UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AVALIAÇÃO DOS CONTROLES SARBOX DA GERÊNCIA DE OPERAÇÕES DE TI DE UMA EMPRESA PROVEDORA DE SERVIÇOS DE TELECOMUNICAÇÕES

LAYANY ZAMBRANO HORTA DAMÁZIO

ORIENTADOR: DR. JOÃO DE SOUZA NETO

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: 048/08

BRASÍLIA/DF: 05 DE MAIO 2008

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

AVALIAÇÃO DOS CONTROLES SARBOX DA GERÊNCIA DE OPERAÇÕES DE TI DE UMA EMPRESA PROVEDORA DE SERVIÇOS DE TELECOMUNICAÇÕES

LAYANY ZAMBRANO HORTA DAMÁZIO

DISSERTAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM

APROVADA POR:

_____
JOÃO SOUZA NETO, Dr.,ECT
(ORIENTADOR)

_____
LUIS FERNANDO RAMOS MOLINARO, Dr.,ENE/UNB
(EXAMINADOR INTERNO)

_____
JORGE KOREEDA, Dr.,BRT
(EXAMINADOR EXTERNO)

BRASÍLIA/DF, 05 DE MAIO 2008

FICHA CATALOGRÁFICA

DAMÁZIO, LAYANY ZAMBRANO HORTA
Avaliação dos controles Sarbox da Gerência de operações de TI de uma empresa provedora de serviços de telecomunicações
xvii, p., 210 x 297 mm (ENC/FT/UnB, Mestre,Engenharia Elétrica
2008).
Dissertação de Mestrado – Universidade de Brasília. Faculdade de Tecnologia.Departamento de Engenharia Elétrica.
1. Lei Sarbanes - Oxley
2. Controles internos aplicado à área de operações de TI 3. Modelos IITL e eTOM
4.Avaliação da conformidade Sarbox de um modelo convergente eTOM X ITIL
I. ENC/FT/UnB II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

DAMÁZIO, L.Z.H. Avaliação dos controles Sarbox da Gerência de operações de TI de uma empresa provedora de serviços de telecomunicações. Dissertação de Mestrado em , Publicação /2008, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, p.

CESSÃO DE DIREITOS

_____

Layany Zambrano Horta Damázio
SQB - Rua Quaresmeira – Quadra 2 – Bloco G – ap 501 – Guará I
Brasília – DF - CEP:70000-009

"... Nunca espere algo que não deseja, e nunca deseje algo que não espera. Quando você espera algo que não quer, está atraindo o indesejado, e quando deseja algo que não espera, está simplesmente dissipando a valiosa força mental. Por outro lado, quando você está na constante expectativa de algo que deseja persistentemente, sua habilidade para atrair se torna irresistível. A mente é um imã e atrai o que quer que corresponda ao seu estado dominante. "

Dr. Raymond Holliwell , em Working with the Law: Eleven Truth Principles for Sucessful Living

AGRADECIMENTOS

A minha mãe, pelo amor, carinho e apoio constante em toda minha vida. Ao Estevão e a minha querida filha Maria Clara, dedico em especial este trabalho, por compreender a minha ausência e colocar uma pitada de alegria infantil neste caminho. A Arlete, por ajudar com sua sabedoria espiritual em todos os momentos. Aos amigos e companheiros de trabalho, pela compreensão, amizade e espírito de colaboração.

Ao Prof. Dr. Souza Neto, pela sua valiosa orientação e sabedoria;

Ao amigo Luciano Henrique Duque, pela grande amizade e pelo seu companheirismo que é uma de suas melhores qualidades;

Ao Prof. Geraldo Moacir, pelo auxílio no desenvolvimento de todo o trabalho;

Ao Ranério, pela amizade e incentivo que me apoiaram durante todo período do mestrado;

Ao Brambila, pelo companheirismo e pela postura positiva em todos os momentos;

A amiga Geórgia, que é responsável pelo meu ingresso nesta jornada;

Tácito e Airton, pela oportunidade e reconhecimento do trabalho.

Ao Frei Galvão, pelo seu exemplo de vida.

RESUMO

AVALIAÇÃO DOS CONTROLES SARBOX DA GERÊNCIA DE OPERAÇÕES DE TI DE UMA EMPRESA PROVEDORA DE SERVIÇOS DE TELECOMUNICAÇÕES

Autora: Layany Zambrano Horta Damázio
Orientador: Dr. João de Souza Neto
Programa de Pós-graduação em Tecnologia
Brasília, 05 de maio de 2008.

Por muito tempo, a gerência de operações de TI foi considerada área de apoio para tecnologia da informação. Porém, depois, houve uma mudança radical nessa concepção, seja pela necessidade crescente e cada vez mais complexa de adequação ao processo de regulamentação, que atribui novas e pesadas responsabilidades aos gestores da organização, seja pela diferenciação exigida pelos respectivos mercados. Assim, a gerência de operações de TI passa a ser percebida pelo negócio com um atributo fundamental para a consecução dos seus objetivos estratégicos. Não se trata mais de uma questão técnica ou tecnológica, mas sim de um fator que permeia toda a cadeia do negócio e o viabiliza. Este trabalho apresenta uma proposta de adequação dos controles estabelecidos na Lei Sarbanes-Oxley para a gerência de operações de TI, baseados no *framework* COBIT e nas regras estabelecidas no documento *IT Control Objectives for Sarbanes-Oxley do ITGI,* e alinhados aos parâmetros estabelecidos pelo *Public Company Accounting Oversight Board - PCAOB*. Para tanto, inicialmente, foi feita uma contextualização da Lei Sarbanes-Oxley, de sua estrutura e do seu posicionamento em relação à empresa pesquisada, apresentando-se seus controles para gerência de operações de TI. Estudou-se o *framework COBIT* e o mapeamento dos controles da Lei segundo as premissas do PCAOB. Foram revisadas as melhores práticas para o gerenciamento dos serviços de TI, o ITIL, e o *framework* eTOM para o serviços de telecomunicações, sendo elaborado um mapeamento dos controles dessa Lei no ITIL e no eTOM. Visualizou-se, então, um futuro convergente para o qual a empresa está se direcionando. Como resultado do estudo, apresenta-se uma proposta de adequação dos controles vigentes para gerência de operações de TI ao modelo PCAOB *versus* COBIT e ao modelo convergente, e a identificação de planos de ação e de oportunidades de trabalhos futuros.

ABSTRACT

EVALUATION OF SARBOX's CONTROLS FROM IT OPERATION MANAGEMENT FOR A TELECOMMUNICATION SERVICE SUPPLIER COMPANY.

For a long time, the IT operation management was considered as a support area for Information Technology. However, moreover, there was a radical change in this conception, as for growing demand and each time more complex adaptation to the regulation process, that assign new and heavy responsibilities to the organization's managers, for the differentiation required by the respective markets. Then the IT operation management starts to be noticed by the business as an essential attribute for the requisition of yours strategic objectives. Is no more a question of techniques or technology, but is for sure a factor that breaks through the business network and makes it feasible. This work presents a control adjustment proposal, established in Sarbanes – Oxley for IT operation management based on COBIT Framework, to the parameters established by "Public Company Accounting Oversight Board" – PCAOB. The future model has as purpose to evaluate the control objectives determined for IT operation management, based in rules established in "IT Control Objectives for Sarbanes – Oxley" document. For this, initially a contextualization of Sarbanes – Oxley law was done, of its structure and its positioning related to company, presenting its controls for IT operation management. The COBIT Framework was studied and the mapping of controls of the law according to PCAOB premises. The best practices for the IT – ITIL and the eTOM Framework for telecommunication services. Then, a convergent future was visualized in which the company is being directed. As result of the study, is presented an adjustment proposal to the controls in vigor for IT operation management to the model PCAOB versus COBIT, the action plans identification and future works opportunities.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS E ABREVIAÇÕES

ABNT - Associação Brasileira de Normas Técnicas

ADRs – *American Depositary Receipts - Os ADRS são recibos emitidos por um banco depositário norte-americano e que representam ações de um emissor estrangeiro que se encontram depositadas e sob custódia deste banco.*

AI – Acquire and Implement

ANS – Acordo de Nível de Serviço

BD – Banco de Dados

BDGC – Banco de Dados da Gerência de Configuração

BI – *Business Inteligence*

BOVESPA - Bolsa de Valores do Estado de São Paulo

BSS – *Business Support System*

BSC - Balanced Scorecard – Painel de resultados balanceados

CAPEX – Capital Expenditure

CCTA - *Central Computer and Telecommunications Agency*

CCM – *Comitê de Controle de Mudanças*

CEO - Chief Executive Officer – Diretor Presidente

CIO - Chief Information Office - Diretor de Tecnologia da Informação

CFO - Chief Financial Officer- Diretor Financeiro

CMDB - Configuration Management Database – Base de Dados da Gerência de Configuração

CMN - Conselho Monetário Nacional

CMMI – Capability Maturity Model Integration

CobiT - Control Objectives for Information Technology - Estrutura de relações e processos para controlar o ambiente de Tecnologia da Informação

COSO - Comitee of Sponsoring Organizations - Comitê das Organizações Patrocinadoras

CVM - Comissão de Valores Mobiliários

DS – Delivery and Support – Entrega e Suporte

DW - Datawarehouse

ERM – Enterprise Risk Management – Gerenciamento de Risco Empresarial

ERP – Enterprise Resource Planning

eTOM – Enhanced Telecom Operation Map

IC – Item de Configuração

IP – Internet Protocol

ISACA - Information Systems Audit and Control Association –www.isaca.org

ISACF - Information Systems Audit and Control Foundation

ISO – Iternational Standards Organization

IT - Information Technology – Tecnologia da Informação

ITIL - Information Technology Infrastructure Library - Biblioteca de Infra-Estrutura de Tecnologia da Informação

ITGI IT – IT Governance Institute

ITSM - IT Service Management - Gerenciamento de Serviços de Tecnologia da Informação

ITSMF- IT Service Management Forum - - Fórum de Gerenciamento de Serviços de Tecnologia da Informação

NYSE - New York Stock Exchange

ME – Monitor and Evaluate – Monitoração e Avaliação

MOF - Microsoft Operations Framework

NDS – Novell Directory Service – Serviço de diretório da Novell

OLA – Operations Level Agreement

OGC - Office of Government Commerce

OPEX – Operational Expenditure

OSS – Operation Support System

PO – Plan and Organize – Planejamento e Organização

PCN – Plano de continuidade de Negócio

PMBoK - Project Management Body of Knowledge

PMI - Project Management Institute

SEC - *Security and Exchange Comission*

SEI - Software Engineering Institute

SLA - Service Level Agreement – Acordo de nível de Serviço

UIM´S – Unidade de Implementação e Manutenção

TMF – Telemanagement Fórum

1 - INTRODUÇÃO

A evolução da tecnologia da informação e sua disseminação nos setores das organizações demonstram uma dependência significativa do negócio em relação aos serviços prestados. Essa dependência exige o cumprimento de critérios essenciais como disponibilidade, garantia de continuidade, segurança, qualidade na entrega e no suporte, controles, conformidade, transparência e eficiência. Nos últimos anos, a informação é reconhecida pelas organizações como um dos mais importantes recursos estratégicos que necessitam de gerenciamento (WEILL & ROSS, 2004). Aliado à importância da informação no provimento do serviço, o aspecto regulatório requer a utilização de estruturas de gerenciamento cada vez mais complexas.

Diversos regulamentos surgiram no cenário internacional, como conseqüência de *megafraudes* e escândalos que vieram à tona principalmente nos Estados Unidos. O novo cenário de forte regulação sancionou o ativismo voluntarista nesse país. De todas as reações regulatórias, uma de maior extensão foi a Lei Sarbanes-Oxley, aprovada em julho de 2002 pelo Congresso americano. A Lei Sarbanes-Oxley promoveu ampla regulação da vida corporativa, fundamentada nas boas práticas de governança. Seus focos são exatamente quatro valores: conformidade legal, prestação de contas responsável, transparência e senso de justiça. Essa evolução regulatória da vida corporativa se estendeu a várias empresas brasileiras com sede nos Estados Unidos, como sociedades de capital aberto e instituições financeiras.

Em 2002, uma empresa brasileira operadora de telefonia iniciou seu sistema regulatório, visando à conformidade de seus processos com os regulamentos vigentes. O mercado de telecomunicações é altamente dinâmico, dependente do uso intenso de Tecnologia da Informação (TI), o que demanda a disponibilização evolutiva constante de produtos e de serviços. Assim, para acompanhar as exigências do mercado, as empresas de telecomunicações utilizam metodologias de gerenciamento de projeto, melhores práticas no provimento de serviços e modelos de referência para provimento dos serviços de telecomunicações. A finalidade é enfrentar a concorrência e oferecer um melhor serviço aos clientes.

