



**PUC**  
**CAMPINAS**  
PONTIFÍCIA UNIVERSIDADE CATÓLICA

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS  
E DE TECNOLOGIAS

**PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO-SENSU***

**CARLOS ALBERTO PONCINELLI FILHO**

**MAPEAMENTO DE PROCESSOS BASEADO EM  
CONTROLES PARA GOVERNANÇA DE  
TECNOLOGIA DA INFORMAÇÃO**

**PUC – CAMPINAS**

**2007**

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

**GRÃO CHANCELER**

Dom Bruno Gamberini

**MAGNÍFICO REITOR**

Prof. Pe. Wilson Denadai

**VICE-REITOR**

Profa. Dra. Ângela de Mendonça Engelbrecht

**PRÓ-REITORA DE PESQUISA E PÓS-GRADUAÇÃO**

Profa. Dra. Vera Engler Cury

**DIRETOR DO CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE  
TECNOLOGIAS**

Prof. Dr. Orandi Mina Falsarella

**COORDENADOR DO PROGRAMA DE  
POS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA  
CURSO DE MESTRADO PROFISSIONAL EM  
TELECOMUNICAÇÕES  
ÁREA DE CONCENTRAÇÃO: GESTÃO DE REDES DE  
TELECOMUNICAÇÕES**

Prof. Dr. Omar Carvalho Branquinho

CARLOS ALBERTO PONCINELLI FILHO

MAPEAMENTO DE PROCESSOS BASEADO EM  
CONTROLES PARA GOVERNANÇA DE  
TECNOLOGIA DA INFORMAÇÃO

Dissertação apresentada como exigência para obtenção do título de Mestre em Engenharia Elétrica, ao Programa de Pós-Graduação na área de Gestão de Redes de Telecomunicações – Gestão de Redes e Serviços, Pontifícia Universidade Católica de Campinas.

Orientador: Prof. Dr. Ettore Bresciani Filho

PUC – CAMPINAS

2007

Ficha Catalográfica  
Elaborada pelo Sistema de Bibliotecas e  
Informação - SBI - PUC-Campinas

t658.4038 Poncinelli Filho, Carlos Alberto.  
P795m Mapeamento de processos baseado em controles para governança de tecnologia da  
informação / Carlos Alberto Poncinelli Filho. - Campinas: PUC-Campinas, 2007.  
143p.

Orientador: Ettore Bresciani Filho.  
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de  
Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.  
Inclui anexos e bibliografia.

1. Tecnologia da Informação - Administração. 2. Reengenharia (Administração).  
3. Framework (Programa de computador). 4. Telecomunicações. 5. Gestão de conhecimento.  
6. Gestão de empresas. 7. Governança. 8. Metadados. I. Bresciani Filho, Ettore. II. Pontifícia  
Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias.  
Pós-Graduação em Engenharia Elétrica. III. Título.

CDD 19.ed – t658.4038

**BANCA EXAMINADORA**

**Presidente e Orientador Prof. Dr. Ettore Bresciani Filho**

**1o Examinador Profa. Dra. Marina Rodrigues de Aguiar**

**2o Examinador Prof. Dr. Fernando Ernesto Kintschner**

**Campinas, 27 de abril de 2007.**

**CARLOS ALBERTO PONCINELLI FILHO**

**MAPEAMENTO DE PROCESSOS BASEADO EM  
CONTROLES PARA GOVERNANÇA DE TECNOLOGIA  
DA INFORMAÇÃO**

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações

Área de Concentração: Gestão de Redes e Serviços .

Orientador: Prof. Dr. Ettore Bresciani Filho

Dissertação defendida e aprovada em 27 de abril de 2007 pela Comissão Examinadora constituída dos seguintes professores:



Prof. Dr. Ettore Bresciani Filho  
Orientador da Dissertação e Presidente da Comissão Examinadora  
Pontifícia Universidade Católica de Campinas.



Prof. Dr. Fernando Ernesto Kintschner  
Pontifícia Universidade Católica de Campinas.



Profa. Dra. Marina Rodrigues de Aguiar  
Universidade Estadual de Campinas

À minha esposa Alessandra e filha Gabriela pelo apoio, compreensão e força durante todo este tempo de dedicação.

À minha mãe Martha pelo total incentivo,

À memória de meu pai Carlos Alberto pelos marcantes ensinamentos.

## AGRADECIMENTOS

A DEUS pelo dom da vida.

Ao professor Dr. Ettore Bresciani Filho  
Incentivador, mestre e guia sempre presente e aplicado em minha formação profissional, além de amigo sincero em toda esta jornada.

Ao professor MSc Eng. Sérgio Roberto Pereira  
Por todo seu empenho e dedicação para com este curso.

À incansável colaboração de revisão e sugestão do colega MSc Anchizes do Egito L. G. Filho, Analista de Sistemas da Petrobras.

Aos colegas de trabalho  
Pelas trocas de experiência, críticas e discussões construtivas.

Aos colegas da turma  
Pelo apoio, incentivo e espírito de equipe durante as aulas, os trabalhos, as apresentações e as críticas construtivas.

À Luzia de Fátima Ataguile Campos Ferraz  
Pelo apoio administrativo tão presente.

À Marjorie Helena Salim Rossignatti  
Bibliotecária da PUC-Campinas pelo empenho na orientação técnica desta dissertação.



“O importante é não seguir nunca os caminhos  
já trilhados, mas procurar sempre novos  
atalhos.”

Graham Bell  
(1847 – 1922)

## RESUMO

PONCINELLI FILHO, Carlos Alberto. **Mapeamento de processos baseado em controles para governança de tecnologia da informação**. 2007. 143f. Dissertação (Mestrado em Engenharia Elétrica) – Pós-graduação em gestão de redes e telecomunicações, Pontifícia Universidade Católica de Campinas, Campinas.

Pesquisa para desenvolvimento de um modelo para mapeamento de processos baseado em controles para a governança de tecnologia da informação. As organizações têm procurado cada vez mais, ter sob controle seus processos de governança, porém, escolher, adotar e utilizar modelos que melhor se adaptem às sua realidade não é tarefa fácil. Este trabalho propõe o desenvolvimento de um processo de Governança de Tecnologia da Informação utilizando o método de estudo de sistemas, denominado Sistemografia para atender as determinações da Lei *Sarbanes-Oxley*. Tal processo está baseado em modelo de controles por objetivos, denominado “Control Objectives for Information and related Technology” (COBIT). Todos esses fatores estão intrinsecamente presentes nas empresas que façam gestão de suas tecnologias, principalmente empresas de telecomunicações que estão relacionadas com a teleinformática e as redes multi-serviço. De forma específica os objetivos são: descrever os elementos que compõem as Governança e a Arquitetura Empresariais; descrever as Seções da Lei *Sarbanes-Oxley*, relacionando-as com o modelo COBIT; descrever o processo para gestão utilizando o método de sistemografia; e propor uma moldura (*framework*) para a gestão dos dados e metadados para Governança de TI, associando um painel de controle (*dashboard*), baseado na maturidade dos processos, de maneira a medi-los em seu estado atual e projetar o estágio estratégico desejado.

### **Palavras-Chave**

Governança de Tecnologia da Informação, COBIT, Sistemografia, Teleinformática, Metadados, Mapeamento de Processos

# ABSTRACT

PONCINELLI FILHO, Carlos Alberto. **Process mapping based in controls for governance of technology informations.** 2007. 143f. Dissertação (Mestrado em Engenharia Elétrica) – Pós-graduação em gestão de redes e telecomunicações, Pontifícia Universidade Católica de Campinas, Campinas.

*Research for the development of a process-mapping model based on control patterns to manage information technology. There is a trend for organizations to try and have their management processes under control; however, choosing, implementing and using the models which would best adapt to their reality are not easy tasks. This paper proposes the development of an information technology Management process using the systems study method named "Sistemografia" in order to meet the demands of the Sarbanes-Oxley law. This process is based on a model of control by objective, named "Control Objectives for Information and related Technology" (COBIT). All of these factors are embedded in companies that manage their technologies, especially telecommunications companies related to tele-information technology and to the multi-service nets. In short, the objectives are: to describe the elements that compose Company Management and Architecture; to describe the articles of the Sarbanes-Oxley law, relating them to the COBIT model; to describe the management model using the "sistemografia" method; and to propose a framework for data management and metadata for the Management of IT, associating a dashboard, and based on the maturity of the processes, so as to measure them at their present stage and plan the aimed strategic stage.*

## **Key Words**

*Information Technology Governance, COBIT, Sistemografia, Tele-information, Metadata, Process-mapping*

# LISTA DE FIGURAS

<b>FIGURA 1</b> – Esquema para a Governança Empresarial .....	26
<b>FIGURA 2</b> – <i>Framework</i> da Matriz de Zachaman .....	29
<b>FIGURA 3</b> – Arquitetura para BI com foco em metadados.....	33
<b>FIGURA 4</b> – Principais elementos de um metamodelo que atenda aos requisitos da Lei SOX e do modelo COBIT para os sistemas empresariais.....	34
<b>FIGURA 5</b> – Metamodelo para qualidade de dados.....	35
<b>FIGURA 6</b> – Família COBIT de produtos.....	40
<b>FIGURA 7</b> – Cubo de Governança de TI.....	42
<b>FIGURA 8</b> – Processos de TI do COBIT agrupados em quatro domínios .....	43
<b>FIGURA 9</b> – Transição de requisitos para os critérios de informação .....	46
<b>FIGURA 10</b> – Representação da estrutura genérica do Processo e componentes.....	48
<b>FIGURA 11</b> – Objetivos de Controle de alto nível COBIT – Tabela Resumo.....	50
<b>FIGURA 12</b> – Modelo de maturidade baseado no CMMI .....	51
<b>FIGURA 13</b> – Processos de TI do Domínio COBIT .....	58
<b>FIGURA 14</b> – Níveis de desdobramento dos processadores.....	94
<b>FIGURA 15</b> – Nível ‘macro’ da sistemografia para os quatro domínios COBIT .....	97
<b>FIGURA 16</b> – Sistemógrafo operacional dos processos COBIT .....	111
<b>FIGURA 17</b> – Sistemógrafo informacional dos processos COBIT .....	113
<b>FIGURA 18</b> – Sistemógrafo decisional dos processos COBIT.....	115
<b>FIGURA 19</b> – Estrutura para representação da governança integrada .....	120
<b>FIGURA 20</b> – <i>Dashboard</i> para controle do processo, baseado no modelo de maturidade CMMI .....	125
<b>FIGURA 21</b> – Ilustração do Gráfico de Radar para análise de lacunas dos processadores ...	126

# LISTA DE QUADROS

<b>QUADRO 1</b> – Principais componentes, seus relacionamentos dentro da estrutura de metadados e as respectivas descrições .....	33
<b>QUADRO 2</b> – Entidades do metamodelo e suas respectivas definições .....	35
<b>QUADRO 3</b> – Descritivo dos grupos de foco e a interação com o COBIT .....	39
<b>QUADRO 4</b> – Descritivo para os recursos de TI e ações desempenhadas para realizar as tarefas .....	45
<b>QUADRO 5</b> – Definições para os Critérios de Informação relacionadas aos requisitos do negócio .....	47
<b>QUADRO 6</b> – Escala para o modelo de maturidade adotado pelo COBIT .....	52
<b>QUADRO 7</b> – Relação dos títulos originais da Lei <i>Sarbanes-Oxley</i> .....	54
<b>QUADRO 8</b> – Classificação dos níveis de complexidade dos processadores.....	96
<b>QUADRO 9</b> – Análise para o processador PO1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	98
<b>QUADRO 10</b> – Análise para o processador PO2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	99
<b>QUADRO 11</b> – Análise para o processador PO8 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	100
<b>QUADRO 12</b> – Análise para o processador PO9 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	101
<b>QUADRO 13</b> – Análise para o processador AI6 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	101
<b>QUADRO 14</b> – Análise para o processador DS1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	102
<b>QUADRO 15</b> – Análise para o processador DS2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	103
<b>QUADRO 16</b> – Análise para o processador DS4 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	104
<b>QUADRO 17</b> – Análise para o processador DS6 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	105
<b>QUADRO 18</b> – Análise para o processador DS11 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	106
<b>QUADRO 19</b> – Análise para o processador M1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	106
<b>QUADRO 20</b> – Análise para o processador M2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	107
<b>QUADRO 21</b> – Análise para o processador M3 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	108

<b>QUADRO 22</b> – Análise para o processador M4 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.....	109
<b>QUADRO 23</b> – Conexões entre os processadores de entrada e de saída .....	116
<b>QUADRO 24</b> – Matriz de relação dos processadores em nível “meso”, contendo categoria, tipo e nível de complexidade.....	117
<b>QUADRO 25</b> – <i>Framework</i> proposto para os itens relacionados ao processador em análise .....	122
<b>QUADRO 26</b> – Instruções para preenchimento do <i>framework</i> proposto para o acompanhamento e controle do processo.....	123
<b>QUADRO 27</b> – Etapas para implementar a gestão de dados e metadados .....	128

# SUMÁRIO

<b>1. INTRODUÇÃO .....</b>	<b>18</b>
1.1 Considerações gerais: A governança empresarial em um cenário globalizado....	18
1.2 Objetivo geral .....	19
1.3 Objetivos específicos .....	20
1.4 Justificativas .....	21
1.5 Método de estudo.....	22
1.6 Organização da dissertação .....	23
<b>2. ARQUITETURA EMPRESARIAL, GOVERNANÇA, QUALIDADE DE DADOS E METADADOS .....</b>	<b>25</b>
2.1 Considerações iniciais.....	25
2.2 Governança empresarial.....	25
2.3 Governança corporativa e de negócios .....	26
2.4 Governança de TI.....	26
2.5 Arquitetura empresarial.....	27
2.6 Arquitetura de informação.....	30
2.7 Qualidade de dados .....	30
2.8 Metadados .....	31
2.8.1 Significado do termo metadados.....	31
2.8.2 Repositório de metadados.....	32
2.8.3 Metamodelo .....	34
<b>3. MODELO DE GESTÃO PROPOSTO PELO COBIT .....</b>	<b>37</b>
3.1 Histórico do COBIT.....	37
3.2 COBIT no contexto de governança .....	37
3.3 Beneficiários de um modelo de governança.....	38
3.4 Família dos produtos componentes do COBIT .....	39
3.5 Estrutura proposta para o <i>Framework</i> COBIT .....	41
3.5.1 Descrição das características relacionadas aos domínios do COBIT .....	44
3.5.2 Descrição dos recursos de TI.....	45
3.5.3 Critérios de Informação para o COBIT.....	46
3.5.4 Estrutura genérica do processo .....	47
3.5.5 Representação e característica do processo.....	48
3.5.6 Definição e métrica para o modelo de maturidade .....	51
<b>4. LEI SARBANES-OXLEY – SOX, UTILIZANDO OS CONTROLES PROPOSTOS PELO COBIT .....</b>	<b>53</b>
4.1 Lei Sarbanes-Oxley – SOX .....	53
4.2. Títulos e Seções da Lei SOX relacionadas aos relatórios financeiros.....	55

4.3	Lei SOX, Título III, Seção 302 – Responsabilidade corporativa sobre os relatórios financeiros .....	55
4.4	Lei SOX, Título IV, Seção 404 – Avaliação anual dos controles e procedimentos internos para a emissão de relatórios .....	56
4.5	Lei SOX, Título IX, Seção 906 – Responsabilidade corporativa pelos relatórios financeiros .....	56
4.6	Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 referentes ao aspecto: “dados” e “metadados” .....	56
4.6.1	Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “PO – Planejamento e Organização” com recursos de TI para o aspecto: “dados” e “metadados” ...	58
4.6.2	Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “AI – Aquisição e Implementação” com recursos de TI para o aspecto: “dados” e “metadados” .....	68
4.6.3	Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “DS – Entrega e Suporte” com recursos de TI para o aspecto: “dados” e “metadados” .....	70
4.6.4	Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “MO – Monitoramento” com recursos de TI para o aspecto: “dados” e “metadados” .....	81

## **5. MODELAGEM DE PROCESSOS PARA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO ..... 91**

5.1	Sistemografia .....	91
5.1.1	Construção do sistemógrafo de um processo .....	92
5.1.2	Processadores e suas subdivisões .....	92
5.1.3	Classificação dos processadores segundo a categoria.....	94
5.1.4	Classificação dos processadores segundo o tipo de atividade.....	95
5.1.5	Classificação dos processadores segundo o nível de complexidade.....	95
5.2	Sistemografia aplicada aos processos para governança de TI com ênfase à gestão dos dados e metadados .....	97
5.2.1	Processos COBIT representados em nível “macro” .....	97
5.2.2	Processos COBIT representados em nível “meso” .....	98
5.2.3	Sistemógrafo dos processos COBIT representado em nível “meso” .....	109
5.2.4	Conexão entre os processos COBIT representados em nível “meso” .....	116
5.2.5	Análise dos resultados .....	117

## **6. PROPOSTA DE FRAMEWORK E DASHBOARD PARA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO..... 119**

6.1	Contexto para se implementar a governança de TI .....	119
6.2	Proposta de um <i>framework</i> para gerir a governança de TI .....	121
6.2.1	<i>Framework</i> proposto para controle e acompanhamento do processo .....	121
6.2.2	<i>Dashboard</i> proposto para avaliação das lacunas .....	124
6.2.3	Gráfico de radar proposto para avaliação das lacunas .....	126



6.3	Procedimentos para a análise dos resultados.....	127
6.3.1	Análise pelos processos sistemografados.....	127
6.3.2	Análise pelo modelo de maturidade.....	127
6.3.3	Análise pelos objetivos de controle .....	127
6.4	Etapas e procedimentos para a aplicação da gestão dos dados e dos metadados	128
<b>7. CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS.....</b>		<b>130</b>
7.1	Objetivo geral atingido.....	130
7.2	Objetivos específicos atingidos .....	131
7.3	Áreas de aplicação .....	131
7.4	Recomendações para trabalhos futuros.....	132
<b>REFERÊNCIAS .....</b>		<b>133</b>
<b>ANEXOS</b>		

# 1. INTRODUÇÃO

---

---

## 1.1 Considerações gerais: A governança empresarial em um cenário globalizado

As empresas inseridas em um ambiente cada vez mais globalizado têm buscado o crescimento ou a ampliação do seu escopo de atuação para o nível transnacional, e desta maneira estar presente em quase todos os países do mundo.

Para que isto ocorra, tais empresas vão conquistando clientes, adquirindo outras empresas ou buscando novos segmentos de mercado. Na maioria das vezes, esta expansão requer cifras financeiras da ordem de milhões ou bilhões de dólares, e o caminho para obtê-las é por meio do lançamento de ações em bolsas de valores, situadas nos países de economia sólida. Desta maneira as empresas garantem recursos para financiamento da produção, a um menor custo do que aquele obtido em empréstimos (BOVESPA, 2006).

Uma dessas bolsas de valores encontra-se no mercado dos EUA e é conhecida como *New York Stock Exchange* (NYSE), nela estão concentradas as ações de duas mil e oitocentas empresas, perfazendo um valor global de mercado de aproximadamente US\$ 20 trilhões. Deste total de empresas, trinta e sete são companhias brasileiras (NYSE GROUP, 2006).

Por outro lado, alguns dirigentes de empresas, desejando obter recursos financeiros a qualquer preço, passaram a infringir as leis e a mascarar os balanços contábeis, o que colocou em risco a credibilidade das bolsas de valores. Os casos mais críticos vieram à tona em 2001 e 2002 com a falência das empresas americanas, *Enron*, na área de energia, e *WorldCom*, gigante mundial de telecomunicações. Esses acontecimentos expuseram a frágil estrutura de controle que existia, impossibilitando assim detectar e acionar as providências para evitar ilegalidades e conseqüentemente vultosos prejuízos (COSIF, 2005).

Uma das ações de controle para coibir as fraudes nos balanços contábeis, foi a Lei denominada *Sarbanes-Oxley Act 2002*, ou SOA (*SARBANES-OXLEY ACT OF 2002*, 2002), Lei SOX, que foi aprovada e sancionada pelo presidente americano para a comissão de valores mobiliários dos EUA, a *US Securities and Exchange Commission* (SEC), em 30 de julho de 2002. A SEC é a autoridade governamental americana responsável por estabelecer as regras e implantar o *Sarbanes-Oxley Act* no mercado de capitais norte-americano (FERNANDES; ABREU, 2006, p. 23).

Em função da complexidade para atender às inúmeras premissas da referida Lei, o que está diretamente relacionado com os sistemas de informação automatizados, as organizações passaram a tratar sua área de processamento de dados, denominada “Tecnologia da Informação” (TI), de maneira diferenciada (FERNANDES; ABREU, 2006, p.28). Neste contexto, a TI não mais deve ser gerida pelo seu lado puramente tecnológico, mas sim, respondendo precisamente com controles e novos processos, aos desafios impostos nesse recente ambiente de negócios.

Por isto, as organizações que possuem ações em bolsas de valores, ou que pretendam lançá-las, devem definir procedimentos para implantação de Governança Empresarial, que estejam em conformidade com a Lei *Sarbanes-Oxley*.

O processo de Governança Empresarial é motivado por vários fatores como: Ambiente de Negócios, Marcos de Regulação, Integração Tecnológica e Responsabilidade Social (FERNANDES; ABREU, 2006, p.7). Todos esses fatores estão intrinsecamente presentes nas empresas, que fazem gestão de suas tecnologias, principalmente naquelas relacionadas à teleinformática e redes multi-serviço.

## **1.2 Objetivo geral**

O objetivo deste trabalho é desenvolver um processo de Governança de Tecnologia da Informação para atender as determinações da Lei *Sarbanes-Oxley*, em seus itens específicos de responsabilidade, que tratam da emissão dos relatórios financeiros, os quais são assinados pelos executivos. Este processo está baseado em um padrão para objetivos de controle, denominado *Control Objectives for Information and related Technology* (COBIT) e será desenvolvido pelo método de estudo de sistemas, denominado Sistemografia.

### 1.3 Objetivos específicos

De maneira específica, os objetivos deste trabalho são:

- 1 – Descrever os elementos que compõem tanto a Governança, quanto a Arquitetura Empresariais, estabelecendo conexão entre dado, metadado e repositório de metadados. Tais elementos são premissas para suportar os controles exigidos pela Lei SOX.
- 2 – Descrever o modelo COBIT, responsável pelos objetivos de controle para informação e tecnologia relacionada.
- 3 – Descrever as Seções 102, 302, 404 e 906 da Lei *Sarbanes-Oxley*, relacionando-as com o modelo COBIT de objetivos de controle, para tratar Governança de TI.
- 4 – Descrever o processo para gestão de dados e metadados utilizando o método de sistemografia, de forma a contemplar os objetivos de controle propostos pelo modelo COBIT, relacionados com a qualidade de serviços de teleinformática e das redes multi-serviço.
- 5 – Propor uma moldura (*framework*<sup>1</sup>) para a gestão dos dados e metadados dentro do contexto de Governança de TI, associando

---

<sup>1</sup> Moldura, armação, quadro, estrutura (MICHAELIS, 1989, p. 130)

um painel de controle (*dashboard*<sup>2</sup>), baseado na maturidade dos processos, de maneira a medi-los em seu estado atual e projetar o estágio estratégico desejado.

## 1.4 Justificativas

Nas duas últimas décadas, as empresas evoluíram em muito a forma e a maneira de tratarem seus dados e informações. Muitos dos métodos empregados em processos industriais para a fabricação de bens tangíveis passaram também a ser empregados para os bens intangíveis, onde os sistemas de informação e de gestão do conhecimento têm sido os principais.

Para representar e descrever tais processos de gestão foi usado a sistemografia. Este método facilita a análise dos processos, pois permite a representação dos sistemas: “Operacional”, “Informacional” e “Decisional”. Além disto, permite representá-los de forma objetiva, inicialmente de modo separado e posteriormente de modo superposto (BRESCIANI FILHO, 2006).

Conforme Fernandes e Abreu (2006), a estrutura de gestão que possui as características técnicas e operacionais aderentes com a Lei SOX é o modelo COBIT. Lahti e Peterson (2005) enfatizam o aspecto de o modelo possuir direcionadores de gestão e de auditoria, objetivos de controle e ferramentas de implementação. Considera-o também como sendo o mais adequado em termos de melhores práticas e padrão de “facto” para os tipos de controle necessários à Lei SOX.

Este trabalho pretende contribuir com as empresas de teleinformática e tecnologia da informação no desenvolvimento de processos de gestão, que necessitem atender à qualidade de serviços de redes multi-serviço, ou que planejam implantar as especificações da Lei SOX em atendimento aos requisitos do negócio e aos marcos de regulação. Tal tema vem ganhando cada vez importância, uma vez que essas empresas estão buscando atingir não apenas

---

<sup>2</sup> *Dashboard*: painel de Controle (MICHAELIS, 1989, p. 78)

uma gerência integrada de redes e serviços, mas um padrão mais abrangente por meio de gestão das redes de telecomunicações, *Telecommunications mangement network* (TMN) (WHATIS.TECHTARGET.COM, 2007) para qualidade de serviços de teleinformática e processos de gestão de negócios. Anteriormente o objetivo das redes eram apenas para atender aos canais de voz, hoje, porém buscam convergência para voz, dados, imagens e vídeo em banda larga e a ubiqüidade dos serviços sob demanda (SOARES NETO, 2003).

## 1.5 Método de estudo

O trabalho será conduzido com a realização das etapas:

- 1 – Descrição e aplicação do modelo COBIT em relação aos quatro domínios: “Planejamento e Organização”, “Aquisição e Implementação”, “Entrega e Suporte”, e “Monitoramento”, assim como sua família de produtos, dentro do escopo da Governança Empresarial, para atingir a qualidade de serviços de teleinformática.
- 2 – Descrição do método da sistemografia com intuito de sistematizar os processos de gestão de dados e metadados especificados pelo COBIT.
- 3 – Descrição dos objetivos de controle propostos pelo COBIT conforme os requisitos necessários para atender às Seções 102, 302, 404 e 906 da Lei SOX, com enfoque em qualidade de dados. O mapeamento dos processos de gestão dentro deste escopo é executado por meio da sistemografia.
- 4 – Desenvolvimento de uma planilha de cálculo, por meio da qual seja possível inserir o nível de capacidade para cada um dos processadores, e gerar a análise de lacuna (*gap*<sup>3</sup>). O COBIT utiliza o modelo de maturidade *Capability Maturity Model*

---

<sup>3</sup> *Gap*: lacuna ou diferença (MICHAELIS, 1989, p. 136)

*Integration* (CMMI), criado pelo *Software Engineering Institute* (SEI) em 2002 (LIU, 2006).

## 1.6 Organização da dissertação

No primeiro capítulo deste trabalho são mencionados os objetivos, as justificativas e os métodos de estudo para o desenvolvimento de processos de gestão aderentes aos controles propostos pelo COBIT, à Lei *Sarbanes-Oxley* e à sistemografia.

O segundo capítulo trata de governança e arquitetura empresariais, relacionadas à qualidade de dados e metadados, elementos para o desenvolvimento dos processos de gestão, que atendam à qualidade de serviços de teleinformática.

O terceiro capítulo descreve o modelo COBIT, seus domínios e inter-relacionamentos entre processos, seu ciclo de gestão e matriz de objetivos de controle.

O quarto capítulo descreve as Seções 102, 302, 404 e 906 da Lei *Sarbanes-Oxley* relacionadas aos relatórios financeiros, responsabilidade corporativa sobre os relatórios financeiros e a avaliação anual dos controles e procedimentos internos para emissão de relatórios, com os processos do modelo COBIT relacionados com dados e metadados.

O quinto capítulo trata o método de sistemografia e sua aplicação em processos de gestão de dados e metadados em área de Tecnologia da Informação.

O sexto capítulo propõe uma moldura (*framework*) e um painel de controle (*dashboard*) para executar a gestão dos dados e metadados no contexto da qualidade dos multi-serviços de rede. Neste capítulo também serão

apresentados as etapas e os procedimentos para a aplicação da gestão dos dados e metadados.

O último capítulo apresenta a conclusão do estudo, e sugestões para trabalhos futuros.



## 2. ARQUITETURA EMPRESARIAL, GOVERNANÇA, QUALIDADE DE DADOS E METADADOS

---

---

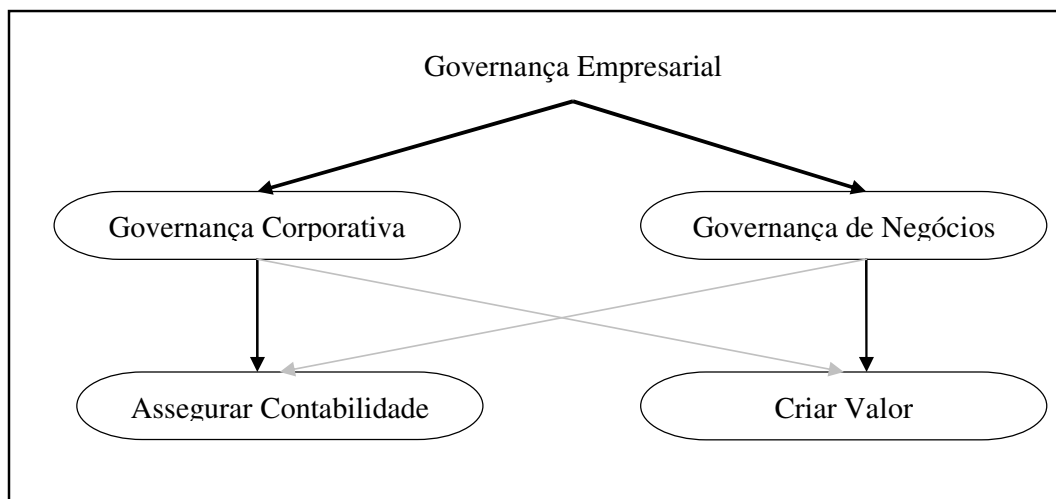
### 2.1 Considerações iniciais

De acordo com Maximiano (2000), Slack (2002) e Fernandes e Abreu (2006), as empresas incorporaram em larga escala a utilização de computadores, resultando transformação na estrutura organizacional e nos processos de produção. Além disto, alterou significativamente os papéis das pessoas para executar tanto a governança, quanto o relacionamento com clientes, fornecedores e agências reguladoras.

### 2.2 Governança empresarial

A entidade *Information Systems Audit and Control Foundation* (ISACF) (BRAND; BOONEN, 2004, p.14) define a Governança Empresarial como o conjunto de responsabilidades e práticas exercidas pela equipe de diretores e gerentes executivos, com as seguintes metas, prover a diretriz estratégica, assegurar que os objetivos sejam alcançados, apurar quais riscos devem ser apropriadamente gerenciados e verificar que recursos da empresa estão sendo utilizados com responsabilidade.

A FIG. 1 ilustra por meio de um esquema o contexto de Governança Empresarial, propondo duas dimensões, uma relacionada com a conformidade, ligada a Governança Corporativa e outra, ao desempenho, para a Governança do Negócio.



**FIGURA 1** – Esquema para a Governança Empresarial.

FONTE – adaptado de Chartered Institute of Management Accountants (CIMAGLOBAL.COM, 2004).

## 2.3 Governança corporativa e de negócios

De acordo com a *Organization of Economic Co-operation and Development* (OECD) (BRAND; BOONEN, 2004, p.15) a Governança Corporativa é um sistema através do qual os negócios corporativos são direcionados e controlados. Especificando a estrutura de ações legais e responsabilidades dos diferentes participantes da organização, relacionadas à diretoria, aos gerentes, acionistas e outros controladores, assim como os responsáveis por tomar decisões dentro da estrutura corporativa.

A Governança de Negócios compreende os direcionadores relacionados com a dimensão de desempenho da Governança Empresarial. O propósito dessa, é a criação de valor agregado e do controle da utilização dos recursos, com foco nos papéis das equipes responsáveis por tomar decisões estratégicas.

## 2.4 Governança de TI

A governança de Tecnologia da Informação (TI) é o sistema por meio do qual as organizações direcionam e controlam os empreendimentos de TI,

assegurando o perfeito alinhamento com as estratégias e processos de negócio, garantindo que a informação empresarial e tecnologia relacionada suportem os objetivos de negócio, com máximo benefício e vantagem competitiva (BRAND; BOONEN, 2004, p.16).

