização pode ser apreendida em vários níveis (LEME; FISCHER, 1991):

- **Nível dos artefatos visíveis**: fáceis de obter, mas difíceis de interpretar. É o ambiente construído da organização, arquitetura, layout, a maneira de as pessoas se vestirem, padrões de comportamento visíveis, documentos públicos;
- **Nível dos valores que governam o comportamento das pessoas**: valores manifestos na cultura, ou seja, expressam o que as pessoas reportam ser a razão do seu comportamento, o que na maioria das vezes são idealizações ou racionalizações;
- **Nível dos pressupostos inconscientes**: são aqueles pressupostos que determinam como os membros de um grupo percebem, pensam e sentem. À medida que um pressuposto vai se incorporando à identidade da organização, vai passando para o nível do inconsciente.

Em sua obra "*Cultura organizacional: formação, tipologias e impactos*", Maria Ester Freitas (1991) sugere que a base conceitual de cultura organizacional se firma em algumas correntes da antropologia, tais como antropologia cognitiva (está nos conhecimentos

compartilhados), antropologia simbólica (está nos significados compartilhados), e, antropologia estrutural (encontra-se nas manifestações e expressões dos processos psicológicos inconscientes).

A sociologia também tem contribuído para melhor compreender as causas e as conseqüências da cultura organizacional. Esta aproximação com a sociologia se dá principalmente quando são aplicados instrumentos e técnicas desta ciência social, como ressalta Rivera (1994):

> "*Os sociólogos aplicam entrevistas sistemáticas, questionários e outros métodos quantitativos de levantamento de dados que permitem obter tipologias claras dos atributos culturais, os quais podem ser utilizados para analisar a cultura de diferentes organizações*".

A contribuição da psicologia social, com ênfase na criação e manipulação de símbolos oferece um ambiente natural para analisar a cultura organizacional. Por exemplo, Carmen Rivera (1994) considera que:

> "*...algumas pesquisas sugerem que as pessoas tendem a fazer juízos baseados em um evento isolado, mais que em múltiplas observações que esse evento pode ter*".

A economia percebe a cultura organizacional como uma ferramenta manipulável que pode ser usada para aumentar a eficiência produtiva e os lucros financeiros das organizações.

Sob a ótica da administração, a cultura organizacional vem sendo considerada ora como uma necessidade vital das organizações, ora como modismo, tanto quanto outros paradigmas que surgem de tempos em tempos.

O entendimento das culturas organizacionais pode ser então trabalhado por várias vertentes, sob várias óticas e possibilidades. Leme e Fischer (1991) indicam alguns caminhos:

- **O histórico das organizações** – o momento de criação de uma organização e sua inserção no contexto político e econômico da época propiciam o pano de fundo necessário para compreensão da natureza da organização, suas metas, seus objetivos. O fundador neste contexto tem um papel fundamental, pois ele detém a concepção global sobre o projeto da organização e tem o poder para estruturá-la, desenvolvê-la e tecer elementos simbólicos consistentes com esta visão;

- **Os incidentes críticos por que passou a organização**, tais como crises, expansões, pontos de inflexão, de fracassos ou sucessos também são formadores de sua história. Nestes momentos, o tecido simbólico se revela mais facilmente ao pesquisador, pois certos valores importantes de serem preservados ou, pelo contrário, questionados, emergem com maior nitidez;

- **O processo de socialização de novos membros** – crucial para a reprodução do universo simbólico. É através das estratégias de integração do indivíduo à organização que os valores e comportamento vão sendo transmitidos e incorporados pelos novos membros;

- **As políticas de recursos humanos** – as políticas de recursos humanos têm papel relevante no processo de construção de identidade da organização por serem as mediadoras da relação entre capital e trabalho;

- **O processo de comunicação** – é um dos elementos essenciais no processo de criação, transmissão e cristalização do universo simbólico de uma organização. É preciso identificar os meios formais orais (contatos diretos, reuniões, telefonemas) e escritos (jornais, circulares, diretrizes) e os meios informais, como, por exemplo, a "*rádio-corredor*";

- **A organização do processo de trabalho** – a análise da organização do processo de trabalho em sua componente tecnológica e em sua componente social, como forma de gestão da força de trabalho, possibilita a identificação das categorias presentes na relação de trabalho; e,

- **As técnicas de investigação** – derivam das propostas teórico-metodológicas desenvolvidas pelos autores. Na ênfase quantitativa utiliza-se levantamento de opinião, através de questionários, escalas, entrevistas, etc. Na ênfase qualitativa utilizam-se dados secundários da própria organização (documentos, relatórios manuais de pessoal, organogramas, jornais, etc.).

Considerada a complexidade de delimitação e diversidade de abordagens para a cultura organizacional, podemos relacionar alguns problemas que transferem impacto ao gerenciamento da cultura de uma organização. Segundo Andrew Pettigrew (1996), alguns destes problemas são:

- **Problema dos níveis** – a cultura existe em uma variedade de níveis diferentes na empresa. Refere-se às crenças e pressupostos das pessoas dentro da

organização;

- **Problema da infiltração** – a cultura refere-se também aos produtos da empresa, às estruturas, aos sistemas, à missão da empresa, recompensas, socialização;
- **Problema do implícito** – é difícil modificar coisas que são implícitas no pensamento e no comportamento das pessoas;
- **Problema do impresso** – a história tem grande peso na administração presente e futura na maioria das organizações;
- **Problema do político** – refere-se às conexões entre a cultura organizacional e a distribuição do poder na empresa;
- **Problema da pluralidade** – a maioria das empresas não possui uma única cultura organizacional, podendo apresentar uma série de sub-culturas;
- **Problema da interdependência** – a cultura está interconectada não apenas com a política da empresa, mas com a estrutura, os sistemas, as pessoas e as prioridades da empresa.

De acordo com Helaine Rosa (2003), mesmo com tanta diversidade aparente nos conceitos de cultura organizacional, há alguns atributos comuns que interligam praticamente todas as correntes. Em especial, podemos destacar os seguintes aspectos:

1. Todas as definições se referem a algum conjunto de valores mantidos por indivíduos em uma organização e que o ajudaria a entendê-la e como atuar nela;
2. Os valores podem ser expressos (escritos) ou definidos implicitamente;
3. As definições possuem ênfase nos significados simbólicos através dos quais os valores são comunicados.

A cultura organizacional tem um papel importante para a realização da segurança da informação. Através do entendimento dessa cultura e do seu aprimoramento, proposto pela inclusão de valores comprometidos com a segurança da informação, torna-se possível transformar os comportamentos das pessoas da organização a respeito da maneira de lidar com as questões cotidianas relacionadas à informação organizacional.

3.7.2 O papel da comunicação na cultura organizacional

As considerações de Helaine Rosa (2003) sugerem que a cultura organizacional tem íntima conexão com a comunicação organizacional, uma vez que aquela se baseia em valores sociais que são mantidos através dos processos de comunicação. Para alguns autores, a partir de certo ponto, tornam-se sinônimas; para outros, apresentam dependências entre si, sem, entretanto, possuírem o mesmo significado.

Sidinéia Freitas (1997) respalda o pensamento de cultura organizacional como fenômeno de comunicação, ou seja, a cultura organizacional não existe sem a comunicação e vice-versa, e apóia-se em Pecanowsky e O'Donnel-Trujillo para referendar que:

> "*O comportamento comunicativo em qualquer organização investigada define a cultura organizacional que se transmite nas imagens das pessoas, objetos, nas linguagens utilizadas, enfim na cultura que é comunicação e na comunicação que é cultura*".

Para criar e manter a cultura, a rede de concepções, normas e valores devem ser afirmados e comunicados aos membros da organização de uma forma tangível, que são as formas culturais, ou seja, os ritos, rituais, mitos, histórias, gestos e artefatos (LEME; FISCHER, 1991).

O estudo da cultura organizacional surge como uma maneira de se conhecer, de forma mais profunda e abrangente, a complexidade da organização, para daí desenvolverem-se planos, programas e projetos efetivos de comunicação, integrados ao planejamento estratégico da comunicação organizacional.

Portanto, toda organização deve desenvolver um espírito crítico e ações efetivas junto ao público interno, para que este possa representá-la da melhor forma possível, uma vez que toda organização é desenvolvida e estimulada pelos indivíduos. Neste sentido, a empresa é tratada como arranjos que podem encorajar o desenvolvimento de culturas, somente por meio da comunicação.

A partir da análise da cultura organizacional, os profissionais de comunicação buscam as ferramentas para "*falar*" no mesmo nível de expectativa do público interno. Segundo Marlene Marchiori (1999):

> "*...gerou atitude, você comunicou; não gerou, você simplesmente informou. A comunicação só se efetiva a partir do momento em que o público interno entenda, deseje, aceite, participe e desempenhe um comportamento que gere a mudança proposta pela organização. A comunicação, portanto, exige credibilidade e comprometimento, tendo o poder de criar valores, impulsionando a organização para frente*".

Comunicação e cultura são fundamentais e devem ser vistas como fatores de ajuste para todo o sistema organizacional. Desta forma, a conquista da credibilidade é o caminho para a comunicação eficaz, sendo preciso observar se os funcionários estão apenas informados ou realmente comprometidos com as mensagens. A comunicação é a fase fundamental neste processo, já que, ainda segundo Marlene Marchiori (1999):

> "*...você só forma uma cultura a partir do momento em que as pessoas se relacionam e, se elas se relacionam, elas estão se comunicando, a comunicação baseia-se na compreensão*".

Compreensão, credibilidade e compromisso são conceitos confluentes sob a ótica da cultura organizacional.

A comunicação integrada vem sendo discutida há muitos anos, e segundo Margarida Kunsch (1997), este tipo de comunicação é uma "*filosofia capaz de nortear e orientar toda a comunicação, como um fator estratégico, para o desenvolvimento organizacional na sociedade globalizada*".

Para Kunsch (1997), a missão da comunicação integrada é estabelecer uma política global de comunicação para empresa, direcionando e orientando todos os setores a atingir os objetivos da organização e controlar para que os objetivos pessoais e/ou de grupos não prevaleçam sobre o objetivo final. Em outras palavras, a comunicação integrada é fundamental para determinar e conduzir os rumos da cultura organizacional.

Segundo Goldhaber, os avanços tecnológicos nem sempre são sinônimos de avanços na comunicação, pois existe um elemento indispensável e complexo para a comunicação ter sucesso: o ser humano (FERREIRA, 2005).

Thomas Davenport (2001) afirma que os recursos tecnológicos ajudaram muito no desenvolvimento das empresas, mas são infinitamente menos eficientes que os seres humanos no processo de percepção e gerenciamento de informação.

A análise das abordagens de vários autores permite inferir que tanto a cultura quanto a comunicação organizacional podem ser estudadas sob os pontos de vista de várias disciplinas. Entretanto, um ponto comum, aceito universalmente pelos mais conservadores e pelos mais inovadores, é o entendimento da forte influência que a cultura organizacional e a comunicação organizacional exercem mutuamente entre si, criando relações de conseqüência e exercendo papel mais forte ou menos intenso nas decisões, definições e até nos destinos das organizações.

A despeito da evolução das tecnologias das comunicações, o ser humano, em quem

se encontra incrustada a cultura de cada organização, é fator de equilíbrio (ou de desequilíbrio) para o processo de manutenção e condução da cultura organizacional através do tempo. A ascendência exagerada da cultura tradicional da organização (presente nos valores sociais dos seus colaboradores) nos processos de comunicação e evolução cultural da organização pode representar um obstáculo às mudanças e acomodações típicas, na sua luta pela sobrevivência, crescimento e prosperidade e ainda, à implantação de novos paradigmas evolutivos sobre a cultura pré-existente.

Por outro lado, a simples desconsideração da cultura adquirida através do tempo nos processos de comunicação, principalmente de mudanças, evoluções, realinhamentos mercadológicos etc. podem redundar em problemas de conduta, comportamentais e produtivos, dos colabores individualmente e da organização como um todo, e, conseqüentemente, produzir impactos nos planos e negócios da organização. Não raramente, é possível encontrar a situação descrita em processos de fusões e aquisições entre empresas, quando culturas organizacionais distintas serão submetidas a choques, por conta de planejamento e comunicação excessivamente lógicos, com pouca atenção para a vitalidade das culturas organizacionais envolvidas.

O aprimoramento da cultura organizacional é possível através de processos de aprendizagem alavancados pela comunicação organizacional, que deve, por sua vez, apresentar os valores de segurança da informação que se pretende agregar à cultura, associados aos valores perenes da organização. Esta concepção, trabalhada pela comunicação organizacional, fortalece a imagem da organização e viabiliza o entranhamento dos conceitos de segurança da informação.

Como resultado, os sujeitos componentes da organização passam a perceber a Segurança da Informação como um valor próprio da organização. Conseqüentemente, esta visão se refletirá genericamente nos comportamentos e processos, introduzindo as mudanças desejadas no tratamento e manuseio da informação organizacional.

4 Resultados

Observam-se comumente nas organizações, políticas de segurança da informação constituídas por declarações genéricas e pouco compreensíveis, que refletem de maneira imprecisa o que a organização considera importante para a realização da segurança da informação.

Nas organizações, a especialização dos itens das políticas de segurança da informação é objeto de regulamentação normativa, proposta por instrumentos próprios, hierarquizados física ou logicamente.

Estes dispositivos propõem-se a registrar e divulgar os ditames desdobrados dos itens maiores das políticas e, de alguma forma, encaminham as determinações dessas políticas na direção dos processos e atividades que realizarão implementações no contexto da prática dessas organizações.

A visão social da Segurança da Informação, proposta por João Luiz Marciano (2006) e adotada neste trabalho, evidencia a necessidade de se estabelecer um modelo referencial para a regulamentação normativa da segurança da informação, que contemple criteriosamente as instâncias administrativas da organização e que reflita as situações atual, ideal e almejada para a organização em seu planejamento estratégico.

Sugere-se que o modelo de regulamentação normativa entendido como necessário constitua-se de uma cadeia hierárquica relacionada às instâncias administrativas das organizações, nos níveis estratégico, tático e operacional, e sustentada pela metodologia M^3 que prevê igualmente três níveis de análise sobre o objeto (epistemológico, científico e prático), tal como é proposta a cadeia de regulamentação em tela.

Outra base de suporte para a definição de uma cadeia de regulamentação normativa hierárquica com elementos da M^3 é a Arquitetura da Informação, que, conforme as definições de Flávia Macedo (2005) também adotadas neste trabalho, apresenta componentes nos níveis da epistemologia, da ciência e da prática.

Uma pesquisa qualitativa realizada junto a organizações envolvidas com segurança da informação oferece elementos de percepção para a aplicação do modelo proposto, ao expor a cultura e vivência cotidiana daquelas organizações no campo da segurança da informação, especialmente no que diz respeito aos seus aspectos normativos.