O modelo adotado para provimento de serviços de telecomunicações é o *eTOM,* um *framework* lógico de referência pré-definido do *Telemanagement Fórum*. O provimento de serviços de TI da empresa baseia-se nas melhores práticas *Information Technology Infraestructure Library* (ITIL) e no *framework Control Objectives for Information and Related Tecnology* (COBIT), que é uma base de conhecimento para os processos de TI e seu

gerenciamento. Os serviços de telecomunicação apóiam-se cada vez mais na TI; assim, a convergência dos modelos é uma realidade que vem sendo discutida mundialmente, para melhor atendimento do cliente final. Com a adoção de um modelo convergente, a base das empresas de telecomunicações divide-se em dois focos: nos processos de negócio fornecido pelo eTOM e nas melhores práticas para o provimento de serviços de TI fornecido pelo ITIL e integração entre os processos.

Na citada operadora, a área de operações de TI é responsável pela estrutura, implantação, operação e manutenção da infra-estrutura de serviços de TI e pela comunicação que sustenta os negócios da empresa. A conformidade com os regulamentos vigentes e as exigências decorrentes do grau de dependência do negócio em relação à área de TI criaram condições propícias ao surgimento de um modelo convergente para alcançar a eficiência no provimento do serviço e a sustentabilidade dos serviços oferecidos pela empresa.

Nesse contexto, o problema desta pesquisa centra-se na ausência de modelo único ou de uma metodologia de trabalho que contemple, simultaneamente, sistema, plataforma e/ou serviços convergentes, para atendimento aos controles estabelecidos pela Lei Sarbanes-Oxley, na área de operações de TI.

O principal objetivo do trabalho é adequar o modelo vigente de controles de operações de TI baseado no COBIT aos parâmetros estabelecidos pela Lei Sarbanes-Oxley via o *Public Company Accounting Oversight Board.*

Essa adequação levará em conta a comparação entre os modelos, para posterior estabelecimento de um conteúdo único.

Metodologicamente, os meios utilizados para desenvolvimento do trabalho foram a pesquisa bibliográfica e a pesquisa documental. Em relação à primeira, foram consultados e citados autores que discorreram sobre o tema, visando à composição de um suporte teórico e técnico que subsidiasse a proposta. Em relação à segunda, foram analisados manuais internos da empresa enfocada, além de documentos legais (Lei Sarbanes-Oxley) e institucionais (*Public Company Accounting Oversight Board* – PCAOB).

A pesquisa é relevante, porque a adequação proposta contribuirá para o melhor cumprimento das determinações da Lei Sarbanes-Oxley, em conseqüência, o enquadramento da empresa nos moldes das boas práticas de governança, amplamente reconhecidas no cenário mundial da TI.

O presente trabalho é singular, pois, ao adequar os parâmetros do COBIT às recomendações da citada Lei não só torna objetivos os respectivos preceitos, como

literalmente torna a área de operações de TI convergente para um desempenho padrão, na resolução de interesses que são comuns aos modelos e às regulamentações.

Vale destacar que não foi encontrada na literatura nenhuma pesquisa relacionando o *framework* COBIT aos controles da Lei Sarbanes-Oxley.

Este trabalho encontra-se estruturado da seguinte forma: no capítulo 2, são descritos os critérios e parâmetros estabelecidos pela Sarbanes-Oxley, cuja estrutura destaca o controle interno como um dos componentes principais. Também são apresentados seus impactos no Brasil e, em especial, na operadora objeto deste trabalho O capítulo 3 trata do controle interno aplicado à área de operações de TI. Apresenta o objetivo da área de operações de TI e sua missão na organização, definindo os controles internos estabelecidos para as áreas de operações de TI, bem como a metodologia utilizada para suportar estes controles. No capítulo 4, faz-se uma revisão da literatura do modelo ITIL, com o histórico de sua criação, suas principais disciplinas e o modelo eTOM, incluindo origem, definições e seus níveis de representação. No capítulo 5, descrevem-se os controles de operações de TI no modelo ITIL e eTOM comparativamente, identificando a aderência entre eles, além de enfocar a criação de um modelo único, baseado nos itens de cada um deles, e a geração de um padrão de conformidade para entrada de um sistema em produção. No capítulo 6**,** são feitas as conclusões sobre o estudo, apresentado-se sugestões para trabalhos futuros.

2 - LEI SARBANES - OXLEY

Neste capítulo, é apresentado um histórico da Lei Sarbanes–Oxley (Sarbox), os acontecimentos mundiais que fomentaram sua criação, as principais normas estabelecidas pela legislação, controles internos, impacto no mercado brasileiro e o posicionamento da empresa enfocada frente ao novo cenário.

2.1 - CONCEITOS E EVOLUÇÃO

O atentado terrorista contra as torres gêmeas (*World Trade Center*) em Nova Iorque, em 11 de setembro de 2001, teve grande impacto junto à população americana quanto à questão da segurança nacional, e seus reflexos também tiveram influência na área de Tecnologia da Informação (TI) das empresas. Pela ótica da contingência dos dados das empresas, o incidente mostrou a importância da questão da duplicação de dados e a necessidade da informação estar armazenada em mais de um espaço físico, evitando assim a perda do histórico empresarial em caso de catástrofe de qualquer natureza.

Muito se tem falado sobre a disponibilidade de serviços e a continuidade dos negócios desde que a TI passou a exercer papel fundamental nos processos de negócios das empresas, entretanto, jamais tal percepção havia sido comprovada na prática com tamanha assertiva como no caso citado acima..

Aquele episódio foi a comprovação factual de que a indisponibilidade de informações pode comprometer a sobrevivência das empresas, tanto quanto à utilização de estratégias incorretas ou a ocorrência de eventos negativos relacionados ao negócio. Desde então, a Gerência de Disponibilidade e o Plano de Continuidade de Negócios passaram a fazer parte das prioridades dos executivos de TI.

No Brasil, 32% dos executivos elegeram a questão da contingência como sua principal prioridade (IDC, 2005a). Esse fato e as conclusões relativas à continuidade do negócio e ao valor intrínseco da informação foram fatores que influenciaram substancialmente a publicação de novas leis para as empresas nos Estados Unidos, com conseqüências determinantes para a área de TI.

Nesse país, os fundos de aposentadoria e pensão detêm cerca de um quarto do valor total das ações das companhias americanas, representando o maior bloco de acionistas institucionais. Além disso, 95 milhões de norte-americanos – metade dos lares do país – investiram pessoalmente em fundos mútuos, objetivando em grande parte, a sua aposentadoria.

O ano 2002 foi marcado pelos escândalos contábeis das empresas norte-americanas Enron e Worldcom: fraudes contábeis produziam resultados fictícios, créditos em liquidação não eram declarados, receitas antecipadas eram apropriadas e bônus por lucros irreais eram pagos aos administradores, tudo isso com a conivência de empresas de auditoria independente.

Após o "11 de setembro" e tais escândalos, foi promulgada uma lei de reforma corporativa para dar maior publicidade às informações e propiciar fiscalizações preventivas pela *Security and Exchange Comission* (SEC), a comissão de valores mobiliários dos Estados Unidos.

Para evitar a perda da confiança no mercado financeiro e o conseqüente esvaziamento dos investimentos, em 30 de junho de 2002, os senadores Paul Sarbanes (Democrata de Maryland) e Michael Oxley (Republicano de Ohio) aprovaram a lei que carrega seus nomes, a Lei Sarbanes-Oxley (Sarbox).

Essa Lei apresenta um rol de responsabilidades a serem cumpridas pela direção das empresas e sanções para as mesmas, tipificando os crimes de "colarinho branco", e proíbe práticas contábeis que possam expor qualquer sociedade anônima a riscos sem provisionamento prévio, bem como veda a concessão de empréstimos a membros do conselho de administração e da diretoria das empresas.

Em julho de 2002, o Presidente George W. Bush assinou a Sarbox, apresentando-a ao conhecimento coletivo dos líderes empresariais e funcionários do governo no mundo inteiro. Repleta de reformas para a governança corporativa, divulgação de novas normas, a nova Lei busca, por meios tangíveis, "reparar" a perda da confiança pública nos líderes empresariais norte-americanos e enfatizar, mais uma vez, a importância dos padrões éticos na preparação das informações financeiras reportadas aos investidores.

– A Sarbox e as regras relacionadas, emitidas pela SEC, são complexas, geraram confusão e causaram consternação à comunidade empresarial. Mas, por trás de todas as regras e regulamentações, a Sarbox é, simplesmente, uma forma encontrada pelo governo para estabelecer recursos legais nos preceitos básicos da boa governança corporativa e das práticas empresariais éticas. A Sarbox codifica a concepção de que a administração da companhia deve conhecer as informações materiais arquivadas na SEC e distribuídas aos investidores e deve, também, responsabilizar-se pela probidade, profundidade e precisão dessas informações.

Muitos observadores acreditam que o estabelecimento dos novos procedimentos para controle interno e para a certificação executiva das empresas na nova Lei representa uma

correção de curso essencial para as companhias de capital aberto, determinando processos cuja adoção as companhias deveriam ter considerado em primeiro lugar. De forma similar, outros estudiosos da Sarbox sustentam que a concentração do foco na boa governança corporativa e na transparência das informações financeiras simplesmente faz despertar o senso empresarial.

Mas as novas regras implicam custo: as mudanças exigem alterações significativas nos procedimentos e nas práticas, bem como na vida cotidiana de executivos e pessoas que a eles se reportam. Entretanto, muitas companhias não vão começar do ponto zero, pois podem adaptar as exigências de controles internos da Sarbox aos respectivos processos em funcionamento.

Talvez a realização mais importante seja a mudança significativa – e permanente – da obrigatoriedade da aplicação da Sarbox. Para uma companhia de capital aberto, a obediência a essa Lei não é negociável. Para os comitês de auditoria e para a alta administração de companhias de capital aberto, particularmente diretores executivos e diretores financeiros, as definições de administradores financeiros e responsabilidade pessoal tornaram-se mais explícitas e os riscos significativamente mais altos. Não só suas obrigações estão claras, mas também suas oportunidades.

– Executivos que têm o pensamento inovador procurarão aproveitar as mudanças impostas para melhorar o desempenho operacional. Companhias de direito privado, embora não obrigadas legalmente a cumprir a nova Lei, também podem optar pela adoção de determinados componentes, como parte de um plano geral para o aperfeiçoamento das operações de seu negócio.

Essa nova ênfase nos controles internos e na divulgação transparente não é um modismo. A Sarbox muda fundamentalmente o cenário empresarial, e as companhias não podem subestimar a tarefa que têm pela frente.

Além disso, empresas que adotam boas práticas de governança corporativa conseguem se financiar a uma taxa menor no mercado, gerando melhores resultados e conseqüentemente, maiores retorno aos acionistas. Segundo Berton (2003), a valorização das ações no mercado é influenciada, positivamente, pelo grau de segurança oferecido pelos direitos concedidos aos acionistas e pela quantidade de informações disponibilizadas pelas empresas.

Essas premissas possibilitam às empresas se financiarem a custos mais baixos a partir do lançamento de ações no mercado, possibilitando, ainda, que os indivíduos efetuem programas de capitalização com vistas à aposentadoria.

A transparência, uma das premissas para boa governança corporativa, envolve uma rede de interessados, reunindo pessoas que possuem envolvimento financeiro ou pessoal com a organização: administradores, funcionários, fornecedores e clientes. Tapscott e Ticoll (2005) definem transparência como a acessibilidade da rede de interessados às informações institucionais referentes a assuntos que afetem seus interesses.

2.2 - ESTRUTURA DA LEI SARBANES – OXLEY

A Sarbox é composta por mais de 1107 artigos, dispostos em várias seções, abrangendo praticamente a totalidade dos temas-chave da governança corporativa, como:

1. separação das funções do presidente do conselho de administração e executivo-chefe;
2. composição, independência e responsabilidades do Conselho de Administração;
3. transparência das transações entre administração e partes interessadas (*stakeholders)*;
4. conflitos de interesse;
5. práticas de auditoria e instituição de um comitê de auditoria;
6. responsabilidade corporativa pelos demonstrativos financeiros;
7. avaliação dos controles internos pela administração;
8. remunerações e benefícios auto-atribuídos pela alta administração;
9. riscos financeiros;
10. Proposição e adoção de código de conduta.