De acordo com Fernandes e Abreu (2006, p.13) por meio da Governança de TI é possível integrar e instituir melhores práticas para planejar, organizar, adquirir, implementar, entregar, suportar e monitorar o desempenho de TI. Weill e Ross (2006) enfatizam que a Governança de TI simultaneamente fortalece e controla o desempenho das empresas, aprimorando-as. Seguindo nesta diretriz, Craig (2004) relaciona a governança ao método multidimensional representado por cartões (*scorecard*) contendo quatro perspectivas para as áreas financeira, cliente, processos internos, e aprendizado e crescimento, denominadas *Balanced Scorecard* (BSC).

## **2.5 Arquitetura empresarial**

Até a década de 1960 as empresas tratavam arquitetura como forma de projetar, construir e organizar as fábricas, as instalações, os equipamentos e os objetos dentro de cômodos e galpões. Com o advento dos computadores esta arquitetura tradicional incorporou outras como tecnologia, informação e aplicação.

Em 1987, John Zachman (1987) propôs uma forma para representar a arquitetura empresarial, baseando-se na arquitetura dos sistemas de informação. Por meio de uma matriz composta por cinco perspectivas e seis dimensões, retratando em suas células os objetos ou modelos, que melhor representem a desejada arquitetura.

A “matriz de Zachman”, como ficou conhecida, identifica por meio de perspectivas, os níveis que vão desde os objetivos e o escopo, passando pela visão do negócio, dos modelos de representação de sistemas de informação e de tecnologia, até a descrição detalhada (ZACHMAN, 1987; SOWA; ZACHMAN, 1992).

As dimensões procuram estabelecer aspectos que respondam às questões relativas como: “o que”, “como”, “onde”, “quem”, “quando” e “porque”, inseridas no contexto do negócio.

Já as perspectivas procuram ser responsável pelos pontos de vista de “contexto”, de “modelo de negócio”, de “modelo de sistemas”, de “modelo de tecnologia” e de “componentes”, inseridas no escopo do negócio.

A FIG. 2 retrata a matriz de Zachman, com suas dimensões, perspectivas, objetos e modelos associados. As dimensões, que se relacionam com as questões apresentadas aos elementos estruturais de TI, podem ser observadas em cada uma das partes superiores das colunas (“dados”, “processos”, “rede”, “pessoal”, “tempo”, “motivação”) (ZIFA.COM, 2005). Encontra-se no ANEXO A, a matriz em seu formato original.

	O QUE	COMO	ONDE	QUEM	QUANDO	PORQUE
<b>DESCRIÇÃO DO ESCOPO</b> {contextual}	<b>DADOS</b> Lista de Entidades importantes para o Negócio Entidade = Classes de Negócio	<b>PROCESSOS</b> Lista de Entidades que a Empresa Executa Função = Atividade de Negócio	<b>REDE</b> Lista de Locais onde a Empresa Opera Nó = Local do Negócio	<b>PESSOAL</b> Lista de Organogramas importantes para o Negócio Pessoal = Organizações Principais	<b>TEMPO</b> Lista Eventos Significativos para o Negócio Tempo = Principais Eventos de Negócio	<b>MOTIVAÇÃO</b> Lista de Metas/Estratégias de Negócio Fins/Meios = Principais Metas/FCS do Negócio
<b>MODELO DE NEGÓCIO</b> {conceitual}	Diagrama de ER ENT = Entidade de Negócio REL = Regra de Negócio	Diagrama de Processos de Negócio Proc. = Processo E/S = Recursos	Rede Logística Nó = Unidade de Negócio Link = Fluxo do Negócio	Modelo de Fluxo de Trabalho Pess.=Unid.Organizacional Trabalho=Produto Trabalho	Cronograma Geral Tempo=Evento de Negócio Ciclo = Ciclo de Negócio	Plano de Negócio Fim = Objetivo de Negócio Meios = Estratégia de Neg.
<b>MODELO DO SISTEMA DE INFORMAÇÃO</b> {lógico}	Modelo de Dados ENT = Entidade de Dados REL = Relac. de Dados	Diagrama de Fluxo de Dados Processo = Função da Aplic. E/S = visão do Usuário	Arquitetura de Sistemas Distribuídos Nó = Função S/I Ligação = Características da Linha	Arquitetura de Organização de Pessoal Pessoal = Papel Trabalho=Produto Trabalho	Estrutura de Processamento Tempo=Evento de Sistema Ciclo=Ciclo Processamento	Modelo de Regras de Negócio Fim = Declaração Estrutural Meios=Declaração de Ação
<b>MODELO DE TECNOLOGIA</b> {físico}	Projeto de Dados ENT = Segmento/Tabela/... REL = Chave/Pointer/...	Mapa de Estrutura Processos=Função Comp. E/S=Formatos/Telas/Form.	Arquitetura de Sistemas Nó=HMI e SII de sistemas Ligação=Espec. de Linha	Arquitetura de Apresentação Pessoal = Usuário Trabalho=Formato de Tela	Estrutura de Controle Tempo = Executar Ciclo=Ciclo do Componente	Projeto de Regra Fim = Condição Meios = Ação
<b>DESCRIÇÃO DETALHADA</b> {fora do contexto}	Descrição de Banco de Dados Entidade = Campos Relac. = Entidades	Programa Proc. = Comandos de Ling. E/S = Bloco de Controle	Arquitetura de Rede Nó = Endereços Ligação = Protocolos	Arquitetura de Segurança Pessoal = Identidade Trabalho = Serviço	Definição de Oportunidade Tempo = Interromper Ciclo = Ciclo de Máquina	Especificação de Regra Fim = Subcondição Meios = Peso (Etapas)
<b>SISTEMA REAL</b>	Dados	Função	Comunicações	Organização	Cronograma	Estratégia

FIGURA 2 – Framework da Matriz de Zachaman.

FONTE – Adaptado de ZIFA.COM (2005).

Em especial para esta dissertação, os aspectos que retratam as perspectivas associadas aos “dados”, composta pelas dimensões “escopo”, “modelo de negócio” e “modelo do sistema de informação”, possuem maior interesse, porém não se deseja dizer com isto, que devam ser tratadas de maneira independentes das demais, uma vez que na realidade, todas elas estão integradas e se interoperam.

## **2.6 Arquitetura de informação**

Esta arquitetura é responsável por identificar e definir os vários tipos de dados que suportam as funções de negócios. Consideram-se para esta arquitetura todas as fontes de informação, como documentos, gráficos, vídeos e multimídia, e também as regras para preservação de conteúdo armazenado, e de segurança. Ainda, consideram-se neste contexto, os papéis que são desempenhados pelos responsáveis por “dados”, onde estão definidos os tipos de dados, formas e as regras que os governam (HEFFNER, 2002).

Magee (1997) ainda complementa, considerando a arquitetura de informação como o projeto, os princípios e as políticas que governam a propriedade, o uso e a administração dos dados, em associação aos modelos do negócio, da organização, dos objetivos e dos processos.

## **2.7 Qualidade de dados**

De forma a suportar os princípios de governança, torna-se necessário e relevante o tratamento da qualidade dos dados. Conforme Maximiano (2000), Slack (2002), Rossato (1996) e SM *Thacker and Associates* (2007) a administração da qualidade total, introduzida por Feigenbaum e aprimorada principalmente por Deming, Juran e Ishikawa, permitiu melhoras significativas nos procedimentos de controle de qualidade de produção industrial e dos serviços. Tais técnicas estão sendo adaptadas e introduzidas para a melhoria da qualidade dos dados em sistemas e aplicativos sob a responsabilidade da área de TI e estão relacionadas com a integridade dos dados, os quais ela armazena,

manipula e entrega em formato de informações, para serem utilizados nos processos de negócio.

Agosta (2004) enfatiza que a qualidade dos dados e informação requer atenção por parte dos envolvidos com a Governança de TI. Esta atenção deve manter seu foco principalmente em padronização, perfil, políticas, e inspeção de defeitos. Além disto, qualidade de dados agora inclui metadados de qualidade e que, os padrões desta qualidade também serão aplicados para os metadados. Referindo-se assim à estreita relação entre os dados e seus metadados.

## **2.8 Metadados**

De acordo com Tannenbaum (2002), a disseminação dos sistemas computacionais e de informação por todas as áreas das empresas, gerou um problema relacionado com a necessidade de descrição precisa de dados e do significado dos termos armazenados. Isto é decorrente do fato de existirem diversos sistemas de informação, e estes muitas vezes acessarem bases de dados diferentes e não integradas conforme descrito por Blechar (2003a) em seu artigo.

### **2.8.1 Significado do termo metadados**

De maneira básica, fazendo-se uma tradução do radical de origem grega – *meta*, significa “sobre algo”, “a respeito de algo”. Na verdade o que se pretende é descrever o significado dos termos ou rótulos armazenados nos sistemas de computação.

Partindo para conceitos mais técnicos e elaborados, o termo “metadados” é considerado pelos autores Inmon (2002, p.113), Tannenbaum (2002, p.85) e Marco (2000, p.48), como sendo todo dado e informação, que contenha conhecimento sobre o negócio, os processos técnicos e também o significado dos dados dentro da empresa. Estejam estes significados relacionados tanto com o dado físico propriamente dito, quanto àqueles contidos em

programas, em mídias, ou presente no conhecimento das pessoas, especificamente dos funcionários das empresas.

### **2.8.2 Repositório de metadados**

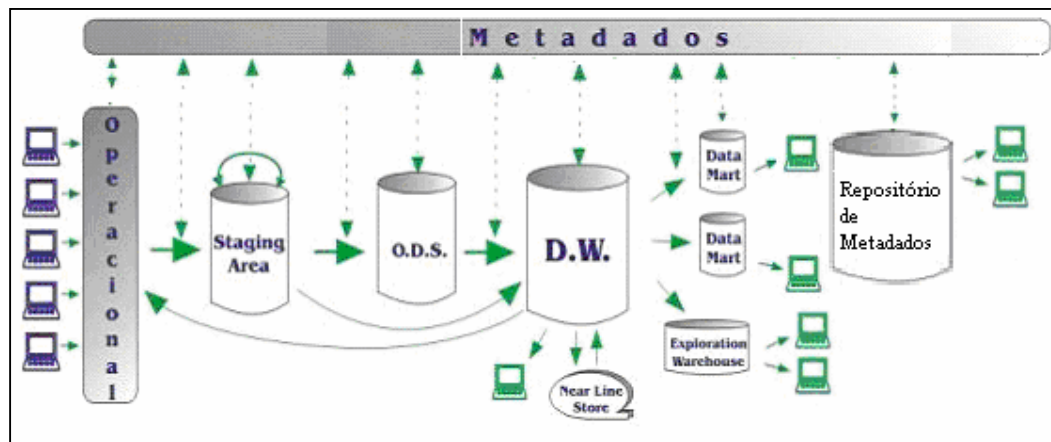
Os repositórios de metadados são os meios físicos e lógicos com os quais os metadados podem ser armazenados e gerenciados.

A criação desse repositório de metadados pode exigir técnicas de projetos de bancos de dados e implementações de melhor desempenho, em Elmasri e Navathe (2002) e Heuser (2001) são encontrados modelos e esquemas físicos para auxiliar na criação destes repositórios.

As soluções para descrever os dados sobre outros dados passam por vários tipos, e naturalmente devem ser analisadas de acordo com o contexto e objetivos que a empresa deseja atingir em determinado prazo. Inmon (2002, p.125) relaciona a preocupação com os metadados ao grau de maturidade das empresas, por sua vez, Tannenbaum (2002, p.140) e Marco (2000, p.47) procuram estabelecer processos e regras para a construção e gerência de todo o ambiente. Critérios para uma seleção de repositório dentro de um escopo balanceado podem ser obtidos em Blechar (2003b). Melhores práticas para o gerenciamento da integração dos metadados está disponível em Schulte, Thompson e Richel (2002).

A FIG. 3 apresentada por Alcântara (DWBRASIL, 2005) mostra os elementos necessários ao ciclo de vida para uma solução de gestão de metadados e como estes se encontram permeados em todas as etapas do processo.





**FIGURA 3** – Arquitetura para BI com foco em metadados.

FONTE – Adaptado de DWBRASIL (2005).

Os componentes importantes da arquitetura estão relacionados no QUADRO 1

**QUADRO 1** – Principais componentes, seus relacionamentos dentro da arquitetura de metadados e as respectivas descrições.

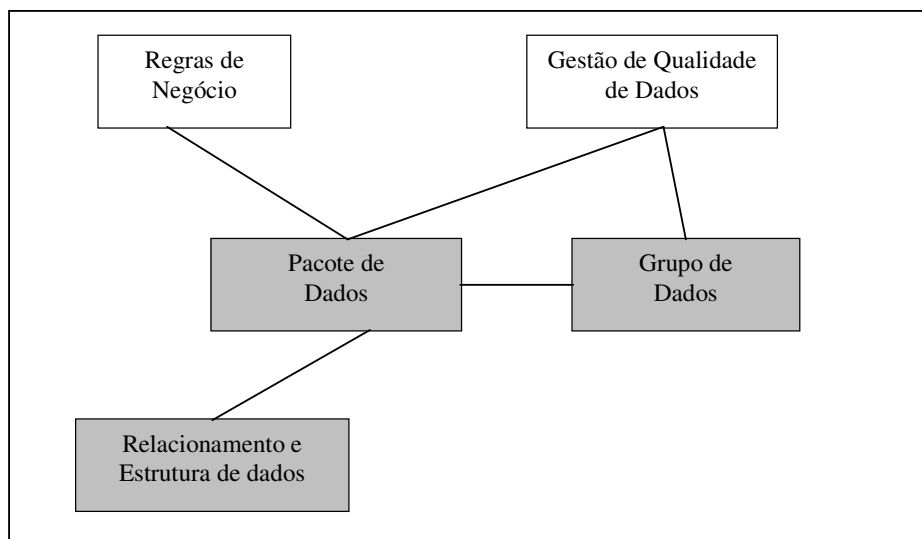
Componente	Descrição
<b>Operacional</b>	Plataforma de dados relativos ao dia-a-dia da organização, vitais para sua operação no mercado. Segundo Inmon (2002), "é chamado assim porque está relacionada com as operações de negócios diários da corporação"
<b>Área e Etapa de Confluência</b> <i>Staging Área (SA)</i>	Também chamada por Inmon (2002) como "camada de integração e transformação", a SA é uma área de tratamento, padronização e transformação das informações operacionais para carga na arquitetura BI
<b>Área de Armazenamento Operacional</b> <i>Operational Data Store (ODS)</i>	Também de acordo com Inmon (2002), ODS é uma base de dados integrada, volátil, de valores correntes, e que contém somente dados detalhados. Também pode ser entendido como uma visão integrada do mundo operacional. Normalmente sua construção adota bases de dados
<b>Armazém de Dados</b> <i>Data Warehouse (DW)</i>	Fonte de dados para consultas na organização, ou nada menos que a união de todos os <i>Data Marts</i> já constituídos
<b>Sub-armazém de Dados</b> <i>Data Mart (DM)</i>	São subconjuntos de um DW completo
<b>Armazém de Exploração</b> <i>Exploration Warehouse (EW)</i>	Ambiente para análises pesadas e inexploradas a serem efetuadas, isolado do <i>warehouse</i> corporativo
<b>Extração, Transformação e Carga</b> <i>Extract, Transformation and Load (ETL)</i>	Extração, transformação e carga, ETL, é o processo de captura das fontes de dados a serem utilizadas em um ambiente de BI, suas transformação, padronização e posterior carga no DW (ou DM ou ODS)

FONTE – adaptado de DWBRASIL (2005).

### 2.8.3 Metamodelo

Um metamodelo é um conjunto de metadados inter-relacionados utilizados para definir modelos. Esse, formalmente define os elementos do modelo, sua sintaxe e semântica. De acordo com Marco e Jennings (2004), o metamodelo é a representação gráfica de um esquema que será materializado por meio da forma física (*schema* físico) para o armazenamento do metadado.

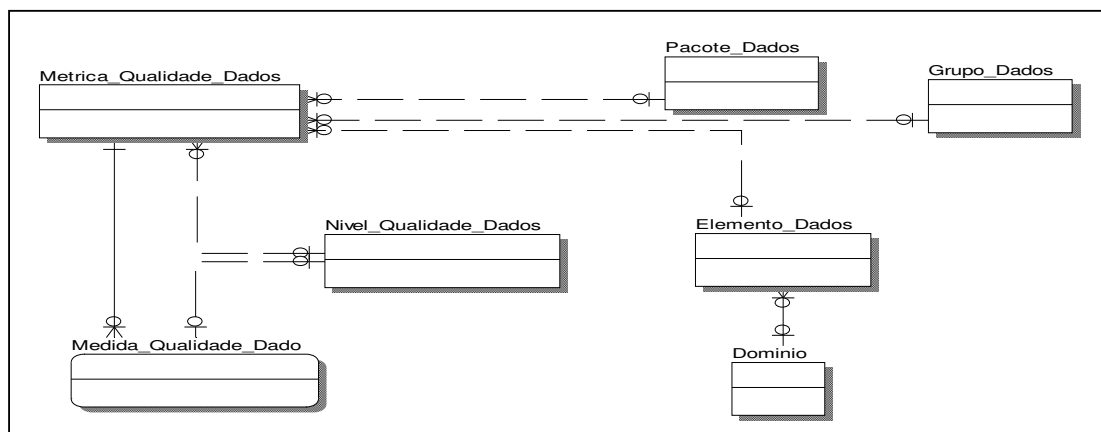
Para o escopo deste trabalho o metamodelo que se deseja representar, refere-se às disciplinas de gestão de qualidade de dados, às regras de negócio e aos sistemas empresariais. A FIG. 4 ilustra os pontos de interações entre os principais elementos dos sistemas empresariais com as regras de negócio e a gestão da qualidade de dados, justamente o foco dos processos a serem controlados para atender aos requisitos da Lei *Sarbanes-Oxley* – SOX e do modelo COBIT.



**FIGURA 4** – Principais elementos de um metamodelo que atenda aos requisitos da Lei SOX e do modelo COBIT para os sistemas empresariais.

FONTE – adaptado de Marco e Jennings (2004, p. 40)

A FIG. 5 apresenta um exemplo de metamodelo simples contendo as entidades e os relacionamentos dos sistemas empresariais e da qualidade de dados.



**FIGURA 5** – Metamodelo para qualidade de dados.

FONTE – adaptado de Marco e Jennings (2004, p. 45)

O QUADRO 2 contém a descrição para cada uma das entidades representadas pelo metamodelo na FIG. 5.

**QUADRO 2** – Entidades do metamodelo e suas respectivas definições.

Entidade	Definição
<b>Pacote de dados</b>	<b>Coleção do contexto e escopo do Grupo de Dados, Elementos de Dados e dos relacionamentos entre esses itens. Contém os formatos dos pacotes de dados; (exemplos: Banco de Dados, Esquema XML, Mensagem, Arquivos Convencionais)</b>
<b>Grupo de dados</b>	<b>Coleção dos Elementos de Dados que o Pacote de Dados representa; (exemplo: Tabela Relacional, Registro em um Arquivo Convencional, Elemento XML, Transação de Mensagem)</b>
<b>Elemento de dados</b>	<b>Coleção das unidades básica dos dados. Representa cada um dos itens dos dados; (exemplo: Coluna da Tabela, Elemento de Mensagem, Elemento de XML)</b>
<b>Domínio</b>	<b>Coleção de cada uma das faixas de possibilidades de valores indivisíveis que um Elemento de Dados pode assumir; (exemplo: lista de caracteres para nomes, faixa de valores numéricos de temperatura, possibilidades de UF para os Estados brasileiros)</b>
<b>Regra de negócio</b>	<b>Regras desenvolvidas e aprovadas pelo negócio utilizadas em processos transacionais e analíticos</b>
<b>Nível da qualidade</b>	<b>Contém as classificações de qualidade aplicadas às medidas de qualidade de dados</b>
<b>Medidas de qualidade de dados</b>	<b>Registra a quantidade de resultados de desempenho relacionados com as medidas de qualidade de dados</b>
<b>Métricas de qualidade de dados</b>	<b>Contém os critérios de qualidade de dados avaliando-os em relação aos itens: Pacote de Dados, Grupo de Dados e Elemento de Dados</b>

FONTE – adaptado de Marco e Jennings (2004, p. 48)

O capítulo tratou de qualidade de dados, metadados e arquitetura de informação como forma de atender aos requisitos para atingir a governança empresarial.

## **3. MODELO DE GESTÃO PROPOSTO PELO COBIT**

---

---

### **3.1 Histórico do COBIT**

O modelo referente aos Objetivos de Controle para Informação e Tecnologia Relacionada (*Control Objectives for Information and Related Technology* – COBIT) teve seu desenvolvimento iniciado em 1994 sob a condução da *Information Systems Audit and Control Foundation* (ISACF), instituto responsável por ações de pesquisa da *Information Systems Audit and Control Association* (ISACA) (ISACA, 2005). Em 2003, a ISACF alterou seu nome para *IT Governance Institute* (ITGI), passando assim a manter o COBIT (BRAND; BOONEN, 2004, p.34).

### **3.2 COBIT no contexto de governança**

O COBIT está inserido no contexto de governança, uma vez que trata e direciona os processos de controle para a empresa, os negócios e a própria TI. De acordo com Brand e Boonen (2004, p.35) ele é um guia abrangente para usuários, auditores, gestores e donos de processos de negócio, e que permite a Governança de TI.

A partir de objetivos de controle, é possível em relação aos processos de TI, examinar suas maturidades, maximizar os benefícios, e conseqüentemente permitir que os processos de negócio ganhem vantagem competitiva.

O instrumento de Governança de TI permite que os gerentes efetuem as ligações relacionadas com os requisitos de controle, os sistemas de informação e o risco do negócio, classificando-os em níveis e comunicando-os aos respectivos responsáveis. Desta forma, a governança é efetuada com políticas claras e boas práticas de TI em toda a organização.

O conjunto de objetivos de controle está orientado para atender aos interesses de negócio das empresas e de seus controladores. Este conjunto de objetivos estabelecem uma declaração de resultados esperados ou propósitos a serem alcançados, pela implementação de procedimentos de controle, dentro de uma atividade particular de TI. Controles incluem políticas, procedimentos, práticas e estruturas organizacionais desenhadas de forma a fornecer segurança, para que os objetivos de negócio sejam alcançados e que eventos indesejáveis possam ser prevenidos ou detectados, e corrigidos.

### **3.3 Beneficiários de um modelo de governança**

De acordo com o IT *Governance Institute* (ITGI), os beneficiários de um modelo de governança de TI são formados de gerentes; auditores; consultores; e os profissionais de TI em nível gerencial e operacional. A partir destes grupos de usuários é possível efetuar o planejamento estratégico e as ações a serem executadas em relação às definições dos papéis e das funções.

O QUADRO 3 descreve de maneira sucinta a interação proposta pelo ITGI entre os principais grupos, suas responsabilidades e quais são as formas com as quais o COBIT atua.

**QUADRO 3** – Descritivo dos grupos de foco e a interação com o COBIT.

<b>Principais grupos</b>	<b>Ação X Interação com o COBIT</b>
<b>Gerente</b>	<b>Responsabilidade por administrar a operação da organização.</b> Para estes, o COBIT auxilia aos gerentes de negócios e de TI a balancear riscos e controlar investimentos em um ambiente imprevisível
<b>Usuário Final</b>	<b>Responsabilidade por assegurar e operar os serviços.</b> Para estes, COBIT oferece um <i>framework</i> para obter garantia em questões de segurança e controle de serviços de TI. Os provedores de serviços de TI realizados por prestadores internos e externos
<b>Auditor</b>	<b>Responsabilidade por prover garantias de qualidade e aplicabilidade de controles independentes.</b> Para estes, COBIT auxilia com estruturas que melhorem os controles para auditoria interna
<b>Consultor</b>	<b>Responsabilidade por trazer e implantar novos <i>frameworks</i> e métodos que se originam fora das empresas.</b> Para estes, COBIT é uma referência em relação aos negócios e à gestão de TI
<b>Profissionais de Serviços de TI</b>	<b>Responsabilidade por administrar e executar o ciclo de vida dos serviços de TI.</b> Para estes, COBIT provê um <i>framework</i> que cubra de forma completa tanto o ciclo de vida dos sistemas e também para serviços de TI

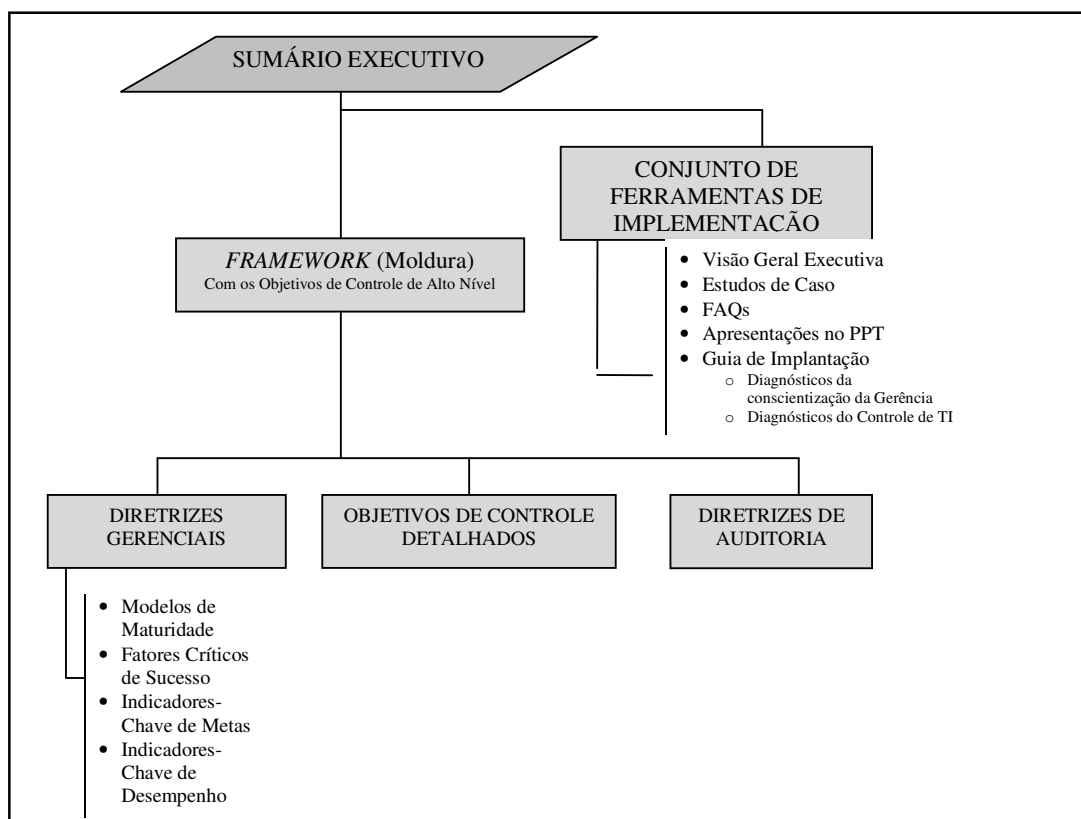
FONTE – adaptado de Brand e Boonen (2004, p.36).

### 3.4 Família dos produtos componentes do COBIT

A família dos produtos que compõem o COBIT é formada por seis livros que estão representados de maneira hierárquica na FIG. 6. Cada livro aborda uma diretriz específica, assim como é recomendado para atender aos usuários de acordo com o perfil determinado.

O livro “Sumário Executivo” (COBIT, 2000a) explica os conceitos e princípios chave. Os livros “*Framework*” (COBIT, 2000b) e “Objetivo de Controle” (COBIT, 2000c) descrevem as metas e os elementos organizacionais do modelo de processos. O livro “Práticas de Controle” (CAMPBELL, 2005) identifica as melhores práticas e descrição de requisitos para controles específicos. O livro “Guia de Gestão” (COBIT, 2000d) relaciona os objetivos de negócio aos de TI e fornece ferramentas para melhorar o desempenho de TI. Por fim, o livro de “Guia

de Auditoria” (COBIT, 2000e) fornece roteiro para evoluir controles, avaliar a conformidade e documentar riscos em relação aos controles internos dos dados financeiros, testes e avaliações dos controles, suporte para auditoria externa, documentos de conformidade e qualquer relatório significativo sobre deficiências e fraquezas.



**FIGURA 6** – Família COBIT de produtos

FONTE – adaptada de Brand e Boonen (2004, p. 54).

No escopo desta dissertação, os livros referentes ao “*Framework*” (COBIT, 2000b) contendo “Diretrizes Gerenciais” e “Objetivos de Controle”, que tratam especificamente de Governança de TI e controles têm maior interesse, portanto serão mais utilizados.



### 3.5 Estrutura proposta para o *Framework* COBIT

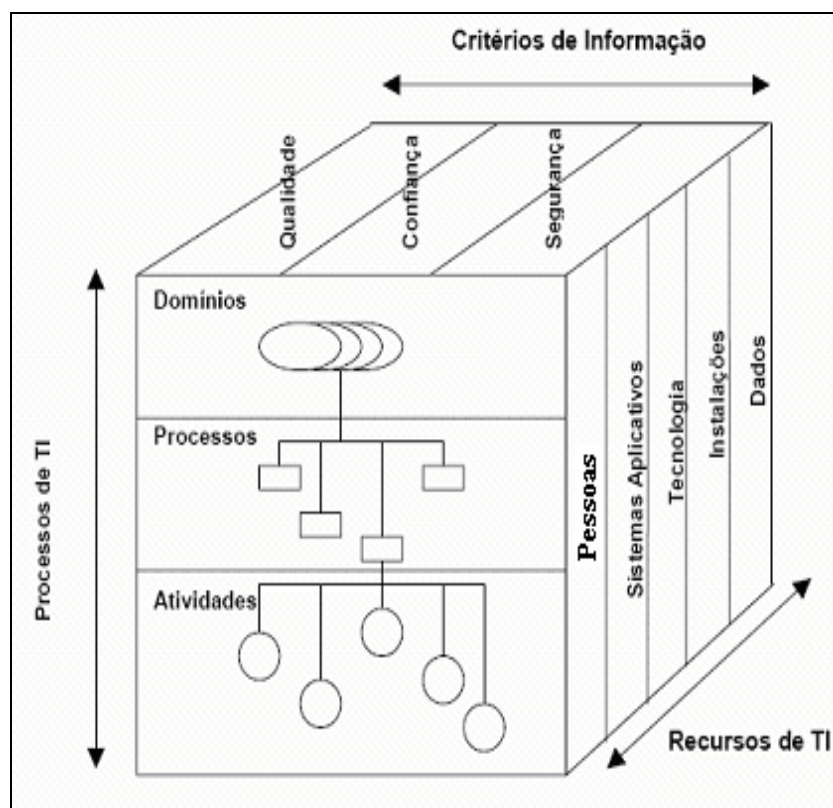
A estrutura proposta pelo ITGI para o “*Framework* COBIT” consiste de objetivos de controle de alto nível e uma estrutura de classificação em três níveis. O nível mais alto composto pelos quatro domínios, o segundo ou intermediário pelos processos, e o nível mais básico composto pelas atividades e tarefas.