4.1 Fenomenologia e Segurança da Informação – alguns resultados

A adoção da Fenomenologia como referencial fundamental para compreensão de conceitos estreitamente relacionados com a Segurança da Informação, como a própria *informação*, conduz a resultados que posicionam a Segurança da Informação também como um fenômeno, o que permite discutir seus aspectos e propriedades sob esta mesma abordagem.

A seguir, serão discutidos os conceitos de informação e registro sob a luz da Fenomenologia, a Segurança da Informação percebida como um fenômeno, e aspectos significativos desta percepção, que colaboram para a proposição de um modelo de cadeia de regulamentação organizacional voltada para a Segurança da Informação.

4.1.1 Informação e registro

Como objeto da Segurança da Informação, a informação deve ser compreendida e claramente definida, de modo a delimitar com precisão os contextos, formas e interações a serem tratados.

Adota-se a Teoria do Conhecimento com base na Fenomenologia como o fundamento para estabelecer a natureza do conhecimento e conseqüentemente, a natureza da informação.

Assume-se a tese de Lima-Marques (2007), conseqüência desta abordagem, que "*a informação possui caráter ontológico*" e, portanto, pertence ao domínio da ontologia e é considerada como substância.

Derivado da abordagem fenomenológica, segundo Lima-Marques (2007), ao materializar o conhecimento, surge a informação em forma de registro. O registro é uma variante lingüística condicionada pelo grau de formalidade existente na situação em que se dá o ato da fala ou o ato da escrita. Na língua falada, podem distinguir-se os registros oratório, formal, coloquial tenso, coloquial distenso e familiar. Na linguagem escrita, os registros podem ser literário, formal, informal, pessoal. A figura 9, página 74, ilustra esta definição.

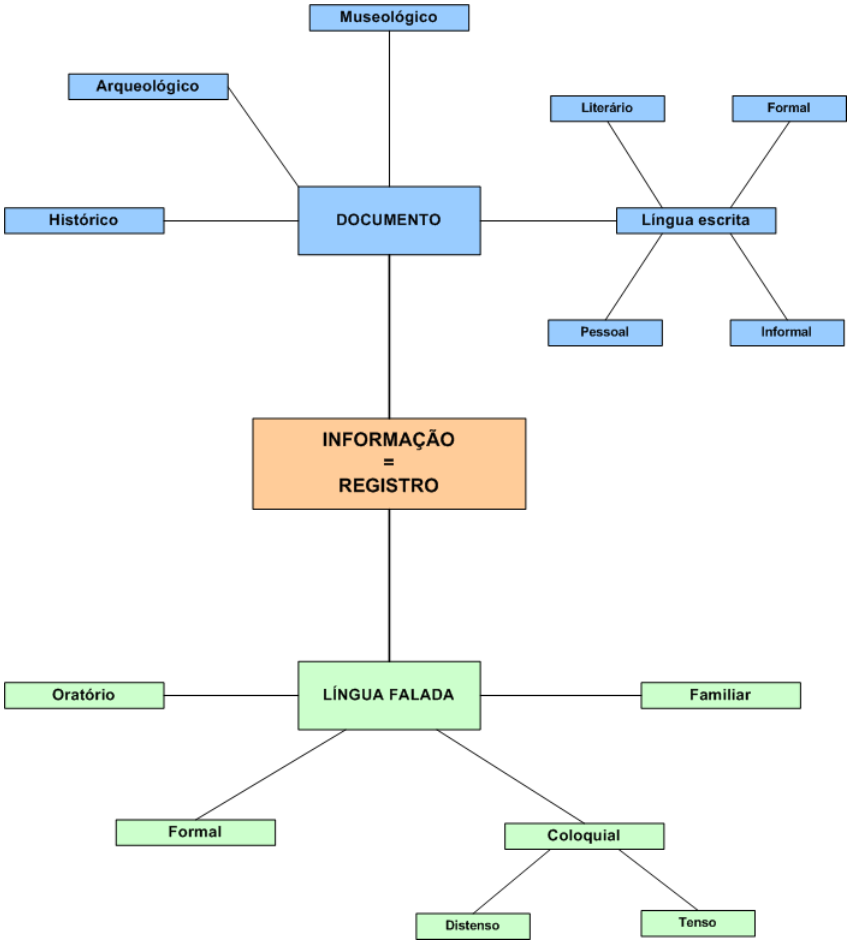

Figura 9: A informação como o registro (Lima-Marques (2007))

4.1.2 A Segurança da Informação como fenômeno

A Segurança da Informação pode ser entendida como um fenômeno que se estabelece a partir de uma interação entre o usuário (sujeito) e a informação (objeto).

A essência do fenômeno da Segurança da Informação é oferecer proteção à informação, nos aspectos de integridade, disponibilidade e confidencialidade, na medida que é atribuído valor à informação como uma propriedade.

Entretanto, a propriedade de *valor da informação* não é inerente ao seu conteúdo em si. A avaliação externa deste conteúdo, conforme um determinado contexto, por um determinado sujeito, é que estabelece o valor da informação para o qual a segurança deverá "*aparecer*".

Em outras palavras, a informação somente assume um valor específico no momento em que é percebida por um usuário. Este a classifica conforme suas experiências acumuladas no tempo, por interações anteriores e conhecimento construído em relacionamentos com

informações de mesma natureza, ou de natureza similar, num contexto bem delimitado, tal qual sugere ser a comunidade organizacional. A percepção de si mesmo e do mundo, bem como a atribuição de valores a elementos desse mundo (informação, por exemplo) é um fenômeno informacional, ao mesmo tempo influenciando e sendo influenciado pelo contexto em que se encontra o usuário (WERSIG, 1993).

Aparentemente, valores semelhantes podem ser atribuídos por usuários distintos a uma mesma informação, desde que que tenham acumuladas experiências semelhantes com informações de mesma natureza, pertençam a um mesmo contexto informacional e sejam influenciados de maneira semelhante. Esta constatação sugere que seja relevante o aspecto da influência do contexto informacional sobre a cultura organizacional e conseqüentemente sobre o fenômeno da segurança da informação. Ela tenderá a "*aparecer*" e determinar a proteção adequada de uma maneira uniforme ao longo dos processos informacionais organizacionais que reconhecem ou compartilham de um mesmo conjunto de símbolos e significados.

Uma abordagem social para a Segurança da Informação preocupa-se em ajustar a importância atribuída ao usuário (sujeito) no fenômeno da segurança da informação, aprimorando o entendimento que este sujeito deve ter em relação aos recursos informacionais. Isto inclui o valor das informações e as possibilidades de manuseio desta informação. Conseqüentemente, a segurança da informação ocorrerá somente no contexto onde o sujeito faz-se presente, e por isto é caracterizada como um fenômeno social.

Entretanto, para guiar as experiências dos usuários nos contextos informacionais, no sentido de realizar a segurança da informação, faz-se necessário um referencial de regulamentação que atue nas instâncias de decisão da organização, ou seja, que esteja comprometido com as tomadas de decisões dos níveis estratégico, tático e operacional organizacionais.

A necessidade de um referencial de regulamentação que atue sobre as instâncias decisórias se justifica pela importância, para a organização, de viabilizar a tomada de decisões equilibradas, alinhadas aos objetivos fundamentais em segurança da informação da organização, e de modo razoavelmente previsível. Isto é possível se o referencial para regulamentar as decisões, em todos os níveis, estiver consistentemente baseado nos princípios organizacionais e contemplando a estratégia, a tática e a prática organizacionais.

Parte deste referencial é inerente às próprias origens e objetivos básicos da organização e é representada pelos *princípios* da organização, do qual devem ser derivadas as políticas no nível estratégico e, por conseguinte, outros elementos de regulamentação para os níveis

tático e operacional, como será visto neste trabalho.

4.2 Parte I - Modelo de cadeia normativa da segurança da informação

Apresentam-se nesta seção os resultados da primeira parte do trabalho em conformidade com os procedimentos definidos no percurso metodológico, seção 2.4.

4.2.1 Cadeia normativa organizacional

Uma cadeia é uma seqüência de elementos conectados, onde cada elemento tem o seu papel bem definido e colabora ou cria condições para que os elementos seguintes desempenhem seus próprios papéis. Isoladamente, cada um dos elementos de uma cadeia pode ter um significado próprio, mas enquanto colaborador com outros elementos, o seu papel de integração destaca-se pela importância para o conjunto dos elementos e de suas funcionalidades.

Uma cadeia de regulamentação organizacional é formada por elementos de natureza normativa, que dispõem sobre comportamentos, cada qual exercendo foco sobre uma determinada instância administrativa e que, em conjunto, definirão os aspectos normativos organizacionais necessários para o desempenho administrativo global da organização.

O relacionamento entre os níveis de uma cadeia normativa organizacional é hierárquico, onde cada um dos elementos dos níveis tem seu próprio papel, mas depende ou recebe orientação do nível superior, e alimenta os níveis seguintes na seqüência hierárquica.

Uma cadeia normativa no contexto organizacional propõe níveis de regulamentação em conformidade com os níveis de decisão da organização e com os tipos de planejamento estratégico organizacional, quando associam a abrangência dos níveis administrativos às características dos elementos dos níveis da própria cadeia.

Os contextos de decisão das organizações considerados neste trabalho foram o nível estratégico, o nível tático e o nível operacional. Assim, deverá haver elementos da cadeia normativa em cada um desses níveis para regulamentar as decisões relacionadas, conforme a figura 10, página 77, que apresenta uma proposta de cadeia normativa genérica para as organizações.

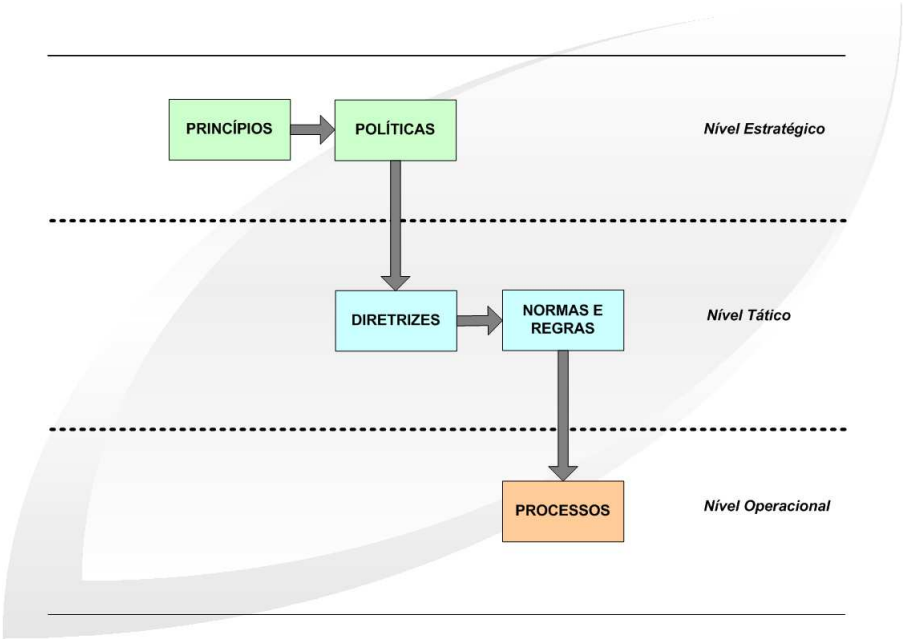

Figura 10: Cadeia normativa genérica para as organizações

No nível estratégico, originam-se as decisões, objetivos, desafios e metas principais das organizações. De acordo com a metodologia M^3 utilizada neste trabalho, é também o nível epistemológico e de fundamentos das organizações.

Neste nível, conforme o diagrama da figura 10, página 77, aparecem *princípios* e *políticas* como elementos de regulamentação.

Os princípios, como sugere o termo, constituem o início da cadeia normativa e podem ser representados por proposições elementares e fundamentais que servem de base a toda orientação normativa organizacional. Por exemplo, no contexto de Estado, pode estabelecer-se uma relação de semelhança entre os princípios organizacionais e princípios nacionais, declarados no documento constitucional.

As políticas, como elemento de regulamentação da cadeia proposta, estão enquadradas na definição de Marciano (2006):

> "*Uma política é uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido. Nestes termos, é um fenômeno eminentemente social e como tal deve ser compreendido.*"

As políticas, neste contexto, são linhas de conduta procedentes dos princípios que regem a existência das organizações, e completam os elementos da cadeia associados ao nível de decisão estratégico.

O nível tático compreende a previsão, descrição e explicação para os problemas e respectivas soluções no contexto organizacional. De acordo com a M^3, é o nível relacionado à ciência e à informação.

O diagrama da figura 10, página 77, apresenta como elementos do nível tático da cadeia normativa as *diretrizes* e as *normas* ou *regras*.

A seguinte definição foi formulada para diretriz:

DEFINIÇÃO 4.2.1 *Diretriz é uma linha mestra, derivada de uma política e orientada por um objetivo de governança, que define um modelo comportamental para a tomada de decisões, conferindo-lhes maior previsibilidade e equilíbrio.*

De acordo com a definição 4.2.1, as diretrizes são derivadas das políticas, elementos do nível estratégico da cadeia normativa estabelecidos acima, e como tal, são orientadas por objetivos de governança das organizações.

Por objetivos de governança entendem-se os alvos pretendidos e estabelecidos pela direção da organização, considerados como marcos de implementação dos itens das políticas da organização. Tais alvos determinam controles objetivos que permitem avaliar o desempenho das ações que colaboram na afirmação das políticas organizacionais.

Atuando no nível tático, as diretrizes estabelecem as orientações pertinentes das políticas, determinando padrões de comportamento apropriados para as tomadas de decisões, de modo que estas sejam dotadas de equilíbrio consistente com as políticas e princípios das organizações.

Ainda, os ditames comportamentais das diretrizes colaboram para que as decisões sejam encaminhadas dentro de um escopo previsto e em plena conformidade com as estratégias organizacionais.

Para *norma*, foi elaborada a seguinte definição:

DEFINIÇÃO 4.2.2 *Norma é uma prescrição fundamentada em uma diretriz e que tem por objetivo regulamentar processos, evidenciando a permissibilidade dos comportamentos sociais associados.*

Estabelecidas no nível tático de decisão das organizações, as normas, conforme a definição 4.2.1 e como parte da cadeia normativa, são submissas às diretrizes e têm o

papel de regulamentar processos, determinando que comportamentos sociais são válidos em cada um dos processos organizacionais.

No diagrama da figura 10, página 77, o elemento referente a normas indica agrupamento com o termo *regras*. Isto ocorre porque no contexto da cadeia proposta, normas e regras apresentam equivalência semântica e partilham da mesma definição apresentada acima.

O nível operacional de decisão organizacional, ou nível da prática conforme a metodologia M^3, abrange a aplicação efetiva dos modelos, teorias, técnicas e tecnologias desenvolvidos nos demais níveis para a solução dos problemas reais.

O diagrama da figura 10, página 77, apresenta como elemento do nível operacional da cadeia normativa a entidade *processos*.