As seções que integram a Sarbox e as respectivas referências são:

Sec.101. Estatuto e regras administrativas;
Sec.102. Inscrição no Conselho;
Sec.103. Auditoria, controle de qualidade, e normas e regras relativas à independência;
Sec.104. Inspeções das empresas de auditoria registradas;
Sec.105. Investigações e procedimentos disciplinares;
Sec.106. Empresas de auditoria estrangeira;
Sec.107. Poderes de supervisão do Conselho;
Sec.108. Normas de contabilidade;
Sec.109. Financiamento;
Sec.201. Serviços fora do âmbito da prática dos auditores;
Sec.202. Aprovação prévia;
Sec.203. Rotatividade do auditor sócio responsável;
Sec.204. Relatórios do auditor ao Comitê de Auditoria;

Sec.205. Modificações acordadas;

Sec.206. Conflitos de interesse;

Sec.207. Estudo da rotatividade obrigatória das empresas de auditoria registradas;

Sec.208. Competências da comissão;

Sec.209. Considerações sobre as competências regulamentadoras estatais;

Sec.301. Os Comitês das empresas públicas;

Sec.302. Responsabilidade da sociedade pelas demonstrações financeiras;

Sec.303. Influência imprópria na condução das auditorias;

Sec.304. Privação de determinados bônus e lucros;

Sec.305. Penas e impedimentos aos gestores e administradores;

Sec.306. Transações internas relativas a fundos de pensões;

Sec.307. Normas de responsabilidade profissional relativas aos advogados;

Sec.308. Fundos equitativos para os investidores;

Sec. 401. Revelações nos relatórios periódicos;

Sec. 402. Provisões aperfeiçoadas relativas a conflitos de interesse;

Sec. 403. Divulgação de transações envolvendo a gestão e os principais acionista;

Sec. 404. Avaliação dos controles internos feita pela gestão;

Sec. 405. Isenção;

Sec. 406. Código de Ética para os gestores financeiros;

Sec. 407. Divulgação do perito financeiro do comitê de auditoria;

Sec. 408. Avaliações melhoradas das divulgações periódicas feitas pelas emissoras;

Sec. 409. Divulgações das emissoras em tempo real;

Sec. 501. Tratamento dos analistas de títulos pelas associações de títulos registradas e bolsas de valores nacionais;

Sec. 601. Autorização de financiamento e recursos;

Sec. 602. Apresentação e práticas perante a comissão;

Sec. 603. Autoridade dos tribunais federais em defesa dos pequenos acionistas;

Sec. 604. Qualificações dos intermediários e corretores;

Sec. 701. Estudo do *General Accounting Office* (GAO) e do relatório de consolidação das empresas de auditoria;

Sec. 702. Estudo da comissão e relatório relativo às agências de avaliação de crédito;

Sec. 703. Estudo e relatório sobre prevaricadores e violações;

Sec. 704. Estudo de ações para a execução;

Sec. 705. Estudo dos bancos de investimento;

Sec. 801. Título abreviado;

Sec. 802. Penas criminais por alteração dos documentos;

Sec. 803. Dívidas não perdoadas se violadas as leis sobre fraudes em títulos;

Sec. 804. Estatuto das limitações por fraudes em títulos;

Sec. 805. Revisão de orientações sobre sentenças federais por obstrução da justiça e fraudes criminais;

Sec. 806. Proteção aos empregados das empresas cotadas com evidência de fraude;

Sec. 807. Penas criminais por defraudação dos acionistas das empresas cotadas;

Sec. 901. Título abreviado;

Sec. 902. Tentativas e conspirações relativas a fraudes criminais;

Sec. 903. Penas criminais por fraudes de correio e telefônicos;

Sec. 904. Penas criminais por violações do *Employee Retirement Income Security Act* de 1974;

Sec. 905. Emendas às orientações de sentenciamento relativas a certas ofensas de crimes de "colarinho branco";

Sec. 906. Responsabilidade das empresas pelos relatórios financeiros;

Sec. 1001. Opinião do Senado sobre a assinatura de responsáveis em reembolso de impostos;

Sec. 1101. Título abreviado;

Sec. 1102. Falsificação de registos ou impedimento de uma execução oficial;

Sec. 1103. Autoridade de congelamento temporário da SEC;

Sec. 1104. Emenda às orientações de sentencia mento federal;

Sec. 1105. Autoridade da Comissão para proibir pessoas de exercer cargos de gestores ou administradores;

Sec. 1106. Penas criminais reforçadas ao abrigo da *Securities Exchange Act* de 1934;

Sec. 1107. Retaliações contra informantes.

As seções mais importantes da Sarbox, que devem ser atendidas são, resumidamente:

Seção 301: O comitê de auditoria estabelece procedimentos para denúncias anônimas por empregados do emissor;

Seção 302: Aborda controles internos e requer trimestralmente certificação do *Chief Executive Officer* (CEO)/ *Chief Financial Officer* (CFO) de todas as empresas públicas americanas no arquivamento de relatórios periódicos sob a seção 13 (a) ou 15 (d) com respeito à *Securities Exchange Act of 1934* e relativos ao preenchimento e à acurácia de

tais relatórios bem como a natureza e eficácia dos controles internos que apóiam a qualidade da informação incluída nos mesmos;

Seção 404: Requer uma afirmação da eficácia da estrutura e procedimentos dos Controles Internos para os relatórios financeiros e um relatório emitido pelos Auditores externos atestando a acurácia da afirmação do gerenciamento;

Seção 409**:** Requer informações atualizadas e rápidas com respeito às condições ou operações financeiras, para informar investidores e interessados;

Seção 806: Penalidades criminais pela alteração de documentos;

Seção 906: Responsabilidade corporativa pelos relatórios financeiros.

Grande parte das companhias que aplicam a Sarbox concentram-se nas Seções 302 e 404. Algumas companhias adotam estratégias que priorizam o cumprimento da Seção 302, em detrimento da Seção 404.

A Seção 302 determina que diretores executivos e diretores financeiros devem declarar pessoalmente sua responsabilidade pelos controles e procedimentos de divulgação. Cada arquivo trimestral deve conter a certificação de que eles executaram a avaliação do desenho e da eficácia desses controles. Os executivos certificados também devem declarar que divulgaram todas e quaisquer deficiências significativas de controles, insuficiências materiais e atos de fraude ao seu Comitê de Auditoria.

A SEC também propôs uma exigência de certificação mais abrangente que inclui os controles internos e os procedimentos para a emissão de relatórios financeiros, além da exigência relacionada com os controles e procedimentos de divulgação.

A Seção 404 determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Além disso, o auditor independente da companhia deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.

Essa Seção obriga as companhias a incluir em seus relatórios anuais um relatório sobre controles internos emitido pela administração que:

- Afirme sua responsabilidade pelo estabelecimento e pela manutenção de controles e procedimentos internos para a emissão de relatórios financeiros;
- Avalie e conclua acerca da eficácia dos controles e procedimentos internos para a emissão de relatórios financeiros;
- Declare que o auditor independente da companhia atestou e reportou a avaliação feita pela administração sobre seus controles internos para a emissão de relatórios financeiros

Segundo as regras propostas pela SEC, a administração também deverá certificar a eficácia de seus controles e procedimentos internos para a emissão de relatórios financeiros em uma base trimestral.

2.3 - PRINCIPAIS NORMAS ESTABELECIDAS

A Sarbox promoveu ampla regulação da vida corporativa, fundamentada nas boas práticas de governança. Seus focos são exatamente quatro valores: conformidade legal, prestação responsável de contas, transparência e senso de justiça (IPAI, 2006).

Conformidade legal:

- Adoção, pelas corporações, de um código de ética para seus principais executivos, o qual deverá conter formas de encaminhamento de questões relacionadas a conflitos de interesse, divulgação de informações das leis e regulamentos;
- As corporações que não adotarem a explicitação de condutas em código de ética deverão explicar as razões da não adoção;
- Uma cópia do código de ética deverá ser entregue à SEC e ter divulgação aberta.

Prestação responsável de contas:

- O principal executivo e o diretor financeiro, respectivamente CEO e CFO, na divulgação dos relatórios periódicos previstos na Lei, devem certificar-se de que os relatórios foram revisados e não havia falsas declarações ou omissões de fatos relevantes:
  - as demonstrações financeiras revelam adequadamente a posição financeira, os resultados das operações e os fluxos de caixa;
  - deficiências significativas eventualmente encontradas nos controles internos foram divulgadas aos auditores e ao comitê de auditoria, bem como quaisquer fraudes evidenciadas ou mudanças significativas ocorridas após a sua avaliação;
  - há responsabilidade pelo estabelecimento de controles internos, pelos seus desenhos e processos e pela avaliação e monitoramento de sua eficácia.
- Constituição de um comitê de auditoria, para acompanhar a atuação dos auditores e dos números da companhia, atendendo às seguintes diretrizes:
  - presença de pelo menos um especialista em finanças;
  - composição exclusiva de membros independentes do conselho de administração, não integrantes da direção executiva que, além dos valores que já recebem pela

participação no conselho, não recebam quaisquer outros, a título de pagamento pelo aconselhamento ou consultoria prestada ao comitê;

- responsável pela aprovação prévia dos serviços de auditoria.
- divulgação, por relatórios periódicos, dos resultados de seus trabalhos.

Transparência:

- Detentores de informações privilegiadas deverão seguir as exigências da Lei, no caso de mudança em suas participações acionárias;
- Redução de prazos para que *insiders (colaboradores da companhia)* comuniquem à SEC qualquer renegociação envolvendo valores mobiliários da companhia;
- Qualquer informação complementar aos relatórios exigidos pela lei, relativa às condições financeiras e operacionais da companhia, deve ser divulgada com rapidez;
- Contingências não incluídas no balanço patrimonial devem ser divulgadas;
- A SEC poderá expedir regras, exigindo a divulgação em tempo real de quaisquer informações relevantes não contabilizadas de transações relevantes que não são obrigatoriamente incluídas nas demonstrações financeiras e (*off balance sheet)* que impactam os negócios e os resultados corporativos.

Senso de justiça:

- A remuneração do executivo principal deverá ser aprovada pelo conselho de administração;
- Aprovação pelos acionistas dos planos de opções de ações (*stock option*);
- Vedação de empréstimos pessoais a diretores executivos. Devolução de bônus e de lucros distribuídos, no caso de a companhia retificar demonstrações financeiras por descumprimento relevante das normas estabelecidas pela SEC. Vedação de quaisquer formas de anistia aos empréstimos concedidos e não liquidados;
- Restrições sobre negociação nos períodos de troca de administração de fundos de investimento;
- Definição de penas historicamente inusitadas para fraudes. As multas podem chegar a US$ 5 milhões, e a prisão, a 20 anos. Entende-se por fraudes corporativas a alteração, a destruição, a mutilação, a ocultação e a falsificação de informações ou documentos, com a intenção de impedir, obstruir ou influenciar o conhecimento e análise do desempenho e da situação dos negócios e da gestão.

2.4 - CONTROLES INTERNOS

A Sarbox torna executivos explicitamente responsáveis por estabelecer, avaliar e monitorar a eficácia da estrutura de controles internos das companhias. Por exemplo, sempre que um membro do departamento financeiro utiliza uma senha exclusiva para obter acesso ao sistema financeiro da companhia, um controle está sendo executado. Em muitas companhias, os controles já estão sendo executados.

Com a implantação da Sarbox nas companhias, a alta direção estabelece controles internos a serem cumpridos.

A definição de controles internos mais amplamente aceita foi desenvolvida pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) como:

> (...) um processo, efetuado pelo Conselho de Administração, pela administração ou por outras pessoas da companhia, que visa fornecer segurança razoável quanto à possibilidade de atingir objetivos nas seguintes categorias: eficácia e eficiência das operações, confiabilidade dos relatórios financeiros, cumprimento de leis e regulamentos aplicáveis (COSO, *apud* DELOITTE, 2003, p. 7).

Os controles internos são divididos em controles contábeis e controles administrativos. Os controles contábeis compreendem o plano de organização e todos os métodos e procedimentos diretamente relacionados com a salvaguarda do patrimônio e fidedignidade dos registros contábeis. Geralmente incluem: sistemas de autorização e aprovação; separação das funções de escrituração e elaboração de relatórios contábeis e outros. Os controles administrativos compreendem o plano de organização e todos os métodos e procedimentos que dizem respeito à eficiência operacional e à decisão política traçada pela administração, abrangendo: relatórios de desempenho, estudos de tempos, análises estatísticas, controle de qualidade, entre outros.