O modelo conceitual COBIT é representado por meio do cubo COBIT, formado de três dimensões inter-relacionadas. A seguir são apresentadas as referidas dimensões:

- ⇒ Domínios e Processos
- ⇒ Recursos de TI
- ⇒ Critérios de Informação

O COBIT mapeia os processos por meio de uma classificação em 4 domínios distintos, e que quando operados de modo conjunto efetuam ações cíclicas. A FIG. 7 representa o cubo COBIT para Governança de TI de acordo com a proposta do ITGI. A seguir estão relacionados os quatro domínios com suas respectivas siglas originais:

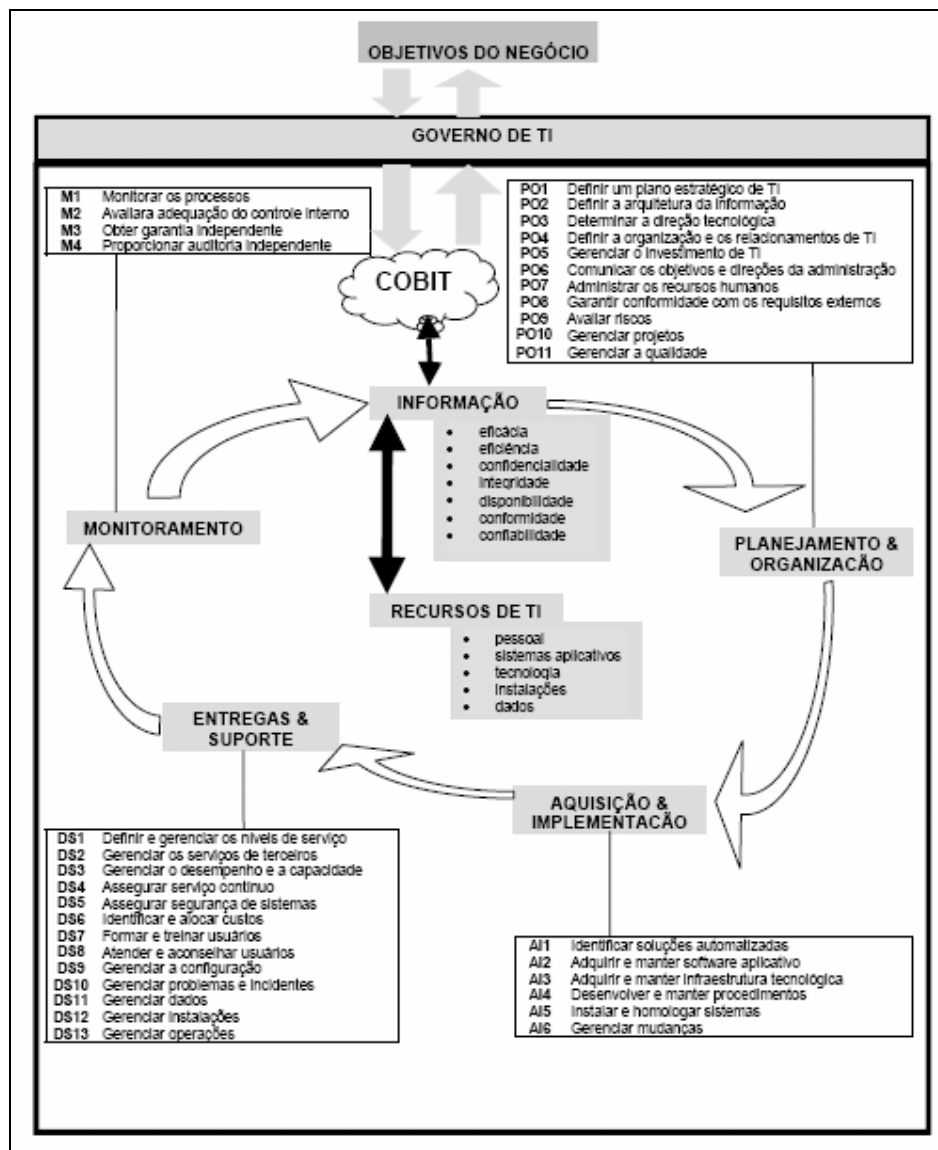
- ⇒ Planejamento e Organização – PO
- ⇒ Aquisição e Implementação – AI
- ⇒ Entrega e Suporte – DS
- ⇒ Monitoramento – M



**FIGURA 7** – Cubo de Governança de TI.

FONTE – adaptado de Dupré (2001, p.14).

A FIG. 8 apresenta a definição de processos de TI do COBIT, que contém os quatro domínios. São trinta e quatro objetivos de controle de alto nível, um para cada processo de TI, agrupados nesses quatro domínios: “Planejamento e Organização”, “Aquisição e Implementação”, “Entrega e Suporte” e “Monitoramento”. Essa estrutura cobre todos os aspectos da informação e da tecnologia que a suporta.



**FIGURA 8** – Processos de TI do COBIT agrupados em quatro domínios.

FONTE – adaptado de Dupré (2001, p.5).

### **3.5.1 Descrição das características relacionadas aos domínios do COBIT**

De modo a tornar as explicações de todos os domínios mais claros, nos próximos tópicos serão efetuados as descrições relativas às principais características para cada um dos quatro domínios propostos pelo COBIT.

#### **3.5.1.1 Domínio de “Planejamento e Organização” (PO – *Planning and Organization*)**

Este domínio cobre as partes estratégicas e táticas, permitindo identificar as formas com as quais a TI possa melhor contribuir para alcançar as metas dos negócios. É muito importante que para a realização de uma visão estratégica exista planejamento, comunicação e gerenciamento de maneira a atender aos vários direcionadores de TI.

#### **3.5.1.2 Domínio de “Aquisição e Implementação” (AI – *Acquisition and Implementation*)**

Este domínio contempla os processos responsáveis por identificar, desenvolver, adquirir, implementar e integrar as soluções de TI aos processos de negócio.

#### **3.5.1.3 Domínio para “Entrega e Suporte” (DS – *Delivery and Support*)**

Este domínio engloba os processos responsáveis por operações tradicionais relacionadas ao processamento dos dados, e aos sistemas de aplicações abrangendo segurança, suporte, configurações e demais procedimentos que assegurem os aspectos de continuidade operacionais.

### 3.5.1.4 Domínio relacionado ao “Monitoramento” (M – *Monitoring*)

Como todos os processos de TI necessitam ser regularmente aferidos, para verificar os indicadores de qualidade, de conformidade e de desempenho, o domínio “M – Monitoramento” permite endereçar tais controles. O processo deste domínio também assegura independência para as auditorias, sejam estas internas ou externas.

### 3.5.2 Descrição dos recursos de TI

Os recursos de TI estão agrupados em cinco classes e dentro do COBIT eles são tratados individualmente ou em conjunto. No QUADRO 4, são apresentadas as cinco classes de recursos e as ações que esses recursos desempenham para realizar suas tarefas.

**QUADRO 4** – Descritivo para os recursos de TI e ações desempenhadas para realizar as tarefas.

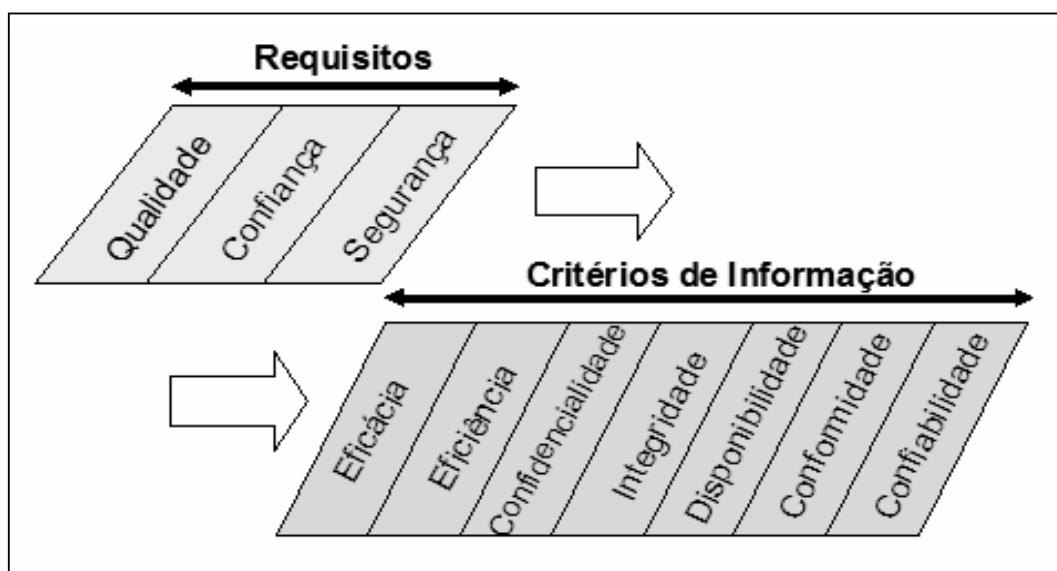
<b>Recursos de TI</b>	<b>Ações desempenhadas</b>
<b>Pessoas (Recursos Humanos)</b>	Planejar Organizar Adquirir Entregar Suportar, monitorar serviços e sistemas de informação
<b>Sistemas de Aplicação</b>	Executar procedimentos manuais Executar procedimentos automatizados
<b>Dados</b>	Representar objetos externos e internos Representar dados estruturados e não estruturados
<b>Infra-estrutura técnica</b>	<i>Hardware</i> Sistemas operacionais Sistemas de gerência de banco de dados Sistemas de rede Telecomunicações
<b>Recursos e instalações</b>	Abrigar e suportar o negócio Abrigar e suportar sistemas de informação

FONTE – adaptado de Brand e Boonen (2004, p. 47).

### 3.5.3 Critérios de Informação para o COBIT

O COBIT estabelece sete critérios relacionados à informação. Estes critérios estão associados a um modelo de referência que permite agrupá-los em três requisitos básicos e desta maneira suportar os requisitos do negócio.

O cubo proposto pelo ITGI para a Governança de TI apresentado anteriormente na FIG. 7 especifica em uma das dimensões o “critério de informação” composto pelos requisitos de “qualidade”, mais os requisitos de “confiança” e também de “segurança”. Em Brand e Boonen (2004, p.50), é apresentado um modelo reproduzido por meio da FIG. 9, o qual permite alcançar a transição entre os requisitos citados anteriormente e os critérios considerados em termos do COBIT como critérios de informação.



**FIGURA 9** – Transição de requisitos para os critérios de informação.

FONTE – adaptado de Brand e Boonen (2004, p. 50).

No QUADRO 5 estão agrupados e relacionados os requisitos do negócio, os critérios de informação e as respectivas definições sobre os critérios de informação.

**QUADRO 5** – Definições para os critérios de informação relacionados aos requisitos do negócio.

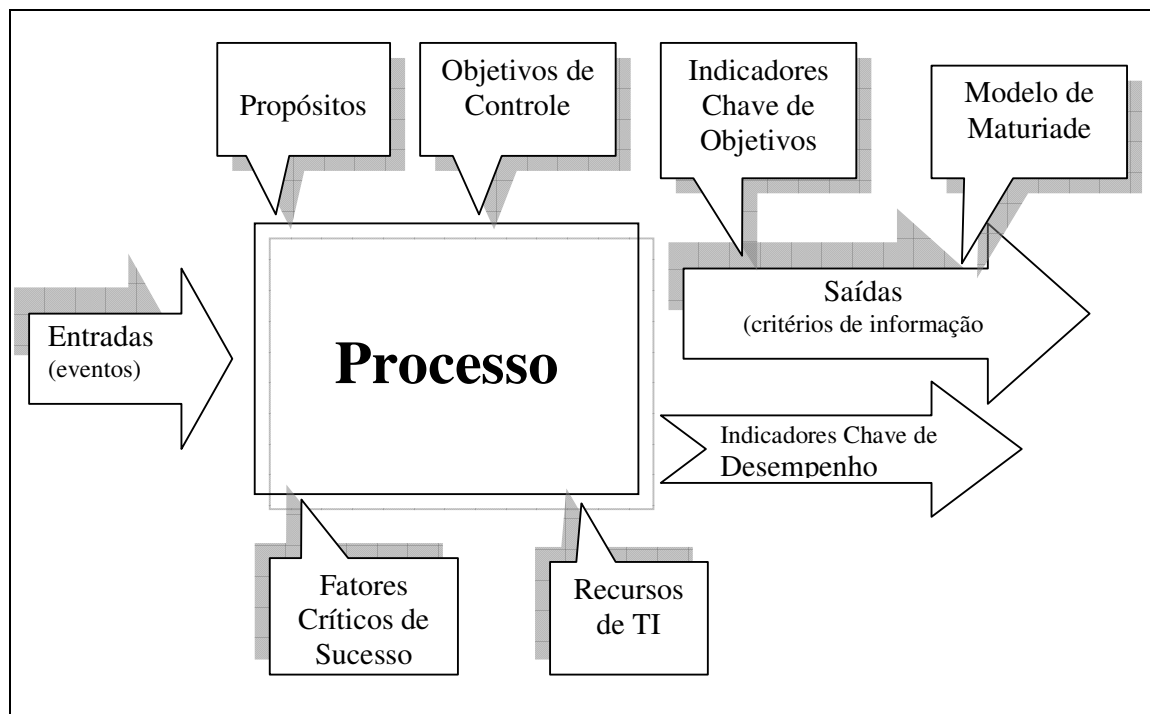
<b>Requisitos do Negócio</b>	<b>Crítérios de Informação</b>	<b>Definições</b>
<b>Qualidade</b>	<b>Eficácia</b>	Trata da informação que está sendo relevante e pertinente ao processo do negócio, bem como que esteja sendo entregue de um modo oportuno, correto, consistente e útil
	<b>Eficiência</b>	Diz respeito à provisão da informação por meio do uso ótimo (produtivo; econômico) dos recursos
	<b>Confidencialidade</b>	Diz respeito à proteção da informação sigilosa contra a revelação não autorizada
<b>Segurança</b>	<b>Integridade</b>	Relaciona-se à exatidão e à incerteza da informação bem como à sua validade de acordo com os valores e expectativas do negócio
	<b>Disponibilidade</b>	Relaciona-se à informação que está sendo disponibilizada quando requerida pelo processo de negócio agora e no futuro
<b>Confiança</b>	<b>Conformidade</b>	Trata do cumprimento das leis, dos regulamentos e arranjos contratuais aos quais o processo de negócio está sujeito. Critérios de negócios impostos externamente
	<b>Confiabilidade</b>	Relaciona-se à provisão de informação apropriada para a gerência operar e exercer suas responsabilidades de relatar aspectos de conformidade e finanças

FONTE – adaptado de Brand e Boonen (2004) e COBIT (2000b).

### 3.5.4 Estrutura genérica do processo

Os componentes do processo são “Eventos”, “Recursos de TI”, “Propósitos”, “Objetivos de Controle”, “Indicadores Chave de Desempenho”, “Indicadores Chave de Objetivos”, “Fatores Críticos de Sucesso”, “Modelo de Maturidade”, e “Critérios de Informação”.

A FIG. 10 representa o relacionamento entre o processo e seus respectivos componentes.



**FIGURA 10** – Representação da estrutura genérica do Processo e componentes.

FONTE – adaptado de Liu (2006, p. 46) e Brand e Boonen (2004, p. 70).

### 3.5.5 Representação e característica do processo

De acordo com Brand e Boonen (2004, p.70) o COBIT está centrado em processos, a sua representação deve ser formalizada a partir de descrições abrangendo objetivos, indicadores, entradas, saídas, critérios, recursos, controles de processos, relacionamento com outros processos, custos e benéficos, fatores críticos e um modelo de maturidade. Este pode ser modelado por meio de um método de representação de processos que contemple os elementos e requisitos citados.

Liu (2006, p.47) e Dupré (2001, p.13), relacionam as Entradas do processo (eventos), com as Saídas (critérios de informação). Os eventos são “Objetivos do Negócio”, “Oportunidades do Negócio”, “Requisitos Externos”, “Leis



e Regulamentos”, e os “Riscos”. Os critérios de informação são “Eficácia”, “Eficiência”, “Confidencialidade”, “Integridade”, “Disponibilidade”, “Conformidade” e “Confiabilidade”.

A FIG. 11 apresenta o diagrama de “Objetivos de Controle de alto nível COBIT” composto pelos trinta e quatro processos de TI, agrupados nos quatro domínios, bem como uma indicação em quais recursos e critérios de TI são aplicáveis.

De acordo com Dupré (2001, p.15), possíveis graus para os critérios de informação são “primário”, “secundário” ou “vazio”:

- ⇒ P (Primário) – grau para o qual o objetivo de controle impacta diretamente o critério da informação a que se refere.
- ⇒ S (Secundário) – grau para o qual o objetivo de controle definido satisfaça apenas minimamente ou indiretamente o critério de informação a que se refere.
- ⇒ Vazio – quando não indicado como primário ou secundário. Poderia ser aplicável, mas os requisitos são mais apropriadamente satisfeitos por outro critério nesse processo e/ou por outro processo.

Para cada processo está incluído um conjunto formal de características, que permite medi-lo, analisá-lo de maneira consistente e também efetuar comparações com processos externos considerados “melhores práticas” ou *benchmarking*. As constatações de defasagens permitem ações corretivas e de melhorias aos referidos processos.

		OBJETIVOS DE CONTROLE												
		TABELA RESUMO												
DOMÍNIO	PROCESSO	Critérios de Informação						Recursos de TI						
		eficácia	eficiência	confidencialidade	integridade	disponibilidade	conformidade	confiabilidade	humano	aplicações	tecnologia	infra-estrutura	dados	
Planejamento & Organização	PO1	Definir um plano estratégico	P	S						v	v	v	v	v
	PO2	Definir a arquitetura da informação	P	S	S	S				v			v	
	PO3	Determinar a arquitetura tecnológica	P	S							v	v		
	PO4	Definir a organização de TI e os relacionamentos	P	S						v				
	PO5	Gerenciar os investimentos de TI	P	P				S		v	v	v	v	
	PO6	Comunicar os objetivos e direção da Administração	P					S		v				
	PO7	Gerenciar recursos humanos	P	P						v				
	PO8	Garantir a conformidade com os requisitos externos	P					P	S	v	v			v
	PO9	Avaliar riscos	P	S	P	P	P	S	S	v	v	v	v	v
	PO10	Gerenciar projetos	P	P						v	v	v	v	
	PO11	Gerenciar a qualidade	P	P		P			S	v	v	v	v	
Aquisição & Implementação	AI1	Identificar soluções automatizadas	P	S						v	v	v		
	AI2	Adquirir e manter software aplicativo	P	P		S		S	S	v				
	AI3	Adquirir e manter infraestrutura tecnológica	P	P		S					v			
	AI4	Desenvolver e manter procedimentos	P	P		S		S	S	v	v	v	v	
	AI5	Instalar e homologar sistemas	P			S				v	v	v	v	v
	AI6	Gerenciar mudanças	P	P		P			S	v	v	v	v	v
Entregas & Suporte	DS1	Definir e gerenciar níveis de serviços	P	P	S	S	S	S	S	v	v	v	v	v
	DS2	Gerenciar serviços de terceiros	P	P	S	S	S	S	S	v	v	v	v	v
	DS3	Gerenciar desempenho e capacidade	P	P			S				v	v	v	
	DS4	Garantir serviço contínuo	P	S			P			v	v	v	v	v
	DS5	Garantir segurança dos sistemas			P	P	S	S	S	v	v	v	v	v
	DS6	Identificar e alocar custos		P					P	v	v	v	v	v
	DS7	Educar e treinar usuários	P	S						v				
	DS8	Assistir e aconselhar clientes	P	P						v	v			
	DS9	Gerenciar a configuração	P				S		S	v	v	v		
	DS10	Gerenciar problemas e incidentes	P	P			S			v	v	v	v	v
	DS11	Gerenciar dados				P			P					v
	DS12	Gerenciar instalações				P	P						v	
	DS13	Gerenciar operações	P	P		S	S			v	v		v	v
Monitoramento	M1	Monitorar processos	P	P	S	S	S	S	S	v	v	v	v	v
	M2	Avaliar a adequação do controle interno	P	P	S	S	S	P	S	v	v	v	v	v
	M3	Obter garantia independente	P	P	S	S	S	P	S	v	v	v	v	v
	M4	Prover auditoria independente	P	P	S	S	S	P	S	v	v	v	v	v

(P) primário (S) secundário (v) aplicável a

FIGURA 11 – Objetivos de Controle de alto nível COBIT – Tabela Resumo.

FONTE – adaptado de COBIT (2000b) e traduzido por Dupré (2001, p. 19).

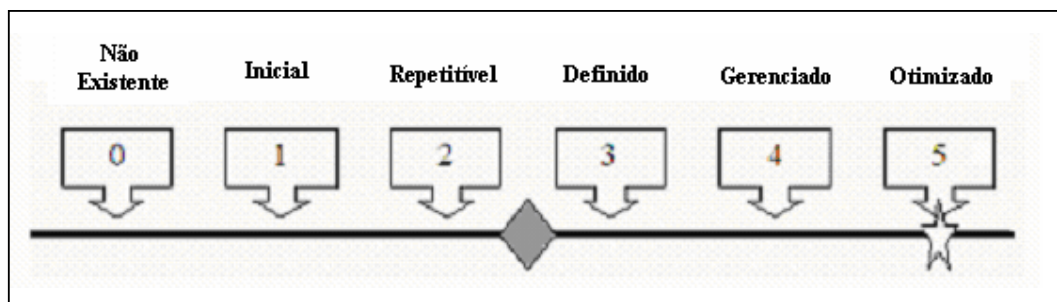
### 3.5.6 Definição e métrica para o modelo de maturidade

A métrica é um recurso que permite a partir de uma escala de valores, indicar em qual posição o objeto analisado está situado. Desta maneira é possível comparar os processos em relação aos padrões e saber sua real situação.

O modelo de maturidade permite identificar o grau de maturidade no qual o processo se encontra e desta maneira determinar onde estão os pontos de melhoria se comparados com as melhores práticas da organização ou do mercado.

De acordo com o Guia de Gestão do COBIT (2000d, p.10), adota-se, em cada um dos seus processos, um modelo de maturidade baseado no *Capability Maturity Model Integraton (CMMI)*, com escala utilizada de seis níveis, e variação de um ponto entre os níveis, estando tal amplitude contida em uma faixa de zero a cinco. Este modelo de maturidade foi criado inicialmente em 1991 e evoluído em 2002 para uma estrutura integrada (LIU, 2006, p.71).

A FIG. 12 ilustra o modelo de maturidade apresentado, assim como os níveis representados de zero a cinco. A indicação feita por meio do símbolo losango representa o grau de maturidade em que o processo se encontra. A indicação por meio do símbolo estrela significa a posição de melhor prática para o processo em busca da melhoria contínua.



**FIGURA 12** – Modelo de maturidade baseado no CMMI.

FONTE – adaptado de Liu (2006, p. 71).

A seguir, no QUADRO 6 estão informadas as legendas para cada nível, o modelo de maturidade relacionado a cada processo é descrito de maneira detalhada no livro Guia de Gestão do COBIT (2000d).

**QUADRO 6** – Escala para o modelo de maturidade adotado pelo COBIT.

<b>Escala</b>	<b>Legenda</b>
<b>0</b>	<b>Não há definição e gerenciamento de processos</b>
<b>1</b>	<b>Processos são informais e irregulares</b>
<b>2</b>	<b>Processos são documentados e comunicados</b>
<b>3</b>	<b>Processos seguem um padrão regular</b>
<b>4</b>	<b>Processos são monitorados e medidos</b>
<b>5</b>	<b>Melhores práticas automatizadas</b>

FONTE – adaptado de Liu (2006) e COBIT (2000d).

Este capítulo descreveu o modelo COBIT, seus domínios e inter-relacionamentos entre processos, assim como seu ciclo de gestão e a matriz de objetivos de controle. Também foram definidas e especificadas as métricas dos níveis de responsabilidades, de acordo com o *Capability Maturity Model Integration* (CMMI).

## 4. LEI SARBANES-OXLEY – SOX, UTILIZANDO OS CONTROLES PROPOSTOS PELO COBIT

---

---

### 4.1 Lei Sarbanes-Oxley – SOX

A Lei, denominada *Public Accounting Reform and Investor Protection Act*, foi publicada em agosto de 2002, por meio da promulgação pelo 107º Congresso dos EUA, para regular as responsabilidades e práticas de auditoria em empresas abertas, protegendo assim, os investidores por meio da precisão e da confiabilidade nas empresas conforme mecanismos de segurança.

Os principais objetivos dessa lei são proteger de fraudes contábeis e financeiras os investidores do mercado de capitais americano em companhias abertas, e instituir penalidades em caso de crimes relacionados (DELLOITE, 2005).

De acordo com Ramos (FERNANDES; ABREU, 2006, p.22), o foco da lei estabelece “controles internos sobre relatórios financeiros”.

O termo é definido como o processo projetado por, ou sob a supervisão do principal executivo e do principal responsável por finanças do emitente, ou pessoas que desempenham funções similares, efetivados pelo comitê de diretores do emitente, pela gerência ou outras pessoas, para prover garantia razoável relacionada à confiabilidade de emissão de relatórios financeiros e a preparação de relatórios de resultados financeiros para propósitos externos, de acordo com princípios de contabilidade geralmente aceitos.

Composta de três Seções iniciais, denominadas “*Section 1*”; “*Section 2*” e “*Section 3*”, seguido por onze outros “Títulos”, e estes subdivididos em seções. O QUADRO 7 mostra esses “Títulos” e os seus principais objetivos.

QUADRO 7 – Relação dos títulos originais da Lei *Sarbanes-Oxley*.

Item	Título original	Principais Objetivos
<i>Section 1</i>	<i>Short title, Table of contents</i>	Contém o sumário do conteúdo
<i>Section 2</i>	<i>Definitions</i>	Contém as definições
<i>Section 3</i>	<i>Commission rules and enforcement</i>	Trata dos papéis e ações penais
<i>Title I</i>	<i>Public company accounting oversight board</i>	Trata da forma com que as auditorias devem ser registradas
<i>Title II</i>	<i>Auditor independence</i>	Estabelece que os auditores sejam independentes e que haja rotatividade entre empresas de auditoria
<i>Title III</i>	<i>Corporate responsibility</i>	Atribui as responsabilidades corporativas, em termos da formação de um comitê de auditoria, da composição e requisitos e condutas requeridas dos executivos e diretores responsáveis
<i>Title IV</i>	<i>Enhanced financial disclosures</i>	Estabelece regras para a publicação de resultados financeiros e sistema de controle interno adequado
<i>Title V</i>	<i>Analyst conflict of interest</i>	Estabelece regras para que não haja conflitos de interesses na atuação de analistas de corretoras de valores ou de administradoras de fundos
<i>Title VI</i>	<i>Commission resources and authority</i>	Estabelece regras de controles de autoridade para a atuação das corretoras e dos fundos
<i>Title VII</i>	<i>Studies and reports</i>	Autoriza a SEC <sup>4</sup> a efetuar estudos e relatórios relativos à consolidação de firmas de auditoria, agências de classificação de risco, violações profissionais em âmbito do mercado de capitais
<i>Title VIII</i>	<i>Corporate and criminal fraud accountability</i>	Estabelece as regras e penalidades em casos de fraudes
<i>Title IX</i>	<i>White-collar crime penalty enhancements</i>	Contém penalidades para crimes do colarinho branco
<i>Title X</i>	<i>Corporate tax return</i>	Estabelece que o principal executivo deve assinar o imposto de renda jurídico
<i>Title XI</i>	<i>Corporate fraud and accountability</i>	Define a responsabilidade corporativa pela comunicação de informações financeiras de resultados fraudulentos

FONTE – adaptado *SARBANES OXLEY ACT OF 2002* (2002) e Fernandes e Abreu (2006).

<sup>4</sup> SEC = *Stock Exchange Comission* (Comissão de Valores Mobiliários) com autoridade para estabelecer regras sobre o mercado de capitais norte-americano e responsável por implantar o *Sarbanes-Oxley Act*.

## **4.2. Títulos e Seções da Lei SOX relacionadas aos relatórios financeiros**

O Título I descreve as responsabilidades de atuação dos executivos em chefia sobre a contabilidade das empresas públicas, encontrando-se na Seção 103, “*Section 103. AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS AND RULES*”, (*SARBANES-OXLEY ACT OF 2002*, 2002, p.755) referências aos papéis de auditoria, controle de qualidade, e padrões e regras.

O Título III trata das responsabilidades corporativas relacionadas principalmente aos relatórios financeiros. Na Seção 302, “*Section 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS*” são encontrados os controles e procedimentos internos para a emissão de relatórios financeiros (*SARBANES-OXLEY ACT OF 2002*, 2002, p.777).

Estão também relacionados aos relatórios financeiros os Títulos IV e IX. O primeiro Título trata da ampliação das descobertas financeiras, a Seção 404, “*Section 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS*”, estabelece a avaliação dos controles e procedimentos internos para a emissão dos relatórios financeiros (*SARBANES-OXLEY ACT OF 2002*, 2002, p.789). O segundo Título trata da amplitude dos crimes do “colarinho branco”, contido na Seção 906, “*Section 906. CORPORATE REPORT FOR FINANCIAL REPORT*”. Nela estão descritas as responsabilidades dos executivos quanto à certificação dos relatórios de demonstração financeira (*SARBANES-OXLEY ACT OF 2002*, 2002, p.806).

## **4.3 Lei SOX, Título III, Seção 302 – Responsabilidade corporativa sobre os relatórios financeiros**

A Seção 302 impõe os níveis de responsabilidade aos diretores executivos (*Chief Executive Officer – CEO*) e diretores financeiros (*Chief Financial Officer – CFO*), que devem declarar pessoalmente a divulgação e procedimentos de controle.

#### **4.4 Lei SOX, Título IV, Seção 404 – Avaliação anual dos controles e procedimentos internos para a emissão de relatórios**

A Seção 404 contém a diretriz que determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Como na Seção 302, esta Seção exige que os diretores executivos e os diretores financeiros avaliem e atestem periodicamente a eficácia desses controles. Nesta Seção também são encontradas diretrizes que obrigam as companhias a incluir em seus relatórios anuais um relatório sobre controles internos emitido pela administração.

#### **4.5 Lei SOX, Título IX, Seção 906 – Responsabilidade corporativa pelos relatórios financeiros**

A Seção 906 exige que diretores executivos e diretores financeiros assinem e certifiquem o relatório periódico contendo as demonstrações financeiras. A certificação executiva declara que o relatório cumpre as exigências da emissão de relatórios determinadas pela *Stock Exchange Commission* (SEC) e que representam adequadamente a condição financeira da companhia, bem como os resultados de suas operações. O descumprimento dessa exigência tem alto valor em multas, assim como outras ações penais.

#### **4.6 Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 referentes ao aspecto: “dados” e “metadados”**

Conforme tratado no item 3.5 (capítulo Três desta dissertação), o modelo conceitual COBIT representado por meio das três dimensões de um cubo, relaciona “Processos de TI”, “Critérios de Informação”, “Recursos de TI” e “Objetivos de Controle”. São estes referidos objetivos que permitem controlar e validar a aderência dos processos com a Lei SOX.

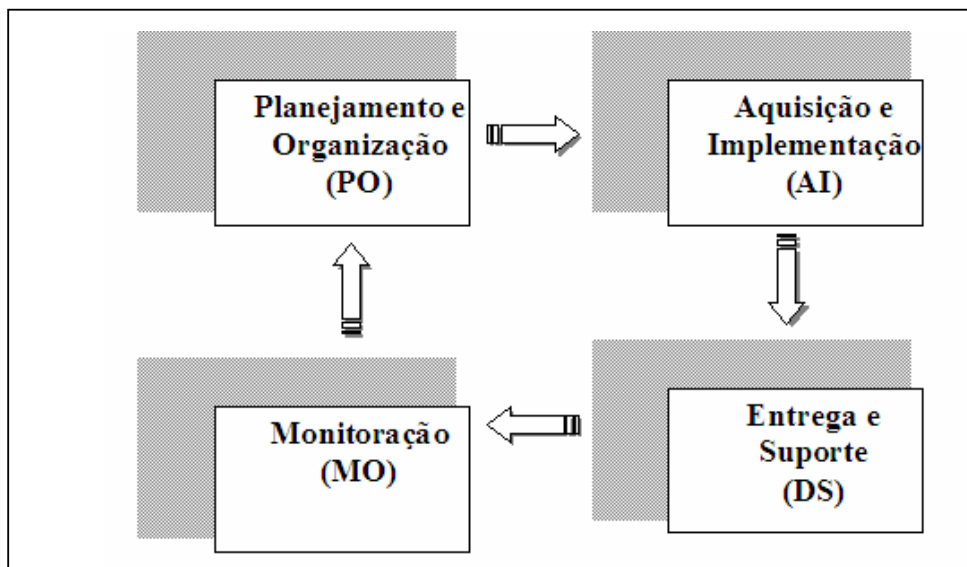


Em cada processo é definido um conjunto de características formais que especificam e estabelecem os meios, não apenas para executar os controles, mas também as métricas para avaliar o estado dos processos no momento presente. Desta maneira é possível planejar qual o grau que os processos devem alcançar em um momento futuro, podendo assim acompanhar o seu comportamento evolutivo (COBIT, 2000d, p.23).