Para *processos organizacionais*, adaptou-se a definição de Lima-Marques e Duarte (2007):

> DEFINIÇÃO 4.2.3 "*Processo organizacional é uma série de atividades alinhadas às prescrições normativas organizacionais, que formam uma cadeia de agregação de valores a partir de um insumo recebido (entrada), gerando um produto final (saída) componente do ciclo operacional da organização*".

Como uma série de atividades voltadas à solução de problemas, os processos constituem o ponto final da cadeia normativa da organização, sendo orientados pelas normas organizacionais na realização de seus objetivos, instituindo de forma estruturada o "*como fazer*" das organizações e colaborando na agregação de valor dos produtos organizacionais.

A existência e aplicação de uma cadeia normativa organizacional tal qual é proposta neste trabalho afeta o desempenho organizacional enquanto determina diretamente as instâncias em que cada elemento normativo deverá atuar, de onde cada elemento receberá sua orientação e para que outros elementos um determinado elemento servirá de orientação. Esta característica permite que os aspectos normativos posicionem-se organizados e os elementos normativos mantenham-se atuando em um escopo administrativo ajustado e previamente estabelecido.

Outro aspecto importante que pode ser observado como um dos benefícios da cadeia normativa organizacional proposta é o seu alinhamento ao planejamento estratégico organizacional, colaborando para que os aspectos desse planejamento sejam viabilizados e tornados exeqüíveis do ponto de vista de regulamentação e de concentração nos objetivos

estabelecidos nos planos da organização.

Ainda como retorno da aplicação de um modelo normativo tal qual é apresentado, deverá haver contribuição efetiva para a cultura organizacional, expressa em termos de valores culturais definidos nos princípios e nas políticas da organização, que fluirão pela cadeia hierárquica e serão refletidos nos conteúdos normativos propostos, projetando-se no cotidiano da organização.

Por sua vez, as contribuições para a cultura organizacional também deverão produzir efeitos nos resultados buscados pelo planejamento estratégico organizacional, colaborando para avalizar ou amortizar eventuais impactos que os planos incidirão no ambiente organizacional. Deve-se considerar novamente aqui o papel importante da comunicação organizacional para a construção da cultura organizacional, com atuação decisiva sobre a velocidade com que novos valores advindos do planejamento estratégico sejam assimilados pelos membros da organização.

4.2.2 Cadeia normativa da segurança da informação

A extensão da cadeia normativa genérica apresentada para a cadeia normativa da segurança da informação segue o diagrama da figura 11, página 80. São elaboradas particularizações em cada um dos níveis, como será visto a seguir.

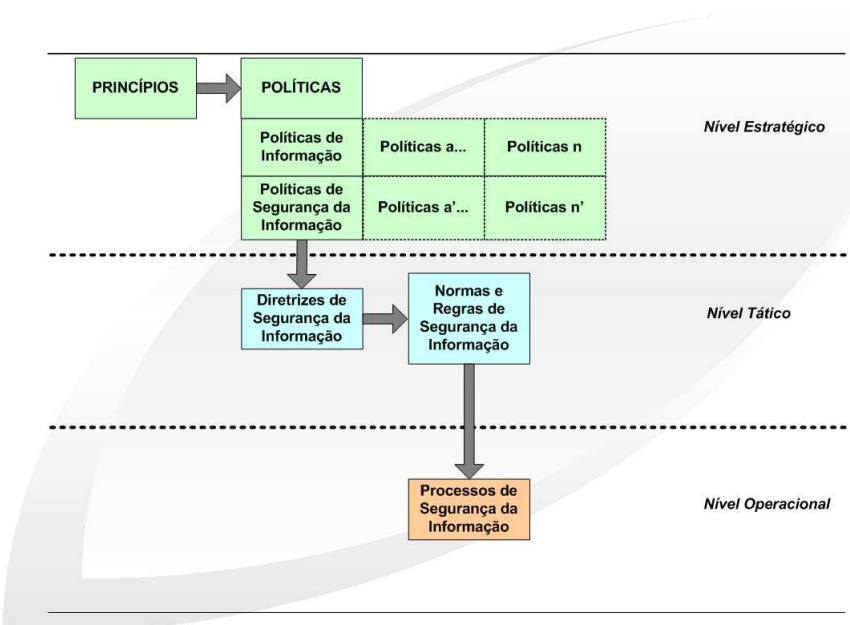

Figura 11: Cadeia normativa da segurança da informação

No nível estratégico, a especialização se dá a partir das políticas. O elemento referente

a princípios é mantido, já que se trata do início da cadeia normativa, das proposições elementares que orientam os objetivos da organização.

A partir do elemento das *políticas*, já apresentado na cadeia normativa genérica, procedem as *políticas de informação* da organização, e destas se originam as *políticas de segurança da informação.*

Foi considerada a definição de Marciano (2006), adaptada por Lima-Marques (2006) para *política de informação* na composição da cadeia normativa de segurança da informação no nível estratégico:

> "*Uma política de informação é uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido voltada à caracterização, ao delineamento e à definição de condutas orientadas à utilização da informação como ativo transformador da sociedade*".

Para as políticas de segurança da informação, foi adaptada a definição de Marciano (2006):

> Definição 4.2.4 *Uma política de segurança da informação é uma política que institui, no ciclo de vida da informação, o como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo Estado.*

A derivação das políticas de segurança da informação do nível estratégico materializa-se no nível tático em forma de diretrizes de segurança da informação, que tem a definição proposta neste trabalho estendida sob a seguinte forma:

> Definição 4.2.5 *Diretriz de segurança da informação é uma linha mestra, derivada de uma política de segurança de informação e orientada por um objetivo de governança, que define um modelo comportamental para a tomada de decisões, conferindo-lhes maior previsibilidade e equilíbrio.*

Na mesma linha, das diretrizes de segurança da informação procedem as normas de segurança da informação do nível tático, cuja definição é uma particularização das normas do nível tático da cadeia normativa genérica:

> Definição 4.2.6 *Norma de segurança da informação é uma prescrição fundamentada em uma diretriz de segurança da informação e que tem por objetivo regulamentar processos, evidenciando a permissibilidade dos comportamentos sociais associados.*

Considerando o nível operacional de decisão organizacional, temos associado o último nível da cadeia normativa da segurança da informação: os processos de segurança da informação. Foi adaptada a definição de Lima-Marques e Duarte (2007):

DEFINIÇÃO 4.2.7 *Processo organizacional de segurança da informação é uma série de atividades alinhadas às prescrições normativas de segurança da informação organizacionais, que formam uma cadeia de agregação de valores a partir de um insumo recebido (entrada), gerando um produto final (saída) componente do ciclo operacional da organização.*

4.2.3 O contexto da cadeia normativa de segurança da informação

A cadeia normativa proposta para a Segurança da Informação encontra-se inserida num contexto característico dos ambientes informacionais das organizações. O entendimento deste contexto torna clara a estrutura constitutiva da cadeia normativa, que percorre todo o contexto informacional organizacional, como seria de se esperar de um modelo de cadeia completa.

É importante ressaltar que o modelo de contexto dos ambientes informacionais apresentado, e no qual está inserida a Cadeia! normativa cadeia normativa proposta, é uma contribuição construída por vários pesquisadores ao longo de vários anos em estudos em Arquitetura da Informação, e foi adaptada neste trabalho a partir de uma compilação de Mamede Lima-Marques e Duarte (2007).

Os ambientes informacionais reais das organizações freqüentemente não se apresentam completamente estruturados conforme o contexto referido, e são caracterizados por distorções, baixa segregação funcional entre os níveis e particularidades dos próprios ambientes. Estas variações, usualmente, tornam complexo o relacionamento e o entendimento dos membros da organização em relação aos aspectos normativos, notadamente aqueles relacionados à Segurança da Informação.

A figura 12, da página 83, apresenta o contexto informacional geral, considerando genericamente um modelo de operacionalização no nível inferior do modelo, estruturado basicamente em três níveis, metodologicamente equivalentes aos níveis da epistemologia, da ciência e da prática postulados pela M^3.

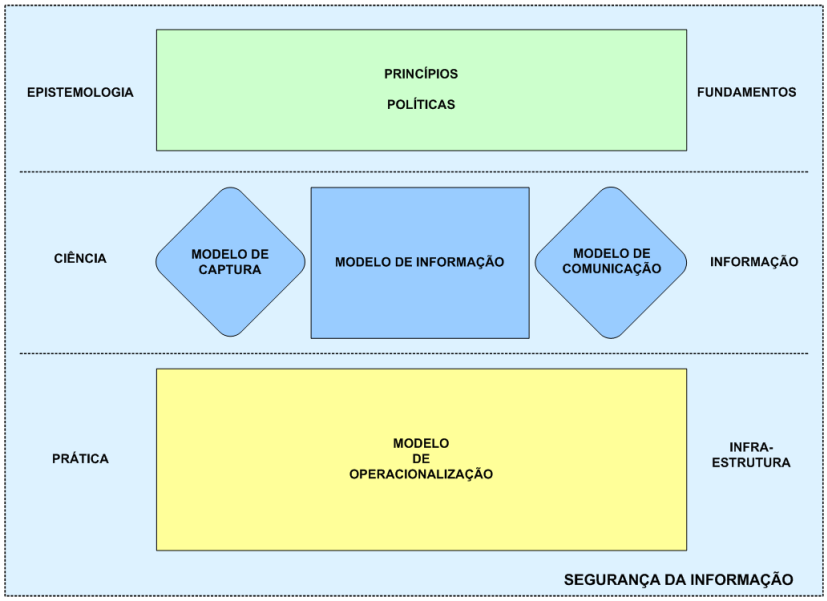

Figura 12: Contexto informacional geral da cadeia de regulamentação normativa

4.2.3.1 Nível epistemológico

O nível epistemológico, conforme o modelo metodológico M^3 adotado neste trabalho, é também denominado estratégico e constitui o arcabouço conceitual e metodológico do contexto informacional. Dele originam-se as decisões e os fundamentos do contexto informacional, representados pelos princípios e pelas políticas da organização, com destaque para a política de informação, significativamente importante para o sucesso das demais políticas e pelo enraizamento dos princípios e das próprias políticas na cultura organizacional.

4.2.3.2 Nível científico

O nível científico, de acordo com a metodologia M^3, é também denominado tático e compreende a previsão, descrição e explicação para os problemas e respectivas soluções, através do desenvolvimento de modelos e teorias no contexto informacional. É neste nível que encontra-se o ciclo de vida da informação, representado no diagrama pelos modelos de captura, de informação e de comunicação.

Modelo de captura de dados

O modelo de captura de dados é constituído por um conjunto de definições elaboradas pelas políticas de aquisição de dados básicos. Sua concepção estabelece as estratégias de coleta, padrões de qualidade e de confiabilidade, e performance de apropriação de dados.

O modelo de captura deve contemplar a identificação de novas necessidades, os mecanismos de entrada de dados, os padrões de troca ou intercâmbio dos dados, a interface com os sistemas originadores dos dados e a adequação dos sistemas receptores dos dados capturados. Por sistema, neste contexto, entende-se o conjunto de elementos, concretos ou abstratos, intelectualmente organizado para atuar no ciclo de vida da informação.

Modelo de informação

O modelo de informação é formado por um conjunto de propriedades que caracterizam o conteúdo das informações, estabelecendo categorias, definindo modos de integração, organização e estruturação, criando relacionamentos, interpretando, contextualizando e atribuindo significado às informações.

Este modelo, portanto, concentra-se no tratamento dos conteúdos e pode ser dividido em três fases: a representação da informação, a organização da informação e o armazenamento da informação.

A fase da representação da informação é responsável pela definição das formas de representação dos conteúdos, viabilizando a sua veiculação.

A fase de organização da informação define os métodos de organização dos conteúdos, por meio da classificação ou categorização das informações. Esta fase é dependente da forma de representação aplicada.

A fase de armazenamento da informação cuida das questões relacionadas ao armazenamento das informações, tais como o suporte físico e a preservação.

Modelo de comunicação

O modelo de comunicação é responsável pela recuperação e disseminação adequada das informações, utilizando-se de meios que interagem com a transmissão de conhecimento aos atores do sistema.

Este modelo considera o estudo do contexto informacional, o levantamento e a análise das informações, a definição e a implementação do modelo de comunicação, a personalização, as interfaces, a interatividade, a ergonomia, a usabilidade e a publicação da informação.

4.2.3.3 Nível prático

O nível da prática, segundo a metodologia M^3 também denominado operacional, ou "de aplicação", abrange a aplicação efetiva dos modelos, teorias, técnicas e tecnologias

desenvolvidos nos demais níveis para a solução dos problemas reais. Este nível é responsável pelo provimento da estrutura de operacionalização dos conceitos providos pelos níveis superiores.

Especificamente nos casos em que a operacionalização é baseada em um ambiente automatizado, o modelo de operacionalização do nível prático do contexto informacional para a cadeia de regulamentação pode ser representado por uma arquitetura em camadas constituída por uma infra-estrutura suportada por tecnologia da informação (TI), conforme sugere a figura 13, da página 85.

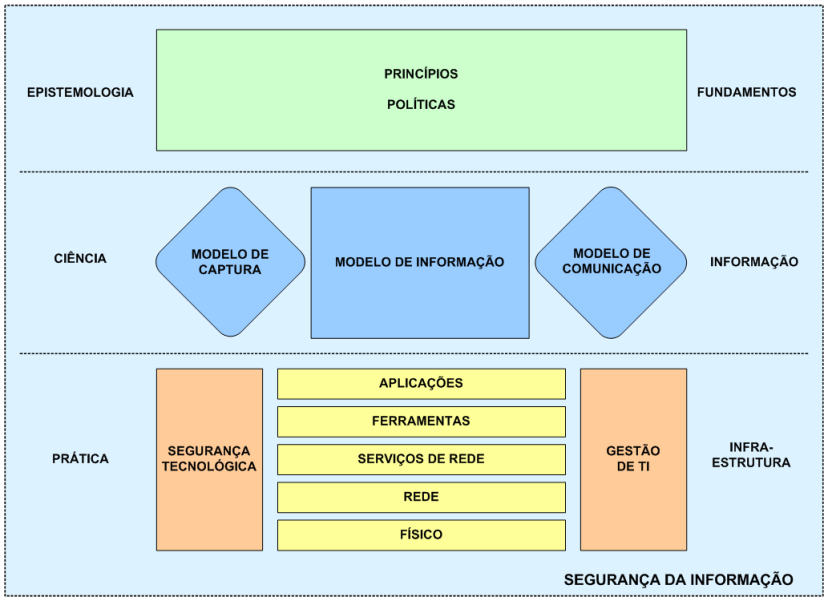

Figura 13: Contexto informacional suportado por uma infra-estrutura automatizada

Modelo de operacionalização automatizado

Como uma arquitetura em camadas, o modelo de operacionalização automatizado apresenta as características próprias de tais arquiteturas:

- funcionalidades bem definidas por camadas, tornando-as autônomas para realizar as funcionalidades que lhes são atribuídas;
- independência de implementação das funcionalidades por camada, tornando-as transparentes no que se refere às técnicas ou tecnologias empregadas na execução das funcionalidades que lhes são atribuídas; e,
- organização hierárquica dos níveis, com as camadas inferiores prestando serviços às camadas superiores.