Várias estruturas para a avaliação dos controles internos estão disponíveis. Entre as mais proeminentes, citam-se:

1. COSO – Estrutura Integrada de Controles Internos: desenvolvida pelo *Committee of Sponsoring Organizations of the Treadway Commission* e patrocinada pela AICPA, FEI e IIA, entre outros, a metodologia COSO é dominante nos Estados Unidos. As diretrizes foram publicadas em 1991, com revisões antecipadas e atualizações posteriores. Acreditamos que esta será a estrutura escolhida pela grande maioria das companhias de capital aberto sediada nos EUA;

2. CoCo – Modelo de Controles: desenvolvido pelo *Criteria of Control Committee of Canadian Institute of Chartered Accountants*, o CoCo concentra-se nos valores comportamentais como a base fundamental para os controles internos de uma companhia, e não na estrutura e nos procedimentos de controle;

3. *Turnbull Report* – Controles Internos. Diretrizes para Diretores sobre o Código Combinado: desenvolvido pelo *Committee on Corporate Governance of the Institute of Chartered Accountants in England & Wales*, em parceria com *a London Stock Exchange* (999). Exige que as companhias identifiquem, avaliem e administrem seus riscos significativos e a eficácia do sistema de controles internos relacionado;

4. ACC – *Australian Criteria of Control*: emitido em 1998 pelo *Institute of Internal Auditors* – Austrália, o ACC enfatiza a competência da administração e dos funcionários para desenvolver e operar a estrutura de controles internos. Trata-se de um controle independente, que inclui atributos, atitudes, comportamentos e competência. É promovido com o enfoque nos custo para os controles internos;

5. *KING REPORT* – expedido pelo *King Committee on Corporate Governance* em 1994: promove padrões gerais para governança corporativa na África do Sul. O *King Report* ultrapassa os aspectos financeiros e reguladores usuais da governança corporativa, direcionando questões sociais, éticas e ambientais (Guia Deloitte, 2003).

A Sarbox não faz menção ao modelo COSO. No entanto, era necessário utilizar um modelo aceitável para avaliar a efetividade dos controles internos. O COSO I datava de alguns anos na época de promulgação da Sarbox e constitui-se em um modelo de controle a ser adaptado às peculiaridades de cada empresa, de modo a resultar em uma metodologia de avaliação dos controles internos. Sua principal característica é promover a integração dos controles internos contábeis, baseada no uso de uma estrutura tridimensional (cubo do COSO), cujas dimensões compreendem os objetos de avaliação, as categorias de atividades de controle e os componentes de controle: (a) na primeira face estão os objetos de avaliação ou unidades administrativas que deverão ser avaliadas; (b) na segunda, estão as três categorias de atividades de controle: processo, registro e conformidade; (c) na terceira, os cinco componentes de controle: ambiente de controle, avaliação de risco, controle das atividades, processo de comunicação e monitoração (figura 2.1).

Figura 2.1- Estrutura COSO I
Fonte: Guia Lei Sarbanes-Oxley Deloitte (2003)

A avaliação dos controles internos é feita com a verificação do alinhamento ou integração de seus componentes: **ambiente de controle** – alicerce de todos os elementos dos controles internos, que inclui os valores éticos e a competência dos funcionários da companhia; **avaliação de riscos** – identificação e análise de riscos pertinentes que podem impedir o alcance dos objetivos do negócio; **atividades de controle** – tarefas específicas para atenuar os riscos identificados anteriormente; **informação e comunicação** – vias que partem da administração para os funcionários e vice-versa; **monitoramento** – avaliação e apreciação dos controles internos.

As vantagens do uso do COSO I de fortalecer os sistemas de controles internos contábeis despertaram os executivos para as possibilidades de promover o fortalecimento de todos os controles internos administrativos. Essa medida resultava no uso do COSO I para desenvolver uma metodologia específica aplicável à gestão pró-ativa dos processos . Para tanto era necessário adicionar alguns ingredientes, o que acabou resultando no COSO II – *Enterprise Risk Management* (ERM).

Em setembro de 2004, a SEC divulgou o documento chamado Gerenciamento de Risco Empresarial - Estrutura Integrada ou ERM, conhecido como COSO II no mercado.

O COSO II define o ERM como o processo realizado por um comitê diretivo de uma empresa, suas gerências e seus funcionários, incluído na estratégia empresarial global e desenhado para identificar eventos que possam, potencialmente, afetar seu desempenho.

Monitora os riscos, assegurando que eles são compatíveis com o previsto, e permite prover, com segurança razoável, o alicerce dos objetivos. O ERM aumenta os controles internos, sem ser necessário substituir sua estrutura vigente, mas incorporá-la à nova abordagem.

Toda empresa deve gerar valor para os acionistas, num ambiente de incerteza que apresenta riscos e oportunidades. Uma vez estabelecida a propensão ao risco, o ERM capacita o corpo gerencial a administrar com eficácia os riscos envolvidos.

O ERM compreende, entre outros, o alinhamento da estratégia implementada com base numa propensão predeterminada ao risco; o aumento das decisões com base no instrumental de risco; a redução de perdas decorrentes de imprevistos operacionais; a identificação e o gerenciamento de forma integrada, dos diversos riscos do negócio; a mensuração das oportunidades e a melhoria no processo e na alocação de capital.

A abordagem tridimensional do cubo do COSO I se repete no ERM, que utiliza um cubo semelhante, acrescentando outros ingredientes: (a) a primeira face, relativa ao objeto do gerenciamento, permaneceu inalterada; (b) à segunda face, relativa aos objetivos do gerenciamento, foi adicionada uma categoria às três existentes – as atividades estratégicas de controle; (c) na terceira face, relativa a componentes de controle, foram acrescentados três aos cinco anteriormente existentes: definição dos objetivos, identificação dos eventos e resposta ao risco, conforme mostrado na figura 2.2.

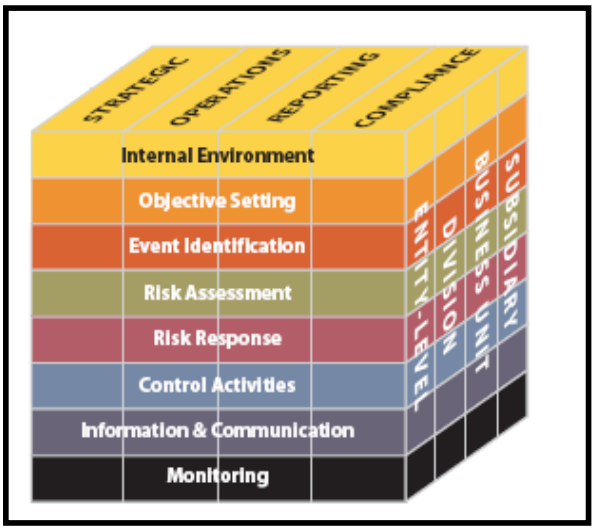

Figura 2.2- Estrutura COSO II
Fonte: COSO (2004)

A finalidade dos controles internos é a de prover as melhores condições para se atingirem os objetivos específicos da empresa. Tais condições decorrem das medidas adotadas pela empresa a fim de fornecer o suporte necessário para o alcance de objetivos, que podem

ser divididos em três grupos: otimizar processos, incrementar a transparência e assegurar a conformidade.

Sem uma estrutura apropriada de controles internos (COSO ou similar), provavelmente não é possível atender às exigências determinadas pela Seção 404 da Sarbox. Segundo essa seção, o auditor independente deve preencher um relatório que ateste sua garantia sobre a eficácia de seus controles e procedimentos internos para a emissão de relatórios financeiros. Se a companhia não tiver adotado uma estrutura de controles internos, não haverá critérios com os quais a companhia ou o auditor independente possa comparar a eficácia.

Para muitas companhias, o cumprimento das medidas da Sarbox relativas aos controles internos exige um esforço significativo. Na verdade, o trabalho inicial - desenvolver um programa de controles internos pode ser intensivo. Entretanto, uma vez que o programa esteja bem estabelecido, a carga será amenizada e a estrutura e os processos tornar-se-ão parte dos procedimentos operacionais padrão de sua companhia.

2.5 - IMPACTO DE SUAS EXIGÊNCIAS NO BRASIL

As limitações do acesso à poupança nacional pelas vias das bolsas de valores e a própria indisponibilidade dos recursos desejados, levaram muitas companhias brasileiras ao mercado internacional, captando recursos de investidores estrangeiros. O canal de acesso prioritário tem sido a *New York Stock Exchange* (NYSE).

Nesse mercado, em resposta aos escândalos e fraudes que abalaram a credibilidade de instituições, até então predominante auto–reguladas, temos o advento, em 2002, da Sarbox, que impôs novas regras rígidas de governança corporativa, estendidas pela SEC às companhias estrangeiras com emissões de ações nos Estados Unidos.

A extraterritorialidade na aplicação dessa Lei e das normas regulatórias conexas é uma das conseqüências da globalização dos mercados, que exige as inter-relações entre ordenamentos jurídicos distintos, sob pena de comprometer o próprio processo de integração mundial de mercados. Há, para tanto, procedimentos previstos no Direito Internacional Privado de reenvio e recepção para solucionar conflitos e normas no mesmo espaço. No caso brasileiro, por exemplo, isso se deu para permitir a adaptação das exigências de criação do Comitê de Auditoria, que conflitavam com os do Conselho Fiscal previstos na nossa legislação. Após a manifestação da Comissão de Valores Mobiliários (CVM), o Conselho Fiscal foi aceito como instituição que cumpria a finalidade desejada, desde que com

adaptações: criou-se assim o chamado Conselho Fiscal "Turbinado" (FREITAS; AGUIAR 2006).

Outro aspecto relevante a ser observado é o fato que as companhias foram obrigadas a incluir em seus relatórios declarações anuais de natureza civil e penal, emitidas pelo Diretor-Presidente e pelo Diretor Financeiro, nos quais esses administradores atestam a veracidade e a precisão das informações prestadas naquele documento, particularmente as contábeis e financeiras. Isto levou as companhias brasileiras à avaliação rigorosa de seus controles internos – pela administração e pelos auditores externos – mapeando-os e elaborando planos de ação para correção de falhas.

O cumprimento dessas exigências envolve elevados custos, aos quais não estão sujeitas as companhias brasileiras que não acessaram o mercado dos Estados Unidos. E mais, além dessa assimetria, ao adquirir outras empresas, as companhias que acessaram a NYSE se expõem aos riscos decorrentes de controles deficientes da empresa-alvo, incorrendo nos custos de remoção das falhas constatadas. Claramente, essas assimetrias impactam negativamente as condições competitivas das empresas sujeitas a Sarbox.

Outra questão importante relacionada com a aplicação dos dispositivos da Sarbox no Brasil diz respeito às diferenças nas estruturas de controle. Nos Estados Unidos, o capital é detido por um universo enorme de investidores; já as companhias brasileiras emissoras de *American Depositary Receipts* (ADRs) têm acionista controlador ou um grupo identificado de controle. O eixo do poder é, portanto, diferente. Enquanto lá, na maior parte das companhias, são os executivos munidos de mandatos que nomeiam os membros do Conselho de Administração, podendo assim ocorrer fraudes, resultados forjados e auto premiações ilegítimas para a administração, aqui são grupos de acionistas controladores que escolhem os administradores (conselheiros e executivos). Dada essa estrutura de poder, as atribuições da Diretoria Executiva são comparativamente mais limitadas.

Tais características se refletem na doutrina brasileira que, ao tratar temas com *affectio societatis,* centra-se nas relações entre os sócios e em sua conduta como acionista controlador, não a Diretoria Executiva. E foi nesse campo que, no Brasil, instalaram-se os embates sobre os limites legais do exercício do poder nas sociedades anônimas.

Pode-se dizer que, da nata das companhias brasileiras, atualmente 38 empresas possuem ações na bolsa de valores norte-americana, com o que passaram, conseqüentemente, a se sujeitar à nova Lei, bem como à sua regulamentação, estendendo a todas as filiais da empresa sua aplicabilidade.

Os reflexos de inúmeros procedimentos exigidos pelas empresas sujeitas ao relatório causam certo, desconforto aos colaboradores, tendo em vista as inevitáveis alterações em diversos processos dentro da empresa, além da necessidade da implantação de novos, que requerem o uso de ferramentas que facilitem o controle e demonstrem a transparência dos atos negociais de seus dirigentes.

No Brasil, o mercado de grandes empresas diz estar cada vez mais bem preparado para colocar sua sustentabilidade à prova, mas a preocupação em aderir à Sarbox ainda impacta mais processos do que a infra-estrutura tecnológica.

2.6 - SARBOX NA OPERADORA BRASILEIRA

No dia 9 de maio de 2002, a operadora em destaque se tornou a primeira empresa do setor a aderir às Práticas Diferenciadas de Governança Corporativa da Bolsa de Valores de São Paulo (Bovespa), reforçando sua política de transparência e valorização do acionista. Desde então, suas ações passaram a fazer parte do Índice de Ações com Governança Corporativa Diferenciada (IGC), que tem por objetivo medir o desempenho de uma carteira teórica composta por ações de empresas que apresentem bons níveis de governança corporativa.

Em 2003, dando continuidade ao processo, foram feitos diagnósticos e avaliações das práticas e procedimentos de governança corporativa. Foram identificadas, nesse trabalho, possíveis lacunas entre a situação da empresa e as exigências da Sarbox. Nesse ano, foi gerada uma documentação da estrutura de controle que suportava a emissão de relatórios financeiros e de controle de divulgação.