As características formais compreendem cada um dos quatro domínios (PO, AI, DS e MO), assim como várias outras especificações, dentre elas recursos, processos, indicadores. Para cada um dos processos são especificados o “Objetivo de Controle”, o “Indicador Desempenho”, os “Fatores Críticos de Sucesso”, os “Critérios de Informação”, os “Recursos de TI”, e as métricas contidas em cada um dos níveis do “Modelo de Maturidade”.

Os quatro domínios devem trabalhar em sincronismo e formar um ciclo para que os processos estejam em constante melhoria e aperfeiçoamento. Este ciclo está representado na FIG. 13.

Para o escopo desta dissertação foram considerados todos os quatro domínios, e dentro destes, os seguintes processos: PO1, PO2, PO8, PO9, AI6, DS1, DS2, DS4, DS6, DS11, M1, M2, M3 e M4. Estes processos foram escolhidos para detalhar e aplicar o modelo de gestão de Governança de TI, que atendem às Seções da Lei em relação ao aspecto dos “dados” uma vez que tratam de processos para “dados” e “metadados”. Tais recursos estão contidos nos objetivos de controle propostos pelo COBIT e são necessários para efetuar os controles internos e atender às Seções, em questão, da Lei SOX (LAHTI; PETERSON, 2005, p.35).



**FIGURA 13** – Processos de TI do Domínio COBIT.

FONTE – adaptado de Liu (2006).

#### **4.6.1 Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “PO – Planejamento e Organização” com recursos de TI para o aspecto: “dados” e “metadados”**

O domínio “PO – Planejamento e Organização” cobre a área estratégica e tática, e contribui para alcançar os objetivos do negócio e atender às solicitações da Lei SOX. A visão estratégica permite planejar, comunicar e gerir o negócio a partir das diversas perspectivas de informação, de arquitetura e de tecnologia. Os processos analisados neste domínio são: “PO1 – Definir um plano estratégico de TI”, “PO2 – Definir uma arquitetura de informação”, “PO8 – Garantir a aderência aos requisitos externos” e “PO9 – Avaliar riscos”.

##### **4.6.1.1 PO1 – Definir um plano estratégico de TI**

###### **Objetivo do processo**

Definir um plano estratégico de longo prazo que satisfaça ao requisito do negócio de efetuar a gestão dos dados e metadados.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “PO1”, devem-se observar os seguintes itens:

- 1 – Conter nos planos de longo e de curto prazos os objetivos da organização e dos negócios, as suas estratégias, e os seus riscos ambientais, tecnológicos, financeiros, e humanos, relacionados à gestão de dados e dos metadados.
- 2 – Comunicar os planos de longo e de curto prazos em todos os níveis da organização.
- 3 – Monitorar os planos de longo e de curto prazos de forma cíclica por meio de um processo de realimentação.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Índice da qualidade do plano estratégico de TI, com aderência aos objetivos de gestão de dados e metadados.

### **Crerios de Informaçaõ**

Os critérios de informaçaõ que impactam o processo e o seu respectivo grau de importãncia sãõ:

- 1 – Eficãcia impacta em grau primãrio.
- 2 – Eficiãcia impacta em grau secundãrio.

### **Recursos de TI**

Descriçaõ dos recursos de TI necessãrios ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicaçaõ.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalaçaõs.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “PO1 – Define um Plano Estratégico de TI”.

**0 – Inexistente.** Não existe um plano estratégico definido para atender aos requisitos do modelo de maturidade.

**1 – Inicial / Ad Hoc.** A necessidade de um planejamento estratégico é conhecida pela gerência de TI, mas não existe processo de decisão estruturado e nem planejamento estratégico para atender aos requisitos do modelo de maturidade.

**2 – Repetitivo, mas intuitivo.** O planejamento estratégico é conhecido, porém não existe processo de decisão documentado. As estratégias são básicas, visam projeto a projeto e não consideram as estratégias de toda a organização.

**3 – Processo definido.** Por meio uma política definida de planejamento estratégico. Não existem procedimentos para examinar o processo de maneira regular. Buscam-se procedimentos inovadores para acompanhar o planejamento estratégico e atender as questões do modelo de maturidade.

**4 – Gerenciado e medido.** O planejamento estratégico é prática padronizada e possui tratamento de exceções. O planejamento financeiro é feito em cascata, de cima para baixo em toda a organização.

**5 – Otimizado.** O planejamento é documentado e considera os objetivos de negócio. Continuamente são atualizados e observados os investimentos, o valor agregado e os riscos. Relatórios financeiros são verificados de maneira a atender as estratégias do negócio.

#### **4.6.1.2 PO2 – Definir a arquitetura de informação**

##### **Objetivo do processo**

Definir a arquitetura de informação que satisfaça ao requisito do negócio de otimizar a organização dos sistemas de informação de efetuar a gestão dos dados e metadados.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “PO2”, devem-se observar os seguintes itens:

- 1 – Alinhar o modelo de arquitetura de informação com as necessidades da organização, dos profissionais e com o plano de longo prazo de TI.
- 2 – Possuir um repositório corporativo dos metadados atualizado e incorporado com as regras de negócio e de sintaxe de dados da organização.
- 3 – Possuir níveis de acesso e regras de segurança para os dados.
- 4 – Monitorar a arquitetura de informação de forma cíclica por meio de um processo de realimentação.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Permite monitorar o desempenho do processo:

- 1 – Percentual de classificação de dados e metadados documentados.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau secundário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 – Integridade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – Os sistemas de aplicação.
- 2 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “PO2 – Definir a arquitetura de informação”.

**0 – Inexistente.** Não existe o reconhecimento da importância da arquitetura de informação para a organização. Também não existe conhecimento técnico e experiência para desenvolver esta arquitetura, que atenda as questões do modelo de maturidade.

**1 – Inicial / Ad Hoc.** A gerência reconhece a necessidade para a arquitetura de informação, mas não formaliza um processo ou um plano para desenvolver uma. Desenvolvimento isolado e reativo dos componentes de uma arquitetura de informação está ocorrendo. É isolado, ocorrem execuções parciais de diagramas dos dados, de documentação, e de regras da sintaxe de dados. As definições dirigem-se aos dados, mais do que à informação, e são efetuadas por meio dos aplicativos.

**2 – Repetitivo, porém intuitivo.** Existe a consciência da importância de uma arquitetura de informação para organização. Os procedimentos são informais e intuitivos, seguidos por indivíduos diferentes dentro da organização. Não há nenhum treinamento formal. As necessidades para atender ao modelo de maturidade direcionam os componentes da arquitetura de informação pelos técnicos de TI.

**3 – Processo definido.** A importância da arquitetura de informação é compreendida e aceita, e a responsabilidade para sua entrega é atribuída e claramente comunicada. Procedimentos relacionados, ferramentas e técnicas que atendam ao modelo de maturidade, embora não sofisticado, foram padronizadas e documentadas. As políticas básicas da arquitetura da informação foram se tornando exigências de algumas estratégicas, mas a conformidade com as políticas, os padrões e as ferramentas não é reforçada consistentemente. A função da administração de dados está presente, ajustando padrões e começando a relatar o uso da arquitetura de informação. Ferramentas automatizadas de administração dos dados estão emergindo, mas os

processos e as métricas usadas são definidos por meio de fornecedores de *software* da base de dados.

**4 – Gerenciado e medido.** O desenvolvimento e o esforço da arquitetura de informação é suportado inteiramente por métodos e por técnicas formais. Existem processos responsáveis por mudanças e necessidades do negócio. A arquitetura de informação é formalizada e existem atividades de treinamento definidas, documentadas e consistentemente aplicadas. Ferramentas automatizadas são difundidas, mas não estão ainda integradas. Melhores práticas internas são compartilhadas e introduzidas ao processo e este é pró-ativo e focalizado às necessidades futuras do negócio. A organização da administração dos dados é envolvida ativamente em todos os esforços do desenvolvimento da aplicação e asseguram os objetivos do modelo de maturidade. Um repositório de metadados automatizado gerencia inteiramente modelos e definições.

**5 – Otimizado.** A arquitetura de informação é consistentemente reforçada em todos os níveis e em seu valor ao negócio. As equipes possuem as habilidades necessárias para desenvolver e manter uma arquitetura robusta e responsiva da informação que reflita todas as exigências do negócio e atenda ao modelo de maturidade. A informação fornecida pela arquitetura de informação é aplicada consistente e extensivamente. Utiliza as melhores práticas da indústria no desenvolvimento e na manutenção da arquitetura de informação incluindo melhoria contínua do processo.

#### **4.6.1.3 PO8 – Garantir conformidade com os requisitos externos**

##### **Objetivo do processo**

Assegurar conformidade com os requisitos externos que satisfaça ao requisito do negócio de efetuar a gestão dos dados e metadados em conformidade com as obrigações legais, regulamentares e contratuais.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “PO8”, devem-se observar os seguintes itens:

- 1 – Identificar e analisar os requisitos externos e seu impacto em TI.
- 2 – Adotar políticas e procedimentos adequados para cumprir com os requisitos externos.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Frequência de revisões dos requisitos externos.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Conformidade impacta em grau primário.
- 3 – Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Os recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “PO8 – Garantir conformidade com os requisitos externos”.

**0 – Inexistente.** Apenas um pequeno reconhecimento de requisitos externos que afetam a TI, com a visão de processos aderentes aos requisitos regulatórios, legais e contratuais. As questões do modelo de maturidade não estão atendidas.



**1 – Inicial / Ad Hoc.** Existe o reconhecimento da aderência regulatória, legal e contratual das questões do modelo de maturidade. Os processos, se existirem, são informais.

**2 – Repetitivo, porém intuitivo.** Há uma consciência da importância de aderência aos requisitos externos e da necessidade de comunicá-los. A conformidade também está relacionada com as exigências aos regulamentos financeiros, de legislação e demais elementos do modelo de maturidade.

**3 – Processo definido.** Políticas, procedimentos e processos estão sendo desenvolvidos, documentados e comunicados, assegurando assim, aderência às obrigações contratuais e legais. Treinamentos, contratos padronizados e processos permitem a redução dos riscos e atendem as questões do modelo de maturidade.

**4 – Gerenciado e medido.** Existe completo entendimento de itens e elementos relacionados aos requisitos externos e às necessidades para garantir a conformidade em todos os níveis. As responsabilidades são claras e os responsáveis pelos processos os compreendem. Existem mecanismos que permitem monitorar a não conformidade dos requisitos externos e implementam ações corretivas nas questões levantadas para o modelo de maturidade.

**5 – Otimizado.** Existem processos bem organizados, eficientes e comprometidos com a aderência aos requisitos externos, baseados em funções centralizadas com ações por toda a organização. Melhores práticas têm sido desenvolvidas assegurando assim aderência aos requisitos externos. Existem sistemas que permitem rastrear e documentar o fluxo de trabalho, garantindo melhorias de qualidade e eficácia no processo de monitoramento nas questões levantadas para o modelo de maturidade.

#### **4.6.1.4 PO9 – Avaliar riscos**

##### **Objetivo do processo**

Avaliar riscos que satisfaça o requisito do negócio de suportar decisões gerenciais por meio da realização de objetivos e da resposta a

ameaças por meio da redução da complexidade, aumento da objetividade e identificação de fatores de decisão importantes.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “PO9”, devem-se observar os seguintes itens:

- 1 – Identificar e analisar tipos diferentes de riscos de TI (tecnologia, segurança, continuidade, regulamentação, etc.).
- 2 – Analisar causas básicas de riscos.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade e frequência de relatórios de monitoramento de risco.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau secundário.
- 3 – Confidencialidade impacta em grau primário.
- 4 – Integridade impacta em grau primário.
- 5 – Disponibilidade impacta em grau primário.
- 6 – Conformidade impacta em grau secundário.
- 7 – Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “PO9 – Avaliar riscos”.

**0 – Inexistente.** Não ocorre a avaliação de risco para processos e conseqüente tomada de decisão nos negócios. A organização não considera os impactos nos negócios associados com vulnerabilidade da segurança e com os fatores relacionados ao modelo de maturidade.

**1 – Inicial / Ad Hoc.** A organização reconhece as responsabilidades legais e contratuais, porém trata riscos de TI sem utilizar processos ou políticas definidos.

**2 – Repetitivo, porém intuitivo.** Existe um entendimento emergente para a importância da avaliação de riscos de TI, assim como da necessidade de considerá-lo. Apenas em grandes projetos os riscos são avaliados e os procedimentos são descritos levando-se em conta as questões tratadas pelo modelo de maturidade.

**3 – Processo definido.** Por toda a organização, políticas de avaliação e gestão de riscos relacionadas ao modelo de maturidade estão documentadas e disponibilizadas aos responsáveis.

**4 – Gerenciado e medido.** Existe a avaliação de risco por meio de procedimentos padronizados e tratamentos de exceções relatados pela gerência de TI. O processo é avançado e aborda em cada projeto as questões propostas para o modelo de maturidade.

**5 – Otimizado.** A avaliação de risco evolui para uma estrutura de avaliação sistemática e integrada de riscos. Os dados são coletados e geridos automaticamente atendendo a todas as questões relativas ao modelo de maturidade.

#### **4.6.2 Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “AI – Aquisição e Implementação” com recursos de TI para o aspecto: “dados” e “metadados”**

A fim de realizar a estratégia de TI, o domínio “AI – Aquisição e Implementação” identifica, desenvolve, adquire, implementa e integra os processos de negócio. Para permitir que o ciclo de vida do processo seja contínuo, o domínio também cobre as manutenções desses sistemas. As soluções para alcançar os objetivos do negócio e atender às solicitações da Lei SOX. O processo analisado neste domínio é “AI6 – Gerenciar mudanças”.

##### **4.6.2.1 AI6 – Gerenciar mudanças**

###### **Objetivo do processo**

Gerenciar mudanças que satisfaçam os requisitos do negócio para minimizar a probabilidade de ocorrência de erros decorrentes das alterações efetuadas. O sistema gerencial deve proporcionar a análise, a implementação e o acompanhamento de todas as mudanças solicitadas e feitas em relação à integridade dos dados e metadados.

###### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “AI6”, devem-se observar os seguintes itens:

- 1 – Padronizar e formalizar os dados com base em procedimentos.
- 2 – Avaliar o impacto na mudança dos dados, com base em procedimentos.
- 3 – Gerenciar mudanças dos dados por meio de políticas, procedimentos e documentações de administração de dados definidas.

###### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Número de sistemas que estejam documentados e controlados por meio do repositório de metadados.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Integridade impacta em grau primário.
- 4 – Disponibilidade impacta em grau primário.
- 5 – Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “AI6 – Gerenciar mudanças”.

**0 – Inexistente.** Não existe processo para a gestão de mudanças. Não há reconhecimento que as mudanças possam comprometer ambas as operações: de negócio e de TI.

**1 – Inicial / Ad Hoc.** Reconhecimento que as mudanças possam ser gerenciadas e controladas, mas não existe processo consistente para o fluxo. Os métodos variam, resultando em ocorrências de mudanças não autorizadas.

**2 – Repetitivo, porém intuitivo.** Existe um processo informal para a gestão de mudanças, porém ele é rudimentar e sem estrutura formal, e está propenso a erro.

**3 – Processo definido.** Existe um processo formal de gestão de mudança. Ele inclui categorização, priorização, procedimentos de emergência, alteração de autorizações e gestão de publicação sem esforço em relação à aderência.

**4 – Gerenciado e medido.** O processo de gerência de mudança é bem desenvolvido e consistente, com todas as etapas confiáveis sem existir exceções. O processo é eficiente e eficaz, porém confia em procedimentos manuais.

**5 – Otimizado.** O processo de gerência de mudança é regularmente revisto e atualizado para manter as melhores práticas. A configuração da informação é feita por meio de procedimentos automatizados e por mecanismos computacionais, *software* e o controle de versão. O uso de um repositório de metadados centralizado permite controlar a gestão de mudanças.

#### **4.6.3 Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “DS – Entrega e Suporte” com recursos de TI para o aspecto: “dados” e “metadados”**

O domínio “DS – Entrega e Suporte” está preocupado com a entrega dos serviços solicitados. Com esta finalidade, os processos de suporte necessários têm de ser aperfeiçoados, contribuindo assim para alcançar os objetivos do negócio e atender às solicitações da Lei SOX. Os processos analisados neste domínio são: “DS1 – Definir e gerenciar níveis de serviços”, “DS2 – Gerenciar serviços de terceiros”, “DS4 – Garantir serviço contínuo”, “DS6 – Identificar e alocar custos”, “DS11 – Gerenciar dados e metadados”.

##### **4.6.3.1 DS1 – Definir e gerenciar os níveis de serviço**

###### **Objetivos do processo**

Definir e gerenciar níveis de serviço que satisfaça ao requisito do negócio de estabelecer um entendimento comum em relação ao nível de serviço para a gestão de dados e metadados.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “DS1”, devem-se observar os seguintes itens:

- 1 – Existir acordos de níveis de serviços relativos aos dados.
- 2 – Formalizar os níveis de serviço contemplando requisitos mínimos, bem como a respectiva responsabilidade em relação à disponibilidade, confiabilidade, desempenho, capacidade de crescimento, suporte aos usuários, plano de continuidade, níveis de segurança dos dados e metadados.
- 3 – Definir responsáveis pelos dados (*data stewards*) assegurando que os níveis de serviços contemplando os dados serão estabelecidos, coordenados e comunicados em todas as áreas envolvidas.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Número de ocorrências da inconsistência dos dados e suas causas são detectados.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 – Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau secundário.
- 7 – Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “DS1 – Definir e gerenciar níveis de serviços”.

**0 – Inexistente.** Não existe reconhecimento da necessidade de gestão em relação ao nível de serviço. São desprezadas a contabilidade e a responsabilidade de monitoramento.

**1 – Inicial / Ad Hoc.** Existe reconhecimento da necessidade da gestão do nível de serviços, porém o processo é informal e reativo.

**2 – Repetitivo, porém intuitivo.** Existem acordos em relação ao nível de serviço, mas eles são informais e não são revisados. O documento do acordo está incompleto e depende de iniciativas individuais.

**3 – Processo definido.** O desenvolvimento do processo de acordos e satisfação do cliente é atendido e verificado por meio de listas de itens. Os critérios são pré-definidos e acordados com os usuários. Pequenos níveis de falhas são identificados, mas o planejamento ainda é informal.

**4 – Gerenciado e medido.** Os acordos de nível de serviço estão sendo ampliados. A satisfação do cliente é tratada de maneira transparente por meio de rotinas medidas e avaliada. Os riscos operacionais e financeiros associados estão definidos e são claramente compreendidos.

**5 – Otimizado.** Os acordos são continuamente reavaliados para assegurar o alinhamento de TI com os objetivos do negócio. Os critérios para o controle da satisfação do consumidor são: disponibilidade, confiabilidade, desempenho, capacidade de expansão, suporte ao usuário, planejamento e segurança. Existem processos para



monitorar e melhorar os procedimentos de níveis de acordos de serviços entre as partes.

#### **4.6.3.2 DS2 – Gerenciar serviços de terceiros**

##### **Objetivo do processo**

Administrar serviços de terceiros que satisfaça ao requisito do negócio para assegurar que os papéis e responsabilidades dos terceiros sejam claramente definidos e estejam aderentes com a administração de dados. Os serviços de terceiros têm que atender aos itens das Seções 103, 302, 404 e 906 da Lei SOX.

##### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “DS2”, devem-se observar os seguintes itens:

- 1 – Possuir procedimentos de revisão e monitoramento que garantam os níveis de serviço de terceiros para a sua eficácia e conformidade com a política da organização.
- 2 – Administrar os serviços levando em consideração os acordos de serviços terceirizados, a administração de contratos do fornecedor do repositório, o monitoramento e controle de serviços de dados, as recompensas e penalidades de desempenho, e a análise das variações do nível de serviço e de custos.

##### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade de contratos de níveis de serviços acertados.

##### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.

- 3 – Confidencialidade impacta em grau secundário.
- 4 – Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau secundário.
- 7 – Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “DS2 – Gerenciar serviços de terceiros”.

**0 – Inexistente.** Não existem processos e políticas formais com relação à contratação de terceiros. As atividades não são medidas e nem existem obrigações contratuais.

**1 – Inicial / Ad Hoc.** Reconhecimento da necessidade de se ter políticas e procedimentos documentados em relação aos serviços de terceiros. Não existem termos padronizados de acordos e as práticas dependem de experiências individuais.

**2 – Repetitivo, porém intuitivo.** Existe um processo informal para a gestão de terceiros. Um contrato pró-forma é assinado entre as partes, mas não suporta os objetivos do negócio.

**3 – Processo definido.** Procedimentos são bem documentados e direcionam a governança dos terceirizados. A relação entre as partes é regida exclusivamente por meio de contrato para os requisitos operacional, legal e de controle.

**4 – Gerenciado e medido.** Critérios formalizados e padronizados são estabelecidos para definir o escopo do serviço, dos artefatos

entregáveis, dos custos, das responsabilidades em termos de negócios e condições. As partes reconhecem a expectativa em relação aos serviços, aos custos e aos marcos.

**5 – Otimizado.** As partes periodicamente revisam os contratos, avaliam a qualidade do serviço entregue e a atuação do fornecedor. Evidência do comprometimento em relação aos aspectos operacional, legal e de controle é regularmente avaliada, e quando for o caso, revistos e atualizados.

#### **4.6.3.3 DS4 – Garantir serviço contínuo**

##### **Objetivo do processo**

Garantir serviço contínuo que satisfaça o requisito do negócio de assegurar que os serviços de TI para gestão dos dados e metadados estejam disponíveis como requerido, e para garantir um mínimo de impacto no negócio em caso de grande falha.

##### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “DS4”, devem-se observar os seguintes itens:

- 1 – Possuir de um plano de continuidade de TI, operacional e testado o qual está alinhado com o plano geral de continuidade relacionado ao negócio.
- 2 – Possuir o monitoramento e a comunicação de desempenho e de problemas. Ações corretivas são tomadas e falhas investigadas. As estatísticas geradas são analisadas por meio de processos e períodos definidos.
- 3 – Tratar de forma sistemática os aspectos de continuidade levando em conta a classificação do nível crítico, os procedimentos alternativos, as cópias de segurança e suas respectivas recuperações (*backup and recovery*).

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Tempo decorrido entre o diagnóstico de um incidente e a execução do plano de continuidade.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau secundário.
- 3 – Disponibilidade impacta em grau primário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “DS4 – Garantir serviço contínuo”.

**0 – Inexistente.** Não existe o entendimento do risco, da vulnerabilidade e do perigo nas operações de TI que resultem em problemas para o negócio.

**1 – Inicial / Ad Hoc.** Reconhecimento relacionado ao risco de continuidade dos serviços. As respostas em relação ao rompimento de continuidade são mais reativas.

**2 – Repetitivo, porém intuitivo.** Existe inventário dos sistemas críticos e o processo de padronização de práticas de serviços contínuos e

monitoramento do processo é emergente. Não existe documentação de usuário e planos de continuidade.

**3 – Processo definido.** Responsabilidades em relação ao planejamento de continuidade dos serviços estão claramente definidas. Os relatórios são periodicamente analisados. Os sistemas críticos são rigorosamente mantidos.

**4 – Gerenciado e medido.** A responsabilidade para manter a continuidade do serviço está assegurada. Os dados estruturados relativos à continuidade do serviço são analisados e relatados.

**5 – Otimizado.** A continuidade do serviço é efetuada por meio de um processo integrado, pró-ativo, automatizado, auto ajustado e auto analisado. É feita de maneira planejada e alinhada com as rotinas de manutenção.

#### **4.6.3.4 DS6 – Identificar e alocar custos**

##### **Objetivo do processo**

Identificar e alocar de custos que satisfaça o requisito do negócio de assegurar a correta interpretação dos custos atribuíveis aos serviços de TI em relação à gestão dos dados e metadados.

##### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “DS6”, devem-se observar os seguintes itens:

- 1 – Possuir um sistema contábil de custos que assegure que os custos sejam registrados, calculados e alocados ao nível de detalhe exigido e esteja apropriado ao serviço oferecido.
- 2 – Possuir serviço de monitoramento e reporte de taxas de custeio.
- 3 – Possuir políticas e procedimentos de custeio.

##### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Porcentagem de variação entre os orçamentos, previsto e realizado para gestão dos dados e metadados.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficiência impacta em grau primário.
- 2 – Confiabilidade impacta em grau primário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicações.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “DS6 – Identificar e alocar custos”.

**0 – Inexistente.** Não existe reconhecimento que enderece a contabilidade de custos para provimento de serviços de TI.

**1 – Inicial / Ad Hoc.** Existe compreensão geral sobre custos dos serviços de informação, mas sem especificá-los por usuários, projetos e sistemas. Não se têm custos relacionados aos sistemas de TI.

**2 – Repetitivo, porém intuitivo.** Existe a necessidade de se identificar e alocar custos. Esses são assumidos de maneira rudimentar e informal.

**3 – Processo definido.** Existe um modelo de custos documentado para os sistemas de informação. O modelo é institucionalizado e comunicado, mas de maneira informal.

**4 – Gerenciado e medido.** Os custos dos serviços de informação são contabilizados e estão completamente compreendidos de maneira

formal. Esses também são monitorados, e ações evolutivas ocorrem quando os processos não estão trabalhando corretamente.

**5 – Otimizado.** Os custos dos serviços são identificados, capturados, resumidos e reportados seguindo processos estruturados. Forte monitoramento e acompanhamento de custos relacionados aos modelos de representação dos dados, a administração dos dados e os metadados.

#### **4.6.3.5 DS11 – Gerenciar dados e metadados**

##### **Objetivo do processo**

Administrar dados e metadados que satisfaçam ao requisito do negócio assegurando que se mantenham completos, exatos e válidos durante sua entrada, atualização e armazenamento.

##### **Objetivos de Controle**

Os objetivos de controle do processo “DS11”, devem:

- 1 – Possuir uma combinação efetiva dos controles das fontes de documentos, entrada, processamento, de saída e demais operações de TI.
- 2 – Escolher, implantar e administrar o repositório de metadados
- 4 – Possuir os controles para qualidade de dados, da informação, e das regras de negócio, por meio de mecanismos de tratamento adequados.
- 5 – Possuir monitoramento e reporte do desempenho e dos problemas de inconsistências de dados. Ações corretivas são tomadas e as falhas investigadas. As estatísticas geradas são analisadas por meio de processos e em períodos definidos.

##### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Porcentagem de dados de entrada com erro.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Integridade impacta em grau primário.
- 2 – Confiabilidade impacta em grau primário.

### **Recurso de TI**

Descrição do recurso de TI necessário ao processo:

- 1 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “DS11 – Gerenciar dados e metadados”.

**0 – Inexistente.** Os dados não são reconhecidos como recursos corporativos e de valor agregado. Não existem dono e contabilidade individual referente à integridade e confiabilidade dos dados. Segurança e qualidade dos dados são inexistentes.

**1 – Inicial / Ad Hoc.** Reconhecimento em relação à necessidade para a precisão dos dados. Alguns métodos são desenvolvidos em nível individual para prevenir e detectar as entradas dos dados. Processos de detecção e correção são individuais. Segurança e integridade dos dados não são gerenciados.

**2 – Repetitivo, porém intuitivo.** Reconhecimento da necessidade de precisão e manutenção da integridade dos dados. Começa a ocorrer o personagem responsável pelos dados (*data steward*), mas em nível muito tênue. Os papéis e requisitos de documentação são individuais e não atravessam toda a organização. Início da função de “custodiante” dos dados exercida pela TI. Princípios de segurança e integridade de dados são aplicados à função dos “serviços de informação”.

**3 – Processo definido.** Necessidade para a integridade dos dados dentro do contexto organizacional é aceita e compreendida. Os processos de entrada e saída dos dados estão padronizados e formalizados. Os processos de identificação e correção de erros são



automatizados. Responsáveis pelos dados acompanham e controlam sua qualidade em nível mais baixo e utilizando técnicas automatizadas. A documentação e manutenção dos sistemas de bancos de dados permitem uma administração centralizada e com papel de custódia.

**4 – Gerenciado e medido.** Os dados são definidos como recursos corporativos e possuem valor agregado. A responsabilidade pela qualidade dos dados está claramente definida e difundida pela organização. Técnicas de controle de qualidade para os dados são empregadas, de forma que a integridade, segurança e precisão sejam monitoradas e em caso de desvio corrigidas.

**5 – Otimizado.** O processo de gerência de dados está maduro, integrado e atravessa toda a organização, assim como é bem compreendido por todos os usuários envolvidos. Existem mecanismos automáticos para a gestão de qualidade dos dados e gestão de metadados por meio de ferramentas apropriadas.

#### **4.6.4 Objetivos de Controle COBIT para atender à Lei SOX em relação às Seções 103, 302, 404 e 906 no que diz respeito ao domínio “MO – Monitoramento” com recursos de TI para o aspecto: “dados” e “metadados”**

O domínio “M – Monitoramento” é responsável pelos procedimentos de monitoramento ou acompanhamento dos demais processos. Desta forma, os processos tanto de planejamento, aquisição e informação e de entrega e suporte podem ser aperfeiçoados, contribuindo assim para alcançar os objetivos do negócio e atender às solicitações da Lei SOX. Os processos analisados são: “M1 – Monitorar o processo”, “M2 – Avaliar a adequação do controle interno”, “M3 – Obter garantia independente” e “M4 – Prover auditoria independente”.

##### **4.6.4.1 M1 – Monitorar os processos**

###### **Objetivo do processo**

Monitorar os processos que satisfaçam ao requisito do negócio de assegurar a gestão dos dados e metadados.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “M1”, devem-se observar os seguintes itens:

- 1 – Possuir definição de indicadores de desempenho relevantes.
- 2 – Analisar as estatísticas por meio de processos e em períodos definidos.
- 3 – Monitorar os processos de avaliação com direcionadores de desempenho e medidas de resultados, avaliação da satisfação de clientes, relatórios gerenciais, base de conhecimento e comparações (*benchmarks*) com outras empresas.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade de processos monitorados.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 - Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau secundário.
- 7 - Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “M1 – Monitorar os processos”.

**0 – Inexistente.** A organização não tem monitoramento de processos implementado. Não há reconhecimento da necessidade de compreender claramente os objetivos dos processos.

**1 – Inicial / Ad Hoc.** Reconhece uma necessidade para coletar e avaliar informações sobre os processos de monitoramento.

**2 – Repetitivo, porém intuitivo.** Medições básicas a serem monitoradas estão sendo identificadas. Métodos e técnicas de coleta e avaliação estão sendo definidos, mas o processo ainda não é adotado em toda a organização.

**3 – Processo definido.** Processos padronizados para monitoramento estão institucionalizados e são comunicados. Também existem programas de treinamento sendo implementados. Ferramentas para monitoramento interno de TI e dos níveis de serviço estão sendo implementados.

**4 – Gerenciado e medido.** Existe integração de métricas para todos os processos e projetos de TI. Os serviços de informação possuem sistemas para relatar e formalizar tudo automaticamente.

**5 – Otimizado.** Processo contínuo de melhoria é desenvolvido e atualizado em toda a organização. Os padrões e políticas incorporam as melhores práticas da indústria e os indicadores são utilizados rotineiramente.

#### **4.6.4.2 M2 – Avaliar a adequação do controle interno**

##### **Objetivo do processo**

Avaliar a adequação do controle interno que satisfaça ao requisito do negócio de assegurar a realização dos objetivos de controle interno estabelecidos para os processos de TI de efetuar a gestão dos dados e metadados.

### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “M2”, devem-se observar os seguintes itens:

- 1 – Definir indicadores relevantes de controle interno, estimando a sua eficácia.
- 2 – Monitorar continuamente o controle interno levando em conta responsabilidades, comparações (*benchmarks*), relatórios de erros e exceções, auto-avaliações, relatórios gerenciais, conformidade com os requisitos legais e regulamentares.

### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade, frequência e cobertura de relatórios de conformidade de controle.

### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 - Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau primário.
- 7 - Confiabilidade impacta em grau secundário.

### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações.
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “M2 – Avaliar a adequação do controle interno”.

**0 – Inexistente.** Ausência de métodos que permitam gerenciar o controle interno.

**1 – Inicial / Ad Hoc.** Controles internos são efetuados de maneira tradicional por meio de auditorias financeiras e não refletem as necessidades dos sistemas de informação.

**2 – Repetitivo, porém intuitivo.** A organização utiliza controles informais como iniciativas de ações corretivas. Processos de planejamento são definidos, mas está em nível individual de dependência. Controle sobre a segurança é monitorado e os resultados são revisados regularmente. Em relação aos fatores de risco específicos do ambiente de TI, estes estão sendo definidos.

**3 – Processo definido.** Procedimentos e políticas estão sendo desenvolvidos para avaliar e reportar as atividades de monitoramento de controle interno.

**4 – Gerenciado e medido.** Gerenciamento tem estabelecido comparações (*benchmarks*) e quantificado os objetivos para os processos de revisão dos controles internos. A Integração e as ferramentas automáticas estão incorporadas aos processos de revisões dos controles internos, com o uso crescente de análise quantitativa e controle. Os processos específicos para tratamento de risco e políticas de mitigação estão definidos para toda função dos serviços de informação. Uma função formal de controle interno de TI está instituída.

**5 – Otimizado.** Gerenciamento estabelece por toda a organização melhoria contínua, programa de lições aprendidas e melhores práticas da indústria referente ao monitoramento de controles internos.

#### 4.6.4.3 M3 – Obter garantia independente

##### **Objetivo do processo**

Obter garantia independente que satisfaça ao requisito do negócio de aumentar a confiança da gestão dos dados e dos metadados da organização.

##### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “M3”, devem-se observar os seguintes itens:

- 1 – Possuir certificações e homologações independente.
- 2 – Avaliar a eficácia de garantia independente.

##### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade de garantias e certificações.

##### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 - Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau primário.
- 7 - Confiabilidade impacta em grau secundário.

##### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.
- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.

4 – As instalações

5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “M3 – Obter garantia independente”.

**0 – Inexistente.** Ausência de processos que assegurem garantias de independência. Políticas de segurança não estão implementadas e garantias do nível de serviço não estão sendo desenvolvidas.

**1 – Inicial / Ad Hoc.** A organização gerencia processos de TI independentemente. Certificações e garantias são executadas por evento e de forma reativa.

**2 – Repetitivo, porém intuitivo.** A função serviços de informação está implementando processos para gerenciar as atividades de garantia. Métodos e técnicas estão sendo desenvolvidos para certificação e garantias que permitam comparações e garantam melhores práticas.

**3 – Processo definido.** Procedimentos e políticas estão sendo desenvolvidos para garantir atividades de TI. Uma base de conhecimento de certificação e garantia de melhores práticas está sendo desenvolvida.

**4 – Gerenciado e medido.** Gerenciamento tem implementado garantias para os processos críticos de TI identificados e tenham planos de garantia específicos. Os processos são revisados no contexto do negócio por eles suportando. A base de conhecimento de processos de certificação é utilizada para garantir as melhores práticas.

**5 – Otimizado.** Gerenciamento tem implementado medidas para garantir que todos os processos de negócio críticos tenham processos de infra-estrutura de TI para suportá-los. A organização possui programas de melhoria contínua e atualização para processos de garantias e certificação.

#### **4.6.4.4 M4 – Prover auditoria independente**

##### **Objetivo do processo**

Prover auditoria independente que satisfaça ao requisito do negócio de aumentar os níveis de confiança em relação à gestão de dados e metadados.

##### **Objetivos de Controle**

Para atender aos objetivos de controle do processo “M4”, devem-se observar os seguintes itens:

- 1 – Possuir independência da auditoria.
- 2 – Planejar e conduzir a auditoria de modo pró-ativo.
- 3 – Possuir pessoal qualificado para desempenhar as auditorias.
- 4 – Divulgar as descobertas e recomendações das auditorias.

##### **Indicador Chave de Desempenho – KPI – *Key Performance Indicator***

Indicador que permite monitorar o desempenho do processo:

- 1 – Quantidade de ações corretivas resultantes das auditorias

##### **Critério de Informação**

Os critérios de informação que impactam o processo e os seus respectivos graus de importância são:

- 1 – Eficácia impacta em grau primário.
- 2 – Eficiência impacta em grau primário.
- 3 – Confidencialidade impacta em grau secundário.
- 4 - Integridade impacta em grau secundário.
- 5 – Disponibilidade impacta em grau secundário.
- 6 – Conformidade impacta em grau primário.
- 7 - Confiabilidade impacta em grau secundário.

##### **Recursos de TI**

Descrição dos recursos de TI necessários ao processo:

- 1 – As pessoas.



- 2 – Os sistemas de aplicação.
- 3 – A infra-estrutura de tecnologia.
- 4 – As instalações
- 5 – Os dados.

### **Modelo de Maturidade**

O modelo estabelece a escala para os diferentes níveis de maturidade relacionada ao processo “M4 – Prover auditoria independente”.

**0 – Inexistente.** Ausência de importância em relação à função de auditoria independente.

**1 – Inicial / Ad Hoc.** Uma função de auditoria independente existe e é realizada de tempos em tempos, porém não existe planejamento e nem coordenação. O plano de qualidade é pobre e os resultados são variados.

**2 – Repetitivo, porém intuitivo.** Uma função de auditoria independente é reconhecida e está sendo providenciada a política de auditoria.

**3 – Processo definido.** Um processo é estabelecido para planejar e gerenciar auditorias. Possui os elementos básicos que assegurem qualidade e padronização aos procedimentos de auditoria.

**4 – Gerenciado e medido.** O plano de auditoria com base em risco está estabelecido e avalia as necessidades presentes e futuras. Auditorias estão coordenadas e integradas com qualquer ligação financeira e processos de auditoria.

**5 – Otimizado.** A função de auditoria é capaz de responder com rapidez aos processos de negócio e controles de riscos de TI por meio de toda a organização. O plano de auditoria está fortemente integrado com negócios e estratégias de TI. Os processos de auditoria são monitorados e analisados para melhor adaptarem-se às condições das mudanças ambientais. A função de auditoria está envolvida com o desenvolvimento dos planos de negócio e avalia o estado da arte das melhores práticas da indústria.

Neste quarto capítulo foram descritas as Seções 102, 302, 404 e 906 da Lei *Sarbanes-Oxley*, que está relacionada com os relatórios financeiros, responsabilidade corporativa sobre estes relatórios e a avaliação anual dos controles e procedimentos internos para emissão de relatórios, utilizando-se para isto os processos do modelo COBIT. Também foram especificados para cada um dos processos analisados, os possíveis níveis de maturidade necessários conforme o *Capability Maturity Model Integration (CMMI)*.

## 5. MODELAGEM DE PROCESSOS PARA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

---

---

### 5.1 Sistemografia

A modelagem do sistema utiliza instrumentos que permitem a concepção de fenômenos ou projetos percebidos como complexos. A sistemografia é uma técnica de modelagem gráfica e descritiva para a concepção, análise e simulação que busca a racionalidade, agilidade e flexibilidade dos sistemas complexos. Entende-se por sistemas denominados como complexos aqueles formados por arranjos que são conectados por meio de relações circulares (retroação, pró-ação, reação), mesmo que não obrigatoriamente com grande número de elementos (BRESCIANI FILHO, 2006).

De acordo com este método é possível projetar a fase de entendimento dos processos da empresa, auxiliando assim, a análise de processos simples e complexos, e também na descoberta de processos ocultos, que estão presentes nas atividades analisadas. Estas atividades podem ser processos de produção industrial, bem como atividades de gestão (KINTSCHNER, 2003).

Os conceitos básicos, descrições e aplicações sobre o método de modelagem podem ser encontrados em trabalhos de Bresciani Filho (2006) e em suas pesquisas sobre as obras de LeMoigne, Bertalanffy, Morin, Blanchard e Fabrycky. Nestas obras também são encontradas as descrições sobre sistema geral, modelagem sistêmica, simulação e análise de sistemas. A partir dos conceitos apresentados nestes trabalhos foi possível a construção do sistemógrafo de processos, definindo um modelo de Governança de TI (BRESCIANI FILHO, 2006).

### **5.1.1 Construção do sistemógrafo de um processo**

A representação de um sistema pode ser realizada por um processo composto por um conjunto de atividades, que são feitas de maneira tanto seqüenciais, quanto recorrentes. Representam-se estas atividades por meio de blocos, sendo o seu conjunto representável em uma forma típica de diagrama de blocos. Esta representação gráfica recebe a denominação de sistemógrafo (BRESCIANI FILHO, 2006, p.23).

De acordo com Bresciani Filho (2006, p.5), os sistemas estão inseridos em um meio-ambiente, de onde recebem objetos e os processam. No momento do processamento tais objetos são tratados em termos do referencial tempo, espaço e forma. Após esse processamento, os objetos transformados são exportados.

### **5.1.2 Processadores e suas subdivisões**

Em seu relatório de pesquisa, Bresciani Filho (2006) apresenta o conceito de processador elementar da seguinte forma:

O exercício de um processo implica a existência ao menos de um processador; o processador – formalização da noção de sistema geral - é uma caixa (máquina) preta, com constituição interna desconhecida, identificada apenas pelas relações entre as suas entradas e saídas, ou seja, pelo seu comportamento observado ou concebido (BRESCIANI FILHO, 2006, p.25).

Este conceito é estendido de modo que os processadores são considerados subsistemas, dos quais somente se conhecem as suas atividades, quando estão recebendo importação e promovendo ações do decorrer do tempo e realizando exportação. Durante a importação, as ações e a exportação existe um processo, representado por processador que envolve energia, matéria ou informação.

Em relação às características dos processadores, Bresciani Filho (2006, p.26) destaca a capacidade de armazenagem, transporte e produção; a

intensidade do nível de consumo próprio; a eficiência (rendimento na relação entrada – saída em um dado instante) e também a eficácia (relação do comportamento esperado – observado).

Bresciani Filho (2006) em seus estudos e trabalhos de orientação, escreve que a sistemografia é utilizada como instrumento de concepção e construção dos modelos de fenômenos ou projetos percebidos como sendo de natureza complexa. Desta maneira, utilizando a técnica de sistemografia é possível construir um modelo de um fenômeno percebido como complexo.

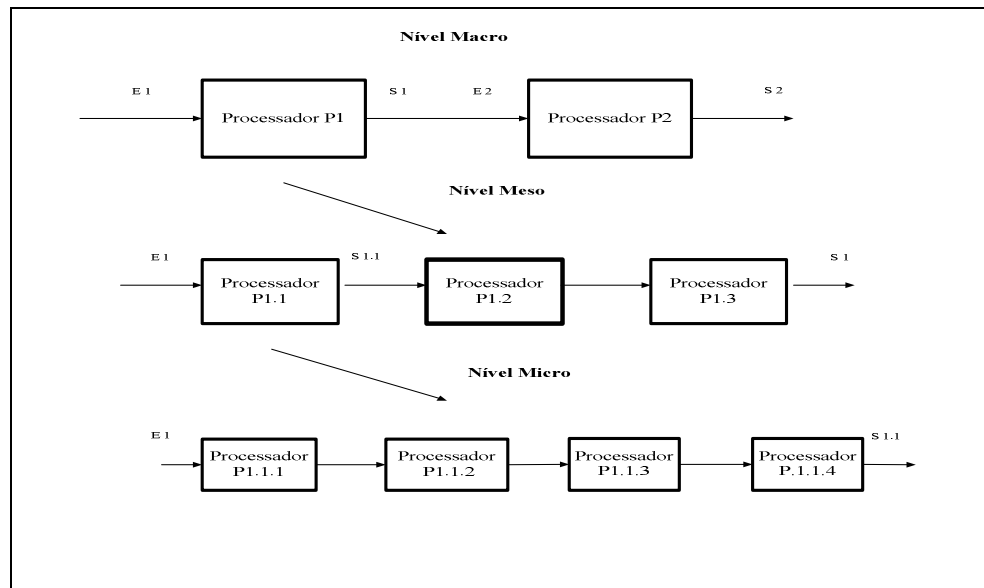
A partir desses estudos, Bresciani Filho (2006) apresenta as seguintes definições:

A sistemografia é a representação de um objeto, identificado por um modelador ou observador, por meio de um sistema, utilizando-se para tanto da teoria do sistema geral. Observadores diferentes e o mesmo observador podem construir sistemógrafos diferentes: a representação do objeto, que o observador constrói, é isomorfa do sistema geral e homomorfa do objeto. Cabe distinguir a família de objetos modificados (processados) da família dos objetos modificadores (processadores). Verifica-se também que os objetos processados podem ter a sua situação modificada, no decorrer do tempo, quanto ao espaço (deslocamento, transporte, transmissão) e à forma (deformação, transformação, produção).

Os conceitos de fluxo e campo podem ser introduzidos neste ponto: fluxo é um conceito associado a objetos em processamento (posteriormente considerados processados) e campo é um conceito associado a objetos exercendo influência no processamento (processadores) (BRESCIANI FILHO, 2006, p.25).

Os processadores são conectados entre si formando um arranjo estruturado denominado “rede de processadores”. Esta rede pode ser de dois tipos básicos: arranjo com conexões arborescentes e arranjo com conexões circulares. Além disso, a rede de conexão pode ser expandida dentro de cada processador tornando-o com características de um sistema.

A FIG. 14 mostra um esquema de processadores com suas entradas, saídas e seus níveis de desdobramento, partindo do nível macro, depois o nível “meso”, até seu nível “micro”.



**FIGURA 14** – Níveis de desdobramento dos processadores.

FONTE – Bresciani Filho (2006, p.25).

O nível Macro representa o processo em seu estado mais abrangente, pouco detalhado, apenas definido seu escopo e meio ambiente. O nível “meso”, mais detalhado, especifica os processadores, as classificações por categoria, por tipo de atividade e por nível de complexidade. No nível “micro” os processadores são detalhados em nível de especificidade da atividade e das classificações por categoria, por tipo e por nível.

### 5.1.3 Classificação dos processadores segundo a categoria

Por categoria, os processadores podem ser classificados em três subsistemas: operacional, informacional e decisional, que devem operar de modo integrado. A sistemografia permite a representação e a descrição dos sistemas Operacional, Informacional e Decisional, inicialmente de modo separado, e posteriormente de modo superposto, levando-se em consideração a complexidade do sistema. Desse modo, os processadores também incorporam as classificações como sendo operacionais, informacionais e decisoriais, e um mesmo processador pode pertencer a uma, a duas ou a três dessas categorias. (BRESCIANI FILHO, 2006, p.30).

#### **5.1.4 Classificação dos processadores segundo o tipo de atividade**

Os processadores são também classificados conforme seus tipos de atividades. Os tipos, relacionados com as atividades elementares, podem ser de forma, de espaço e de tempo. Em determinados casos, de dois ou mesmo, de três desses tipos elementares.

Processador do tipo 'forma' atua transformando o objeto a ser processado (energia, matéria ou informação); essa transformação pode se apresentar de modo concreto como uma efetiva mudança de forma física (de matéria e energia), ou abstrata como um cálculo matemático executado em uma informação apresentada de forma numérica ou algébrica.

Por sua vez, o processador do tipo 'espaço' atua de modo a promover o deslocamento no espaço do objeto a ser processado, e pode ser ilustrado como tendo a atribuição de transportar matéria, transmitir energia e realizar a comunicação de informação.

Por fim o processador do tipo 'tempo' é aquele no qual se considera o tempo como um fator de influência importante na transformação, no deslocamento, ou mesmo na permanência sem qualquer atividade do objeto. A rigor, qualquer atividade consome algum tempo, mas na modelagem trata-se de identificar se esse tempo é ou não relevante para a definição do tempo total de processamento (BRESCIANI FILHO, 2006, p.30).

#### **5.1.5 Classificação dos processadores segundo o nível de complexidade**

Os processadores também podem ser classificados em níveis diferentes conforme suas características de complexidade, de acordo com uma escala variando entre os valores de 1 a 9, onde cada nível superior engloba as características do nível inferior. O QUADRO 8, adaptado de Bresciani Filho (2006, p.32), descreve os nove níveis de complexidade dos processadores.

**QUADRO 8** – Classificação dos níveis de complexidade dos processadores.

<b>Nível</b>	<b>Processador</b>	<b>Descrição</b>
1º	<b>Passivo</b>	O processador é inerte e não exerce qualquer atividade pelo menos no momento em que a sistemografia do processo do sistema está sendo realizada;
2º	<b>Ativo</b>	Exerce uma atividade – processando matéria, energia ou informação. Realiza e exterioriza um comportamento de forma suficientemente estável ao longo do tempo mantendo sua identidade;
3º	<b>Regulado</b>	O processador exerce uma atividade de modo regular, envolvendo matéria e energia, sendo essa regularidade de comportamento obtida por meio de retroação (relação circular), que recicla parte da saída, como resultado da atividade, na entrada; essa retroação tem o objetivo de corrigir desvios de comportamento previstos, reduzindo ou anulando a sensibilidade a determinados eventos, que possam alterar o desempenho do processador;
4º	<b>Informado</b>	Exerce uma atividade de modo regular, envolvendo matéria e energia e também informação, sendo essa regularidade de comportamento obtida por meio de retroação (relação circular) de informação, que realimenta a informação da saída, como resultado da atividade, na entrada; essa retroação, informacional, tem o objetivo de corrigir desvios de comportamento previstos, reduzindo ou anulando a sensibilidade a determinados eventos, que possam alterar o desempenho do processador;
5º	<b>Com decisão</b>	O processador exerce uma atividade com capacidade de tomar decisão com base em uma informação que provoca uma ação, ou seja, um comportamento predefinido e conhecido. Nesse caso convém distinguir pelo menos dois tipos de processadores, que fazem parte do processador decisional e são interligados pelo menos com uma conexão circular (laço informacional): o processador decisional com informação de representação (informação que faz com que esse processador seja o detentor do projeto e da finalidade do sistema); e processador operacional que leva à ação de decisão;
6º	<b>Com Memória</b>	Exerce uma atividade tomando decisões que se apóiam em um processo de memorização; a representação do processador é feita com a inclusão, pelo menos de três outros processadores: decisional, informacional e operacional;
7º	<b>De Coordenação</b>	O processador de coordenação é um sistema amplo que se articula segundo três subsistemas integrados: decisional, informacional e operacional; o sistema interno de coordenação é de natureza hierarquizada no qual o processador decisional deve ter a capacidade de coordenação, isto é, capacidade de se relacionar e também com a capacidade de tratamento de informação e geração de conhecimento;
8º	<b>Com Criação</b>	O processador exerce uma atividade de criação de comportamento, de geração de informação simbólica, de aprendizagem, de inteligência, e de auto-organização;
9º	<b>Com Auto-Finalização</b>	O processado passa a ter no seu sistema de coordenação um subsistema de finalização, que lhe dá a capacidade de gerar os seus próprios objetivos e de ter ciência da sua existência e identidade; e, ainda, no seu sistema de coordenação engloba o sistema de diagnóstico, e no seu sistema de operação o sistema de manutenção;

FONTE – Adaptado de Bresciani Filho (2006, p.32).



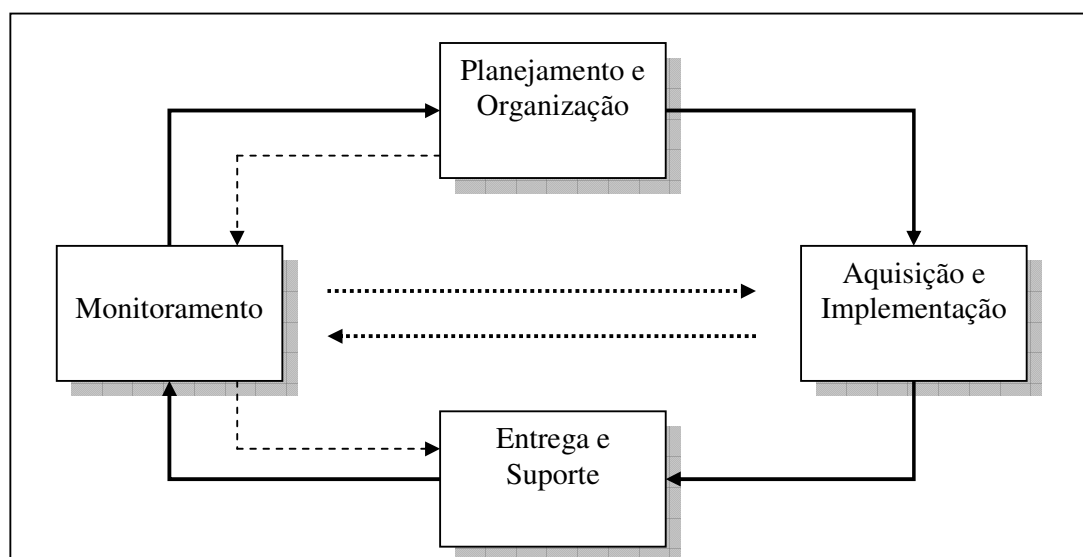
## 5.2 Sistemografia aplicada aos processos para governança de TI com ênfase à gestão dos dados e metadados

A partir da técnica de modelagem apresentada no item 5.1, ela deve ser aplicada de maneira a efetuar os processos de Governança de TI tratados no Capítulo 3 desta dissertação.

O modelo de gestão, baseado no cubo de Governança de TI proposto pelo COBIT, mapeia os processos a partir do nível “macro” passando pelo nível “meso” e chegando ao nível “micro”. Neste último, os processos são relacionados por suas atividades.

### 5.2.1 Processos COBIT representados em nível “macro”

No modelo baseado no cubo de Governança de TI os processos são agrupados em quatro domínios: “Planejamento e Organização”, “Aquisição e Implementação”, “Entrega e Suporte”, e “Monitoramento”. Tais domínios mostrados na FIG. 15 representam em termos do nível ‘macro’, os processadores com seus fluxos e interações.



**FIGURA 15** – Nível ‘macro’ da sistemografia para os quatro domínios COBIT.

FONTE – Adaptado de Brand e Boonen (2004, p.40).

A FIG. 15 mostra as linhas contínuas, representando o ciclo para o fluxo de atividades em macro processo, onde a entrada ou alimentação é resultado da ação de outra atividade, e as linhas pontilhadas, os ciclos das interações e controles desses macros processos.

## 5.2.2 Processos COBIT representados em nível “meso”

Os processadores que representam os processos COBIT atendendo às Seções 103, 302, 404 e 906 da Lei SOX são: PO1, PO2, PO8, PO9, AI6, DS1, DS2, DS4, DS6, DS11, M1, M2, M3 e M4 conforme especificado no item 4.6 desta dissertação. A representação em nível “meso” é feita por meio dos sistemógrafos, que são desdobrados em subsistemas: “O – Operacional”, “I – Informacional” e “D – Decisional”.

### 5.2.2.1 PO1 – Definir um plano estratégico de TI

O objetivo desse processador é ser responsável por definir um plano estratégico de longo prazo para realizar a gestão dos dados e metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Executar plano estratégico de longo prazo; 2 - Executar plano estratégico de curto prazo; 3 - Comunicar plano estratégico; 4 - Aperfeiçoar plano estratégico; 5 - Monitorar o processo. O QUADRO 9 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 9** – Análise para o processador PO1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>PO1</b>	<b>Definir um Plano Estratégico de TI</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>6o.</b>
PO1-1	Executar plano estratégico de "Longo prazo"	X	X				X	4o.
PO1-2	Executar plano estratégico de "Curto prazo"	X	X				X	4o.
PO1-3	Comunicar plano estratégico	X				X		2o.
PO1-4	Aperfeiçoar plano estratégico	X	X	X			X	5o.
PO1-5	Monitorar o processo	X	X	X	X	X	X	6o.

### 5.2.2.2 PO2 – Definir a arquitetura de informação

O objetivo deste processador é definir a arquitetura de informação para efetuar a gestão dos dados e dos metadados

Em nível “micro” o processador possui os seguintes processadores: 1 - Criar e regularmente atualizar um modelo de arquitetura de informação; 2 - Criar e regularmente atualizar o repositório de metadados; 3 - Definir as regras de acesso às classes de informação; 4 - Definir, implementar e manter as classes de segurança; 5 - Aprimorar o modelo de arquitetura de informação; 6 - Monitorar o processo. O QUADRO 10 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 10** – Análise para o processador PO2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>PO2</b>	<b>Definir Arquitetura de Informação</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>6o.</b>
PO2-1	Criar e regularmente atualizar um modelo de arquitetura de informação	X	X			X	X	4o.
PO2-2	Criar e regularmente atualizar o repositório de metadados	X	X			X	X	4o.
PO2-3	Definir as regras de acesso às classes de informação	X				X		4o.
PO2-4	Definir, implementar e manter os classes de segurança	X				X		4o.
PO2-5	Aprimorar o modelo de arquitetura de informação	X	X	X			X	5o.
PO2-6	Monitorar o processo	X	X	X	X	X	X	6o.

### 5.2.2.3 PO8 – Garantir a conformidade com os requisitos externos

O objeto desse processador é garantir conformidade com os requisitos externos em relação à gestão dos dados e metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Definir e manter o plano de requisitos; 2 - Comunicar o plano de conformidade; 3 - Definir e manter os procedimentos de conformidade e as regras; 4 - Comunicar os procedimentos de conformidade e as

regras; 5 - Aprimorar os itens de conformidade; 6 - Monitorar a conformidade. O QUADRO 11 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 11** – Análise para o processador PO8 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>PO8</b>	<b>Garantir a Conformidade com os Requisitos Externos</b>	<b>X</b>	<b>X</b>				<b>X</b>	<b>4o.</b>
PO8-1	Definir e manter o plano de requisitos	X					X	2o.
PO8-2	Comunicar o plano de conformidade	X					X	2o.
PO8-3	Definir e manter os procedimentos de conformidade e as regras	X					X	2o.
PO8-4	Comunicar os procedimentos de conformidade e as regras	X					X	2o.
PO8-5	Aprimorar os itens de conformidade	X	X				X	4o.
PO8-6	Monitorar a conformidade	X	X				X	4o.

#### 5.2.2.4 PO9 – Avaliar riscos

O objetivo desse processador é avaliar riscos referentes à gestão do dados e dos metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Definir e manter as políticas de risco; 2 - Comunicar as políticas de risco; 3 - Estabelecer um *framework* para risco; 4 - Estabelecer os itens de risco; 5 - Identificar os itens de risco; 6 - Medir os riscos; 6 - Classificar os tipos riscos; 7 - Gerenciar os riscos; 8 - Definir e implementar o plano de ação de riscos; 9 - Aprimorar política de riscos; 10 - Monitorar o processo. O QUADRO 12 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 12** – Análise para o processador PO9 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>PO9</b>	<b>Avaliar Riscos</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>6o.</b>
PO9-1	Definir e manter as políticas de risco	X				X		2o.
PO9-2	Comunicar as políticas de risco	X				X		2o.
PO9-3	Estabelecer um <i>framework</i> para risco	X				X		2o.
PO9-4	Estabelecer os itens de risco	X				X		2o.
PO9-5	Identificar os itens de risco	X				X		2o.
PO9-6	Medir os riscos	X				X		2o.
PO9-7	Classificar os tipos riscos	X	X			X	X	4o.
PO9-8	Gerenciar os riscos	X	X	X		X	X	5o.
PO9-9	Definir e implementar o plano de ação de riscos	X				X		2o.
PO9-10	Aprimorar política de riscos	X	X	X			X	5o.
PO9-11	Monitorar o processo	X	X	X	X	X	X	6o.

### 5.2.2.5 AI6 – Gerenciar mudanças

O objetivo desse processador é gerenciar mudanças relacionadas com a gestão dos dados e metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Definir as solicitações de mudança; 2 - Medir o impacto; 3 - Autorizar mudanças; 4 - Planejar e controlar mudanças; 5 - Selecionar recursos; 6 - Documentar os procedimentos de mudança; 7 - Aprimorar as mudanças; 8 - Monitorar o processo. O QUADRO 13 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 13** – Análise para o processador AI6 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>AI6</b>	<b>Gerenciar Mudanças</b>	<b>X</b>	<b>X</b>			<b>X</b>	<b>X</b>	<b>4o.</b>
AI6-1	Definir as solicitações de mudança	X				X		2o.
AI6-2	Medir o impacto	X				X		2o.
AI6-3	Autorizar mudanças	X				X		2o.
AI6-4	Planejar e controlar mudanças	X	X			X	X	4o.
AI6-5	Selecionar recursos	X					X	3o.
AI6-6	Documentar os procedimentos de mudança	X					X	3o.
AI6-7	Aprimorar as mudanças	X	X				X	4o.
AI6-8	Monitorar o processo	X	X				X	4o.

### 5.2.2.6 DS1 – Definir e gerenciar os níveis de serviço

O objetivo desse processador é definir e gerenciar níveis de serviço para a gestão dos dados e dos metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Identificar as solicitações dos níveis de serviço; 2 - Definir o *framework* para o nível de serviço; 3 - Definir o acordo de níveis de serviço; 4 - Gerenciar o nível de serviço; 5 - Monitorar o nível de serviço; 6 - Relatar o nível de serviço para os consumidores; 7 - Aprimorar o nível de serviço; 8 - Monitorar o processo. O QUADRO 14 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 14** – Análise para o processador DS1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>DS1</b>	<b>Definir e Gerenciar Níveis de Serviço</b>	<b>X</b>	<b>X</b>			<b>X</b>	<b>X</b>	<b>5o.</b>
DS1-1	Identificar as solicitações dos níveis de serviço	X				X		2o.
DS1-2	Definir o <i>framework</i> para o nível de serviço	X				X		2o.
DS1-3	Definir o acordo de níveis de serviço	X				X		2o.
DS1-4	Gerenciar o nível de serviço	X	X			X	X	5o.
DS1-5	Monitorar o nível de serviço	X	X			X	X	5o.
DS1-6	Relatar o nível de serviço para os consumidores	X					X	2o.
DS1-7	Aprimorar o nível de serviço	X	X				X	5o.
DS1-8	Monitorar o processo	X	X				X	5o.

### 5.2.2.7 DS2 – Gerenciar serviços de terceiros

O objetivo desse processador é administrar serviços de terceiros relacionados com a gestão dos dados e dos metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Identificar as solicitações de terceiros; 2 - Definir os contratos de serviços; 3 - Organizar as interfaces com os fornecedores; 4 - Gerenciar serviços e contrato de serviços terceirizados; 5 - Monitorar a

realização dos serviços terceirizados; 6 - Relatar os níveis de serviço; 7 - Aprimorar os serviços e contratos de serviços terceirizados; 8 - Monitorar o processo. O QUADRO 15 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 15** – Análise para o processador DS2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>DS2</b>	<b>Gerenciar Serviços de Terceiros</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>6o.</b>
DS2-1	Identificar as solicitações de terceiros	X				X		2o.
DS2-2	Definir os contratos de serviços	X			X	X		3o.
DS2-3	Organizar as interfaces com os fornecedores	X			X	X		3o.
DS2-4	Gerenciar serviços e contrato de serviços terceirizados	X	X	X	X	X	X	6o.
DS2-5	Monitorar a realização dos serviços terceirizados	X	X	X		X	X	5o.
DS2-6	Relatar os níveis de serviço	X				X		2o.
DS2-7	Aprimorar os serviços e contratos de serviços terceirizados	X	X	X	X		X	5o.
DS2-8	Monitorar o processo	X	X	X			X	5o.