Como premissa, assume-se que o modelo de operacionalização automatizado, bem como cada uma dos níveis, deve ser flexível para responder a requisitos específicos para a infra-estrutura, tais quais alta performance, escalabilidade, interatividade, alta confiabilidade, interoperabilidade, dentre outros.

O modelo de operacionalização automatizado proposto é formado por cinco níveis hierárquicos: físico, rede, serviços de rede, ferramentas e aplicações. Através de todos estes cinco níveis, atuam a gestão de tecnologia da informação e a segurança tecnológica. Todos estes elementos serão detalhados a seguir.

Gestão de tecnologia da informação

A gestão de tecnologia da informação tem por objetivo prover as definições para implementação dos processos organizacionais, viabilizar esta implementação em condições adequadas de risco e funcionalidade para os negócios da organização, considerando circunstâncias de mudanças, escalabilidade, compatibilidade, pesquisa e prospecção tecnológica, desenvolvimento de soluções, interação entre atores internos e externos etc.

Os modelos de gestão de tecnologia da informação atuais incluem a adoção de processos baseados em melhores práticas, comumente documentadas em padrões e normas internacionalmente aceitas tais como normas ISO, ITIL e COBIT, e contemplam, dentre outros:

- determinação de necessidades e exigências de controle;
- suporte a riscos operacionais para o negócio;
- discussão e estruturação de requisitos tecnológicos;
- viabilização de certificações e auditorias;
- estabelecimento sistemático de metas;
- estabelecimento de métricas para ações e resultados;
- gerenciamento de qualidade; e,
- operação baseada em níveis de serviço contratados.

Segurança tecnológica

A segurança tecnológica busca a aplicação de técnicas, ferramentas e configurações dos recursos tecnológicos de suporte à informação e correlatos, objetivando a preservação, no

âmbito da infra-estrutura, dos aspectos de confidencialidade, integridade e disponibilidade da informação, e ainda, o controle sistematizado de incidentes de segurança relacionados com a infra-estrutura.

Como exemplos práticos de elementos colaboradores com a segurança tecnológica, podemos destacar:

- tecnologias de *firewall*;
- *Intrusion Detection Systems* (IDS) e *Intrusion Prevention Systems* (IPS);
- ferramentas de varredura e análise de vulnerabilidades;
- criptografia sobre dados digitais;
- mecanismos de autenticação e controle lógico de acesso;
- infra-estrutura de chaves públicas;
- tecnologias de armazenamento redundante e de alta disponibilidade;
- mecanismos de detecção e correção de erros de dados em tráfego ou armazenados;
- ferramentas *anti-spam*;
- antivirus e ferramentas de controle contra *software* malicioso;
- filtros de conteúdo;
- trilhas de auditorias (*logs*).

Camada física

No nível físico estão todos os equipamentos e dispositivos de conectividade da infra-estrutura, voltados a suportar fisicamente os demais níveis.

Camada rede

O nível de rede é caracterizado pelos modelos de topologia, ou modelos de interconexão, modelos de organização e modelos de distribuição dos recursos de comunicação.

Camada serviços de rede

No nível de serviços de rede situam-se os serviços de administração da rede, endereçamento e localização de recursos, mensageria, sistemas de arquivos, diretórios, segurança da rede, gerenciamento físico e demais serviços de apoio operacional.

Camada ferramentas

O nível de ferramentas abriga o conjunto de recursos destinado a viabilizar e apoiar a construção de soluções automatizadas. As ferramentas devem estar alinhadas a padrões institucionalizados.

Camada aplicações

No nível das aplicações são definidas as soluções automatizadas de caráter operacional, gerencial e de tomada de decisão. É definido aqui o ambiente adequado ao desenvolvimento de produtos considerando-se os aspectos metodológicos, organizacionais e de gestão.

4.2.3.4 Segurança da Informação

No diagrama da figura 13, página 85, referente ao contexto informacional da organização, provendo cobertura para todos os níveis e todas as estruturas de cada nível, aparece a segurança da informação, caracterizada como um fenômeno social no qual os usuários dos recursos informacionais têm razoável conhecimento sobre o uso destes recursos, bem como sobre os papéis que devem desempenhar no exercício deste uso (MARCIANO, 2006).

4.2.4 Cadeia normativa, modelo metodológico, instrumentos e arquitetura da informação

O quadro a seguir, da figura 14, página 89, apresenta um paralelo entre os níveis dos elementos da cadeia normativa proposta, do modelo metodológico utilizado(M^3), dos instrumentos de aplicação e dos elementos da Arquitetura da Informação.

Partindo do modelo metodológico M^3 e considerando o seu nível mais alto, o epistemológico ou estratégico, é possível associá-lo ao nível da Arquitetura da Informação composto por teorias, fundamentos e metodologias, uma vez que estes elementos refletem o aspecto epistemológico da Arquitetura da Informação.

Ainda considerando o nível epistemológico da M^3, outra associação pode ser feita, desta vez com o conjunto de instrumentos de aplicação formado por leis, tratados, acordos, arbitragens e convênios, dentre outros.

Por fim, os resultados deste trabalho sugerem que os níveis de princípios e políticas

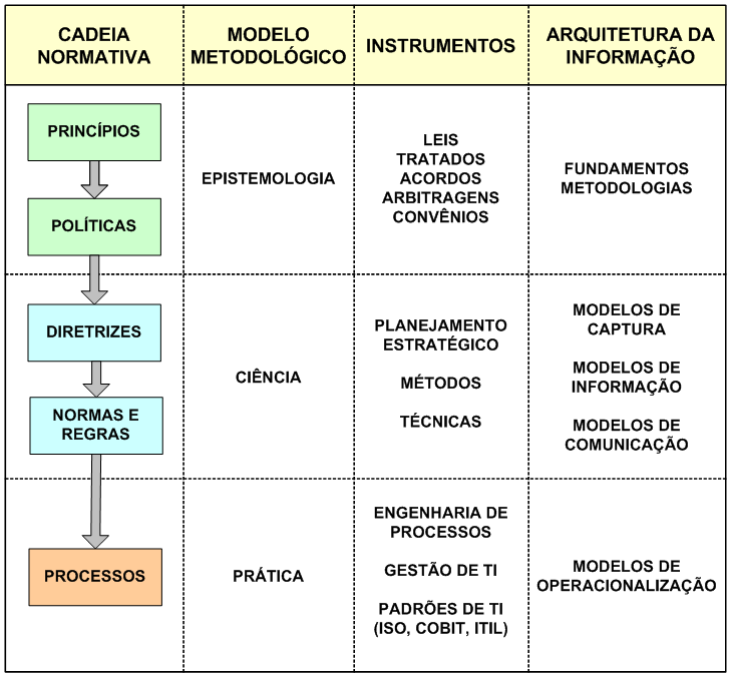

Figura 14: Relações da cadeia de regulamentação normativa com modelo metodológico, instrumentos e arquitetura da informação

da cadeia normativa proposta possam ser associados ao mesmo nível epistemológico da M^3.

Todas as associações propostas para o nível epistemológico da M^3 podem ser estendidas reciprocamente aos demais elementos associados, tal qual ilustra o quadro da figura 14, página 89, refletindo essencialmente o aspecto estratégico da Arquitetura da Informação, dos instrumentos de aplicação e da cadeia normativa.

Para o nível da ciência na metodologia M^3, ou nível tático, também podem ser feitas associações com elementos da Arquitetura da Informação, dos instrumentos de aplicação e da cadeia normativa.

Conforme o quadro da figura 14, página 89, para o nível da ciência são associados os modelos de captura, de informação e de comunicação da Arquitetura da Informação, os instrumentos de aplicação de planejamento estratégico, métodos e técnicas, e dos elementos diretrizes e normas da cadeia normativa organizacional.

O mesmo tipo de associação pode ser feito para o nível da prática da metodologia M^3, com os modelos de operacionalização da Arquitetura da Informação, os instrumentos de engenharia de processos, gestão de tecnologia da informação, padrões e melhores práticas de tecnologia de informação, e o elemento *processos* da cadeia normativa organizacional proposta.

O quadro da figura 14, página 89, apresenta as associações discutidas neste tópico, de maneira estruturada.

4.2.5 O Planejamento estratégico situacional e a cadeia de regulamentação normativa

Enquanto instrumento participativo de gestão, o planejamento estratégico situacional (PES) tem a preocupação de envolver todo o contexto social da organização, das bases ao topo, nas definições de seus planos, assumindo, ao fim, por estratégias, somente as linhas de comportamento viáveis.

Por viáveis, consideram-se as estratégias constituídas em conformidade com as políticas vigentes na organização, especialmente com as políticas de informação, e ainda, sujeitas ao crivo de avaliações técnicas, políticas, administrativas, financeiras, climáticas, geográficas, históricas, sociais, tecnológicas, demográficas, ou quaisquer outras que sejam relevantes frente ao conjunto de possibilidades da organização.

As políticas de informação são consideradas fundamentais para a existência de várias outras políticas organizacionais, porquanto centralizam o ciclo de vida das informações relacionadas àquelas políticas, mantendo-as significativamente dependentes da forma como as informações são tratadas no contexto organizacional.

O dimensionamento da realidade atual da organização refletido no *momento explicativo* do PES constrói a identidade situacional da organização, a partir da qual poderá ser concebido o *momento normativo* que, por sua vez, projetará uma situação ideal, perfeita para a organização, e desprovida, entretanto, de qualquer ponderação restritiva.

Deste momento normativo, que expressa "*como deve ser*" a situação organizacional, advém o *momento estratégico*, que preocupar-se-á em delinear "*como pode ser*" a organização, mediante a ponderação da situação normativa projetada frente a questões incidentes determinantes no contexto da organização, tais quais relacionadas acima.

A situação resultada do momento estratégico delimita o universo de diretrizes possíveis, a partir do qual serão produzidos os modelos comportamentais para a tomada de decisões na organização, e que, por sua vez, orientarão as definições de normas que regulamentarão os processos organizacionais, relacionados pela situação construída no momento tático/operacional do planejamento estratégico situacional.

A figura 15, página 91, ilustra todo o ciclo relacionando a cadeia de regulamentação proposta, envolvendo as políticas de informação, políticas de segurança da informação,

diretrizes, normas e processos organizacionais com os momentos do planejamento estratégico situacional.

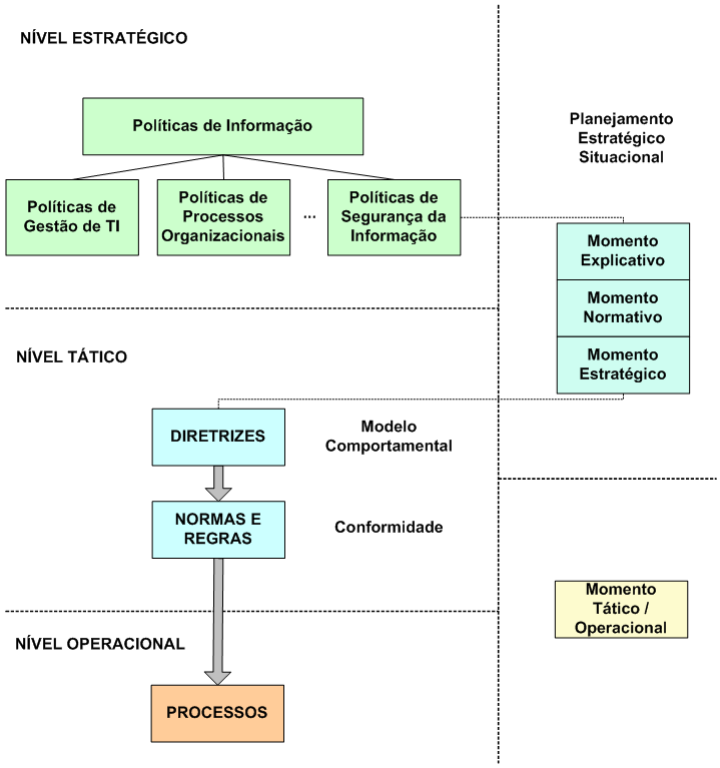

Figura 15: Relações da cadeia de regulamentação com o planejamento estratégico

No contexto da Segurança da Informação, as políticas de segurança da informação, incluídas dentre as que são profundamente dependentes das políticas de informação, balizam a construção dos momentos explicativo, normativo e estratégico de um planejamento estratégico situacional voltado para segurança da informação.

Na mesma linha de raciocínio anteriormente postulada, deste planejamento estratégico situacional voltado para a segurança da informação, nascerão as diretrizes e normas de segurança da informação para a organização.

Enquanto atores efetivos do planejamento estratégico situacional, os usuários terão papéis importantes na construção de um conjunto normativo organizacional baseado no modelo de cadeia proposto. Em cada um dos níveis administrativos de decisão, haverá participação dos usuários nos processos de definição e cumprimento das determinações normativas advindas da aplicação da cadeia de regulamentação sobre o contexto organizacional.

Do ponto de vista do nível estratégico, haverá a contribuição dos usuários vinculados a este nível de decisão para a estruturação dos princípios organizacionais e a elaboração de

políticas concordantes com tais princípios, ancoradas nos objetivos postos em evidência nos planos da organização.

Na esfera tática, os usuários de ofício desenvolverão diretrizes e normas em conformidade com as políticas e objetivos advindas do nível estratégico, com foco em comportamentos qualificados para a tomada de decisões, buscando previsibilidade e equilíbrio para essas decisões, e estabelecendo o contexto permissivo dos comportamentos dos usuários dos níveis tático e operacional, bem como a regulamentação para todos os processos organizacionais.

No âmbito operacional de decisões, os usuários adotarão os comportamentos prescritos no nível tático e desenvolverão as decisões sobre como realizar o ciclo operacional da organização, elaborando os processos que agregarão os valores da organização aos insumos de entrada para dar-lhes as características dos produtos próprios da organização.

4.3 Parte II - Entrevista semi-estruturada

As entrevistas semi-estruturadas foram realizadas com profissionais de segurança da informação de nível sênior, atuantes em empresas dos seguintes segmentos:

- bancário público e privado;
- serviços em tecnologia e segurança da informação; e,
- órgão público do poder judiciário.

Os entrevistados foram previamente contactados por telefone e mediante sua concordância em colaborar, foram enviados a eles as perguntas constantes da entrevista, através de mensagem correio eletrônico da Internet. As entrevistas foram realizadas entre julho e setembro de 2006.