No ano seguinte, novas frentes de trabalho foram iniciadas, contemplando a revisão da estrutura de controle e dos seus principais processos: mediação, tarifação, interconexão, faturamento, contas a receber, fraude, atendimento a clientes, cadastro de clientes, TI, jurídico e outros. Essa revisão tinha como objetivo principal a avaliação de riscos financeiros, embasada na metodologia COSO.

Em 27 de julho de 2005, em Assembléia Geral Extraordinária, foram destituídos os membros do Conselho de Administração das participações, ligados ao antigo gestor, o Banco *Opportunity*. Em uma reunião desse Conselho, em 25 de agosto de 2005, foi eleita a nova diretoria, que manteve no cargo o então Diretor Técnico. O processo de troca dos administradores da área das participações e da própria empresa foi litigioso.

Em 25 de agosto do mesmo ano, o Conselho de Administração da Companhia, em uma que contou com a presença de todos os seus membros titulares, aprovou, por

unanimidade, a destituição de todos os integrantes da Diretoria da área das participações, outra vez mantendo o Diretor Técnico. Em seguida, o Conselho de Administração, também por deliberação unânime, elegeu os Srs. Ricardo Knoepfelmacher, Luiz Francisco Tenório Perrone e Charles Laganá Putz para as funções, respectivamente, de Diretor Presidente, Diretor de Recursos Humanos e Diretor Financeiro, cabendo ao último, ainda, as funções inerentes à Diretoria de Relações com Investidores.

A nova administração procurou reconquistar a credibilidade dos acionistas e dos clientes da empresa. A partir daí, a operadora iniciou, em 2005, um plano de transformação estrutural, com ênfase no projeto de governança corporativa. À época, a nova administração promoveu uma auditoria e encontrou uma série de irregularidades e desvios, entre os quais:

- Custos referentes ao aluguel e à reforma do Banco *Opportunity* - acionista minoritário - em São Paulo, pagos pela empresa;
- A operadora arcava com 70% dos custos de utilização de aeronaves, independentemente de utilizá-las ou não;
- A operadora emprestou recursos ao fundo controlado pelo CVC/*Opportunity* e arcou com os prejuízos da operação, quando o respectivo fundo foi desconstituído.

Além disso, um dos maiores conflitos societários da história envolvendo a empresa contribuiu para a erosão do valor das ações, visto que o mercado percebeu a operação como um negócio conturbado e envolvido pela insegurança jurídica.

Diante disso, o caminho encontrado pela nova administração foi construir um sistema de governança que, independentemente do controle acionário, fosse transparente a todos acionistas e apoiasse o desenvolvimento sustentável da empresa. O próprio organograma da empresa passou por profundas transformações. Foi criada, por exemplo, uma Diretoria de Governança Corporativa que passou a funcionar como um elo entre acionistas e diretoria da empresa, para embasar as tomadas de decisão.

Essa nova estrutura de decisões está representada na figura 2.3.

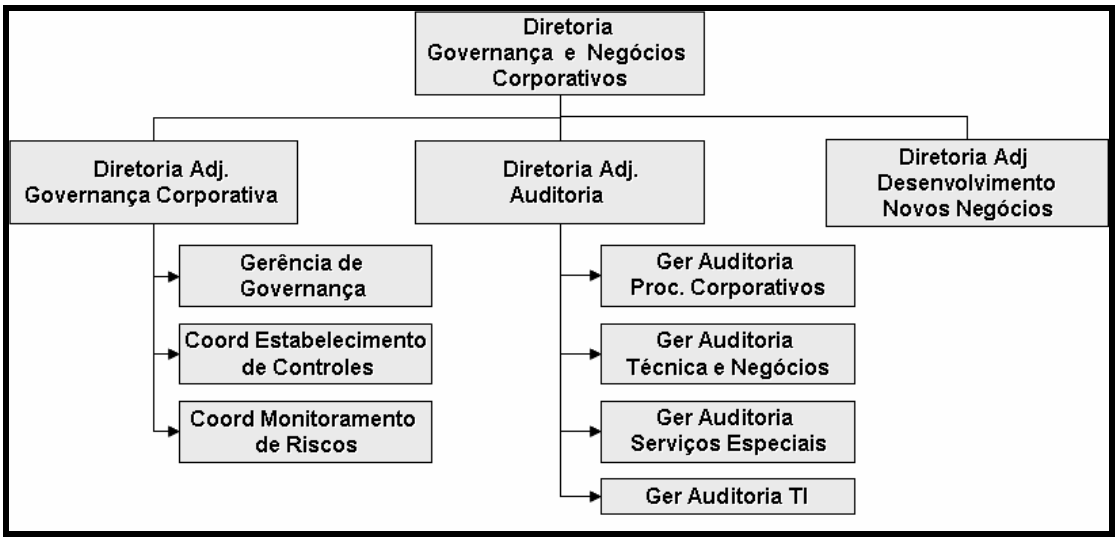

Figura 2.3 – Diretoria de Governança e Negócios Corporativos
Fonte: CNASI (2007)

O Comitê Sarbox foi implementado em maio de 2006, para acompanhamento das ações necessárias ao cumprimento à Lei Sarbox, focalizando os esforços em: *status* dos planos de ação; controles que dependem de melhorias de sistemas; análise das pendências do ambiente geral de controles; cronograma de trabalho da auditoria interna e externa.

O Comitê Sarbox é composto de uma Diretoria de Governança Corporativa; Diretoria Adjunta de Governança Corporativa; Diretoria Adjunta de Auditoria; Vice-Presidência de Operações e/ou Diretoria de Tecnologia e Planejamento Técnico; Vice-Presidência de Finanças e/ou Diretoria de Controladoria; representantes do Conselho de Administração e Conselho Fiscal

Baseada nas principais normas estabelecidas pela Sarbox, a empresa em destaque implantou ações de conformidade legal, de ética e de transparência como:

- Criação do Código de Conduta para colaboradores e fornecedores;
- Formação do comitê de Ética;
- Elaboração e disseminação de Código de Ética;
- Programas Canal Aberto e Linha Direta para sugestões e denúncias;
- Célula na Auditoria Interna para apurar denúncias graves de desvio de conduta;
- Mapeamento, cobrança e acompanhamento da implementação dos controles relevantes nas diversas áreas da empresa;

Para implantação da Sarbox, foi elaborado um desenho do processo de gestão de riscos e uma documentação contendo os riscos de negócio e a estrutura de controles internos, nos

processos selecionados pela Companhia, observando diretrizes de padrões internacionalmente conhecidos: COSO e COBIT.

Estar em conformidade com a Sarbox não é uma opção. As companhias que se negam a instituir os controles exigidos nessa Lei, com toda certeza, geram desconfiança no mercado, com impactos no valor da ação para o acionista. O aumento da credibilidade das empresas que cumprem seu papel em relação à Sarbanes-Oxley é, com certeza, o resultado mais louvável e um ponto a mais na reputação de seus gestores.

Em 20 de junho de 2007, a área de participações e a empresa comunicaram ao mercado o cumprimento, com sucesso, dos dispositivos exigidos pela seção 404 da Sarbox, relativos aos controles internos sobre as demonstrações contábeis consolidadas para o exercício fiscal findo em 31 de dezembro de 2006.

A operadora trabalha para obter a certificação desde o fim de 2005, com a chegada da atual administração. O primeiro passo para essa conquista se deu com a criação da Diretoria de Governança Corporativa, que além de implementar as melhores práticas, como o Código de Ética e o Canal de Denúncias, estabeleceu relacionamento estreito com todas as áreas da operadora, que trabalharam em conjunto para a obtenção da certificação.

Agora, a companhia faz parte de um seleto grupo de empresas que possuem um padrão de gestão corporativa mundial. A certificação é o reconhecimento de meses de muito trabalho e esforços de todas as áreas e também um desafio que se renova a cada ano. Mais uma vez, a companhia confirma que é uma corporação transparente e dispõe de controles que garantem a confiabilidade das informações.

3 –CONTROLES INTERNOS APLICADOS À ÁREA DE OPERAÇÕES DE TI

O presente capítulo tem como objetivo descrever a estrutura da área de operações de TI, sua missão, o *framework* COBIT, os controles internos estabelecidos pela Sarbox para essa gerência e o alinhamento dos objetivos de controle do COBIT e o PCAOB.

3.1- ASPECTOS INTRODUTÓRIOS

No segundo semestre de 2006, a Diretoria de Tecnologia da Informação da empresa sofreu uma grande reestruturação organizacional, fomentada pela visão convergente que os serviços de telecomunicações vêm adotando nos últimos tempos.

A empresa possuía uma estrutura organizacional composta por uma Diretoria de Tecnologia da Informação e uma Diretoria de Rede. Essa separação gerava uma divisão dos mundos de telecomunicações e da TI, sendo que, para muitos serviços oferecidos pela empresa, essas tecnologias são complementares (RFP, 2006).

A Diretoria de Tecnologia da Informação possuía duas frentes, uma ligada aos sistemas de suporte ao negócio, e outra, aos sistemas de informação de suporte à gestão, contando as duas com Diretorias Adjuntas. Além dessas frentes, havia três gerências: Gerência de Planejamento e Controle de Resultados de TI, Gerência de Integração e Qualidade de TI e Gerência de Arquitetura e Segurança de TI.

A Diretoria Adjunta de Suporte ao Negócio era responsável pelo desenvolvimento, e manutenção dos sistemas de informação de suporte a operação (OSS) e de suporte ao negócio (BSS).

A Diretoria Adjunta de Suporte à Gestão tinha sob sua responsabilidade o desenvolvimento e a manutenção de sistemas de informação de gestão empresarial como o *Enterprise Resource Plannig* (ERP), solução do fornecedor (SAP), gestão de recursos humanos (solução do fornecedor *peoplesoft*), gestão dos sistemas de arrecadação e de cobrança, gestão de sistemas ligados à inteligência de negócio, como o *Datawarehouse* (DW) e *Business Intelligence* (BI), além disso, as gerências de teste integrado.

Em agosto de 2006, houve a fusão das Diretorias de Rede e de Tecnologia da Informação, cujo objetivo principal foi a convergência entre o mundo de telecomunicações e o de TI. Outros aspectos também fomentaram essa transformação: o desenvolvimento de sistemas de informação passou a ser de responsabilidade das diretorias de negócio, sendo

criadas as Unidades de Implementação e Manutenção (UIM´s) e a segregação das atividades de planejamento e prospecção, projeto, implantação e operação.

A Gerência de Operações de TI passou a integrar a Diretoria de Gestão de Rede no final de 2005, pouco antes dessa reestruturação. Em 2006, a área de operações de TI sofreu uma grande mudança em sua estrutura organizacional e em seu modelo de terceirização.

A estrutura organizacional da Gerência de Operação de TI se subdivide em cinco gerências e uma coordenação. São elas: Gerência de Produção e Suporte de TI; Gerência de Cyber Data Center RS; Gerência de Cyber Data Center SP; Gerência de Cyber Data Center PR; Coordenação de Microinformática; Centro Nacional de Operação de TI (CNOTI); Gerência de Mudanças; Gerência de Configuração; *Service Desk*; Investigação e Operação de Sistemas; Monitoração de Serviços de TI; Coordenação de Plataformas e Serviços; Coordenação de Plataformas de *Call Center*.

Todos os processos de negócio de um provedor de serviços de telecomunicações são apoiados significativamente por sistemas, plataformas e estruturas computacionais. Falhas no desenvolvimento de um sistema e implantações inadequadas de infra-estrutura têm grandes impactos no provimento de serviços da empresa e, conseqüentemente, prejuízos financeiros podem vir a acontecer.

A Gerência de Operações de TI tem um papel essencial na sustentação dos serviços da empresa e sua missão consiste em implantar, operar e manter a infra-estrutura de serviços de TI e de comunicação, que sustentam seus negócios.

Uma das premissas da Sarbox é que as empresas demonstrem eficiência na governança corporativa. Nesse contexto, a área de operações de TI tem um papel importante, conforme declarado no próprio COSO: “A área de TI deve cobrir todos os aspectos de segurança e controle das informações digitais da empresa, devendo desenhar processos de controle das aplicações para assegurar a confiabilidade do sistema operacional, a veracidade dos dados de saída e a proteção de equipamentos e arquivos” (COSO, *apud* MAYER, 2007).

Para alcançar esse objetivo, a delimitação clara de papéis e de responsabilidades, estabelecida pelos controles implantados pela Sarbox, a formalização de normas e de procedimentos para a estrutura normativa da empresa, o estabelecimento de regras e de termos de responsabilidades a serem cumpridos são aspectos essenciais para a melhoria do provimento dos serviços prestados pela área de operações.