#### 5.2.2.8 DS4 – Garantir serviço contínuo

O objetivo desse processador é garantir serviço contínuo da gestão dos dados e dos metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Definir os requisitos e estratégias de continuidade de TI; 2 - Afastar os riscos de interrupção dos serviços; 3 - Desenvolver e manter o plano de continuidade de TI; 4 - Testar e implementar o plano de continuidade de TI; 5 - Criar e manter os planos e procedimentos de recorrência; 6 - Treinar usuários e gerentes; 7 - Aprimorar a continuidade dos planos e procedimentos de continuidade; 8 - Monitorar o processo. O QUADRO 16 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 16** – Análise para o processador DS4 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>DS4</b>	<b>Garantir Serviço Contínuo</b>	<b>X</b>	<b>X</b>			<b>X</b>	<b>X</b>	<b>4o.</b>
DS4-1	Definir os requisitos e estratégias de continuidade de TI	X	X				X	3o.
DS4-2	Afastar os riscos de interrupção dos serviços	X					X	2o.
DS4-3	Desenvolver e manter o plano de continuidade de TI	X	X			X	X	4o.
DS4-4	Testar e implementar o plano de continuidade de TI	X				X		2o.
DS4-5	Criar e manter os planos e procedimentos de recorrência	X	X			X	X	4o.
DS4-6	Treinar usuários e gerentes	X				X		2o.
DS4-7	Aprimorar a continuidade dos planos e procedimentos de continuidade	X	X				X	4o.
DS4-8	Monitorar o processo	X	X				X	4o.

#### 5.2.2.9 DS6 – Identificar e alocar custos

O objetivo desse processador é identificar, alocar e controlar os custos relacionados com a gestão dos dados e metadados.

Em nível “micro” o processador possui os seguintes processadores: 1 - Definir e manter a estrutura de alocação de custos; 2 - Identificar itens de obrigação de custos; 3 - Definir os procedimentos de custos; 4 - Definir as tarifas de usuários; 5 - Relatar os desvios e estruturas de alocação de custos; 6 - Aprimorar a identificação e a estrutura de alocação de custos; 7 - Monitorar o processo. O QUADRO 17 mostra a análise para os processos de níveis “meso” e “micro”.



**QUADRO 17** – Análise para o processador DS6 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F1	
<b>DS6</b>	<b>Identificar e Alocar Custos</b>	<b>X</b>	<b>X</b>				<b>X</b>	<b>5o.</b>
DS6-1	Definir e manter a estrutura de alocação de custos	X	X				X	4o.
DS6-2	Identificar itens de obrigação de custos	X						2o.
DS6-3	Definir os procedimentos de custos	X	X				X	3o.
DS6-4	Definir as tarifas de usuários	X	X				X	3o.
DS6-5	Relatar os desvios e estruturas de alocação de custos	X						2o.
DS6-6	Aprimorar a identificação e a estrutura de alocação de custos	X	X				X	5o.
DS6-7	Monitorar o processo	X	X				X	5o.

#### 5.2.2.10 DS11 – Gerenciar dados e metadados

O objetivo desse processador é administrar os dados e os metadados mantendo-os completos, exatos e válidos durante sua entrada, atualização e armazenamento.

Em nível “micro” o processador possui os seguintes processadores: 1 - Desenvolver e manter estratégias e políticas de gestão de dados e metadados; 2 - Desenvolver e monitorar procedimentos de aquisição de dados e metadados; 3 - Definir e implementar o processamento e controle dos dados e metadados; 4 - Assegurar a integridade dos dados e metadados; 5 - Definir e implementar: cópia de segurança, de recorrência dos dados e metadados; 6 - Organizar a manipulação de dados e metadados de saídas; 7 - Aprimorar a gestão de dados e metadados; 8 - Monitorar o processo. O QUADRO 18 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 18** – Análise para o processador DS11 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>DS11</b>	<b>Gerenciar Dados e Metadados</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>6o.</b>
DS11-1	Desenvolver e manter estratégias e políticas de gestão de dados e metadados	X	X		X	X	X	5o.
DS11-2	Desenvolver e monitorar procedimentos de aquisição de dados e metadados	X	X		X	X	X	5o.
DS11-3	Definir e implementar o processamento e controle dos dados e metadados	X	X		X	X	X	5o.
DS11-4	Assegurar a integridade dos dados e metadados	X			X	X	X	4o.
DS11-5	Definir e implementar: cópia de segurança, de recorrência dos dados e metadados	X	X		X	X	X	5o.
DS11-6	Organizar a manipulação de dados e metadados de saídas	X	X		X	X	X	5o.
DS11-7	Aprimorar a gestão de dados e metadados	X	X	X	X	X	X	6o.
DS11-8	Monitorar o processo	X	X	X	X	X	X	6o.

#### 5.2.2.11 M1 – Monitorar os processos

O objetivo desse processador é monitorar os processos relacionados com a gestão dos dados e dos metadados.

Composto pelos seguintes processadores de nível “micro”: 1 - Definir, manter e comunicar as políticas de monitoramento; 2 - Definir, manter e comunicar os planos; 3 - Coletar o monitoramento de dados; 4 - Medir desempenho; 5 - Medir a satisfação do consumidor; 6 - Aprimorar o monitoramento; 7 - Monitorar o processo. O QUADRO 19 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 19** – Análise para o processador M1 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>M1</b>	<b>Monitorar os Processos</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>5o.</b>
M1-1	Definir, manter e comunicar as políticas de monitoramento	X	X	X	X		X	5o.
M1-2	Definir, manter e comunicar os planos	X	X	X	X		X	5o.
M1-3	Coletar o monitoramento de dados	X			X		X	2o.
M1-4	Medir desempenho	X	X		X		X	4o.
M1-5	Medir a satisfação do consumidor	X	X		X		X	4o.
M1-6	Aprimorar o monitoramento	X	X	X	X	X	X	5o.
M1-7	Monitorar o processo	X	X	X	X	X	X	5o.

### 5.2.2.12 M2 – Avaliar a adequação do controle interno

O objetivo desse processador é avaliar a adequação do controle interno para a gestão dos dados e dos metadados.

Composto pelos seguintes processadores de nível “micro”: 1 - Definir, manter e comunicar as políticas de controle interno; 2 - Definir, manter e comunicar os planos de controle interno; 3 - Definir procedimentos para controle interno; 4 - Monitorar os controles internos; 5 - Executar procedimentos de controle interno; 6 - Relatar nível de controle interno; 7 - Aprimorar controle interno adequados; 8 - Monitorar o processo. O QUADRO 20 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 20** – Análise para o processador M2 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>M2</b>	<b>Avaliar a Adequação do Controle Interno</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>5o.</b>
M2-1	Definir, manter e comunicar as políticas de controle interno	X	X	X	X		X	5o.
M2-2	Definir, manter e comunicar os planos de controle interno	X	X	X	X		X	5o.
M2-3	Definir procedimentos para controle interno	X	X	X	X		X	5o.
M2-4	Monitorar os controles internos	X	X	X	X		X	5o.
M2-5	Executar procedimentos de controle interno	X					X	2o.
M2-6	Relatar nível de controle interno	X					X	2o.
M2-7	Aprimorar controle interno adequados	X	X	X	X	X	X	5o.
M2-8	Monitorar o processo	X	X	X	X	X	X	5o.

### 5.2.2.13 M3 – Obter garantia independente

O objetivo desse processador é obter garantia de gestão independente dos dados e dos metadados.

Composto pelos seguintes processadores de nível “micro”: 1 - Definir, manter e comunicar as políticas de garantia; 2 - Definir, manter e

comunicar os planos de garantia; 3 - Contratar empresas de garantia independentes; 4 - Atribuir e certificar segurança e controle interno de serviços de TI e de terceirizados; 5 - Aprimorar eficiência de serviços de TI e de provedores terceirizados; 6 - Garantir compromisso com as leis e requisitos regulatórios; 7 - Garantir parcerias para a organização interna de TI com os provedores terceirizados; 8 - Aprimorar as garantias independentes; 9 - Monitorar o processo. O QUADRO 21 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 21** – Análise para o processador M3 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>M3</b>	<b>Obter Garantia Independente</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>5o.</b>
M3-1	Definir, manter e comunicar as políticas de garantia	X	X	X	X		X	5o.
M3-2	Definir, manter e comunicar os planos de garantia	X	X	X	X		X	5o.
M3-3	Contratar empresas de garantia independentes	X			X			2o.
M3-4	Atribuir e certificar segurança e controle interno de serviços de TI e de terceirizados	X			X		X	4o.
M3-5	Aprimorar eficiência de serviços de TI e de provedores terceirizados	X	X	X	X	X	X	5o.
M3-6	Garantir compromisso com as leis e requisitos regulatórios	X	X	X			X	4o.
M3-7	Garantir parcerias para a organização interna de TI com os provedores terceirizados	X	X		X		X	4o.
M3-8	Aprimorar as garantias independentes	X	X	X	X	X	X	5o.
M3-9	Monitorar o processo	X	X	X	X	X	X	5o.

#### 5.2.2.14 M4 – Proporcionar auditoria independente

O objetivo desse processador é prover auditoria independente em relação à gestão dos dados e dos metadados.

Composto pelos seguintes processadores de nível “micro”: 1 - Definir, manter e comunicar as políticas de auditoria; 2 - Definir, manter e comunicar os planos de auditoria; 3 - Elaborar a carta de tópicos da auditoria; 4 - Atualizar os planos de auditoria; 5 - Monitorar o trabalho de auditoria; 6 - Relatar os resultados e o acompanhamento da

auditoria; 7 - Aprimorar o trabalho de auditoria independente; 8 - Monitorar o processo. O QUADRO 22 mostra a análise para os processos de níveis “meso” e “micro”.

**QUADRO 22** – Análise para o processador M4 de níveis “meso” e “micro”, contendo categoria, tipo e nível de complexidade.

		Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>M4</b>	<b>Proporcionar Auditoria Independente</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>5o.</b>
M4-1	Definir, manter e comunicar as políticas de auditoria	X	X	X	X		X	5o.
M4-2	Definir, manter e comunicar os planos de auditoria	X	X	X	X		X	5o.
M4-3	Elaborar a carta de tópicos da auditoria	X	X				X	3o.
M4-4	Atualizar os planos de auditoria	X	X		X		X	3o.
M4-5	Monitorar o trabalho de auditoria	X	X	X	X		X	5o.
M4-6	Relatar os resultados e o acompanhamento da auditoria	X					X	2o.
M4-7	Aprimorar o trabalho de auditoria independente	X	X	X	X	X	X	5o.
M4-8	Monitorar o processo	X	X	X	X	X	X	5o.

### 5.2.3 Sistemógrafo dos processos COBIT representado em nível “meso”

Após as definições e especificações dos processadores nos níveis “meso” e “micro” é possível construir o sistemógrafo dos processos COBIT. Os desdobramentos são representados por meio dos subsistemas: “O – Operacional”, “I – Informacional” e “D – Decisinal”.

As entidades externas consideradas ao processo são “Atender aos Requisitos Externos” (RE) e “Atender aos Requisitos de Negócio” (RN). Os processadores responsáveis pelo monitoramento possuem interação direta com todo os demais processadores do sistemógrafo.

A FIG. 16 mostra o sistemógrafo em nível “meso” referente à categoria operacional para os processadores COBIT. Na parte central do sistemógrafo, delimitada pelo retângulo central em linha escura, estão os processadores contendo seus respectivos código e nome. Os processadores operacionais estão representados com as bordas pontilhadas e em tom de cinza (PO1, PO2, PO8,

PO9, AI6, DS1, DS2, DS4, DS6 e DS11). O sistemógrafo contém também as interações com as entidades externas (localizadas fora do retângulo central) e os processadores de monitoramento, representados com hachuras (M1, M2, M3 e M4). Os fluxos de entrada e saída contêm as interações entre processadores e as entidades externas.

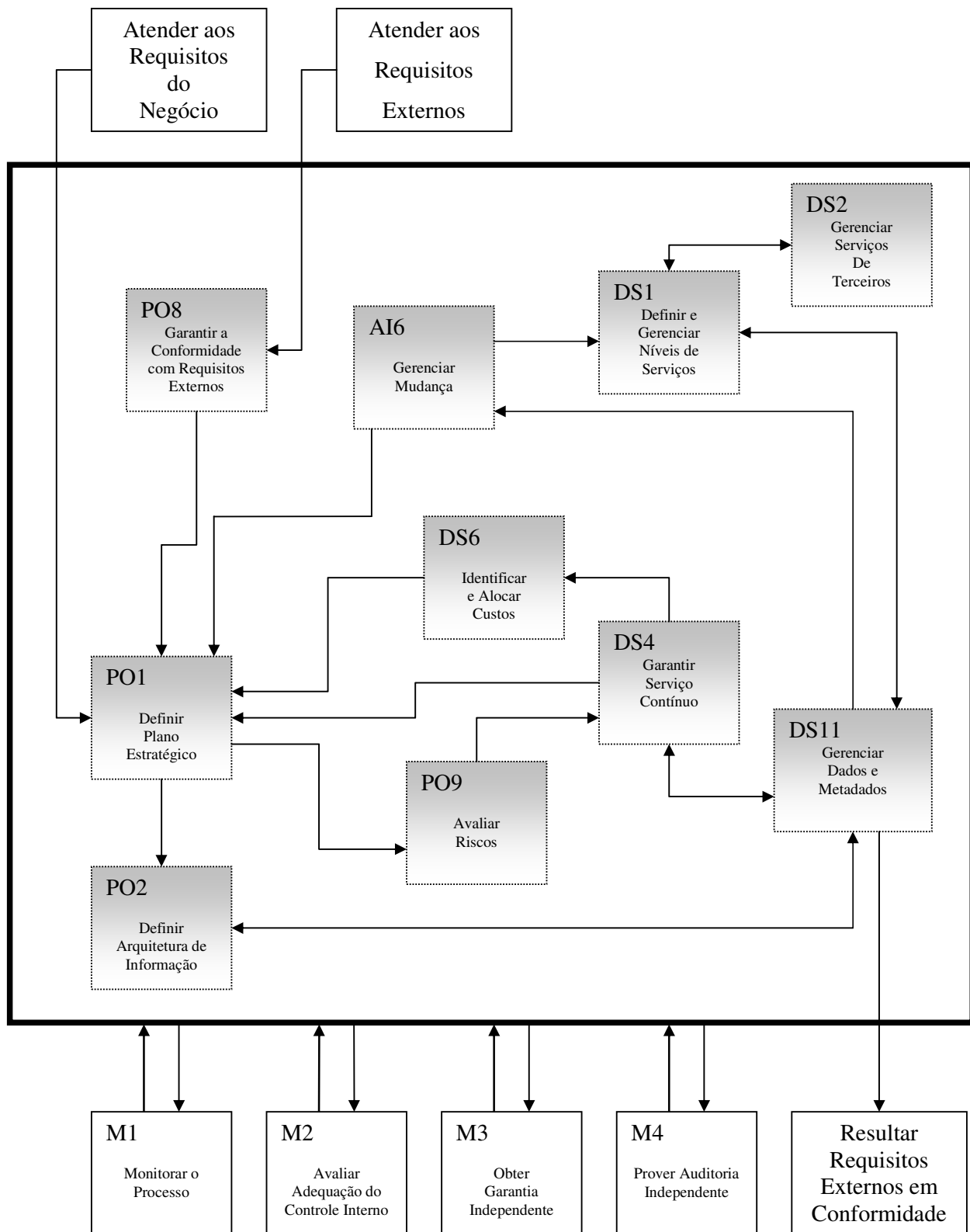


FIGURA 16 – Sistemógrafo operacional dos processos COBIT.

A FIG. 17 mostra o sistemógrafo em nível “meso” referente à categoria informacional para os processadores COBIT. Na parte central do sistemógrafo, delimitada pelo retângulo central em linha escura, estão os processadores contendo seus respectivos código e nome. Os processadores informacionais estão representados com as bordas em traço e dois pontos, e em tom de cinza (PO1, PO2, PO8, PO9, AI6, DS1, DS2, DS4, DS6 e DS11). O sistemógrafo contém também as interações com as entidades externas (localizadas fora do retângulo central) e os processadores de monitoramento, representados com hachuras (M1, M2, M3 e M4). Os fluxos de entrada e saída contêm as interações entre processadores e as entidades externas.



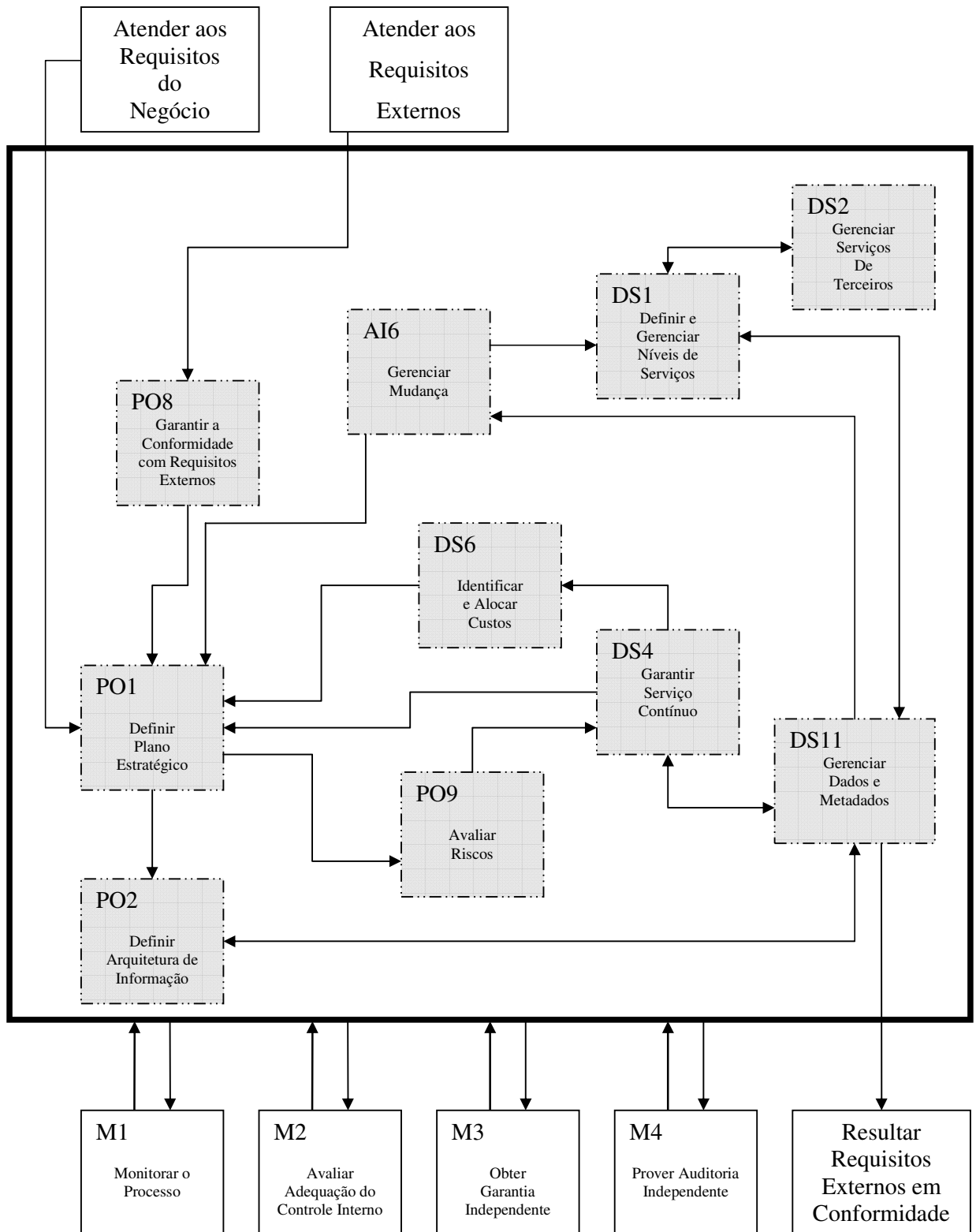


FIGURA 17 – Sistemógrafo informacional dos processos COBIT.

A FIG. 18 mostra o sistemógrafo em nível “meso” referente à categoria decisional para os processadores COBIT. Na parte central do sistemógrafo, delimitada pelo retângulo central em linha escura, estão os processadores contendo seus respectivos código e nome. Os processadores decisional estão representados com as bordas em traço e ponto, e em tom de cinza (PO1, PO2, PO9, DS2 e DS11). O sistemógrafo contém também as interações com as entidades externas (localizadas fora do retângulo central) e os processadores de monitoramento, representados com hachuras (M1, M2, M3 e M4). Os fluxos de entrada e saída contêm as interações entre processadores e as entidades externas.

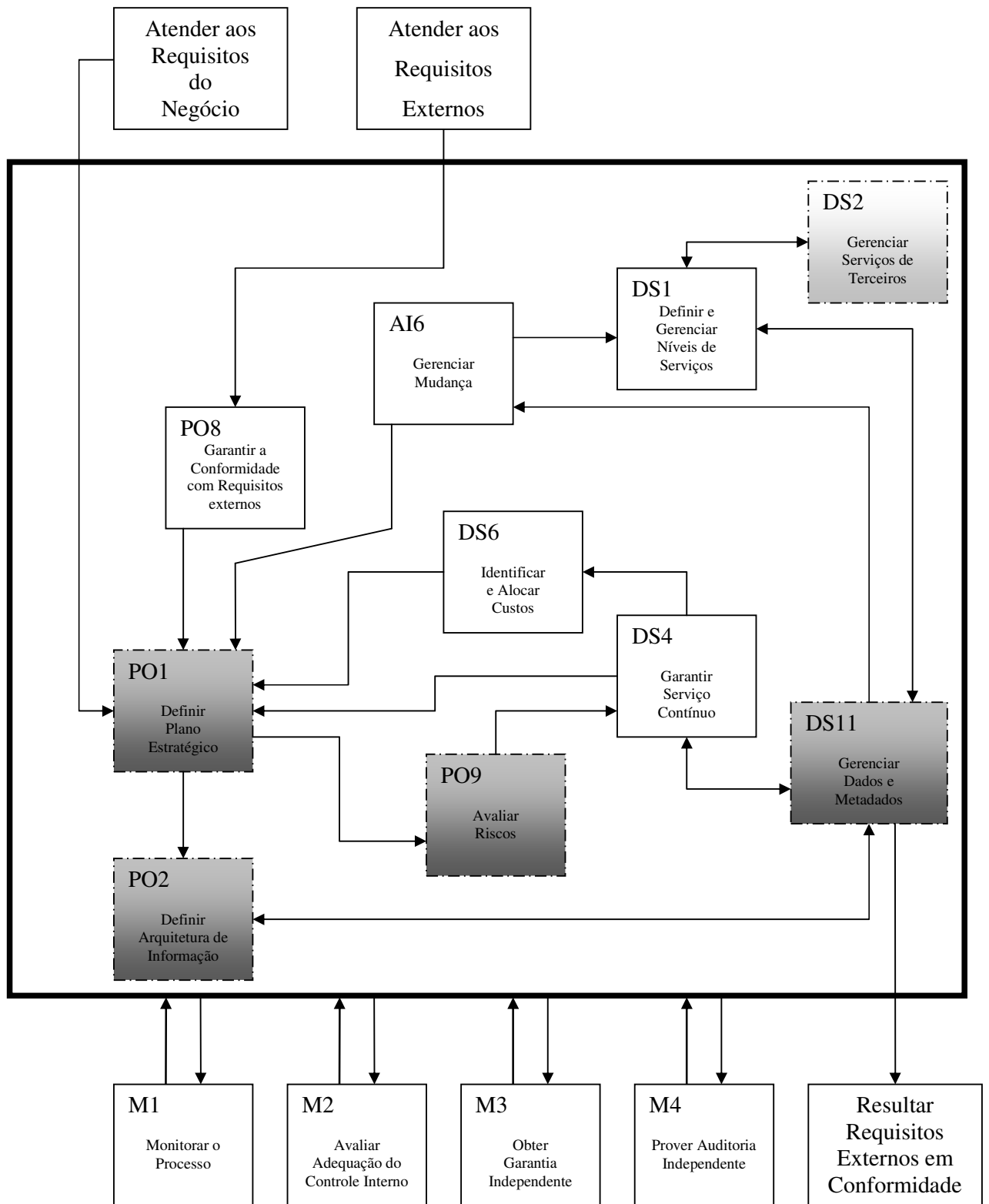


FIGURA 18 – Sistemógrafo decisional dos processos COBIT.

### 5.2.4 Conexão entre os processos COBIT representados em nível “meso”

O QUADRO 23 permite verificar as seguintes conexões: Saída da entidade externa “Atender aos Requisitos de Negócios” (RN), entrada em PO1, saída de “Atender aos Requisitos Externos” (RE) entrada em PO8. Saída de PO1, entrada em PO2 e PO9. Entrada e saída de PO2, entrada e saída em DS11. Saída de PO8, entrada em PO1. Saída de PO9, entrada em DS4. Saída de AI6, entrada em PO1 e DS1. Entrada e saída de DS1 e entrada e saída de DS2. Saída DS4 e entrada em PO1, DS6 e DS11. Saída DS6, entrada em PO1. Saída DS11, entrada em PO2, AI6, DS1, DS4 e entidade externa “Resultar Requisitos Externos em Conformidade”.

Os processadores de monitoramento M1, M2, M3 e M4 possuem entradas e saídas cíclicas, justamente como são os papéis pertinentes ao monitoramento e controle.

**QUADRO 23** – Conexões entre os processadores de entrada e de saída.

		Saída dos Processadores															
		RN	RE	PO1	PO2	PO8	PO9	AI6	DS1	DS2	DS4	DS6	DS11	M1	M2	M3	M4
Entrada	Atender aos Requisitos do Negócio - RN																
	Atender aos Requisitos Externos - RE											X					
	PO1	X				X		X			X	X		X	X	X	X
	PO2			X									X	X	X	X	X
	PO8		X											X	X	X	X
	PO9			X										X	X	X	X
	AI6												X	X	X	X	X
	DS1							X		X			X	X	X	X	X
	DS2								X					X	X	X	X
	DS4						X						X	X	X	X	X
	DS6										X			X	X	X	X
	DS11				X				X		X			X	X	X	X
	Processadores	M1			X	X	X	X	X	X	X	X	X				
		M2			X	X	X	X	X	X	X	X	X				
M3				X	X	X	X	X	X	X	X	X					
M4				X	X	X	X	X	X	X	X	X					

### 5.2.5 Análise dos resultados

Por meio dos QUADROS 23 e 24 é possível realizar a análise do processo de implantação dos objetivos de controle para gestão de dados e metadados, baseado no COBIT, para atender a Lei SOX em suas Seções, que tratam da Governança Corporativa e da Governança de TI.

**QUADRO 24** – Matriz de Relação dos processadores em nível “meso”, contendo categoria, tipo e nível de complexidade.

	PROCESSADORES	Categoria			Tipo			Nível
		O	I	D	E	T	F	
<b>PO1</b>	Definir um Plano Estratégico de TI	X	X	X	X	X	X	6o.
<b>PO2</b>	Definir Arquitetura de Informação	X	X	X	X	X	X	6o.
<b>PO8</b>	Garantir a Conformidade com os Requisitos Externos	X	X				X	4o.
<b>PO9</b>	Avaliar Riscos	X	X	X	X	X	X	6o.
<b>AI6</b>	Gerenciar Mudanças	X	X			X	X	5o.
<b>DS1</b>	Definir e Gerenciar Níveis de Serviço	X	X	X		X	X	5o.
<b>DS2</b>	Gerenciar Serviços de Terceiros	X	X	X	X	X	X	6o.
<b>DS4</b>	Garantir Serviço Contínuo	X	X				X	4o.
<b>DS6</b>	Identificar e Alocar Custos	X	X	X			X	5o.
<b>DS11</b>	Gerenciar Dados e Metadados	X	X	X	X	X	X	6o.
<b>M1</b>	Monitorar os Processos	X	X	X	X	X	X	5o.
<b>M2</b>	Avaliar a Adequação do Controle Interno	X	X	X	X	X	X	5o.
<b>M3</b>	Obter Garantia Independente	X	X	X	X	X	X	5o.
<b>M4</b>	Prover Auditoria Independente	X	X	X	X	X	X	5o.

Observando o QUADRO 24, que contém os processadores, suas categorias, seus tipos e níveis de complexidade, percebe-se, que aqueles processadores com maior nível (6º nível), possuem as atividades mais complexas. Os processadores que fazem parte desse caso são: PO1, PO2, PO9, DS2 e DS11. Neles estão concentrados as atividades com poder de decisão e controle dos dados aderentes com as Seções 103, 302, 404 e 906 da Lei SOX. Estes processadores se apóiam em um processo de memorização e decisão os quais utilizam conexões circulares.

Especificamente, os processadores PO1, PO2 e DS11 são, nesse contexto, aqueles responsáveis diretamente pelo planejamento, implantação e atendimento às políticas e à gestão dos dados e dos metadados da organização.

Como o modelo COBIT utiliza quatro processos de monitoramento permanentes, representados aqui no modelo sistemografado por meio dos processadores M1, M2, M3 e M4, garante assim, o controle da qualidade total dos processadores, fechando o ciclo conhecido como PDCA (*Plan, Do, Check, Act*) proposto por Deming (DEMING, 1990).

O método de sistemografia ao consolidar os conceitos e aplicações do modelo COBIT e da Lei SOX em processos de gestão de dados e metadados para área de Tecnologia da Informação permitiu validar, que a representação e análise de processadores complexos foi executada com racionalidade e agilidade.

## 6. PROPOSTA DE *FRAMEWORK* E *DASHBOARD* PARA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

---

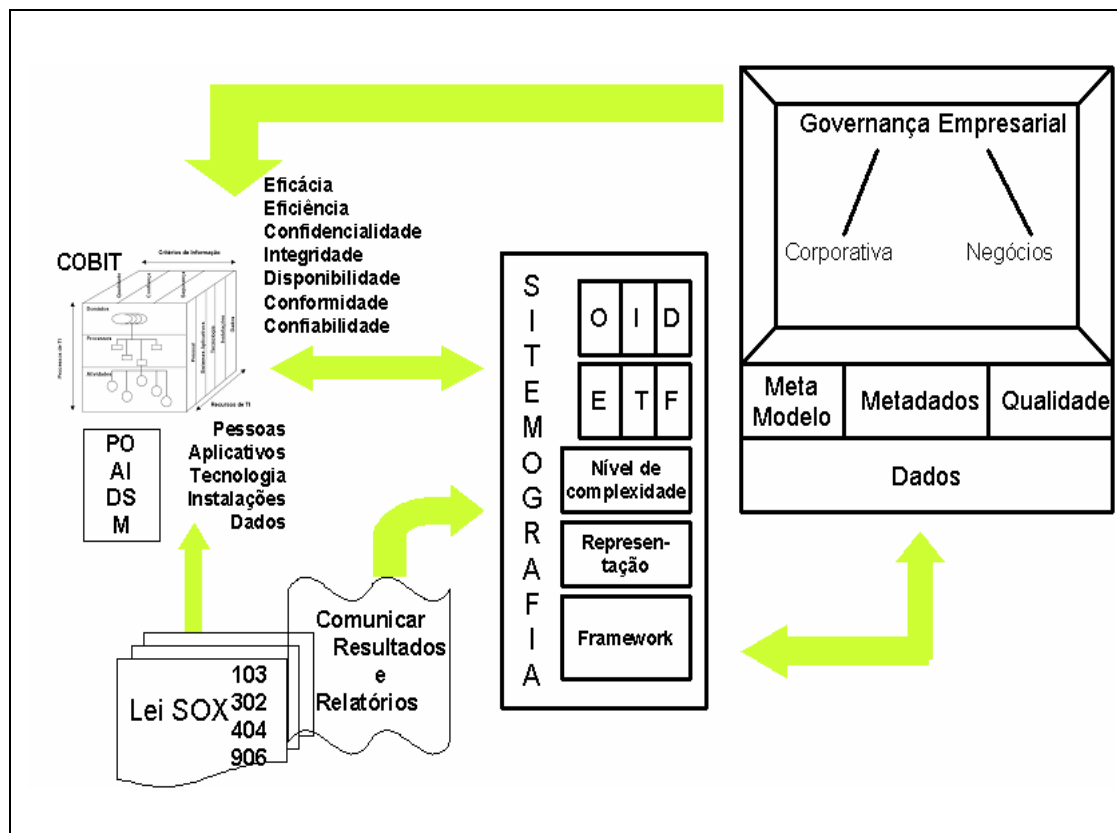
---

Conforme apresentado em capítulos anteriores, o contexto da Governança Empresarial é formado pelas governanças Corporativa e de Negócios. Na obra de Weill e Ross (2006) é mencionado que para se obter plena Governança Empresarial é fundamental que as organizações também possuam a Governança de TI, pois esta fortalece e controla ao mesmo tempo a estrutura empresarial. Conforme Fernandes e Abreu (2006), os fatores que motivam tal Governança são o Ambiente de Negócios, os Marcos Reguladores, a Segurança da Informação, a Dependência do Negócio em relação à TI e a Integração Tecnológica.