Um dos especialistas entrevistados, empregado de um dos bancos, ao ser contactado, solicitou que a entrevista fosse realizada pessoal e verbalmente, e autorizou expressamente a gravação da conversa. A entrevista foi realizada conforme solicitado e o diálogo foi transcrito para efeito da análise.

Outro potencial entrevistado, apesar de ter se prontificado a responder às perguntas no momento do contato inicial, não respondeu. Ao ser solicitado por várias vezes a

retornar suas respostas, o especialista sempre sinalizou positivamente, mas efetivamente não respondeu.

No instrumento elaborado para esta pesquisa, cada especialista entrevistado tenta responder às questões recorrendo a seus próprios conceitos, à compreensão sobre os problemas e à visão institucional estabelecida na sua realidade, evitando recorrer aos documentos institucionais como fonte de consulta. O objetivo é refletir nas respostas, tanto quanto possível, a cultura organizacional sedimentada em si, priorizada à norma oficial registrada.

A escolha dos especialistas a serem entrevistados obedeceu basicamente aos seguintes critérios:

- Reconhecimento técnico em segurança da informação, com experiência representativa no seu ramo de negócio e em segurança da informação;
- Vínculo a organizações com tradição em preocupação com segurança da informação aplicada ao negócio, proporcionada pela própria natureza dos negócios das organizações; e,
- Vínculo a organizações de médio e grande porte, públicas ou privadas, com cultura organizacional sedimentada, ou ainda, que atendam a de clientes com estes requisitos, condicionadas ao exercício de um alto grau de interatividade junto ao contexto organizacional dos clientes;

Consideradas as premissas de perfil dos especialistas, foram selecionados uma instituição financeira pública, duas sociedades financeiras de economia mista, um banco privado, três empresas de consultoria em segurança da informação e um órgão público do poder judiciário.

Para que os especialistas estivessem confortáveis em responder sinceramente às questões apresentadas, sugeriu-se a manutenção do sigilo de identidade das organizações, o que foi prontamente aceito por todos os entrevistados.

Em razão da não publicação explícita de identidade acordada com as organizações, elas foram referenciadas neste trabalho da seguinte maneira:

- BG - Banco público;
- BM1 - Banco misto 1
- BM2 - Banco misto 2

- BP - Banco privado
- CS1 - Consultoria em segurança da informação 1
- CS2 - Consultoria em segurança da informação 2
- CS3 - Consultoria em segurança da informação 3
- OP - Órgão público

Na parte inicial da mensagem de correio eletrônico com as perguntas da entrevista, foram solicitadas informações da organização para facilitar a análise das respostas e permitir comparações categorizadas em nível dessas informações solicitadas, que foram as seguintes:

- Nome da organização
- Principais áreas de atuação
- Faturamento anual aproximado
- Quantidade aproximada de colaboradores diretos e indiretos

A tabela 3, página 95, posiciona as organizações de acordo com as informações coletadas especificadas acima.

As entrevistas semi-estruturadas realizadas foram constituídas todas por um conjunto de seis perguntas para as quais o entrevistado deveria emitir respostas baseadas na sua vivência organizacional, partindo de seus próprios conceitos organizacionais consolidados e de sua experiência em segurança da informação. As perguntas propostas foram as seguintes:

1. Qual é a visão corporativa da organização para “segurança da informação”?
2. Qual a definição corporativa da organização para “política de segurança da informação”?
3. Qual é o conceito corporativo da organização para “usuários”?
4. Que níveis de regulamentação derivam da política de segurança da informação na organização (diretrizes, normas, procedimentos, regras, etc.)?

Tabela 3: Organizações dos especialistas entrevistados

Organização	**Principais áreas de atuação**	**Faturamento anual aproximado (R$)**	**Quantidade aproximada de colaboradores**
BG	Bancária, execução de políticas sociais e apoio à administração pública	28 bilhões	145.000
BM1	Bancária e seguros	753 milhões	3.800
BM2	Financeira	707 milhões	3.500
BP	Bancária de atacado e varejo, seguros, previdência e gestão de patrimônios	9,5 bilhões	28.000
CS1	Tecnologia, segurança da informação, consultoria e infra-estrutura	Não informado	550
CS2	Consultoria em TI	34 milhões	268
CS3	Serviços gerenciados de segurança, treinamento em tecnologias de rede e software livre, soluções software livre, terceirização de infra-estrutura	1,2 milhões	20
OP	Julgamento de processos judiciais	7,4 bilhões*	Não informado

$*$ Orçamento para 2006

5. De acordo com a visão corporativa da organização, defina cada um dos níveis de regulamentação derivados da política de segurança, relacionados na pergunta anterior. (por exemplo, o que são as diretrizes, as normas, etc. para a organização).

6. A política de segurança e as demais instâncias de regulamentação são formais na organização? Por quê ?

Pelo método de análise escolhido, as respostas de todos os entrevistados para cada uma das perguntas serão discutidas em sessões próprias, visando aprofundar o debate sobre os temas questionados, sem necessariamente produzir comparações entre as respostas, o que não é o objetivo principal. Antes, busca-se o entendimento dos quadros captados e a compreensão dos modelos praticados.

4.3.1 Pergunta 1 - Qual é a visão corporativa da organização para "segurança da informação"?

Um dos objetivos desta primeira pergunta foi captar o entendimento organizacional para o assunto "segurança da informação" através da visão do entrevistado, que é um indivíduo com perfil privilegiado em conhecimentos de segurança da informação, com plenas condições de demonstrar a visão da organização sobre este tema. A idéia é delimitar a amplitude com que o tema é abordado no contexto organizacional, detectar possíveis vieses ou

paralelos em relação aos conceitos revisados neste trabalho, sem contudo questionar-lhes a validade ou razão.

Outro objetivo desta pergunta foi trazer o entrevistado à reflexão sobre o tema "segurança da informação" no seu contexto organizacional, de modo a ampliar as possibilidades das respostas para as próximas perguntas da entrevista, à medida que os conceitos básicos fossem trazidos à memória.

Como relatado anteriormente, a entrevista no banco público BG foi realizada presencialmente. Dois especialistas em segurança da informação se dispuseram a responder as perguntas e assim foi feito.

4.3.1.1 Banco público BG

Para a primeira pergunta, os representantes do banco público BG, ao serem interpelados, concentraram-se em destacar a importância da segurança da informação para a organização, entendendo que a "visão para segurança da informação" colocada na pergunta referia-se ao nível de importância da segurança da informação para a organização. Este entendimento ficou claro a partir dos seguintes trechos das respostas dos dois representantes entrevistados:

> "*...é uma necessidade para o negócio... mas na realidade, a conscientização da necessidade, da importância disso ainda não é um fato...*"

> "*...deveria ser uma preocupação que deveria partir da alta direção da empresa; e hoje ainda não é assim, a alta direção da empresa não tem ainda a sensibilidade para entender a importância da segurança da informação...*"

Outro ponto importante observado nas respostas é a preocupação de ambos os representantes do banco público BG sobre a necessidade de conscientização e sensibilização do corpo diretivo e de toda a comunidade organizacional em torno da segurança da informação. Ficou evidente que existe uma movimentação da área responsável pela segurança da informação do banco público BG no sentido de realizar a mudança na visão corporativa sobre o tema.

Ainda na visão dos representantes do BG, o maior motivador para a realização da segurança da informação na organização é a exigência por parte de legislações, de auditorias interna e externa no cumprimento de normas e padrões internacionais, de determinações de órgãos reguladores e do próprio governo central.

Não houve uma intervenção do entrevistador no sentido de obter exatamente uma definição corporativa para a segurança da informação. Esta estratégia se justificou primeiramente para manter o espírito de captar as impressões dos entrevistados exatamente como elas estão, sedimentadas pela cultura organizacional, sem nenhuma interferência normativa. Em segundo lugar, procurou-se manter tanto quanto possível, as condições de igualdade para todos os entrevistados (presenciais ou virtuais) na interpretação das perguntas e formulação das respostas.

4.3.1.2 Banco misto BM1

Na resposta do representante do banco misto BM1, houve uma preocupação em definir compreensivamente a segurança da informação no contexto da organização e relacionar a informação como "*patrimônio da empresa*". Outro foco da primeira resposta daquele entrevistado foi a necessidade de capacitação de indivíduos para gerenciar e disseminar a cultura de segurança da informação na organização, conforme denota o trecho abaixo:

> "*...efetuar o adequado tratamento de suas informações, sejam elas convencionais ou informatizadas, com vistas à sua preservação enquanto patrimônio da Empresa, mediante capacitação de uma área específica, que terá a responsabilidade pela sua implantação/gestão, bem como a disseminação de uma cultura de segurança na empresa...*"

4.3.1.3 Banco misto BM2

O representante do banco BM2, ao responder a primeira pergunta da entrevista considerou a segurança da informação como "*um dos pilares que suportam as atividades da organização*" e defendeu que a segurança da informação "*não está apenas ligada aos ativos tecnológicos e aos processos, mas sobretudo aos ativos humanos*". Ele destacou ainda a importância da conscientização dos usuários e da "*distribuição adequada dos investimentos em segurança, e assim buscar o alinhamento entre a segurança e os objetivos negociais do Banco*" e demonstrou que uma preocupação da área de segurança da informação do BM2 é "*garantir a perenidade da instituição, evitando perdas significativas para o Banco, seja financeira ou de imagem*".

4.3.1.4 Banco privado BP

Para responder à primeira pergunta, o entrevistado do banco privado BP enfatizou o papel da segurança da informação em sua organização, descrevendo a trajetória da área que trata da segurança da informação, desde o tempo em que era subordinada à área de tecnologia da informação até os dias atuais, quando está vinculada à diretoria de prevenção a fraudes. Segundo o entrevistado, com o decorrer do tempo, a segurança da informação tem alçado cada vez mais espaço e visibilidade no cenário organizacional, com destaque para a participação nos projetos de desenvolvimento de produtos do banco, conforme o trecho do depoimento do representante do banco privado BP:

> "*...recentemente, através de trabalhos de melhoria de qualidade, a diretoria ganhou destaque em nossa vice-presidência, sendo conhecida pelas mais diversas áreas, incluindo negócios. Hoje nos envolvemos diretamente na segurança de projetos incluindo produtos que serão lançados e disponibilizados aos nossos clientes.*"

4.3.1.5 Consultoria CS1

O especialista da consultoria CS1 abordou várias faces da segurança da informação em sua resposta à primeira pergunta da entrevista. Ele iniciou sua resposta sinalizando o foco da segurança no negócio, relatando algumas atividades executadas pela organização no campo da segurança da informação e ressalvando a visão corporativa da segurança da informação como parte da área de tecnologia.

Depois, enfatizou a preservação da informação conforme o seu grau de importância e também nos processos de criação, guarda, transmissão e descarte. O entrevistado concluiu sua resposta destacando a proteção de integridade, disponibilidade e confidencialidade e a importância de normas e metodologias que aplicam segurança da informação:

> "*...fora os preceitos básicos da preservação da integridade, disponibilidade e confidencialidade, ainda devem ser lembradas as importâncias de normas e metodologias como Sarbanes Oxley, BS 7799, ISO 27001 e ITIL, que prevêem a sua aplicabilidade e necessidade [da segurança da informação]*"

Observa-se nesta resposta uma ampla variedade de processos envolvidos no conceito atribuído a segurança da informação corporativa, sugerindo que a segurança da informação configure-se como um macroprocesso, composto por processos menores de várias

naturezas, tais como auditoria, análise, classificação, inspeção de conformidade, dentre outros, e uso extensivo de ferramentas para garantia de integridade, disponibilidade e confidencialidade.

4.3.1.6 Consultoria CS2

A consultoria CS2 participou da entrevista com dois especialistas respondendo às perguntas, de maneira independente. Um aspecto interessante dessa experiência foi o foco dado por cada um dos dois respondentes da CS2. Enquanto a primeira respondente concentrou-se em aspectos conceituais e crenças da organização, o segundo utilizou-se de elementos da prática para expressar seu entendimento acerca dos temas abordados na entrevista.

A primeira respondente da CS2 propôs uma definição para a segurança da informação segundo a visão daquela organização:

> "*...conjunto de responsabilidades, termos e regras que objetivam definir e manter o ambiente (hardware, software e infra-estrutura) e os dados de propriedade ou sob a responsabilidade da organização.*"

Esta resposta sugere a segurança da informação como um arcabouço normativo para regulamentar o uso do ambiente de sustentação das informações sob a guarda da organização.

O segundo respondente evidenciou que a segurança da informação é um assunto prioritário para aquela organização, no sentido de "*cuidar dos dados da empresa*". Ressaltou a importância da conscientização dos usuários através de treinamento sobre a norma de segurança da informação, da exigência de assinatura de termos de ciência da norma e da preocupação com o trânsito dos dados da empresa fora do seu próprio ambiente.

Seguindo a linha de raciocínio estabelecida anteriormente, esta resposta sugere o comportamento prático incidente sobre os fundamentos conceituais relacionados à segurança da informação enraizados na cultura daquela empresa, refletindo a adoção de medidas práticas para proteger a informação organizacional e manter o marco de regulamentação no consciente coletivo dos colaboradores.

4.3.1.7 Consultoria CS3

Para o entrevistado da consultoria CS3, a visão de segurança da informação da organização está associada ao controle de acesso, ao controle da manipulação e ao controle do armazenamento da informação, sugerindo implicitamente a adoção e o uso de técnicas e de tecnologias como ferramental para realização dos controles constitutivos da segurança da informação.

4.3.1.8 Órgão público OP

De acordo com o especialista do órgão público OP, a segurança da informação em seu contexto organizacional pode ser definida como:

> "*... necessidade de garantir um ambiente tecnológico controlado e seguro, de forma a oferecer todas as informações necessárias aos processos desta corte com integridade, confidencialidade e disponibilidade*".

Nesta resposta percebe-se uma visão essencialmente tecnológica para a segurança da informação, permitindo a inferência de que a manutenção de um ambiente tecnológico controlado e seguro para as informações da organização é o fator de sucesso para a segurança da informação.

A análise do conjunto de respostas para a primeira pergunta permite concluir que não há um padrão de definição para "*segurança da informação*" entre as organizações pesquisadas. Entretanto, foi consensual a importância atribuída ao papel da segurança da informação e ao valor da informação para as organizações.

Outra percepção que ficou evidenciada foi que há uma oscilação entre as organizações ao conceber a segurança da informação do ponto de vista de posicionamento como disciplina, variando, no âmbito das organizações, de conjunto de processos a contexto comportamental, passando por atividade da área de tecnologia da informação e controles baseados em técnicas e ferramentas.

4.3.2 Pergunta 2 - Qual a definição corporativa da organização para "política de segurança da informação"?

A segunda pergunta da entrevista teve a intenção de recuperar, junto às organizações pesquisadas, o conceito de um tradicional elemento associado à segurança da informa-

ção, reconhecido como peça fundamental para realização de segurança da informação: as "políticas de segurança da informação".