Baseadas nos processos críticos que suportam o negócio da empresa, foram definidas 44 aplicações elegíveis para serem auditadas no processo de certificação da Sarbox. Após essa definição, foram formalizados os sistemas envolvidos com os respectivos gestores,

objetivando nivelar conceitos e responsabilidades entre as áreas de negócios e de TI. O Objetivo era promover a conscientização das áreas usuárias de seus recursos, quanto aos aspectos de segurança e cuidados na manipulação das informações, tais como: e-mails, compartilhamento de diretórios, compartilhamento de senhas de acesso aos aplicativos, definição de dados para recuperação dos ambientes e outros.

Para efetivar as ações de responsabilidade da área de TI, foi criado um repositório de controles, que passou a funcionar como uma central de informações de todos os controles internos a serem implementados ou avaliados. Esse repositório de ações foi denominado "Caderno 21" da área de TI. A metodologia de mapeamento desse caderno identificou os fluxos das atividades com os respectivos responsáveis e sistemas associados; associou as contas contábeis ao processo e identificou os eventos de risco nos objetivos de controle. Para as atividades de controle não implementadas, foi estabelecido um plano de ação.

O Caderno 21 possui a seguinte estrutura: matriz de risco, contas contábeis, matriz de controles e plano de ação. A matriz de risco é responsável pela identificação de cada risco que possa prejudicar ou impedir o alcance do objetivo identificado e priorizado pela companhia. Contas Contábeis fazem referência à identificação e à descrição das contas relacionadas com o processo de TI.

A matriz de controles se destina a identificar todas as atividades de controle, classificando-as quanto à função, freqüência em que o controle é realizado, tipo de controle manual, controle preventivo, estágio da implementação, detalhamento do controle segundo as melhores práticas COSO. Essa matriz está dividida em subprocessos: planejamento e organização, aquisição e implementação, entrega e suporte e monitoramento.

A conformidade regulatória é tarefa normalmente onerosa e depende da natureza da empresa e de seu porte; ainda é necessária a submissão a regras estabelecidas por padrões reconhecidos no mercado. É mais fácil demonstrar a conformidade requerida pela regulação se houver um *framework* de controle baseado em padrões aceitos.

O mercado está cada vez mais competitivo, usuários e clientes mais exigentes, aspectos regulatórios sendo cobrados, entre outros. Assim, o casamento entre a necessidade do negócio e a área de TI tornou-se inseparável, para que a empresa alcance seus objetivos.

No caso da operadora em destaque, o *framework* de controle seguido pela área de TI é o COBIT, que tem o propósito de assegurar que os recursos de TI estarão alinhados com os objetivos da organização, focalizando a Governança de TI e, por conseguinte, a Governança Corporativa.

3.2 *FRAMEWORK* COBIT

3.2.1 História e evolução

O *framework* COBIT volta-se para a gestão de TI e foi recomendado pelo *Information Systems Audit and Control Foundation* (ISACF) (ISACA, 1999). Sua primeira publicação remonta a abril de 1996 e enfoca o controle e a análise dos sistemas de informação. Em 1998, à segunda edição, adicionou-se o guia prático de implantação e execução; a terceira consistiu em desenvolver o *Management Guidelines* ou Diretrizes Gerenciais e atualizar a segunda edição, com base em novas e revisadas referências internacionais. Além disso, o *framework* foi revisado e ampliado para suportar o controle gerencial, introduzir o gerenciamento de desempenho e desenvolver ainda mais a governança de TI. A quarta edição foi publicada em 2005, tendo sua ênfase na governança de TI. Essa edição gerou uma redução nos objetivos de controle da edição anterior e também a modificação no nome de um dos domínios do *framework.* O COBIT 4.1 é a versão mais atual e foi construído sobre diretrizes práticas de gerentes de todo o mundo que utilizam o framework para melhorar a governança de TI em suas organizações.

O COBIT fornece um detalhado conjunto de procedimentos e de diretrizes, que devem ser aplicados na auditoria dos processos de TI, bem como uma avaliação dos riscos e das probabilidades de suas ocorrências (ISACA, 2005).

As práticas de gestão do COBIT auxiliam a otimização dos investimentos em TI e fornecem métricas para a avaliação dos resultados, por meio de um conjunto de recursos. O COBIT compreende um sumário executivo, um *framework*, o controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implantação e um guia com técnicas de gerenciamento (IT GOVERNANCE INSTITUTE, 2005).

3.2.2 Composição do COBIT

Os produtos COBIT estão organizados em três níveis projetados para suportar: a Diretoria Executiva, a Gerência de TI e de Negócio e profissionais de governança, garantia, controle e segurança.

A família COBIT é composta de vários produtos. A figura 3.1 apresenta estes componentes.

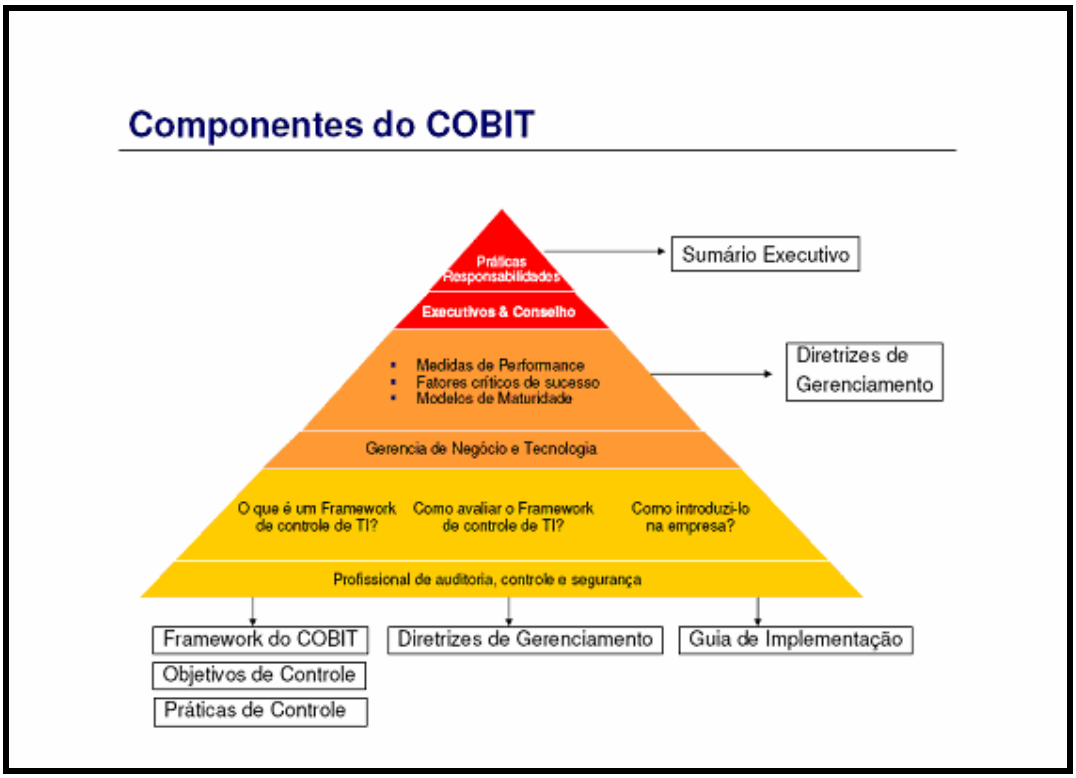

Figura 3.1- Produtos do COBIT
Fonte: Adaptado de ISACA (2005)

O Sumário Executivo, como o nome sugere, é um resumo geral do modelo, dos conceitos-chaves, da história e da evolução, do projeto de concepção, da motivação do desenvolvimento e, em resumo, o que é o COBIT. Sua finalidade é possibilitar uma avaliação rápida do modelo pelos executivos, gerentes e demais interessados, por meio de informações concisas e relevantes.

As diretrizes de gerenciamento são ferramentas orientadas à ação e visam a fornecer, à administração, informações sobre a organização e sobre os processos associados ao controle. A finalidade é monitorar o atendimento dos objetivos organizacionais e o desempenho de cada processo de TI, servindo de referência para as respectivas ações. Para apoiar as necessidades da organização nesse sentido, as diretrizes de gerenciamento do COBIT possuem indicadores de fatores críticos de sucesso, de metas, de desempenho e também um modelo de maturidade associado para a governança de TI.

O guia de implementação é um conjunto de ferramentas de suporte, de relatos de lições aprendidas por organizações que aplicaram o COBIT rapidamente e com sucesso. As práticas orientam os controles que devem ser priorizados e a respectiva implementação. Traduzem os objetivos de controle do COBIT de forma detalhada e fornecem os argumentos para a implantação do negócio, a partir de uma perspectiva de valor e de risco. Práticas de controle

são mecanismos-chave que suportam: a realização dos objetivos de controle e a prevenção; a detecção e a correção de eventos indesejáveis. As práticas de controle são alcançadas com: o uso responsável dos recursos, o gerenciamento apropriado de riscos e o alinhamento da TI com o negócio.

O *framework* explica como os processos de TI entregam as informações conforme as necessidades do negócio, para que a organização alcance seus objetivos. Isso é feito por meio de 34 objetivos de controle de alto nível, um para cada processo. Esses objetivos se encontram nos quatro domínios do COBIT ("PO" para Planejamento & Organização; "AI" para Aquisição & Implementação; "DS" para Entregas & Suporte; "ME" para Monitoramento e Avaliação), identificando que critérios de informação e que recursos de TI são importantes para que seus processos suportem os objetivos de negócio.

Os objetivos evidenciam a importância do controle para otimizar os recursos e os processos de TI em um ambiente constantemente em mudanças. Incluem recomendações para se alcançarem os resultados desejados, implementando 214 objetivos específicos de controle, detalhados ao longo dos 34 controles de alto nível, um para cada processo.

3.2.3 Princípios do *framework*

O COBIT é orientado ao negócio da empresa; fornece informações detalhadas para se gerenciar processos apoiados em objetivos de negócio. Os gerentes devem avaliar o risco e administrar os investimentos em TI. Os usuários precisam de garantias de nível de serviço de TI, das quais dependem os produtos e serviços entregues aos clientes internos e externos. A figura 3.2 demonstra a representação dos princípios básicos do COBIT, em sua seqüência lógica de funcionamento e concomitante interdependência.

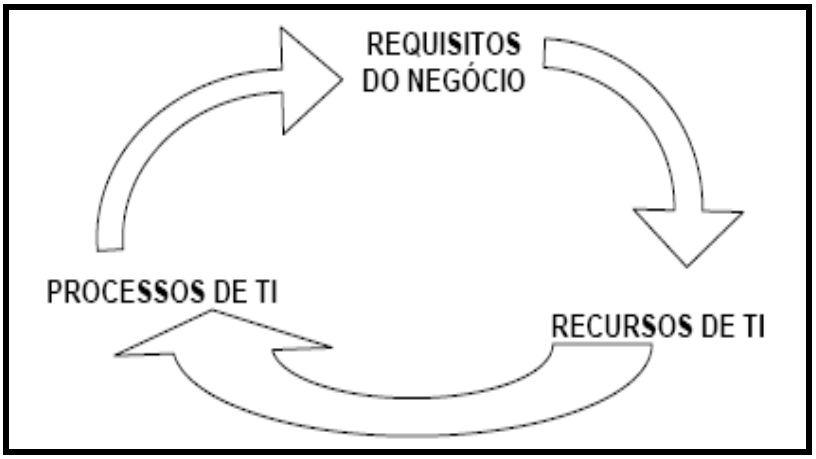

Figura 3.2- Princípios Básicos do COBIT
Fonte: Adaptado de ISACA (2005)

Para satisfazer os objetivos do negócio, a informação deve ser gerenciada segundo critérios especificados pelo COBIT: qualidade, confiança e segurança. Por sua vez, as organizações devem satisfazer os critérios de eficácia, de eficiência, de disponibilidade, integridade, confidencialidade, confiabilidade da informação e conformidade para suas informações. A administração deve também otimizar o uso dos recursos de TI, incluindo dados, aplicativos, tecnologia, instalações e pessoal.

O COBIT parte da premissa de que os processos, critérios da informação e recursos de TI devem estar absolutamente alinhados com os requisitos de negócio, a fim de prover a entrega eficaz da informação para a organização. O modelo conceitual desse *framework* pode ser abordado a partir de três dimensões: (1) critérios de informação, (2) recursos de TI e (3) processos de TI. Esses pontos estão representados no cubo do COBIT (figura 3.3).