Devido ao fato da Governança de TI estar fortemente centrada em dados e tecnologia, ela possui importantes elementos definidos a partir de um metamodelo de qualidade de dados. Além da definição do metamodelo é também necessária a representação de processos, utilizando uma metodologia consistente com mecanismos de controle, como por exemplo, o COBIT, que garantam o alinhamento estratégico e atendam aos agentes externos, como as solicitações à Lei *Sarbanes-Oxley* (LIU, 2006).

### 6.1 Contexto para se implementar a governança de TI

Fundamentando-se na matriz de Zachman (original apresentado no ANEXO A), (ZACHMAN, 1987; SOWA; ZACHMAN, 1992; ZIFA.COM, 2005), a partir da dimensão “Dados” e das perspectivas: “Escopo”, “Modelos de Negócio (visão conceitual)” e “Modelo de Sistemas (visão lógica)”, foi possível elaborar uma estrutura que representasse e integrasse os elementos responsáveis pela governança, assim como atendesse às imposições da Lei SOX. A FIG. 19 representa a estrutura para a governança integrada. Nela, estão identificados os principais aspectos da Governança Empresarial, do COBIT, da Sistemografia e da Lei SOX, além das interações e dos fluxos.



**FIGURA 19** – Estrutura para representação da governança integrada.

De acordo com Bresciani Filho (2006), a representação dos processos por meio da sistemografia é uma forma clara e objetiva, para tratar tipos de processos com alto grau de complexidade.

Encontram-se no Capítulo 5 desta dissertação, representados por meio das FIG. 16, FIG. 17 e FIG. 18, os três sistemógrafos detalhados “O – Operacional”, “I – Informacional” e “D – Decisional”. Em tais representações, os processadores que atendem aos processos propostos pelo COBIT estão em conformidade com as Seções da Lei SOX (103, 302, 404 e 906). Nestas figuras também estão os requisitos Externos (RE) e os requisitos de Negócio (RN) atendidos.

A representação dos processos, fluxos e processadores estão especificados por meio do método da sistemografia, conforme apresentado no Capítulo 5 desta dissertação. De acordo com este capítulo, os sistemógrafos possuem as Categorias dos Sistemas: “Operacional”, “Informacional” e



“Decisional”, acrescidos do Tipo de Atividade: “Espaço”, “Tempo” e “Forma”, e do Nível de Complexidade (escala variando de 1 a 9, onde 1 significa o nível inferior e 9 o nível superior). A matriz de relação entre os processadores (QUADRO 24) representou as conexões entre os processadores de entrada e saída.

## **6.2 Proposta de um *framework* para gerir a governança de TI**

De modo a integrar todo o ambiente empresarial em torno de uma arquitetura controlada e documentada, propõe-se um *framework*, que relacione as especificações do modelo COBIT descritos anteriormente no Capítulo 3 com as Seções 103, 302, 404 e 906 da Lei SOX descritas no Capítulo 4.

O *framework* contém o Nome do Processador, os Objetivos de Controle, as Entradas e Saídas, os Critérios de Informação, os Recursos de TI contendo Tipo do Impacto, os Recursos de TI, as Categorias do Sistema, os Tipos de Atividade, o Nível de Complexidade, o Indicador de Desempenho (KPI) e o Documento Gerado, este, materializado por meio de produtos entregáveis como documentos, procedimentos e relatórios.

Por fim, outro elemento importante é o Grau de Maturidade ao qual cada processador está sujeito. Este grau de maturidade, que atende ao *Capability Maturity Model Integration* (CMMI), deve contemplar o modelo e suas métricas, conforme especificado anteriormente no item 3.5.6.

### **6.2.1 *Framework* proposto para controle e acompanhamento do processo**

O QUADRO 25 mostra a estrutura proposta para o *framework*, que deve ser aplicado em cada processador como forma de controle e execução do processo. Nas células do *framework* estão entre parênteses os números índices dos campos para preenchimento. No QUADRO 26 encontra-se descrito como os conteúdos dos campos devem ser preenchidos, de acordo com cada processo que está sendo tratado.

**QUADRO 25** – Framework proposto para os itens relacionados ao processador em análise

<b>Código e Nome do Processador:</b> (1)		<b>Sistemografia/COBIT aplicados ao escopo dos processos</b> (2)	
<b>Objetivos de Controle</b>	(3)	(4)	
<b>Entrada</b>	(5)	(6)	
<b>Saída</b>	(7)	(8)	
<b>Crítérios de Informação</b>	<b>Eficácia</b>	< tipo de impacto: “P” ou “S” > (9)	
	<b>Eficiência</b>	< tipo de impacto: “P” ou “S” > (10)	
	<b>Confidencialidade</b>	< tipo de impacto: “P” ou “S” > (11)	
	<b>Integridade</b>	< tipo de impacto: “P” ou “S” > (12)	
	<b>Disponibilidade</b>	< tipo de impacto: “P” ou “S” > (13)	
	<b>Conformidade</b>	< tipo de impacto: “P” ou “S” > (14)	
	<b>Confiabilidade</b>	< tipo de impacto: “P” ou “S” > (15)	
<b>Recursos de TI</b>	<b>Pessoas</b>	(16)	
	<b>Sistemas de aplicação</b>	(17)	
	<b>Infra-estrutura de tecnologia</b>	(18)	
	<b>Instalações</b>	(19)	
	<b>Dados</b>	(20)	
<b>Categorias do sistema</b>	<b>Operacional</b>	(21)	
	<b>Informacional</b>	(22)	
	<b>Decisional</b>	(23)	
<b>Tipos de atividade</b>	<b>Espaço</b>	(24)	
	<b>Tempo</b>	(25)	
	<b>Forma</b>	(26)	
<b>Nível de Complexidade</b>	<b>Nível de complexidade</b> (1º até 9º) (27)	(28)	
<b>Indicador de Desempenho – KPI</b>	(29)	(30)	
<b>Documento gerado</b>	<b>Produtos entregáveis</b>	(31)	
<b>Nível de maturidade</b>	<b>Nível levantado para o processo conforme o modelo de maturidade</b>	<b>Atual</b>	<b>Estratégico</b>
		(32)	(33)

**QUADRO 26** – Instruções para preenchimento do *framework* proposto para o acompanhamento e controle do processo.

<b>Código e Nome do Processador (1)</b>	Contém o código e nome de um dos tipos do processador está sendo tratado: PO1, PO2, PO8, PO9, AI6, DS1, DS2, DS4, DS6, DS11, M1, M2, M3, M4
<b>Sistemografia/COBIT aplicados ao escopo</b>	A coluna contém a descrição da ação ou do tipo de responsabilidade da ação referente às linhas.( 2 )
<b>Objetivos de Controle</b>	Contém o(s) item(ns) e o(s) nome(s) do(s) objetivo(s) do(s) controle(s) ( 3 ) e sua(s) respectivas descrição(ões) ( 4 )
<b>Entrada</b>	Contém o(s) código(s) do(s) processo(s) da entrada conforme o código de processador ( 5 ) e o respectivo nome do processador ( 6 ).
<b>Saída</b>	Contém o(s) código(s) do(s) processo(s) da saída conforme o código de processador ( 7 ) e o nome do processador ( 8 ).
<b>Crítérios de Informação</b>	<p><b>Eficácia &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação é relevante e se está sendo entregue de modo oportuno, correto, consistente ao processo de negócio.Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 9 )</p> <p><b>Eficiência &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação é produtiva ao processo de negócio. Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 10 )</p> <p><b>Confidencialidade &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação está segura para o processo de negócio. Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 11 )</p> <p><b>Integridade &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação é exata e válida ao processo de negócio. Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 12 )</p> <p><b>Disponibilidade &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação está sendo disponibilizada quando requerida ao processo de negócio Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 13 )</p> <p><b>Conformidade &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a informação está em conformidade com leis e regulamentos ao processo de negócio. Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 14 )</p> <p><b>Confiabilidade &lt; tipo do impacto (P ou S)&gt;</b> - quando presente, indica se a provisão de informação é apropriada ao processo de negócio. Qual o tipo de impacto causado, se P = Primário ou S = Secundário. ( 15 )</p>
<b>Recursos de TI</b>	Se um ou mais dos recursos a seguir existirem, e forem aplicáveis ao processo de negócio: Pessoas, Sistemas de Aplicação, Infra-estrutura de tecnologia, Instalações, Dados. ( 16 ), ( 17 ), ( 18 ), (19) e ( 20 )
<b>Categorias do sistema</b>	Descreve processador conforme cada uma de suas categorias: Operacional, Informacional e Decisional. ( 21 ), ( 22 ) e ( 23 )
<b>Tipos de atividade</b>	Descreve o processador em termos das atividades elementares e individuais de tipo: Forma, Espaço e Tempo. ( 24 ), ( 25 ) e ( 26 )
<b>Nível de complexidade</b>	Indica o nível de complexidade para o processador de acordo com a escala 1 a 9. ( 27 ) Descreve o nível de complexidade do processador, conforme apresentado no QUADRO 8. ( 28 )
<b>Indicador de desempenho - KPI</b>	Estabelece o indicador que permite monitorar o desempenho do processador. ( 29 ) Descreve a ação de monitoramento de desempenho do processador. ( 30 )
<b>Documento gerado</b>	Descreve qual ou quais os produtos devem ser entregues pelo processador. ( 31 )
<b>Nível de maturidade</b>	Indica de acordo com a escala proposta pelo CMMI [0 a 5] qual devem ser os níveis: Atual e Estratégico, para o processador. Atual – indica o nível atual levantado para o processo. ( 32 ) Estratégico – indica qual deverá ser o nível pretendido para ser alcançado naquele processo. ( 33 )

### 6.2.2 *Dashboard* proposto para avaliação das lacunas

O termo *dashboard* refere-se a um painel de controle exibindo indicadores. Neste caso, o que se propõe é a criação de um painel de controle utilizando uma planilha de cálculo, por meio da qual seja possível inserir os dados relacionados aos processadores, e gerar a análise de lacuna (*gap*<sup>5</sup>), baseada no modelo de maturidade (CMMI).

A FIG. 20 apresenta a estrutura para o *dashboard*, o qual deve ser usado como forma de controle e execução do processo. Maiores detalhes e especificações de programação encontram-se no ANEXO B.

A partir do momento em que os dados estejam preenchidos nos campos (32) e (33) do *framework*, referentes a cada processador em análise, eles devem ser inseridos no *dashboard*, em seus respectivos campos de nível de maturidade “Atual” e “Estratégico”.

A “Escala do Processo” exibe de maneira gráfica, conforme os símbolos na legenda, a posição em escala para os níveis de maturidade “Atual” e “Estratégico”.

O cálculo do desvio é resultante da razão entre o valor informado para o nível de maturidade “Atual” e o correspondente valor informado para o nível de maturidade “Estratégico”. O resultado deste cálculo aparece de modo instantâneo na coluna “Desvio”, indicado em formato percentual, qual a defasagem entre tais níveis de maturidade “Atual” e “Estratégico”.

---

<sup>5</sup> Gap: lacuna ou diferença (MICHAELIS, 1989, p. 136)

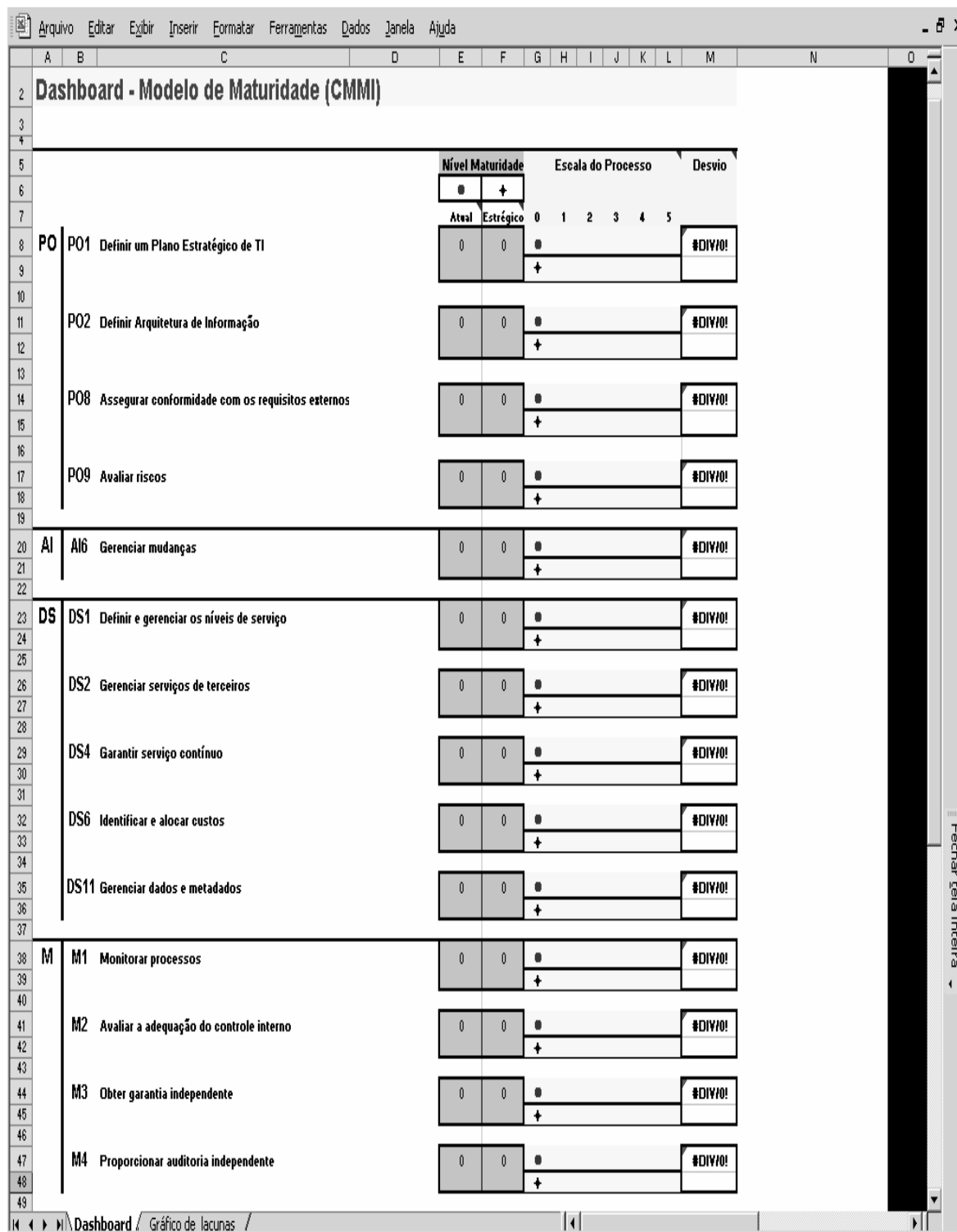
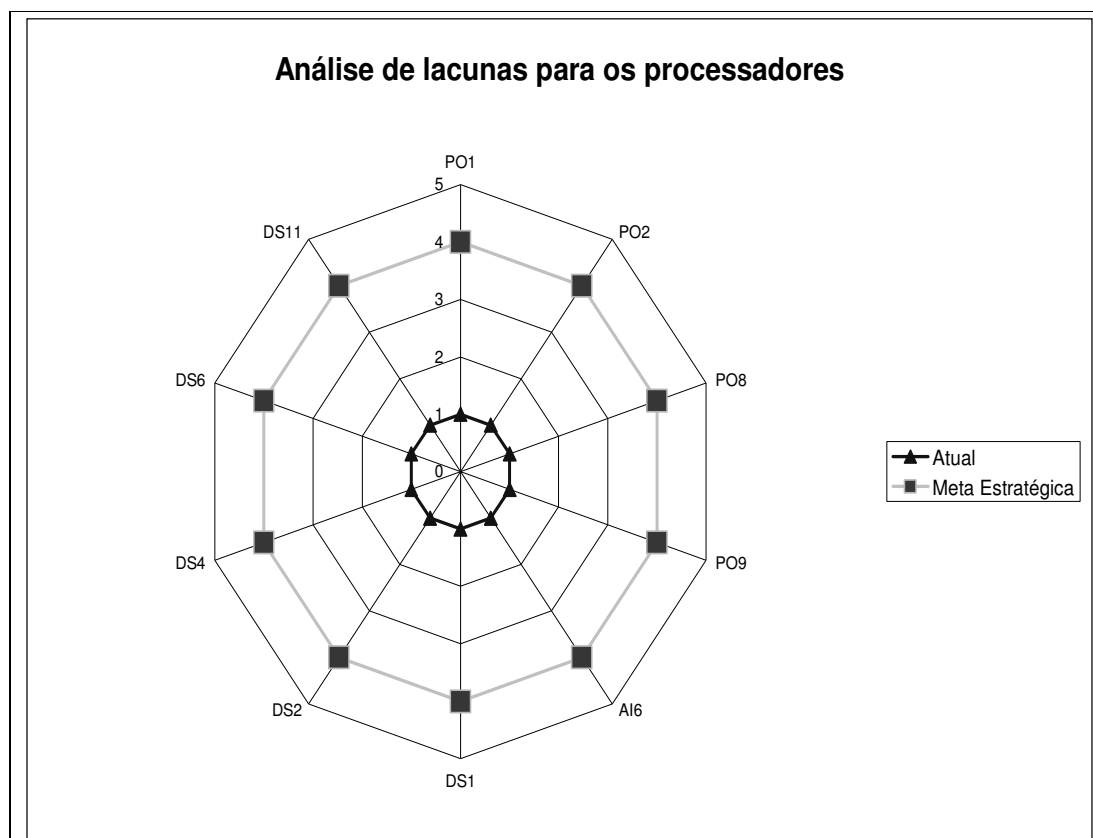


FIGURA 20 – Dashboard para controle do processo, baseado no modelo de maturidade CMMI.

### 6.2.3 Gráfico de radar proposto para avaliação das lacunas

A partir dos dados inseridos no *dashboard*, automaticamente é gerado em uma outra planilha, denominada “Gráfico de lacunas”, contendo o gráfico em forma de radar. Neste gráfico é possível fazer o acompanhamento dos níveis de maturidade dos processos em relação à situação “Atual” e àquela “Estratégica”, para a qual se deseja alcançar.

A FIG. 21 apresenta um exemplo ilustrativo do gráfico de radar, que simula a maturidade para todos os processos. Os níveis de maturidade são “Atual” igual a “1” e “Estratégica” igual a “4”.



**FIGURA 21** – Ilustração do Gráfico de Radar para análise de lacunas dos processadores.

## **6.3 Procedimentos para a análise dos resultados**

### **6.3.1 Análise pelos processos sistemografados**

A partir dos três sistemógrafos elaborados é possível analisar os processadores: “Operacional”, “Informacional” e “Decisional”, os fluxos de entradas, saídas com seus sentidos e também as entidades externas.

Por meio da sistemografia, também se analisam os processadores em relação aos seus tipos: “Espaço”, “Tempo” e “Forma”, e em relação ao respectivo “Nível de complexidade”.

### **6.3.2 Análise pelo modelo de maturidade**

Em relação ao modelo de maturidade, é possível analisar o nível de maturidade em que se encontram os processos e seus processadores. Ao se gerar um gráfico de radar automaticamente a partir dos dados inseridos no *dashboard* é efetuada a análise de lacunas. Esta análise facilita a visualização da situação atual, assim como o planejamento estratégico, para alcançar os objetivos de médio e longo prazo.

### **6.3.3 Análise pelos objetivos de controle**

O COBIT tem sido aplicado como o modelo “de fato” para a Governança de TI. Nesta linha, os “Objetivos de Controle”, os “Critérios de Informação” e os “Recursos de TI” ao serem utilizados conjuntamente, asseguram que os relatórios financeiros necessários ao atendimento das Seções 103, 302, 404 e 906 da Lei SOX são atendidos. Com os campos preenchidos no *framework* proposto são possíveis a análise, o acompanhamento e o controle dos processos de forma estruturada e documentada.

Em relação a esta dissertação, as especificações de controle foram para os diversos aspectos da qualidade e da administração de dados, assim

como dos processos relacionados, como forma de manter a governança e a conformidade com a Lei SOX de responsabilidades e transparência dos relatórios financeiros.

## 6.4 Etapas e procedimentos para a aplicação da gestão dos dados e dos metadados

O QUADRO 27 contempla todas as etapas e procedimentos relacionados com a implementação da gestão dos dados e metadados. É importante ressaltar, que algumas das etapas podem ser suprimidas de acordo com o escopo da empresa onde se deseja implementar o modelo de gestão.

**QUADRO 27** – Etapas para implementar a gestão de dados e metadados.

<b>Etapa</b>	<b>Ações a serem executadas</b>	<b>Referência às seções da dissertação</b>
<b>1 – Escopo da governança</b>	<b>Definir qual é o escopo da Governança de TI que trata a gestão dos dados e dos metadados</b>	<b>Seção 2.3</b>
<b>2 – Representação por meio da matriz de Zachman</b>	<b>Os modelos de dados e metadados devem seguir a coluna da matriz de Zachman (ZIFA.COM, 2005) para a Dimensão “Dados” e as Prespectivas: Escopo: elenco dos elementos importantes ao negócio em forma de entidades ou classes de objetos, os quais representam o negócio Modelo de Negócio: representa o modelo semântico em forma de entidades (entidades de negócio) e relacionamentos (relacionamentos de negócio) Modelo de Sistema: (Modelo Lógico de Dados), em forma de entidade dados e entidade relacionamento</b>	<b>Seção 2.4</b>
<b>3 – Escolha do repositório de metadados</b>	<b>Escolher o modelo que atenda à arquitetura dos metadados de acordo com os componentes representados na FIG. 3</b>	<b>Seção 2.8.2</b>
<b>4 – Metamodelo</b>	<b>Desenvolver o metamodelo apresentado na FIG. 5, conforme os elementos da FIG. 4</b>	<b>Seção 2.8.3</b>
<b>5 – Grupo de foco</b>	<b>Definir o grupo de foco com ações, papéis e responsabilidades</b>	<b>Seção 3.3</b>



<b>6 – Aplicação das Seções da Lei SOX com COBIT</b>	<b>Definir todos os itens para serem aplicados à Lei SOX em suas Seções 103, 302, 404 e 906, utilizando os controles definidos pelo COBIT para os processos PO1, PO2, PO8, PO9, AI6, DS1, DS2, DS4, DS6, DS11, M1, M2, M3, e M4</b>	<b>Seção 4.6</b>
<b>7 – Sistemografia para representação dos modelos</b>	<b>Representar os modelos sistemografados: “Operacional”, “Informacional” e “Decisional”, conforme as figuras: FIG. 16; FIG. 17; FIG. 18</b>	<b>Seção 5.2.3</b>
<b>8 – Conexão entres os processadores</b>	<b>Executar a matriz de conexões entre os processadores de entrada e saída</b>	<b>Seção 5.2.4</b>
<b>9 – <i>Framework</i> do processo</b>	<b>Preencher o <i>framework</i> do processo (QUADRO 25) para cada um dos processadores, de acordo com os dados coletados nas Etapas 6, 7 e 8, e explicados no QUADRO 26</b>	<b>Seção 6.3.1</b>
<b>10 – <i>Dashboard</i> do processo</b>	<b>Preencher o <i>dashboard</i> do processo relacionado ao nível de maturidade em que se encontra o processo na atualidade e o nível que se deseja alcançar, ou estratégico</b>	<b>Seção 6.3.2</b>
<b>11 – Gráfico do modelo</b>	<b>Gerar automaticamente o gráfico de radar a partir dos dados preenchidos no <i>dashboard</i> do processo, descritos na Etapa 10 deste quadro (QUADRO 27).</b>	<b>Seção 6.3.3</b>
<b>12 – Análise dados</b>	<b>Analisar os dados obtidos nas Etapas 6, 7, 8, 9, 10 e 11</b>	<b>Seção 5.3.5 e Seção 6.4</b>
<b>13 – Relatório final</b>	<b>Elaborar um relatório a partir de todos os dados obtidos nas etapas deste processo</b>	

FONTE – Adaptado de Lahti e Peterson (2005), Brand e Boonen (2004) e Fernandes e Abreu (2006).

## 7. CONCLUSÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

---

---

### 7.1 Objetivo geral atingido

A presente dissertação teve como objetivo desenvolver um processo de Governança de TI para a gestão de dados e metadados, atendendo às determinações da Lei *Sarbanes-Oxley* – SOX, em suas Seções específicas (103, 302, 404 e 906), que cuidam dos controles e responsabilidades na emissão dos relatórios financeiros.

Por meio da sistemografia foi possível representar, estudar e analisar os processadores complexos buscando a racionalidade, agilidade e funcionalidade desses sistemas (BRESCIANI FILHO, 2006, p.1).

O uso da sistemografia permitiu identificar o grau de relacionamento, os níveis de complexidade e o tipo do processador, quer seja esse de tempo, de espaço ou de forma. Permitiu ainda identificar a presença desnecessária e a ausência de presença necessária de processadores e de conexões entre processadores, bem como a coerência das relações estabelecidas, possibilitando a apresentação de proposta de modificação, que possa levar à racionalização, flexibilização e agilização do sistema.

A sistemografia também representou os diferentes pontos de vista em relação às componentes do fluxo do processo. Isto se deve ao fato de que ela permite a representação do sistema e a sua descrição pelas dimensões “Operacional”, “Informacional” e “Decisional”, inicialmente separadas e posteriormente de modo superposto.

A praticidade e flexibilidade da sistemografia permitiram adaptar o modelo proposto pelo COBIT aos seus processadores e estruturas funcionais e assim desenvolver a proposta para um *framework* e para um *dashboard*.

## 7.2 Objetivos específicos atingidos

Em relação aos objetivos específicos, estes foram detalhados, e amplamente explicados, assim como os elementos, que compõem a governança e a arquitetura empresarial, sempre com foco nos dados e nos metadados (descrição sobre os dados).

A escolha do modelo COBIT como um padrão “de facto”, ocorreu em função de que este possui um tratamento completo para atuar em processos de tecnologia, e também por sua simplicidade na especificação de processos complexos. De acordo com Lahti e Peterson (2005, p.34) o COBIT é o modelo escolhido pela maioria dos auditores, para especificar e acompanhar os controles de Governança de TI.

Ao se descreverem as etapas e os procedimentos para a aplicação da gestão dos dados e dos metadados, descritos no QUADRO 27, espera-se contribuir de forma objetiva para a execução do ciclo de Governança de TI, com foco nos processos de gestão de dados e de metadados. O ciclo de Governança de TI é empregado aos diversos tipos de empresas, que necessitem de controle, e pretendam atingir a conformidade com a Lei SOX, ou atender aos Marcos de Regulação, à Inovação de Negócios, à Segurança da Informação, e também à Integração Tecnológica em processos de negócio.

## 7.3 Áreas de aplicação

Foi possível observar que os conceitos propostos nesta dissertação podem ser utilizados nos vários segmentos de negócio que tenham sua estratégia na dependência de TI, para obterem o melhor desempenho. Alguns destes segmentos são a empresas de telecomunicações, tanto em seu nível de gestão e planejamento de rede, quanto de operações de infra-estrutura; empresas industriais; empresas comerciais; empresas prestadoras de serviços; empresas de produção de *software* (fábrica de *software*), empresas provedoras de Internet e entidades de governamentais.

Isto ocorre em função de todos estes segmentos estarem baseados em tecnologia e precisarem atentar para pontos como, a necessidade de governança, tanto em nível corporativo, quanto de tecnologia da informação; a necessidade de terem uma arquitetura de informação bem definida, a necessidade de possuírem controles sobre as bases de dados, com garantia de qualidade e segurança e a necessidade de definição consistente de dados. Além disto, necessitam de mecanismos para controles permanentes, que garantam todos os aspectos tratados ao longo desta pesquisa.

#### **7.4 Recomendações para trabalhos futuros**

Para trabalhos futuros recomenda-se que os processos tratados e sistemografados nesta dissertação sejam aprimorados por meio de automação, e possam assim, serem gerados com orquestração de fluxos (tipo *workflow*) e depois tratados pelas tecnologias de gerenciamento de processos, *Business Process Management* (BPM). Proposta de um modelo de referência pode ser encontrada em Delphi Group (2003), para um modelo matemático baseado na teoria dos grafos pode ser consultado Bresciani Filho (2006).

## REFERÊNCIAS

---

---

AGOSTA, L. **Trends 2005: information quality**, Nov. 10, 2004. Disponível em: <<http://www.forrester.com>>. Acesso em: 10 fev. 2006.

BLECHAR, M. **What is metadata and why should you care?** Apr. 22, 2003a. Disponível em: <<http://www.gartner.com>>. Acesso em: 10 jul. 2005.

BLECHAR, M. **Metadata repository selection: balancing scope and focus**, Jul. 29, 2003b. Disponível em: <<http://www.gartner.com>>. Acesso em: 10 jul. 2005.

BOVESPA: bolsa de valores de São Paulo. Disponível em: <<http://www.bovespa.com.br/principal>>. Acesso em: 30 ago. 2006.

BRAND, K; BOONEN, H. **IT Governance: a pocket guide based on COBIT**, Netherlands: Van Haren, 2004. 151p.

BRESCIANI FILHO, E. **Modelagem de processos com aplicação de sistemografia**, 2006. (Mimeo).

CIMAGLOBAL.COM. **Enterprise governance: a CIMA discussion paper (CIMA)**. Disponível em: <[www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC564-DA3B89A6/live/entgov\\_DiscussionPaper\\_2004.pdf](http://www.cimaglobal.com/cps/rde/xbcr/SID-0AAAC564-DA3B89A6/live/entgov_DiscussionPaper_2004.pdf)> Acesso em: 30 ago. 2005.

CAMPBELL, P. L. **Sandia report: a COBIT primer**, Jun. 2005. Disponível em: <[www.itgi.org/TemplateRedirect.cfm?Template=/ContentManagement/ContentDisplay.cfm&ContentID=22339](http://www.itgi.org/TemplateRedirect.cfm?Template=/ContentManagement/ContentDisplay.cfm&ContentID=22339)>. Acesso em: 15 jul. 2005.

COBIT. **Executive summary**. 3. ed. ISACAF, Jul. 2000a.

COBIT. **Framework**. 3.ed. ISACAF, Jul. 2000b.

COBIT. **Control objectives**. 3.ed.ISACAF, Jul. 2000c.

COBIT. **Management guidelines**. 3.ed. ISACAF, Jul. 2000d.

COBIT. **Audit guidelines**. 3 ed. ISACAF, Jul. 2000e.

COSIF. Disponível em: <<http://www.cosif.com.br/publica.asp?arquivo=20040122fraudecontabil>>. Acesso em: 18 ago. 2005.

CRAIG, S. **IT Governance and the balanced scorecard**, Aug. 20, 2004. Disponível em: <<http://www.forrester.com>>. Acesso em: 10 jul. 2005.

DELLOITTE. **Lei Sarbanes-Oxley: guia para melhorar a governança corporativa por meio de controles internos**. Disponível em: <[http://www.deloitte.com/dtt/cda/doc/content/guia\\_sarbanes\\_oxley%281%29.pdf](http://www.deloitte.com/dtt/cda/doc/content/guia_sarbanes_oxley%281%29.pdf)>. Acesso em: 18 ago. 2005.