As políticas de segurança da informação também são entendidas como a raiz do sistema normativo de segurança da informação das organizações, ainda que não exista uma cadeia normativa estabelecida, tal qual é proposta neste trabalho.

4.3.2.1 Banco público BG

Um dos representantes do banco público BG definiu a política de segurança da informação no contexto da organização, e foi acompanhado pela outra representante, como uma "*norma que determina como agir*" e observou que a política de segurança da informação é vista pelos colaboradores como mais uma dentre as centenas de normas, ou seja, mais um regulamento a ser cumprido no cotidiano do trabalho.

4.3.2.2 Banco misto BM1

O entrevistado do banco BM1 definiu assim a política de segurança da informação no contexto da organização:

> "*...um conjunto de critérios e soluções que visam a mitigação de riscos de ordem tecnológica e humana, focado em seus ativos de maior relevância/relação com o negócio da empresa*".

Esta resposta demonstra uma visão abrangente para as políticas de segurança da informação, considerando-a todo o arcabouço normativo (critérios) e todo o conjunto de "*soluções*" para minimização de riscos. É possível inferir que soluções, na visão do entrevistado, envolvam técnicas, processos, ferramentas, procedimentos e todo tipo de atividades que colaborem com o objetivo de redução de riscos.

4.3.2.3 Banco misto BM2

Para a segunda pergunta, o representante do banco BM2 apresentou como resposta a seguinte definição para política de segurança da informação:

> "*...o documento base que contém as diretrizes gerais e estruturais para a criação das normas e procedimentos específicos em segurança da informação a serem aplicados em áreas particulares do Banco*".

O entrevistado do BM2 destacou ainda que "*a elaboração da Política de Segurança da Informação foi o primeiro passo de uma estratégia de segurança da informação voltada para pessoas, processos e tecnologia, levando também em consideração os negócios.*" e observou que a política de segurança da informação do banco foi inspirada na norma NBR ISO/IEC 17799 (Código de melhores práticas em segurança da informação).

O posicionamento do especialista do BM2 demonstra uma intenção efetiva da instituição em manter um alinhamento com as normas internacionais vigentes que propõem as melhores práticas para a segurança da informação na constituição do seu modelo normativo sobre o tema.

A definição apresentada na resposta sugere a visão de uma cadeia normativa hierárquica, onde a política de segurança da informação assume um caráter geral e referencial para os demais níveis, que regulamentarão situações mais específicos.

4.3.2.4 Banco privado BP

O especialista do banco privado BP definiu a política de segurança da informação no seu contexto organizacional como "*um conjunto de diretrizes que refletem regulamentações de mercado tais como Sarbanes-Oxley e Basiléia II dentre outros, permitindo que os usuários acessem ou tenham recursos necessários para execução de suas funções*" e considerou que a política de segurança vigente atualmente no banco carece de ajustes para que se torne aplicável e conhecida. Salientou ainda que um novo texto tramita na organização contemplando os ajustes indicados.

A resposta do especialista do BP aponta a política de segurança da informação como um delimitador de comportamentos organizacionais disposto em termos necessariamente em conformidade com padrões internacionais. Os padrões citados pelo entrevistado referem-se respectivamente a uma lei norte-americana e a um acordo internacional entre os sete países mais ricos do mundo, o G-7, voltados à prevenção contra fraudes e gerenciamento de riscos através de mecanismos de auditoria e segurança confiáveis, e tem sido aplicados como modelos para as instituições financeiras de todo o mundo.

Pode-se inferir que a área de segurança da informação daquele banco está atenta e sensível à aplicabilidade e disseminação da política de segurança da informação, considerando-a importante para o negócio da organização.

4.3.2.5 Consultoria CS1

O especialista da empresa de consultoria CS1 considerou que a política de segurança da informação em sua organização:

> "*...é um dos elementos que norteiam os aspectos de Segurança da Informação, sendo um dos pilares que auxiliam e embasam um Plano Diretor de Segurança da informação, que deve prever não apenas a documentação, mas os diversos pontos que são passíveis de atuarem sobre a Informação, sejam meios tecnológicos, comportamentais, documentais ou físicos, dando, inclusive, o apoio necessário à estrutura jurídica da empresa.*"

O entrevistado reforçou também em sua resposta a necessidade de atualização periódica da política de segurança da informação com o objetivo de manter a política aderente às melhores práticas do mercado e ainda adequada às necessidades da organização advindas de mudanças estruturais que podem ocorrer ao longo do tempo.

Nesta resposta, pode ser observada uma significativa diversidade de aspectos que a política de segurança da informação deve contemplar naquela organização, com ascendência sobre uma variedade de instâncias que lidam ou tratam da informação.

4.3.2.6 Consultoria CS2

A primeira entrevistada da consultoria CS2, definiu assim a política de segurança da informação:

> "*Política de Segurança da Informação é o conjunto de orientações, regras, metas e/ou objetivos estratégicos que norteiam as normas e procedimentos relativos à segurança da informação.*"

O segundo entrevistado da mesma consultoria, definiu a política de segurança da informação como "*uma norma contendo um conjunto de regras comportamentais deliberadas com vistas a garantir a segurança das informações da empresa*" e lembrou que a norma é uma das componentes do sistema de qualidade da organização.

Das duas respostas, é possível apreender o conceito de cadeia normativa hierárquica, sendo a política de segurança da informação um referencial para outros níveis. Também é percebido o foco da política sobre os comportamentos, o que sugere que a política seja dirigida basicamente a pessoas.

4.3.2.7 Consultoria CS3

O especialista da consultoria CS3 definiu a política de segurança da informação como "*regras e procedimentos que definem como a informação será manipulada, lida, armazenada ou recuperada*".

A análise desta resposta sugere que, no contexto daquela organização, a política de segurança da informação seja definidora dos processos de manuseio da informação e que seja constituída de prescrições de regulamentação (*regras*) desses processos e de métodos (*procedimentos*) para implementação do manuseio da informação.

4.3.2.8 Órgão público OP

O entrevistado do órgão público OP definiu a política de segurança da informação como:

> "*Política de segurança da informação é o conjunto das diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos desta corte com integridade, confidencialidade e disponibilidade*".

Mantendo a linha da resposta da pergunta anterior, o especialista adota uma abordagem essencialmente tecnológica também para a política de segurança da informação.

Também é sugerido implicitamente aqui o conceito de um arcabouço normativo hierarquizado no âmbito daquela organização, sendo a política de segurança da informação a raiz de *diretrizes, padrões e processos*, todos convergentes na promoção dos aspectos de segurança integridade, confidencialidade e disponibilidade.

4.3.3 Pergunta 3 - Qual é o conceito corporativo da organização para "usuários"?

Esta pergunta visou primeiramente entender qual é a visão dos especialistas em segurança da informação em relação aos usuários e ainda, identificar como a visão de usuários relaciona-se com os conceitos organizacionais de segurança da informação e política de segurança da informação.

4.3.3.1 Banco público BG

Na visão dos dois especialistas do banco público BG, no contexto da organização, o usuário é um colaborador (empregado, terceirizado, estagiário, etc.) com metas a atingir dentro da organização, que se ampara no conjunto de normas da organização para obter sucesso nessas metas, e que, infelizmente, nem sempre é visto como um ser humano.

A segunda entrevistada acrescentou ainda que dentre este conjunto de colaboradores, podem ser considerados usuários aqueles "*que de alguma forma interagem com a informação da organização, fazem uso dela*".

Observa-se na resposta do primeiro especialista um conflito pessoal entre o que a organização considera ser um usuário e o que o entrevistado pessoalmente concebe. Pode-se imaginar que, sendo o especialista um formador de opinião, e integrante da equipe que conduz segurança da informação na organização, possa iniciar ou colaborar com uma mudança de paradigma na organização relacionada à humanização da figura do usuário.

A segunda entrevistada do banco BG apresentou ainda uma visão complementar, associando o usuário ao uso da informação e dos recursos informacionais.

4.3.3.2 Banco misto BM1

Para o entrevistado do BM1, o usuário é a "*pessoa física ou jurídica que faz uso dos ativos de tecnologia da informação*" a quem é imputada responsabilidade pelo uso desses recursos na política de segurança da informação.

A visão do especialista e da organização BM1 considera o usuário somente aquele que utiliza recursos de tecnologia, responsabilizando-o pelo uso adequado ou não desses recursos.

4.3.3.3 Banco misto BM2

A resposta do entrevistado do BM2 define o usuário como o "*custodiante da informação da organização e principal responsável pela classificação desta informação*".

Ele ainda considera que o usuário seja "*o elo mais fraco da corrente constituída por tecnologia, processos e pessoas*", e que por isso, merece atenção e tem papel importante para obtenção de sucesso na implementação da política de segurança da informação no Banco.

Como meio de fortalecer a conscientização dos usuários, o especialista declara que naquela organização são realizadas palestras sobre segurança da informação para os novos colaboradores, além da divulgação de notas sobre segurança da informação através dos canais internos do banco. Segundo ele, estão em andamento projeto para realização de um trabalho de conscientização mais abrangente junto ao corpo de colaboradores.

A resposta sugere que o usuário seja visto como peça fundamental para a segurança da informação, enquanto custodiante e classificador da informação.

Pode também ser percebida uma preocupação com a cultura de segurança do usuário enquanto recurso chave para a segurança da informação, ao passo que entende que o treinamento pode contribuir para a melhoria da cultura do usuário em segurança da informação.

4.3.3.4 Banco privado BP

O entrevistado do banco privado BP definiu os usuários no seu contexto organizacional como "*os possuidores de credenciais de acesso a sistemas*". Segundo ele, podem se enquadrar nesta definição "*funcionários, terceiros, prestadores de serviços, clientes e sistemas, além de equipamentos*".

Também no banco privado, o usuário aparece como aquele que tem acesso a recursos tecnológicos, presumidamente manuseadores de informação. São considerados usuários inclusive entidades não-humanas tais quais sistemas e equipamentos.

4.3.3.5 Consultoria CS1

Para o especialista da consultoria CS1, são considerados usuários "*todos aqueles que possuem acesso às estruturas da empresa, tanto física quanto logicamente*". Enfatizou que os usuários são classificados e qualificados "*de acordo com as normativas internas da empresa*".

Esta visão sugere que os usuários não são necessariamente elementos com acesso a recursos tecnológicos. Apesar de não ser claramente expresso o conceito de "*estruturas*", é possível inferir que trata-se das instalações físicas da organização, recursos informacionais variados e sistemas computacionais.

4.3.3.6 Consultoria CS2

Na consultoria CS2, usuários são "*todos os indivíduos que acessam física e/ou logicamente as instalações e infra-estrutura de hardware e software da organização*", segundo a primeira entrevistada da CS2.

Já para o segundo especialista da CS2, o usuário é um "*colaborador ou prestador de serviços que se utiliza dos recursos computacionais e telefônicos disponibilizados pela empresa para execução de seu trabalho diário*".

As duas visões são convergentes e recorrentes na pesquisa: o usuário é aquele com acesso aos recursos da organização.

4.3.3.7 Consultoria CS3

O especialista de CS3 definiu usuário no seu contexto organizacional como "*qualquer entidade que faça uso das informações da empresa*".

Para esta organização, a figura do usuário não se restringe a pessoas e mesmo um sistema de informações pode ser considerado *usuário*.

4.3.3.8 Órgão público OP

Na resposta do especialista do órgão público OP, o usuário figura como "*aquele que tem acesso aos recursos computacionais da organização*".

4.3.4 Pergunta 4 - Que níveis de regulamentação derivam da política de segurança da informação na organização?

O objetivo principal desta pergunta foi identificar níveis de regulamentação derivados da política de segurança e também tentar detectar o conceito de cadeia normativa para a segurança da informação incluindo os significados dos níveis existentes em cada organização.

4.3.4.1 Banco público BG

Os dois entrevistados do banco público BG concordaram que formalmente existe apenas um nível de regulamentação na organização, reconhecido universalmente como

"*norma*". Entretanto, as normas contêm estruturas lógicas de vários níveis de regulamentação, a saber: políticas, procedimentos e padrões. Os procedimentos e padrões referenciam e precisam estar em conformidade com o nível ou os níveis lógicos superiores. Há sim uma hierarquia, mas em termos documentacionais existe apenas um nível de documento normativo.

Percebe-se a existência de uma cadeia tácita de regulamentação, formalizada através de um tipo de documento denominado "*norma*".

4.3.4.2 Banco misto BM1

À quarta pergunta, o especialista do banco BM1 respondeu que os níveis de regulamentação derivados da política de segurança da informação naquela organização são:

- Diretrizes;
- Normas gerais de segurança;
- Normas técnicas de segurança;
- Normas de classificação de informações; e,
- Procedimentos.

A resposta sugere que existe uma cadeia normativa definida segundo o contexto organizacional.

4.3.4.3 Banco misto BM2

O entrevistado do banco BM2 respondeu que em sua organização existem três níveis normativos de regulamentação derivados das políticas de segurança da informação:

- Nível genérico;
- Nível de usuário; e,
- Nível técnico.

Neste banco, conforme sugere a resposta, existe uma estrutura de regulamentação segmentada em três níveis que direcionam o público alvo das normas.

4.3.4.4 Banco privado BP

Segundo o entrevistado do banco privado BP, há quatro principais políticas derivadas da política central de segurança da informação:

- Política de Senhas;
- Política de E-mail e Acesso a Internet;
- Política de Tratamento de Incidentes de Segurança;
- Política de Microinformática;
- Política do uso de planilhas (Bancos de dados em baixa plataforma/estações de trabalho); e,
- Política de Gestão de Acessos.

Também há naquela organização documentos para diretrizes e normas, gerenciados pelas áreas de risco e conformidade do banco e procedimentos derivados das políticas relacionadas acima.

Neste banco, há várias políticas de segurança derivadas de uma política de segurança da informação central para tratar de questões relativamente específicas. Outros níveis aparecem localizados para suprir demandas localizadas.

4.3.4.5 Consultoria CS1

Na empresa de consultoria CS1, segundo o entrevistado, há os níveis de diretrizes, políticas, normas, procedimentos, termos e instruções. Como exemplos de documentos de alguns desses níveis, elencou os seguintes:

- Procedimentos de controle da certificação ISO;
- Normas de uso da internet;
- Procedimentos de habilitação de usuário e senha;
- Política de Microinformática;
- Instruções de instalação de software e de cadastro de usuários; e,

– Termo de sigilo e confidencialidade.

Dentre as organizações pesquisadas a que apresentou a maior diversidade de níveis de regulamentação foi a CS1. Entretanto, não parece haver uma relação perfeitamente hierárquica entre elas e a resposta sugere que não há também uma vinculação rigorosa entre a estrutura administrativa da organização e os níveis de regulamentação.

4.3.4.6 Consultoria CS2

Os dois entrevistados da consultoria CS2 responderam que naquela organização existem os níveis de normas, diretrizes e regras, derivados da política de segurança da informação.