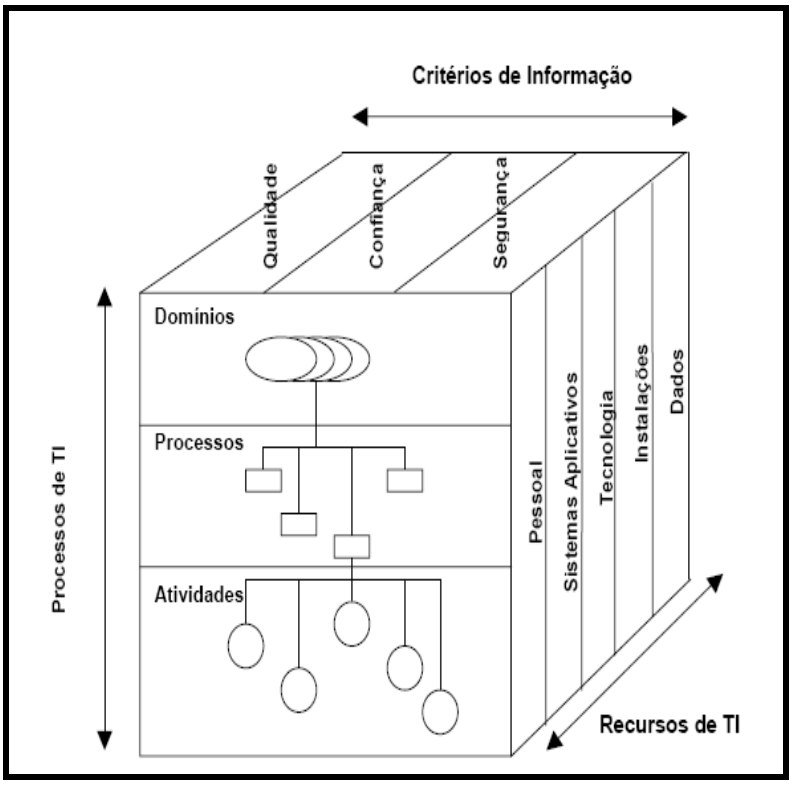

Figura 3.3- Cubo do COBIT
Fonte: Adaptado de ISACA (2005)

A dimensão "critério de informação" diz respeito às exigências do COBIT para cumprimento dos requisitos de qualidade, de confiança e de segurança. Esses critérios são

chamados de requisitos de negócio para informação e representam uma combinação de princípios embutidos em modelos de referência amplamente conhecidos.

A dimensão "recursos de TI" representa os recursos gerenciados pelos respectivos processos, para fornecer informação de que a organização precisa para alcançar seus objetivos. São eles: aplicações: sistemas automatizados e procedimentos manuais para processar informações; informação: os dados de todos os formulários de entrada, processados e exibidos pelos sistemas de informação, podendo ser qualquer formulário que seja usado pelo negócio; infra-estrutura, incluindo *hardware*, sistemas operacionais, sistemas de banco de dados, rede, multimídia e outros necessários ao funcionamento das aplicações; pessoas, que envolve o pessoal necessário para planejar, organizar, adquirir, implementar, entregar, dar suporte, monitorar e avaliar os sistemas de informação e serviços.

A "dimensão processos de TI" está distribuída em quatro domínios:

- Planejamento e organização: cobre o uso da tecnologia e o modo como ela pode ser melhor utilizada na organização, para que os objetivos e metas sejam atingidos. Destaca a organização e a forma como a infra-estrutura de TI está preparada para otimizar resultados e gerar maiores benefícios em seu uso (de TI);
- Aquisição e implementação: aborda a estratégia da empresa na identificação de requerimentos de TI, na aquisição de tecnologia e na implementação dentro dos processos de negócio;
- Entrega e suporte: enfoca os aspectos da entrega da TI. Cobre áreas como: execução de aplicações de sistemas de TI e seus resultados, bem como os processos de suporte que habilitam a execução desses sistemas com efetividade e eficiência. Os processos de suporte incluem objetivos de segurança e treinamento;
- Monitoramento e avaliação: alinha-se à estratégia da empresa; avalia se as necessidades do negócio são atingidas pelos sistemas de TI e se os objetivos de controle cobrem os requerimentos regulatórios. Engloba a auditoria e os objetivos de controles internos e externos e os objetivos de efetividade e de disponibilidade.

A figura 3.4 ilustra a estrutura completa do *framework* com os quatro domínios, onde o ponto central é o gerenciamento da informação com os recursos de TI para garantir o negócio da organização.

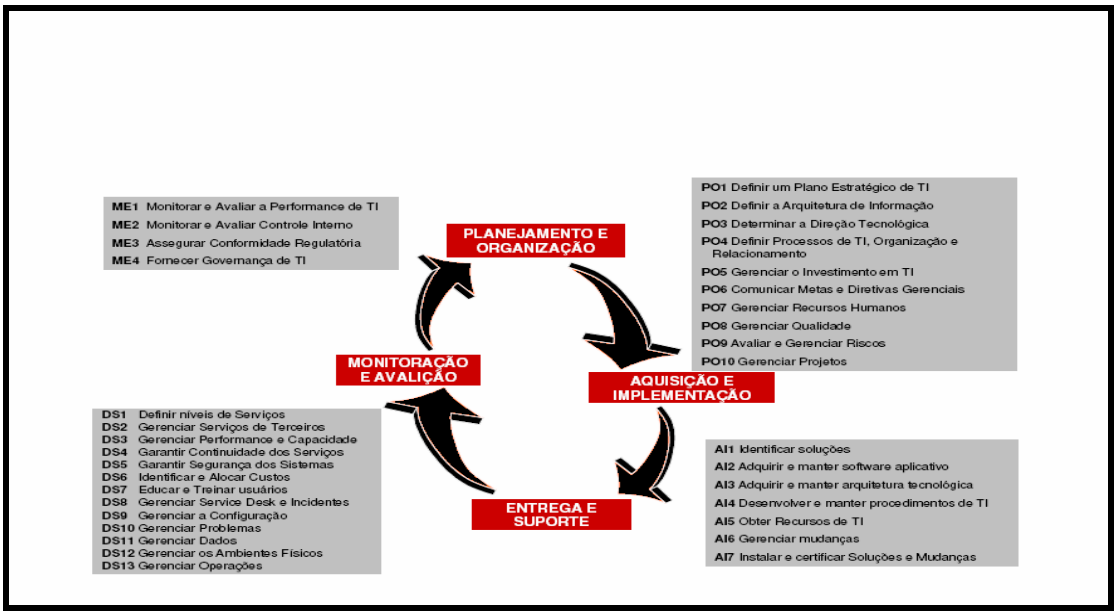

Figura 3.4- Domínios do COBIT
Fonte: Adaptado de ISACA (2005)

3.2.4 Objetivos de controle

Cada processo de TI, no *framework* COBIT, tem um objetivo de controle de alto nível definido, o qual, por sua vez, contém vários objetivos de controle detalhados.

Objetivo de controle de alto nível é a declaração de um resultado desejado, a ser alcançado por meio da implementação de procedimentos de controle dentro de uma atividade de TI específica. Os objetivos de controle detalhados se baseiam em objetivos de controle de alto nível, focando o controle de tarefas-chaves e atividades relacionadas com os processos de TI.

Os domínios do COBIT são subdivididos em processos, cujos objetivos garantem a completude da gestão de TI.

Na figura 3.5, encontra-se representado o domínio do Planejamento e Organização (PO) do COBIT, com dez objetivos de alto nível a cargo das respectivas áreas, os quais servem de referência ao domínio geral do PO.

Figura 3.5- Objetivos de Controle – Planejamento e Organização
Fonte: Apostila COBIT (2006)

Os objetivos de controle de alto nível para cada domínio estão definidos a seguir, segundo as características da área à qual se referem:

– **Domínio planejamento e organização (PO) e áreas de responsabilidade:**

- PO1: define a estratégia de TI; clarifica e formaliza, por meio de um plano estratégico, onde a organização pretende chegar, vinculando as diretrizes de TI às necessidades do negócio;
- PO2: define a arquitetura da informação; descreve como a organização dos sistemas de informação é suportada pela manutenção de um modelo de informações de negócio e pela garantia de que os sistemas são apropriados e são definidos para otimizar o uso de informações;
- PO3: é a visão de futuro da tecnologia e de adesão a padrões; determina sua direção;
- PO4: define a organização de TI e seus relacionamentos; estabelece a estrutura da área de TI, o plano de carreira, os cargos e seus papéis e os relacionamentos com as outras áreas da organização;
- PO5: gerencia os investimentos de TI; avalia o retorno dos investimentos, contabiliza o custeio e os investimentos e os apropria por centro de custos;
- PO6: gerencia a comunicação das diretrizes de TI; desenvolve e implanta planos de comunicação que visam disseminar o conhecimento das estratégias de TI em toda a organização;

- PO7: gerenciam os recursos humanos, desde o recrutamento, contratação e capacitação da equipe em relação ao negócio e às tecnologias que compõem a diretriz tecnológica;
- PO8: gerencia a qualidade; observa a qualidade da entrega dos *softwares* e a utilização de modelos;
- PO9: avalia os riscos; analisa ameaças, impactos no negócio e vulnerabilidades da informação e das instalações, bem como a probabilidade das respectivas ocorrências;
- PO10: gerencia os projetos; administra os projetos de TI, observando modelos e melhores práticas de mercado.

– **Domínio aquisição e implementação (AI) e áreas de responsabilidade:**

- AI1: identifica as soluções de automação; analisa as necessidades de automação dos processos de negócio;
- AI2: adquire os *softwares* e provê sua manutenção; define e aplica modelos de avaliação para a contratação de *softwares;*
- AI3: adquire equipamentos da infra-estrutura tecnológica e provê sua manutenção; desenvolve modelos de avaliação dos equipamentos e de serviços de infra-estrutura;
- AI4: desenvolve procedimentos para a operacionalização da TI e provê sua manutenção; cuida das descrições formais dos processos da área e promove treinamento para garantir o uso apropriado e a operação dos sistemas e infra-estrutura;
- AI5: obtém recursos de TI; também responde pela obtenção de recursos de pessoal, *hardware*, *software*, seleção de fornecedores, contratos e outros;
- AI6: gerencia mudanças; avalia e aprova mudanças no ambiente de TI, tanto em equipamentos e arquitetura como em sistemas e processos;
- AI7: instala e valida soluções; homologa os novos sistemas que necessitam ser colocados em operação, após concluído o respectivo desenvolvimento. Para tanto, é necessário teste em um ambiente apropriado.

Domínio entrega e suporte (DS) e áreas de responsabilidade:

- DS1: define e gerencia acordos de níveis de serviço (SLA) e provê sua manutenção;
- DS2: gerencia os serviços de terceiros; acompanha e avalia os serviços contratados;

- DS3: gerencia o desempenho e a capacidade do ambiente; define os recursos computacionais, garante o suprimento das necessidades desses e sua total utilização, evitando problemas de desempenho nas aplicações ou desperdício de investimentos;
- DS4: assegura a continuidade de serviços; implanta arquiteturas computacionais de alta disponibilidade, que visam à manutenção dos sistemas e a processos operacionais, reduzindo o impacto de sua indisponibilidade sobre o negócio;
- DS5: responde pela segurança dos serviços; visa à preservação da confidencialidade, da integridade e da disponibilidade na prestação dos referidos, garantindo que somente pessoas autorizadas possam ter acesso à informação, a sua exatidão e completude, e que, quando necessário, a informação estará disponível;
- DS6: aloca custos, correlacionando as despesas e investimentos de TI com os devidos centros de custos;
- DS7: responde pelo treinamento de usuários;
- DS8: gerencia incidentes; registra e acompanha todos os incidentes no ambiente de sistemas e infra-estrutura, por meio de uma central de serviços, *Service Desk;*
- DS9: gerencia a configuração do inventário de TI; provê a manutenção do banco de dados de configuração de *hardware*, *software* e demais itens de configuração;
- DS10: administra problemas; área responsável pela identificação, classificação, análise e solução de problemas. Um efetivo processo de gerenciamento de problemas melhora os níveis de serviço, reduz os custos e atende a satisfação do cliente;
- DS11: gerencia os dados; define o modelo de dados e o ciclo de vida da informação, especificando prazos para sua manutenção, segundo os requisitos do negócio e a legislação pertinente;
- DS12: gerencia a infra-estrutura; administra, desenha e planeja essa estrutura, fornece suporte técnico, focado nos desafios da infra-estrutura de TI;
- DS13: gerencia as operações; administra o funcionamento das operações de TI.