DELPHI GROUP. **BPM2003: market milestone report (White paper)**. Disponível em: <[http://www.bpminstitute.org/uploads/media/Delphi\\_Group\\_BPM\\_2003\\_Market\\_Milestone\\_Whitepaper.pdf](http://www.bpminstitute.org/uploads/media/Delphi_Group_BPM_2003_Market_Milestone_Whitepaper.pdf)>. Acesso em: 5 maio 2005.

DEMING, W. E. **Qualidade: a revolução da administração**. Rio de Janeiro: Marques Saraiva, 1990. 367p.

DUPRÉ, T. R. L. **Relatório de pesquisa COBIT: framework**. 3.ed; 2001.(Mimeo)

DWBRASIL. Disponível em: <[http://www.dwbrasil.com.br/html/artbi\\_20030602.html](http://www.dwbrasil.com.br/html/artbi_20030602.html)>. Acesso em: 1 set. 2005.

ELMASRI, R; NAVATHE, S. B. **Sistemas de banco de dados, fundamentos e aplicações**. Rio de Janeiro: LTC, 2002.

FERNANDES A. A; ABREU V. F. **Implantando a governança de TI**. Rio de Janeiro: Brasport, 2006. 338p.

HEFFNER, R. **The pillars of enterprise architecture terminology**, Nov. 11, 2002. Disponível em: <<http://www.forrester.com>>. Acesso em: 15 jul. 2005

HEUSER, C. A. **Projeto de banco de dados**. Porto Alegre: Sagra Luzzatto, 2001.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). Disponível em: <<http://www.isaca.org>>. Acesso em: 30 ago. 2005.

INMON, W. H. **Building the data warehousing**. New York: John Wiley and Sons, 2002. 356p.

KINTSCHNER, F. E. **Método de modelagem de processos para apoio ao desenvolvimento de software**. 2003. 161f. Tese (Doutorado em Engenharia Mecânica) – Faculdade de Engenharia Mecânica, Universidade Estadual de Campinas, Campinas.

LAHTI, C; PETERSON, R. **Sarbanes-Oxley IT compliance using COBIT and open source tools**. New York: Syngress, 2005. 450p.

LIU, L. **Sistemas de gestão de TI: framework COBIT**. São Paulo: IBC, 2006. 200p.

MAGEE, F. **IT architecture is a process, not a document**. Dec. 8, 1997, Disponível em: <<http://www.gartner.com>>. Acesso em: 15 jul. 2005.

MARCO, D. **Bulding and managing the meta data repository: a full lifecycle guide**. New York: Wiley, 2000. 416p.

MARCO, D; JENNINGS, M. **Universal meta data models**. New York: Wiley, 2004. 478p.

MAXIMIANO, A. C. A. **Teoria geral da administração**. São Paulo: Atlas, 2000. 530p.

MICHAELIS: pequeno dicionário inglês-português / português-inglês. São Paulo: Melhoramentos, 1989.

NYSE GROUP. Disponível em: <<http://www.nyse.com/about/listed/>> . Acesso em: 30 ago. 2006.

ROSSATO, I. F. **Uma metodologia para a análise de problemas**. Universidade Federal de Santa Catarina, 1996, (Dissertação). Disponível em: <<http://www.eps.ufsc.br/disserta96/rossato/cap2/capitulo2.htm>>. Acesso em: 16 de mar. 2007.

SARBANES-OXLEY ACT OF 2002. Disponível em: <<http://www.sec.gov/about/laws.shtml#sox2002>>. Acesso em: 18 ago. 2005.

SCHULTE, R; THOMPSON, J; RICHEL, B. **Best practices: managing application integration metadata**, March 1, 2002. Disponível em: <<http://www.gartner.com>>. Acesso em: 10 jul. 2005.

SLACK, N. et. al. **Administração da produção**. São Paulo: Atlas, 2002. 747p.

SOARES NETO, V. **Telecomunicações convergência de redes e serviços**. São Paulo: Érica, 2003. 254p.

SOWA, J. F; ZACHMAN, J. A. **Extend and formalizing the framework for information system architecture**. IBM, 1992. (White paper). Disponível em: <<http://www.research.ibm.com/journal/sj/313/sowa.pdf>>. Acesso em: 22 set. 2005.

SM Tracker and Associates. **Lean Manufacturing**. Disponível em: <[http://www.smthacker.co.uk/lean\\_manufacturing.htm](http://www.smthacker.co.uk/lean_manufacturing.htm)>. Acesso em: 15 mar. 2007.

TANNENBAUM, A. **Metadata solutions**. New York: Addison-Wesley, 2002. 528p.

ZACHMAN, J. A. **A framework for information systems architecture**. IBM, 1987. (White paper). Disponível em: <<http://www.research.ibm.com/journal/sj/263/ibmsj2603E.pdf>>. Acesso em: 22 set. 2005.

ZIFA.COM. Disponível em: <<http://by119fd.bay119.hotmail.msn.com/cgi-bin/premail/8895>>. Acesso em: 18 ago. 2005.

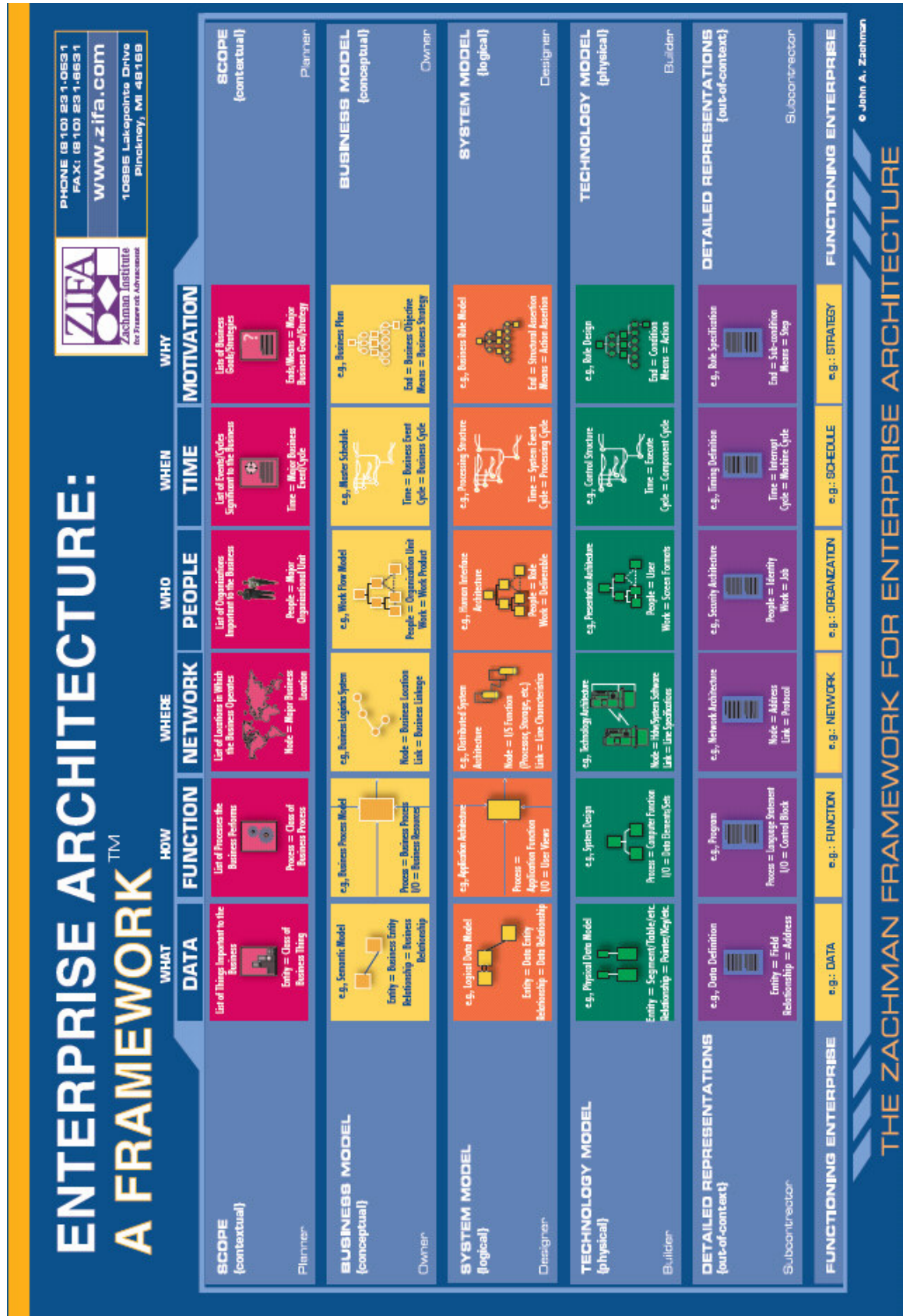
WHATIS.TECHTARGET.COM. Disponível em: <[http://whatis.techtarget.com/definition/0,,sid9\\_gci214182,00.html](http://whatis.techtarget.com/definition/0,,sid9_gci214182,00.html)>. Acesso em: 30 abr. 2007.

WEILL, P; ROSS, J. W. **Governança de tecnologia da informação**. São Paulo: M.Books, 2006. 274 p.

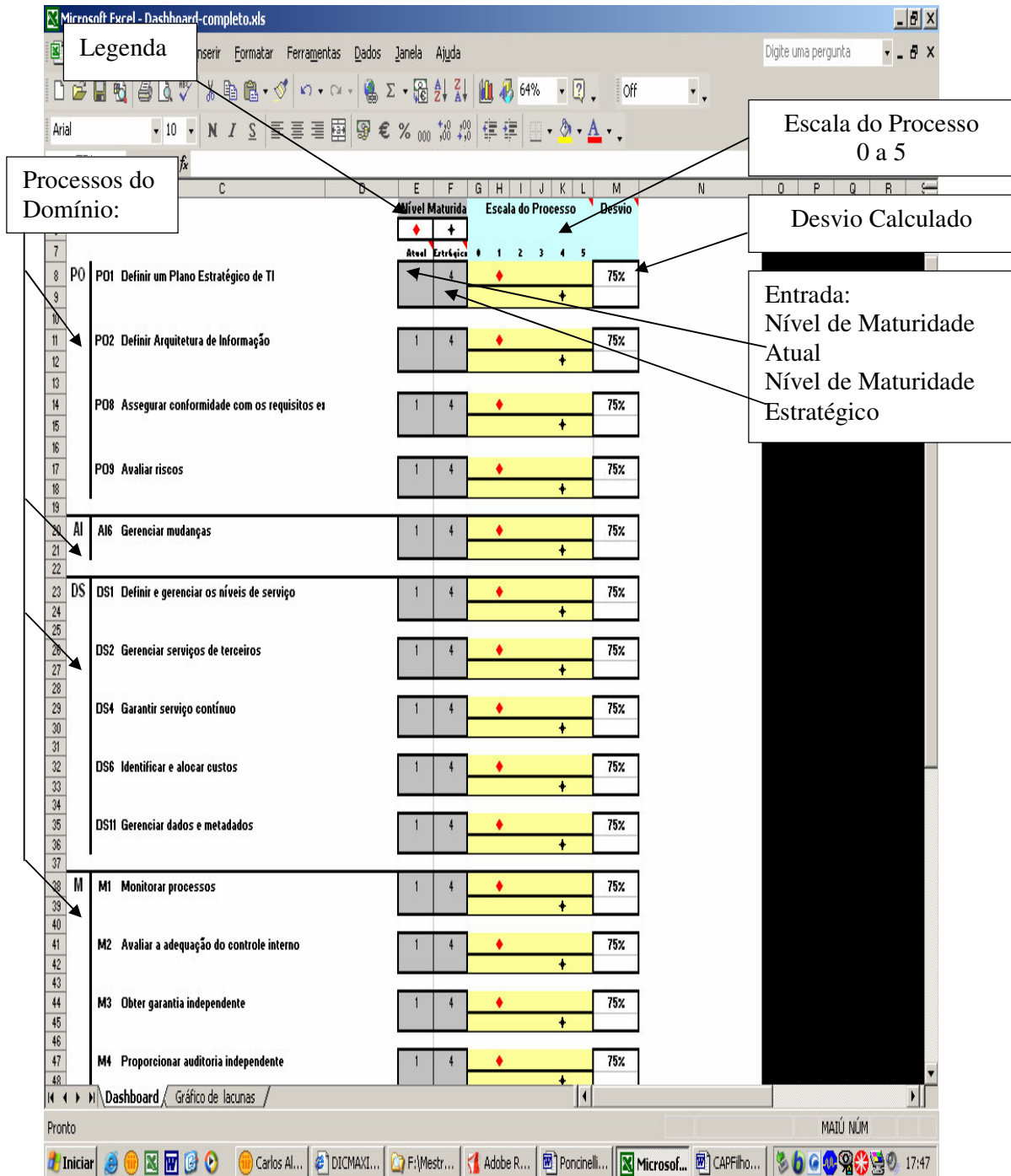
## **ANEXOS**

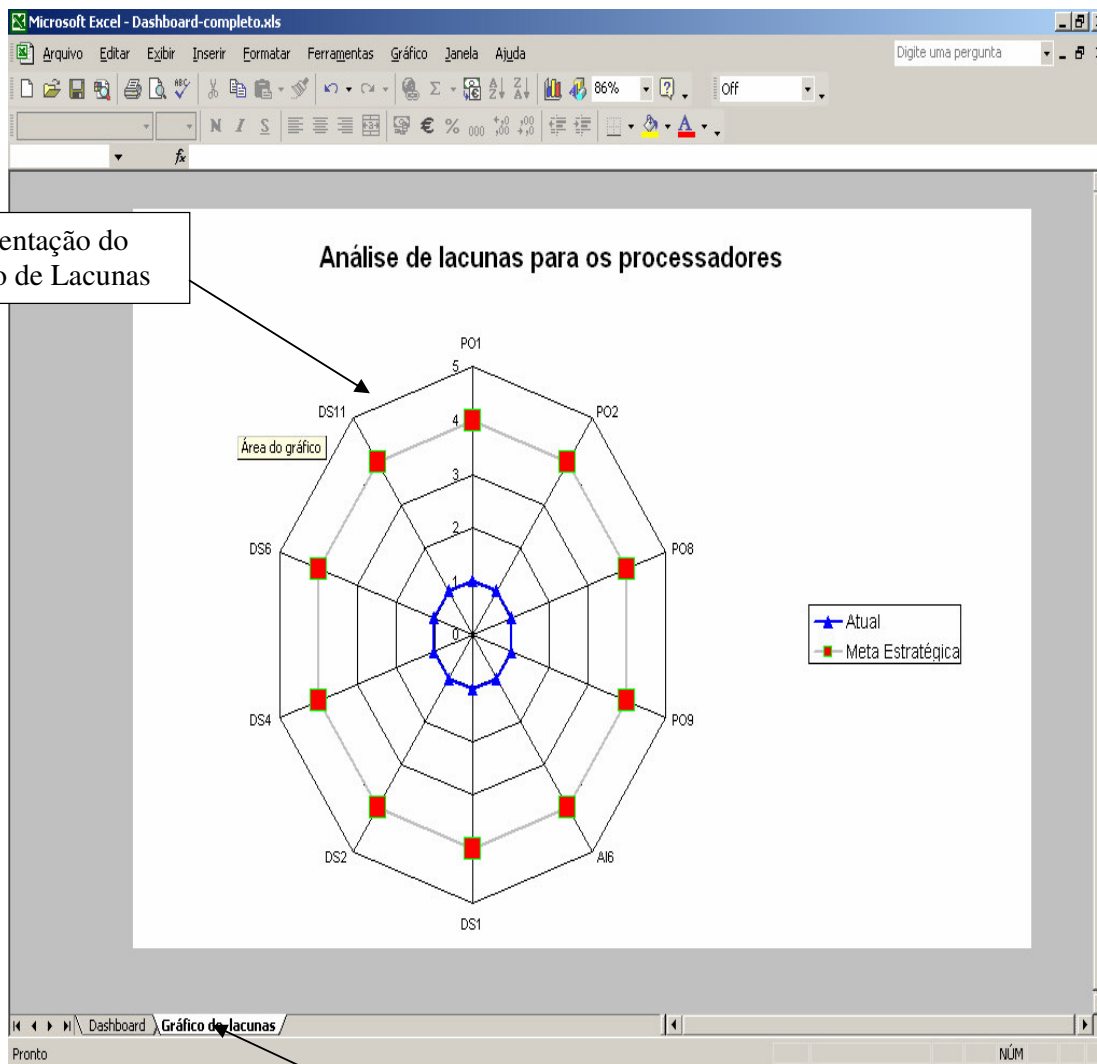


ANEXO A – FRAMEWORK DE ZACHMAN



ANEXO B – PROPOSTA PARA AVALIAR O MODELO DE MATURIDADE (CMMI) UTILIZANDO O SOFTWARE MS-EXCEL DE ACORDO COM O FRAMEWORK COBIT





Indicação do Gráfico

## Linhas de código:

Escala do processo PO1	
Atual:	=SE(\$E\$8<0,5;"@";" =SE(\$E\$8>=0,5;SE(\$E\$8<1,5;"@";" =SE(\$E\$8>=1,5;SE(\$E\$8<2,5;"@";" =SE(\$E\$8>=2,5;SE(\$E\$8<3,5;"@";" =SE(\$E\$8>=3,5;SE(\$E\$8<4,5;"@";" =SE(\$E\$8>=4,5;SE(\$E\$8<5,5;"@";" 
Estratégico:	=SE(\$F\$8<0,5;"@";" =SE(\$F\$8>=0,5;SE(\$F\$8<1,5;"@";" =SE(\$F\$8>=1,5;SE(\$F\$8<2,5;"@";" =SE(\$F\$8>=2,5;SE(\$F\$8<3,5;"@";" =SE(\$F\$8>=3,5;SE(\$F\$8<4,5;"@";" =SE(\$F\$8>=4,5;SE(\$F\$8<5,5;"@";" 
Cálculo do Desvio:	=SE(D8<>"";"ERRO";1-E8/F8)
Escala do processo PO2	
Atual:	=SE(\$E\$11<0,5;"@";" =SE(\$E\$11>=0,5;SE(\$E\$11<1,5;"@";" =SE(\$E\$11>=1,5;SE(\$E\$11<2,5;"@";" =SE(\$E\$11>=2,5;SE(\$E\$11<3,5;"@";" =SE(\$E\$11>=3,5;SE(\$E\$11<4,5;"@";" =SE(\$E\$11>=4,5;SE(\$E\$11<5,5;"@";" 
Estratégico:	=SE(\$F\$11<0,5;"@";" =SE(\$F\$11>=0,5;SE(\$F\$11<1,5;"@";" =SE(\$F\$11>=1,5;SE(\$F\$11<2,5;"@";" =SE(\$F\$11>=2,5;SE(\$F\$11<3,5;"@";" =SE(\$F\$11>=3,5;SE(\$F\$11<4,5;"@";" =SE(\$F\$11>=4,5;SE(\$F\$11<5,5;"@";" 
Cálculo do Desvio:	=SE(D11<>"";"ERRO";1-E11/F11)
Escala do processo PO8	
Atual:	=SE(\$E\$14<0,5;"@";" =SE(\$E\$14>=0,5;SE(\$E\$14<1,5;"@";" =SE(\$E\$14>=1,5;SE(\$E\$14<2,5;"@";" =SE(\$E\$14>=2,5;SE(\$E\$14<3,5;"@";" =SE(\$E\$14>=3,5;SE(\$E\$14<4,5;"@";" =SE(\$E\$14>=4,5;SE(\$E\$14<5,5;"@";" 
Estratégico:	=SE(\$F\$14<0,5;"@";" =SE(\$F\$14>=0,5;SE(\$F\$14<1,5;"@";" =SE(\$F\$14>=1,5;SE(\$F\$14<2,5;"@";" =SE(\$F\$14>=2,5;SE(\$F\$14<3,5;"@";" =SE(\$F\$14>=3,5;SE(\$F\$14<4,5;"@";" =SE(\$F\$14>=4,5;SE(\$F\$14<5,5;"@";" 
Cálculo do Desvio:	=SE(D14<>"";"ERRO";1-E14/F14)
Escala do processo PO9	
Atual:	=SE(\$E\$17<0,5;"@";" =SE(\$E\$17>=0,5;SE(\$E\$17<1,5;"@";" =SE(\$E\$17>=1,5;SE(\$E\$17<2,5;"@";" =SE(\$E\$17>=2,5;SE(\$E\$17<3,5;"@";" =SE(\$E\$17>=3,5;SE(\$E\$17<4,5;"@";" =SE(\$E\$17>=4,5;SE(\$E\$17<5,5;"@";" 
Estratégico:	=SE(\$F\$17<0,5;"@";" =SE(\$F\$17>=0,5;SE(\$F\$17<1,5;"@";" =SE(\$F\$17>=1,5;SE(\$F\$17<2,5;"@";" =SE(\$F\$17>=2,5;SE(\$F\$17<3,5;"@";" =SE(\$F\$17>=3,5;SE(\$F\$17<4,5;"@";" =SE(\$F\$17>=4,5;SE(\$F\$17<5,5;"@";" 
Cálculo do Desvio:	=SE(D17<>"";"ERRO";1-E17/F17)

Escala do processo AI6	
Atual:	=SE(\$E\$20<0,5;"@";"") =SE(\$E\$20>=0,5;SE(\$E\$20<1,5;"@";"")) =SE(\$E\$20>=1,5;SE(\$E\$20<2,5;"@";"")) =SE(\$E\$20>=2,5;SE(\$E\$20<3,5;"@";"")) =SE(\$E\$20>=3,5;SE(\$E\$20<4,5;"@";"")) =SE(\$E\$20>=4,5;SE(\$E\$20<5,5;"@";""))
Estratégico:	=SE(\$F\$20<0,5;"@";"") =SE(\$F\$20>=0,5;SE(\$F\$20<1,5;"@";"")) =SE(\$F\$20>=1,5;SE(\$F\$20<2,5;"@";"")) =SE(\$F\$20>=2,5;SE(\$F\$20<3,5;"@";"")) =SE(\$F\$20>=3,5;SE(\$F\$20<4,5;"@";"")) =SE(\$F\$20>=4,5;SE(\$F\$20<5,5;"@";""))
Cálculo do Desvio:	=SE(D20<>"";"ERRO";1-E20/F20)
Escala do processo DS1	
Atual:	=SE(\$E\$23<0,5;"@";"") =SE(\$E\$23>=0,5;SE(\$E\$23<1,5;"@";"")) =SE(\$E\$23>=1,5;SE(\$E\$23<2,5;"@";"")) =SE(\$E\$23>=2,5;SE(\$E\$23<3,5;"@";"")) =SE(\$E\$23>=3,5;SE(\$E\$23<4,5;"@";"")) =SE(\$E\$23>=4,5;SE(\$E\$23<5,5;"@";""))
Estratégico:	=SE(\$F\$23<0,5;"@";"") =SE(\$F\$23>=0,5;SE(\$F\$23<1,5;"@";"")) =SE(\$F\$23>=1,5;SE(\$F\$23<2,5;"@";"")) =SE(\$F\$23>=2,5;SE(\$F\$23<3,5;"@";"")) =SE(\$F\$23>=3,5;SE(\$F\$23<4,5;"@";"")) =SE(\$F\$23>=4,5;SE(\$F\$23<5,5;"@";""))
Cálculo do Desvio:	=SE(D23<>"";"ERRO";1-E23/F23)
Escala do processo DS2	
Atual:	=SE(\$E\$26<0,5;"@";"") =SE(\$E\$26>=0,5;SE(\$E\$26<1,5;"@";"")) =SE(\$E\$26>=1,5;SE(\$E\$26<2,5;"@";"")) =SE(\$E\$26>=2,5;SE(\$E\$26<3,5;"@";"")) =SE(\$E\$26>=3,5;SE(\$E\$26<4,5;"@";"")) =SE(\$E\$26>=4,5;SE(\$E\$26<5,5;"@";""))
Estratégico:	=SE(\$F\$26<0,5;"@";"") =SE(\$F\$26>=0,5;SE(\$F\$26<1,5;"@";"")) =SE(\$F\$26>=1,5;SE(\$F\$26<2,5;"@";"")) =SE(\$F\$26>=2,5;SE(\$F\$26<3,5;"@";"")) =SE(\$F\$26>=3,5;SE(\$F\$26<4,5;"@";"")) =SE(\$F\$26>=4,5;SE(\$F\$26<5,5;"@";""))
Cálculo do Desvio:	=SE(D26<>"";"ERRO";1-E26/F26)
Escala do processo DS4	
Atual:	=SE(\$E\$29<0,5;"@";"") =SE(\$E\$29>=0,5;SE(\$E\$29<1,5;"@";"")) =SE(\$E\$29>=1,5;SE(\$E\$29<2,5;"@";"")) =SE(\$E\$29>=2,5;SE(\$E\$29<3,5;"@";"")) =SE(\$E\$29>=3,5;SE(\$E\$29<4,5;"@";"")) =SE(\$E\$29>=4,5;SE(\$E\$29<5,5;"@";""))
Estratégico:	=SE(\$F\$29<0,5;"@";"") =SE(\$F\$29>=0,5;SE(\$F\$29<1,5;"@";"")) =SE(\$F\$29>=1,5;SE(\$F\$29<2,5;"@";"")) =SE(\$F\$29>=2,5;SE(\$F\$29<3,5;"@";"")) =SE(\$F\$29>=3,5;SE(\$F\$29<4,5;"@";"")) =SE(\$F\$29>=4,5;SE(\$F\$29<5,5;"@";""))
Cálculo do Desvio:	=SE(D29<>"";"ERRO";1-E29/F29)

Escala do processo DS6	
Atual:	=SE(\$E\$32<0,5;"@";" =SE(\$E\$32>=0,5;SE(\$E\$32<1,5;"@";" =SE(\$E\$32>=1,5;SE(\$E\$32<2,5;"@";" =SE(\$E\$32>=2,5;SE(\$E\$32<3,5;"@";" =SE(\$E\$32>=3,5;SE(\$E\$32<4,5;"@";" =SE(\$E\$32>=4,5;SE(\$E\$32<5,5;"@";"
Estratégico:	=SE(\$F\$32<0,5;"@";" =SE(\$F\$32>=0,5;SE(\$F\$32<1,5;"@";" =SE(\$F\$32>=1,5;SE(\$F\$32<2,5;"@";" =SE(\$F\$32>=2,5;SE(\$F\$32<3,5;"@";" =SE(\$F\$32>=3,5;SE(\$F\$32<4,5;"@";" =SE(\$F\$32>=4,5;SE(\$F\$32<5,5;"@";"
Cálculo do Desvio:	=SE(D32<>"ERRO";1-E32/F32)
Escala do processo DS11	
Atual:	=SE(\$E\$35<0,5;"@";" =SE(\$E\$35>=0,5;SE(\$E\$35<1,5;"@";" =SE(\$E\$35>=1,5;SE(\$E\$35<2,5;"@";" =SE(\$E\$35>=2,5;SE(\$E\$35<3,5;"@";" =SE(\$E\$35>=3,5;SE(\$E\$35<4,5;"@";" =SE(\$E\$35>=4,5;SE(\$E\$35<5,5;"@";"
Estratégico:	=SE(\$F\$35<0,5;"@";" =SE(\$F\$35>=0,5;SE(\$F\$35<1,5;"@";" =SE(\$F\$35>=1,5;SE(\$F\$35<2,5;"@";" =SE(\$F\$35>=2,5;SE(\$F\$35<3,5;"@";" =SE(\$F\$35>=3,5;SE(\$F\$35<4,5;"@";" =SE(\$F\$35>=4,5;SE(\$F\$35<5,5;"@";"
Cálculo do Desvio:	=SE(D35<>"ERRO";1-E35/F35)
Escala do processo M1	
Atual:	=SE(\$E\$38<0,5;"@";" =SE(\$E\$38>=0,5;SE(\$E\$38<1,5;"@";" =SE(\$E\$38>=1,5;SE(\$E\$38<2,5;"@";" =SE(\$E\$38>=2,5;SE(\$E\$38<3,5;"@";" =SE(\$E\$38>=3,5;SE(\$E\$38<4,5;"@";" =SE(\$E\$38>=4,5;SE(\$E\$38<5,5;"@";"
Estratégico:	=SE(\$F\$38<0,5;"@";" =SE(\$F\$38>=0,5;SE(\$F\$38<1,5;"@";" =SE(\$F\$38>=1,5;SE(\$F\$38<2,5;"@";" =SE(\$F\$38>=2,5;SE(\$F\$38<3,5;"@";" =SE(\$F\$38>=3,5;SE(\$F\$38<4,5;"@";" =SE(\$F\$38>=4,5;SE(\$F\$38<5,5;"@";"
Cálculo do Desvio:	=SE(D38<>"ERRO";1-E38/F38)
Escala do processo M2	
Atual:	=SE(\$E\$41<0,5;"@";" =SE(\$E\$41>=0,5;SE(\$E\$41<1,5;"@";" =SE(\$E\$41>=1,5;SE(\$E\$41<2,5;"@";" =SE(\$E\$41>=2,5;SE(\$E\$41<3,5;"@";" =SE(\$E\$41>=3,5;SE(\$E\$41<4,5;"@";" =SE(\$E\$41>=4,5;SE(\$E\$41<5,5;"@";"
Estratégico:	=SE(\$F\$41<0,5;"@";" =SE(\$F\$41>=0,5;SE(\$F\$41<1,5;"@";" =SE(\$F\$41>=1,5;SE(\$F\$41<2,5;"@";" =SE(\$F\$41>=2,5;SE(\$F\$41<3,5;"@";" =SE(\$F\$41>=3,5;SE(\$F\$41<4,5;"@";" =SE(\$F\$41>=4,5;SE(\$F\$41<5,5;"@";"
Cálculo do Desvio:	=SE(D41<>"ERRO";1-E41/F41)

Escala do processo M3	
Atual:	=SE(\$E\$44<0,5;"@";" =SE(\$E\$44>=0,5;SE(\$E\$44<1,5;"@";" =SE(\$E\$44>=1,5;SE(\$E\$44<2,5;"@";" =SE(\$E\$44>=2,5;SE(\$E\$44<3,5;"@";" =SE(\$E\$44>=3,5;SE(\$E\$44<4,5;"@";" =SE(\$E\$44>=4,5;SE(\$E\$44<5,5;"@";"
Estratégico:	=SE(\$F\$44<0,5;"@";" =SE(\$F\$44>=0,5;SE(\$F\$44<1,5;"@";" =SE(\$F\$44>=1,5;SE(\$F\$44<2,5;"@";" =SE(\$F\$44>=2,5;SE(\$F\$44<3,5;"@";" =SE(\$F\$44>=3,5;SE(\$F\$44<4,5;"@";" =SE(\$F\$44>=4,5;SE(\$F\$44<5,5;"@";"
Cálculo do Desvio:	=SE(D44<>"ERRO";1-E44/F44)
Escala do processo M4	
Atual:	=SE(\$E\$47<0,5;"@";" =SE(\$E\$47>=0,5;SE(\$E\$47<1,5;"@";" =SE(\$E\$47>=1,5;SE(\$E\$47<2,5;"@";" =SE(\$E\$47>=2,5;SE(\$E\$47<3,5;"@";" =SE(\$E\$47>=3,5;SE(\$E\$47<4,5;"@";" =SE(\$E\$47>=4,5;SE(\$E\$47<5,5;"@";"
Estratégico:	=SE(\$F\$47<0,5;"@";" =SE(\$F\$47>=0,5;SE(\$F\$47<1,5;"@";" =SE(\$F\$47>=1,5;SE(\$F\$47<2,5;"@";" =SE(\$F\$47>=2,5;SE(\$F\$47<3,5;"@";" =SE(\$F\$47>=3,5;SE(\$F\$47<4,5;"@";" =SE(\$F\$47>=4,5;SE(\$F\$47<5,5;"@";"
Cálculo do Desvio:	=SE(D47<>"ERRO";1-E47/F47)

Geração do Gráfico:

Gráfico; Tipo de Gráfico; Radar; Faixa de E8:E35 e F8:F35. Escala 0 a 5.