4.3.4.7 Consultoria CS3

Na organização CS3 existem os níveis de diretrizes, normas e procedimentos, segundo a resposta do especialista entrevistado.

4.3.4.8 Órgão público OP

De acordo com a resposta do especialista do órgão público OP, existem naquela organização os níveis de normas e regras, derivados da política de segurança da informação, formalizada por um "*Ato principal*", que é um documento institucional.

4.3.5 Pergunta 5 - De acordo com a visão corporativa da organização, defina cada um dos níveis de regulamentação derivados da política de segurança.

Com esta pergunta, a intenção era entender em que instância administrativa cada nível de regulamentação atua, além de captar a abrangência de cada um dos níveis existentes.

4.3.5.1 Banco público BG

Como relatado anteriormente, no banco público BG, existe apenas um nível documental normativo, institucionalizado como "*norma*".

Uma norma, naquela organização, pode conter políticas, padrões e procedimentos. As políticas refletem as linhas de conduta vigentes para a organização, os padrões denotam

configurações e modelos específicos que devem ser adotados e os procedimentos contêm o detalhamento operacional para a implementação dos itens das políticas, seguindo os moldes dos padrões.

4.3.5.2 Banco misto BM1

O entrevistado do banco BM1 apresentou as seguintes definições para os níveis de regulamentação derivados da política de segurança da informação:

- Diretrizes: definidas e aprovadas pelo Colegiado da Diretoria, servem para nortear as demais normas de segurança contidas na política de segurança da informação;
- Normas gerais de segurança: regras de conduta que deverão ser obedecidas por todos os empregados, terceiros, estagiários ou aqueles que tenham acesso às informações da empresa;
- Normas técnicas de segurança: regras definidas para todo o corpo técnico da área de tecnologia da informação, específicas para as atividades consideradas críticas e importantes para a segurança e continuidade dos negócios da empresa;
- Normas de classificação de informações: definem os procedimentos a serem adotados por toda a empresa para o transporte, armazenamento, descarte e divulgação de todas as informações geradas no âmbito da empresa; e,
- Procedimentos: especificações operacionais articuladas para implementar os processos relacionados à segurança da informação.

4.3.5.3 Banco misto BM2

No banco BM2, os níveis de regulamentação, segundo o especialista daquela organização entrevistado são os seguintes:

- Nível genérico - estratégico: diretrizes gerais que apresentam os objetivos do Banco no que concerne à proteção da informação em seus ativos tecnológicos, pessoas e processos;
- Nível de usuário - tático: normas para conscientização dos usuários quanto ao seu papel na manutenção da segurança da informação; e,

– Nível técnico - operacional: procedimentos e regras específicas para que a informação tenha um nível aceitável de segurança, quando do seu manuseio.

4.3.5.4 Banco privado BP

Segundo o especialista do banco privado BP, as políticas mencionadas, derivadas da política central de segurança da informação, determinam as condutas e processos relacionados sob o seu tema, no âmbito da organização.

Destas políticas específicas, podem ser derivados procedimentos que discorrem sobre a operacionalização dos itens das próprias políticas.

Outros documentos contendo diretrizes e normas, são gerenciados pelas áreas de risco e conformidade do banco e aplicam-se a processos específicos do negócio do banco.

4.3.5.5 Consultoria CS1

A definições apresentadas pelo especialista da CS1 foram as seguintes:

– Diretrizes: documentos estratégicos que refletem as vertentes da organização;

– Políticas: documentos que estruturam as diretrizes para o corpo da organização;

– Normas: documentos táticos que embasam juridicamente os aspectos do manuseio e tratamento da informação;

– Procedimentos: documentos operacionais que fornecem o direcionamento das atividades específicas dos usuários;

– Termos: documentos orientados juridicamente para estabelecimento formal de entendimento e aceitação das condições normatizadas;

– Instruções: documentos de detalhamento técnico dos procedimentos;

4.3.5.6 Consultoria CS2

Segundo os dois especialistas entrevistados da consultoria CS2, as definições para os níveis de regulamentação derivados das políticas naquela organização são:

– Normas: documentos que regulam as responsabilidades e atividades relativas à segurança da informação, em conformidade com a política de segurança da informação;

– Diretrizes: orientações para o comportamento dos usuários quanto à utilização dos recursos computacionais e das informações da empresa; e,

– Regras: padrões de uso dos recursos computacionais e das informações da empresa que o usuário tem o dever de seguir.

4.3.5.7 Consultoria CS3

O entrevistado da CS3 definiu assim os níveis de regulamentação derivados das políticas existentes naquela organização:

– Diretrizes: Definições de amplo espectro estabelecidas pela alta direção da organização em relação à segurança da informação;

– Normas: Definições que especificam como as informações devem ser utilizadas e armazenadas; e,

– Procedimentos: Detalhamentos que definem, passo a passo, as atividades relacionadas ao acesso, armazenamento e recuperação das informações.

4.3.5.8 Órgão público OP

De acordo com o entrevistado do órgão público OP, no seu contexto organizacional, as normas são os documentos derivados da política de segurança da informação que têm a finalidade de estabelecer os critérios para classificar, monitorar, controlar e contingenciar o uso de recursos tecnológicos. As regras, por sua vez, delimitam o modo de implementar os critérios definidos nas normas.

4.3.6 Pergunta 6 - A política de segurança e as demais instâncias de regulamentação são formais na organização? Por quê ?

A última pergunta da entrevista teve o objetivo de identificar, no contexto das organizações, o grau de formalidade da política de segurança da informação e dos níveis de regulamentação e entender o impacto da formalização junto aos indivíduos que manuseiam a informação organizacional.

4.3.6.1 Banco público BG

No contexto do banco público BP, tanto a política de segurança da informação quanto os padrões e procedimentos são formais e mantidos através da instituição "norma" implementada por um sistema de controle e uma base de dados.

Por conta da formalização e acesso universal na organização, nenhum colaborador pode alegar desconhecimento para descumprir os normativos.

Os processos administrativos e de auditoria interna tomam como base, além da legislação vigente no país, o manual normativo da organização, usando-o como letra de lei do contexto organizacional.

Também foi apontada como fator importante para a formalização o tamanho da empresa e a extensão das suas área de atuação.

4.3.6.2 Banco misto BM1

Conforme o especialista entrevistado do banco BM1, naquela organização todas as instâncias de regulamentação são formais.

Ele considerou como fatores importantes para a formalização a relevância e o caráter legal das questões abordadas na política de segurança da informação, e a necessidade de conscientização e comprometimento de todo o corpo funcional com as regras estabelecidas.

4.3.6.3 Banco misto BM2

O entrevistado do banco BM2 respondeu à sexta pergunta afirmando que naquela organização a política de segurança da informação é formalizada, assim como parte das normas, procedimentos e regras, que aparecem em manuais publicados internamente.

De acordo com ele, o banco caminha para universalizar e institucionalizar as regulamentações derivadas da política de segurança, patrocinado pelo compromisso da alta direção da empresa com segurança da informação.

4.3.6.4 Banco privado BP

Segundo o especialista do banco privado BP, a política de segurança da informação é publicada formalmente e um novo corpo normativo contendo uma nova política central e políticas derivadas está em vias de aprovação e serão publicadas formalmente.

4.3.6.5 Consultoria CS1

O entrevistado da consultoria CS1 respondeu que nem todas as regulamentações são formais e atribuiu o fato a questões de tempo e prioridade negocial da organização.

4.3.6.6 Consultoria CS2

Os representantes da consultoria CS2 responderam que todas os níveis de regulamentação são formais naquela organização e compõem o seu sistema de gestão de qualidade.

O segundo representante da CS2 considerou ainda que a formalização demonstra o zelo e a preocupação da empresa com relação às suas informações.

4.3.6.7 Consultoria CS3

De acordo com o representante entrevistado da CS3, as normas e procedimentos são formalmente registrados no manual de qualidade da organização. Ele atribuiu a formalização à necessidade de cumprimento dos programas de certificação de qualidade que a empresa obteve.

4.3.6.8 Órgão público OP

O especialista do órgão público OP respondeu que tanto a política de segurança da informação quanto os normativos derivados são formais, porém, até a data da entrevista, aguardavam a aprovação na instância superior do órgão.

4.3.7 Conclusões da entrevista

O conjunto de respostas obtidas nas entrevistas realizadas permitiu concluir que realizar segurança da informação e manter uma política de segurança da informação são objetivos comuns de todas as organizações incluídas na pesquisa.

Foi possível identificar dentre as definições para segurança da informação propostas pelos especialistas das organizações alguns enunciados com viés tecnológico. Entretanto, além do que se previa, pôde ser observada uma preocupação maior com o aspecto humano da segurança da informação. As respostas obtidas sugerem que a forma tradicional de se pensar a segurança da informação, considerando somente ferramentas e tecnologias aplicadas sobre os processos da organização, estão cedendo lugar à busca por definições

mais abrangentes, que envolvam significativamente as pessoas e os objetivos de negócio das organizações.

Outro ponto observado nas definições de segurança da informação apresentadas pelos entrevistados é a carência por enunciados que expressem claramente o que é a Segurança da Informação. A visão do que ela realiza, ou ainda, de que comporia "*um conjunto de processos organizacionais*" foi recorrente para tentar prover, sem sucesso, uma definição objetiva para o termo. Esta condição reflete a necessidade de avanços no estudo de segurança da informação, e de abertura para novas propostas, que consigam enxergá-la como um fenômeno social.

Nas definições propostas para política de segurança da informação houve uma diversidade de conceitos e nenhum consenso sobre o que é e o deve estar realmente sob a abrangência da política de segurança da informação, apesar de todos reconhecerem a importância da existência da política como instituição no campo de segurança da informação.

Observou-se também que todos consideraram importante a formalização das políticas de segurança e dos instrumentos de regulamentação, mesmo aqueles que não a tem por completo.

Um resultado significativo é que todas as organizações pesquisadas, independentemente do tamanho, implementam algum tipo de cadeia de regulamentação para a segurança da informação, variando de organização para organização o número de níveis, a abrangência de cada um deles, o significado perante a comunidade organizacional e a relação com os demais níveis.

Os resultados sugerem que há espaço nos ambientes organizacionais para a adoção de um modelo de cadeia de regulamentação para segurança da informação, nos moldes da cadeia apresentada neste trabalho. Obviamente, são necessários ajustes nos modelos atuais para que os resultados sejam efetivos.

O resultado esperado mediante a adoção de um modelo de cadeia nas organizações, tal qual é discutida nesta dissertação, é a efetiva estruturação dos aspectos normativos da segurança da informação, o entendimento sobre o posicionamento e tratamento de cada nível proposto e definições claras para a Segurança da Informação, política de segurança da informação, diretrizes, normas e processos de segurança da informação.

5 Conclusão

A partir da percepção de que os modelos organizacionais de regulamentação de segurança da informação vigentes careciam de uma estruturação fundamentada cientificamente, esta dissertação buscou estabelecer um modelo de cadeia sustentado metodologicamente, que estivesse de acordo com os conceitos da Arquitetura da Informação, que refletisse o planejamento estratégico organizacional e que considerasse uma abordagem social para a Segurança da Informação.

A observação do cotidiano, respaldada pela pesquisa de campo realizada, permitiu identificar que a inconsistência entre os planejamentos estratégicos e as visões de segurança da informação das organizações introduzem distorções nos seus modelos normativos, tornando-os ineficientes, quando não inexeqüíveis.

As visões vigentes de segurança da informação, salvo raras exceções, desconsideram ou subestimam a figura do usuário desde a sua definição, o que inevitavelmente dificulta e elaboração de regulamentação de segurança da informação destinada a tais usuários.

Por outro lado, uma visão de fenômeno social para a segurança da informação, recentemente demarcada e amplamente utilizada neste trabalho, percebe o usuário como a figura central da segurança da informação, cuja existência passa a depender das relações fenomenológicas dos usuários com os recursos informacionais.

A fragilidade dos modelos normativos em segurança da informação atuais, ocasionada pelo uso de definições incompletas ou equivocadas para a Segurança da Informação e pela falta de alinhamento da segurança da informação com os planejamentos estratégicos organizacionais, introduz efeitos colaterais nas culturas organizacionais, com destaque para o surgimento de resistências por parte parte dos corpos organizacionais à introdução de conceitos de segurança da informação nas próprias culturas organizacionais.

Partindo dos princípios organizacionais, foram adotadas definições compatíveis com a abordagem social para a segurança da informação escolhida, de *política*, *política de informação* e *política de segurança da informação*, objetivando o estabelecimento dos

elementos da cadeia normativa no nível estratégico das decisões organizacionais.

Na continuidade da cadeia, no âmbito do nível tático foram elaboradas as definições para os elementos *diretriz* e *norma*.

Encerrando a cadeia, foi adotada uma definição de processo organizacional para o nível operacional de decisão organizacional, consistente com o restante do modelo e com a visão social da segurança da informação.

Todos os elementos da cadeia proposta relacionam-se com o planejamento estratégico situacional e dele dependem para instruir suas aplicações: as *políticas de segurança da informação* são determinantes para os momentos *explicativo*, *normativo* e *estratégico* do planejamento estratégico situacional.

Os planos obtidos como produtos do momento estratégico orientam as *diretrizes* e *normas*, que passam a influenciar, conjuntamente com os *processos organizacionais*, o momento *tático/operacional* do planejamento estratégico situacional.

Contextualizando a cadeia, foi possível entender e expressar o papel de cada um dos elementos nos níveis da epistemologia, da ciência e da prática, e relacionar os componentes associados a esses níveis.

A pesquisa qualitativa de campo permitiu reconhecer a validade do modelo especificado, ao identificar espaço nos contextos organizacionais para a implementação da cadeia normativa proposta.

Por fim, considera-se que a presente proposta de modelo de cadeia normativa estabelece várias possibilidades para temas de trabalhos futuros, dentre os quais podem ser sugeridos:

- Derivações da cadeia para aspectos normativos específicos vinculados a políticas específicas das organizações diferentes das políticas de segurança da informação;
- Modelos e Métodos para implementação da cadeia normativa em contextos organizacionais gerais ou específicos;
- Estudos de casos organizacionais orientados a métodos para implementação da cadeia normativa;
- Elaboração de modelos de operacionalização alternativos ao modelo automatizado e estabelecendo suas ligações e interfaces no contexto da cadeia normativa;

- Avaliação de impacto sobre a cultura organizacional após a implementação da cadeia normativa em um contexto organizacional; e,
- Modelo de comunicação para a implementação da cadeia normativa em um ambiente organizacional produtivo com características normativas diferentes das propostas.

Índice Remissivo

Referências

ABNT, Associação Brasileira de Normas Técnicas. *Tecnologia da informação - Código de prática para a gestão da segurança da informação*: Nbr iso/iec 17799:1999. Rio de Janeiro, 2000.

ABNT, Associação Brasileira de Normas Técnicas. *Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos*: Nbr iso/iec 27001:2005. Rio de Janeiro, 2005.

ANDERSON, James. Why we need a new definition of information security. *Computers Security*, v. 22, n. 4, p. 308–313, 2003.

BAILEY, Samantha. Information architecture: a brief introduction. março 2003. Disponível em: <http://iainstitute.org/tools/download/Bailey-IAIntro.pdf>. Acesso em: abril de 2007.

BARKER, Iain. What is information architecture? maio 2005. Disponível em: <www.steptwo.com.au/papers/kmc_whatisinfoarch/index.html>. Acesso em: abril de 2007.

BÖORZEL, Tanja A. Organizing babylon: on the different conceptions of policy networks. *Public Administration*, v. 76, n. 2, p. 252–273, janeiro 1998.

BUSH, Vannevar. As we may think. the atlantic on-line. *The Atlantic Monthly*, n. 1, p. 101–108, julho 1945. Disponível em: <http://www.theatlantic.com/unbound/flashbks-/computer/bushf.htm>. Acesso em: abril de 2007.

CALDER, Alan; WATKINS, Steve. *International IT governance: an executive guide to ISO 17799/ISO 27001*. USA: Kogan Page, 2006.

CAPURRO, Rafael. Epistemologia e ciência da informação. In: ENANCIB. *5º Encontro Nacional de Pesquisa em Ciência da Informação*. Belo Horizonte, 2003.

CASTELLS, Manuel. *A sociedade em rede*. 7. ed. [S.l.]: Paz e Terra, 2003.

CLARKE, Roger. Introduction to information security. fevereiro 2001. Disponível em: <http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html>. Acesso em: maio de 2007.

COADIC, Yves-François Le. *A ciência da informação*. 2. ed. Brasília: Briquet de Lemos, 2004.

COBIT, COBIT Steering Committee. *COBIT Framework*. 3. ed. [S.l.]: IT Governance Institute, 2000.

DAVENPORT, Thomas H. *Ecologia da Informação*. São Paulo: Futura, 2001.

DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books do Brasil, 2000.

EVERNDEN, Roger; EVERNDEN, Elaine. Third-generation information architecture. *Communications of the ACM*, v. 46, n. 3, p. 95–09, Março 2003.

FERREIRA, Ediene. Comunicação e cultura nas organizações. 2005. Disponível em: <http://www.pucrs.br/famecos/geacor/texto2-03.html>. Acesso em: maio de 2007.

FERREIRA, Rubens S. A sociedade da informação no brasil: um ensaio sobre os desafios do estado. *Ciência da Informação*, v. 32, n. 1, p. 36–41, jan/abr 2003.

FLEURY, Maria Teresa L. Estórias, mitos, heróis - cultura organizacional e relações do trabalho. *Revista de Administração de Empresas*, São Paulo, v. 27, n. 4, p. 7–18, out/dez 1987.

FONSECA, Edson. *Introdução à Biblioteconomia*. São Paulo: Livraria Pioneira, 1991.

FREITAS, Maria Ester de. *Cultura organizacional: formação, tipologias e impactos*. São Paulo: Makron, 1991.

FREITAS, Sidinéia. Cultura organizacional e comunicação. In: *Obtendo resultados com relações públicas*. São Paulo: Pioneira, 1997.

GIGCH, John P. van; PIPINO, Leo L. In search for a paradigm for the discipline of information systems. *Future Computing Systems*, v. 1, n. 1, p. 71–97, 1986.

GIL, Antonio C. *Métodos e técnicas de pesquisa social*. 5. ed. São Paulo: Atlas, 1999.

GILCHRIST, Alan; MAHON, Barry. *Information architecture: designing information environments for purpose*. Londres: Facet Publishing, 2004.

GREENHALGH, Trisha; TAYLOR, Rod. *How to read a paper: papers that go beyond numbers (qualitative research)*. Londres: BMJ Publishing Group, 1997.

HAMPTON, David. *Administração: processos administrativos*. São Paulo: McGraw-Hill, 1990.

HAVE, Steven Ten et al. *Modelos de gestão: o que são e quando devem ser usados*. Londres: Pearson, 2003.

HEIDEGGER, Martin. *Ser e tempo*. Petrópolis: Vozes, 1988.

HESSEN, Johannes. *Teoria do conhecimento*. São Paulo: Martins Fontes, 1998.

HOUAISS. *Dicionário Houaiss da Língua Portuguesa*. Universo On Line, 2000. Disponível em: <http://houaiss.uol.com.br>. Acesso em: abril de 2007.

HUSSERL, Edmund. *The crisis of european sciences and transcendental phenomenology: an introduction to phenomenological philosophy*. Evanston, Illinois: Northwestern University Press, 1970.

HUSSERL, Edmund. *Idéia da fenomenologia*. Lisboa: Ed 70, 1990.

HUSSERL, Edmund. *Investigações lógicas: Sexta investigação - elementos de uma elucidação fenomenológica do conhecimento*. São Paulo: Nova Cultural, 1996.

IBM, Global Services. Ibm and the it infrastructure library: How ibm supports itil and provides itil-based capabilities and solutions. Somers, NY, 2003. Disponível em: <http://www-5.ibm.com/services/ch/ism/download_ism/itil.pdf>. Acesso em: maio de 2007.

ISACA, Information Systems Audit *and* Control Association. Isaca overview and history. *Site Institucional - ISACA*, Rolling Meadows, Illinois, 2007. Disponível em: <http:-//www.isaca.org/Content/NavigationMenu/About_ISACA/Overview_and_History-/Overview_and_History.htm>. Acesso em: abril de 2007.

ISO27001, ISO 27001 Security. Iso 27001 security. março 2006. Disponível em: <http://www.iso27001security.com/html/iso27001.html>.

JAPIASSU, Hilton. *Dicionário básico de filosofia*. 3. ed. Rio de Janeiro: Zahar, 1996.

JÚNIOR, João Ribeiro. *Introdução à Fenomenologia*. Campinas: Edcamp, 2003.

KAY, Adrian. A critique of the use of path dependency in policy studies. *Public Administration*, v. 83, n. 3, p. 553–571, agosto 2005.

KUHN, Thomas S. *A estrutura das revoluções científicas*. 6. ed. São Paulo: Perspectiva, 2001.

KUNSCH, Margarida M. K. *Obtendo resultados com relações públicas*. São Paulo: Pioneira, 1997.

LEME, Maria Tereza; FISCHER, Rosa Maria. *Cultura e poder nas organizações*. Rio de Janeiro: Atlas, 1991.

LIEBSCHER, Peter. *Quantity with quality? Teaching quantitative and qualitative methods in a LIS Master's program*. [S.l.]: Library Trends, 1998.

LIMA-MARQUES, Mamede. Políticas de segurança da informação. *Treinamento em Segurança da Informação - SERPRO*, dezembro 2006.

LIMA-MARQUES, Mamede. Notas de aulas. *Universidade de Brasília*, junho 2007.

LIMA-MARQUES, Mamede; DUARTE, Jorge. Processos organizacionais. *Treinamento em planejamento estartégico - STJ*, maio 2007.

LOWI, Theodore J. American business, public policy, case studies and political theory. *World Politics*, v. 16, n. 4, p. 677–715, 1964.

LÜBCKE, Poul. *A semantic interpretation of Husserl's epoché: a debate on technology and ethics*. EUA: Synthese, 1999.

MACEDO, Flávia L. O. *Arquitetura da informação: aspectos epistemológicos, científicos e práticos*. Dissertação (Mestrado em Ciência da Informação) — Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2005.

MARCHIORI, Marlene Regina. Comunicação é cultura. cultura é comunicação. *Comunicação Empresarial*, n. 31, 2T 1999. Disponível em: <http://www.portal-rp.com.br/bibliotecavirtual/culturaorganizacional/0067.htm>. Acesso em: maio de 2007.

MARCIANO, João Luiz P. *Segurança da informação: uma abordagem social*. Dissertação (Doutorado em Ciência da Informação) — Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006.

MARTINS, José Carlos. *Gestão de projetos de segurança da informação*. Rio de Janeiro: Brasport, 2003.

MATUS, Carlos. *Política, Planejamento & Governo - Tomos I e II*. Brasília: IPEA, 1993.

MATUS, Carlos. *O Método PES: roteiro de análise teórica*. São Paulo: FUNDAP, 1997.

MCDANIEL, George. *IBM Dictionary of Computing*. New York, NY: McGraw-Hill, 1994.

MERLEAU-PONTY, Maurice. *Fenomenologia da Percepção*. Rio de Janeiro: Freitas Bastos, 1971.

MICROSOFT, Academia de Segurança da Informação. Implementação prática do programa de segurança iso17799 / bs7799 / cobit - parte 1. *Programa integral de formação profissional em implementação prática de medidas de segurança da informação*, Microsoft, 2005.

MINGERS, John. Embodying informations systems: the contribution of phenomenology. *Information and organization*, v. 11, n. 2, p. 103–128, August 2001.

MIRANDA, Antonio; SIMEÃO, Elmira. *A conceituação de massa documental e o ciclo de interação entre tecnologia e o registro do conhecimento. In: Nakayama, H. (Org.) Análise da Informação*. Brasília: UnB, 2002.

MOODY, Daniel; WALSHI, Peter. Measuring the value of information: an asset evaluation approach. *European Conference on Information Systems*, 1999. Disponível em: <http://wwwinfo.deis.unical.it/~zumpano% -/2004-2005/PSI/lezione2-/ValueOfInformation.pdf>. Acesso em: maio de 2007.

MOOERS, Clovis N. Zatocoding applied to mechanical organization of knowledge. *American Documentation*, v. 2, p. 20–32, 1951.

OGC, Office of Government Commerce. Itil refresh statement. *Site Institucional*, 2005. Disponível em: <http://www.itil.co.uk/refresh.htm>. Acesso em: maio de 2007.

OLIVEIRA, Djalma. *Planejamento estratégico: conceitos, metodologia e práticas*. 22. ed. São Paulo: Atlas, 2005.

PELTIER, Thomas R. *Information security policies and procedures: a practitioner´s reference*. Boca Raton: Auerbach Publications, 1998.

PELTIER, Thomas R. *Information security risk analysis*. Boca Raton: Auerbach Publications, 2001.

PETTIGREW, Andrew M. A cultura organizacional é administrável? In: _____. *Cultura e poder nas organizações*. São Paulo: Atlas, 1996.

POPPER, Karl R. *Conjectures and refutations: The growth of scientific knowledge*. Londres: Routledge & Kegan Paul, 1963.

RENEKER, Maxine. A qualitative study of information seeking among members of na academic community: methodological issues and problems. *Library Quarterly*, v. 63, n. 4, Outubro 1993.

RIEG, Denise; FILHO, Targino Araújo. O uso das metodologias "planejamento estratégico situacional" e "mapeamento cognitivo" em uma situação concreta: o caso da pró-reitoria de extensão da ufscar. *Gestão & produção*, v. 9, n. 2, p. 163–179, Agosto 2002. Disponível em: <http://www.scielo.br/pdf/gp/v9n2/a05v09n2.pdf>. Acesso em: maio de 2007.

RIVERA, Carmen Cecilia. Descripción de cultura organizacional. *Dialogos de la comunicación*, Cali, Colômbia, n. 39, p. 36–41, junho 1994.

ROBREDO, Jaime. *Documentação de hoje e de amanhã*. 4. ed. Brasília: Edição do autor, 2005.

ROSA, Helaine Abreu. Organização e cultura organizacional: tentativas epistemológicas. *Comunicação Organizacional*, 2003. Disponível em: <http://www.pucrs.br/famecos-/geacor/texto16.html>. Acesso em: abril de 2007.

ROSENFELD, Louis; MORVILLE, Peter. *Information Architecture for the World Wide Web - designing large-scale Web Sites*. 3. ed. [S.l.]: O'Reilly, 2006.

ROVAI, Ricardo. Modelo estratégico de projeto para implantação da governança de ti: estudo de caso. *Revista BSP*, IPBSP-Instituto de Pesquisa BSP, São Paulo, n. 2, 2007. Disponível em: <http://www.revistabsp.com.br/0701/caso1% -.htm>. Acesso em: maio de 2007.

SANDERS, Patricia. Phenomenology: a new way of viewing organizational research. *Academy of Management Review*, v. 7, n. 3, p. 353–360, julho 1982.

SARACEVIC, Tefko. Interdisciplinary nature of information science. *Ciência da Informação*, v. 24, n. 1, 1995.

SARACEVIC, Tefko. Ciência da informação: origem, evolução e relações. *Perspectivas em Ciência da Informação*, v. 1, n. 1, p. 41–62, jan./jul. 1996.

SCHAIK, Edward A. Van. *A Management system for the Information Business*. 2. ed. USA: Red Swan Publishing, 2006.

SCHEIN, Edgar H. *Guia de sobrevivência da cultura corporativa*. Rio de Janeiro: José Olympio, 2001.

SEARLE, John R. *The construction of social reality*. New York: THe Free Press, 1995.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003.

SMITH, David Woodruff. Phenomenology. *The Stanford Encyclopedia of Philosophy*, Winter 2003. Disponível em: <http://plato.stanford.edu/archives/win2003/entries-/phenomenology>. Acesso em: maio de 2007.

SOARES, Hebbertt de Farias. *Uma contribuição da fenomenologia para a arquitetura da informação.* Dissertação (Monografia (Graduação em Biblioteconomia)) — Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2004.

SROUR, Robert Henry. *Poder, cultura e ética nas organizações*. Rio de Janeiro: Campus, 1998.

STEGMÜLLER, Wolfgang. *A filosofia contemporânea: introdução crítica*. São Paulo: EdUSP, 1977.

STRAIOTO, Fabiana. *A arquitetura da informação para a World Wide Web: um estudo exploratório*. Dissertação (Dissertação (Mestrado em Ciência da Informação)) — Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2002.

SUMMERS, Rita C. *Secure computing: threats and safeguards*. New York: McGraw-Hill, 1997.

TORQUATO, Gaudêncio. *Cultura, poder, comunicação e imagens: fundamentos da nova empresa*. São Paulo: Pioneira, 1991.

TRIVIÑOS, Augusto. *Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação*. São Paulo: Atlas, 1987.

VERGEZ, André; HUISMAN, Denis. *Historia dos filósofos*. 3. ed. Rio de Janeiro: Freitas Bastos, 1976.

WEILL, Peter; ROSS, Jeanne W. *IT Governance - how top performers manage IT decision rights for superior results*. Boston, Massachusetts: Harvard Business School Publishing, 2004.

WERSIG, Gernot. Information science: the study of postmodern knowledge usage. *Information Processing & Management*, v. 29, n. 2, p. 229–239, mar/abr 1993.

WIKIPEDIA, Encyclopedia. Information technology infrastructure library. Wikimedia Foundation, Inc, 2006. Disponível em: <http://en.wikipedia.org/wiki/ITIL>. Acesso em: abril de 2007.

WURMAN, Richard S. *Ansiedade de informação*. São Paulo: Cultura, 1991.