Domínio Monitoramento e Avaliação (ME) e áreas de responsabilidade:

- ME1: monitora e avalia o desempenho de TI; processo que abrange a definição de indicadores de desempenho, com um sistemático e objetivo relatório de desvios e da pronta ação sobre eles;

- ME2: analisa e monitora a adequação dos controles internos; responsável pelo monitoramento do controle interno, garantindo operações eficientes, efetivas e em conformidade com as leis e com os regulamentos aplicáveis;
- ME3: assegura o cumprimento de normas regulamentares; seu propósito é garantir a conformidade com as leis e regulamentos relacionados a TI;
- ME4: provê governança de TI; responde pelo estabelecimento de uma estrutura de governança efetiva, abrangendo a definição de estruturas organizacionais, processos, liderança, papéis e responsabilidades, visando a assegurar que os investimentos em TI sejam alinhados e segmentados com as estratégias e objetivos da empresa.

O COBIT promove a organização das atividades de TI em torno de processos e fornece um modelo para as organizações adotarem ou adaptarem a suas atividades, se necessário. Após a definição dos processos, eles podem ser delegados a colaboradores e gerentes que são responsáveis por eles e deverão prestar contas pelo respectivo desempenho. Com essa estrutura implementada, as atividades de TI podem ser mais bem entendidas, organizadas e mais fáceis de controlar.

3.2.5 Mapeamento dos objetivos de controle do COBIT e PCAOB

A Lei Sarbanes-Oxley impôs à *United States Securities and Exchange Commission* (SEC, 1934) a obrigação de regulamentar a coibição de práticas ilícitas dentro das organizações na elaboração dos relatórios financeiros. A SEC criou o *Public Company Accounting Oversight Board* (PCAOB, 2002), órgão encarregado de fiscalizar as companhias abertas e as empresas de auditoria, e esse recomendou a adoção da estrutura de controles internos definidos e apresentados pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, 1985). Entretanto, o COSO elaborou uma definição comum de controles internos voltados para a transparência na elaboração dos controles internos, não sendo muito detalhado e objetivo para aplicação de controles na área de TI. Para cobrir essa lacuna, os auditores buscaram no *Control Objectives for Information and related Technology* (COBIT, 1992) a estrutura de controle mais adequada para estabelecer objetivos de controle para a área de TI.

Os controles básicos estabelecidos pelo PCAOB para a área de tecnologia da informação (*IT Control Objectives for Sarbanes-Oxley*, 2006) são:

- **Ambiente de TI** – Refere-se ao processo de governança de TI, ao planejamento estratégico em relação aos sistemas de informação, ao processo de gerenciamento de

risco de TI, aos processos regulatórios, às políticas de segurança, aos procedimentos e padrões;

- **Operações computacionais** – Referem-se à definição, à aquisição, à instalação, configuração, integração e manutenção da infra-estrutura de TI;
- **Acesso a sistemas e dados** – São controles efetivos de senhas, criptografia, regras de firewall, termos de exceção para usuários genéricos e sistemas integrados com o metadiretório da empresa ilustram alguns procedimentos que devem ser adotados para efetivação deste controle;
- **Mudança na infra-estrutura e em sistemas** – O desenvolvimento de novas aplicações, a entrada de novos produtos em produção, a manutenção preventiva ou corretiva de um servidor, de um banco de dados, a atualização de versão de um aplicativo ilustram atividades corriqueiras no ambiente tecnológico de uma empresa. Para executá-las com segurança, são necessários controles para mitigar o impacto no negócio. Para reduzir o risco durante a execução de algumas destas tarefas, empresas adotam uma metodologia para gerenciar mudanças ocorridas no ambiente, sejam estas sistêmicas ou de infra-estrutura.
- **Desenvolvimento de Sistemas** – Refere-se ao processo de desenvolvimento de novas aplicações ou aquisição de sistemas. O estabelecimento desse controle tem como objetivo garantir que os sistemas desenvolvidos estejam alinhados com as expectativas dos usuários, que as necessidades de negócio da empresa sejam atendidas dentro do orçamento estabelecido e que a implementação atenda também o tempo estabelecido para este desenvolvimento. Metodologia de desenvolvimento, contratos, acordo de níveis de serviço são peças essenciais para este controle.

Em abril de 2004, o instituto de Governança de Tecnologia da informação (*IT Governance Institute*) publicou um documento com diretrizes específicas para a implementação dos controles internos na área de Tecnologia da Informação, *The Role of IT in the Design and Implementation of Intenal Control Over Financial Reporting*. A proposta era compartilhar informações do processo de adequação dos controles de TI para atendimento à Sarbox e à criação de um guia contendo as melhores práticas para atingir a conformidade legal. Uma das contribuições desse documento é um comparativo dos controles estabelecidos pelo PCAOB e os objetivos de controle do COBIT. A figura 3.6 ilustra essa contribuição.

Mapeamento PCAOB - COBIT					
	COBIT	PCAOB - Controles de TI			
Controles de TI - SOX	**Processos COBIT 4.0**	**Desenv. de Sistemas**	**Mudanças em sistemas**	**Operações Computacionais**	**Acesso a sistemas/dados**
1.Adquirir e manter Software/Aplicação	AI2	o	o	o	o
2.Adquirir e manter infra-estrutura Tecnológica	AI3	o	o	o	o
3.Desenvolver procedimentos para operacionalização de TI	AI4	o	o	o	o
4.Instalar e validar soluções e mudanças	AI7	o	o	o	o
5.Gerenciar Mudanças	AI6	o	o	o	o
6.Definir e gerenciar níveis de serviço	DS1	o	o	o	o
7.Gerenciar Serviços de Terceiros	DS2	o	o	o	o
8.Garantir a segurança dos sistemas	DS5	o	o	o	o
9.Gerenciar Configuração	DS9	o	o	o	o
10.Gerenciar Problemas e Incidentes	DS8 eDS10	o	o	o	o
11.Gerenciar dados	DS11	o	o	o	o
12.Gerenciar o ambiente físico e gerenciar operações	DS12 e DS13	o	o	o	o

Figura 3.6- Mapeamento PCAOB – COBIT
Fonte: Adaptado de *IT Control Objectives for Sarbanes-Oxley* (2006)

3.3 - DEFINIÇÕES DOS CONTROLES INTERNOS DA ÁREA DE OPERAÇÕES DE TI

O Caderno 21 da empresa baseou-se e foi segmentado segundo os domínios do *framework* COBIT 3.0, ou seja: planejamento e organização, aquisição e implementação, entrega e suporte e monitoração. O domínio no qual se concentram as atividades de controle de responsabilidade da área de operações de TI é o de entrega e suporte (DS). Entre suas responsabilidades estão as entregas reais dos serviços de TI, alinhadas aos requisitos de negócio da empresa, que constituem seu escopo principal.

O domínio aquisição e implementação também possui atividades de controle de responsabilidade da área de operações de TI. O processo Gerência de Mudanças (AI6-ISACA-COBIT 3.0) pertence a esse domínio, e a área de gestão de mudanças faz parte da estrutura organizacional da área de operações de TI, evidenciando assim a exigência desse objetivo de controle de alto nível.

Finalizado o mapeamento dos processos críticos da empresa e a identificação das aplicações envolvidas, o escopo de responsabilidades relativas à área de TI foi definido e desmembrado nas seguintes atividades de controle: controle de acesso lógico; segregação do ambiente de produção; revisão e adequação das políticas de *backup*; formalização de processos críticos de TI; e plano de contingência e recuperação de desastre. Tais atividades encontram-se abaixo caracterizadas:

3.3.1 Controle de acesso lógico

Consiste na revisão e na adequação das contas de usuários e privilégios de acesso, contemplando as camadas de aplicação, os banco de dados e os sistemas operacionais. Inclui a padronização e a adequação das contas de usuários; a revisão das contas de usuários com privilégios de administrador; a revisão periódica dos acessos concedidos; a eliminação de usuários genéricos; a eliminação de usuários e de colaboradores desligados da empresa; os parâmetros padrões de expiração e de configuração de senhas; a integração das aplicações ao metadiretório da empresa e a análise de relatórios e de alarmes de identificação de violações ou tentativas de acesso não autorizadas aos sistemas.

Para suportar esse controle, os seguintes componentes obrigatórios são envolvidos no processo:

- Ativo de informação: todos os dados, informações, aplicações, sistemas, equipamentos de rede, centrais telefônicas, *hardware*, *software* e *firmware* utilizados pelas entidades da companhia, quais sejam: coligadas, controladas e terceiras indicadas. Também se refere a informações de qualquer forma, documentação, enunciados de controle de tarefas, controle de *jobs*, código fonte, código objeto e quaisquer utilitários necessários para suporte;
- Ativos de informação de uso corporativo: conjunto de ativos que provêem serviços e suporte à corporação, bem como a suas controladas e coligadas;
- Gestor do ativo: pessoa detentora da responsabilidade por um serviço, produto, informação, aplicação, sistema ou tecnologia providos pela área de negócios ou de infra-estrutura;
- Usuário: qualquer entidade com acesso a ativos de informação da empresa e/ou de suas afiliadas ou coligadas;
- Usuário ativo: trata-se daquele que possui contrato de fornecimento de serviços vigentes e que, por contrato, deve ter acesso aos ativos de informação da operadora. Inclui aqueles que não estão em situação de afastamento;
- Metadiretório: serviço centralizado para armazenamento e integração de informações de identidade digital na organização.

Esses controles têm como objetivo assegurar que o acesso aos ativos de informações seja limitado apenas àqueles que necessitem dessas informações e restrito à respectiva função. Além disso, responsabiliza os usuários pelas ações de acesso.

O controle de acesso lógico é função de um processo muito importante na empresa, que é o gerenciamento de identidade digital integrada. Este consiste em fornecer uma visão única do usuário na organização, permitindo o gerenciamento de identidades, a autenticação, permissões aos usuários, auditoria e rastreabilidade de informações de um determinado usuário. Tal visão é suportada pela integração das aplicações ao metadiretório master da empresa, sendo esse um serviço centralizado para armazenar e integrar as informações de identidade digital da organização.

O processo de concessão de acesso engloba as seguintes etapas: solicitação, aprovação e liberação do acesso lógico ao colaborador ou terceiro. O gestor da aplicação e a gerência imediata do colaborador respondem pela aprovação da referida solicitação de acesso, avaliando a necessidade e o perfil solicitado. Os perfis de acesso resultam da delegação de atividades aos subordinados, pelo gestor de cada área, conforme as atribuições previstas no organograma da empresa.

Os sistemas de informação críticos ou vitais para o negócio devem estar em conformidade com os requisitos mínimos de controle de acesso estabelecidos na Política de Segurança da Informação, assim como a concessão e a gerência de privilégios de acordo com os perfis de usuários. Todos os procedimentos elaborados para esse controle foram baseados na Norma Brasileira de Referência (NBR) ISO/IEC 17799, de 2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação da Associação Brasileira de Normas Técnicas (ABNT).

3.3.2 Segregação do ambiente de produção

Esse controle engloba as seguintes ações:

- Segregação física dos ambientes: tem como objetivo principal garantir que todos os acessos ao prédio e às salas de ativos do ambiente de produção, nas quais se encontram hospedadas as aplicações Sarbox, sejam controlados, com registros e autorizações formais de acesso. Prevê a necessidade de revisão periódica no sistema de controle de acesso físico, visando a mitigar qualquer falha que possa ocorrer. As autorizações ou revogações de acesso a esses ambientes devem ser efetuadas pelo gestor do ativo, via sistema, registrando no livro de visitas a evidência da solicitação de acesso. Em caso de desligamento de usuários, esse controle se torna mais rigoroso, pois é expressamente proibida a entrada de usuários desligados às dependências onde se encontram os recursos relativos a essas aplicações;
- Acesso lógico ao ambiente de produção: implementação de segregação de funções por meio da restrição de acesso ao ambiente de produção pelos analistas de desenvolvimento e gestores não autorizados nas aplicações Sarbox;
- Processo de modificação em aplicações em produção: revisão de pedidos de manutenção e de alteração em aplicações gerenciadas pelas Unidades de Implementação e Manutenção e pela área de operações de TI.

Para adequar o desenvolvimento de novas aplicações, novas entregas e manutenções, esse controle tem como objetivo principal garantir a segurança dos sistemas envolvidos. A segregação do ambiente é feita através da identificação e da negociação dos requisitos de segurança antes de o desenvolvimento do sistema, do módulo ou da melhoria ser iniciado.

Para implementação da segregação física do ambiente de produção dos demais ambientes, foram criadas normas e procedimentos padrões, que se encontram divulgados no portal de documentos normativos da empresa, do qual constam todas as atividades necessárias

para garantir a segurança de ambientes de desenvolvimento, homologação e produção. Para tanto, alguns aspectos devem ser seguidos com rigor:

- Proprietários são responsáveis pelos sistemas e pela segurança aplicada aos ambientes de desenvolvimento, aceite e produção;
- Ambientes de desenvolvimento, de homologação e de produção não devem coexistir em um mesmo equipamento e, caso seja possível, em um mesmo domínio. Nesse último caso, não deve haver possibilidade de acesso entre os domínios ou compartilhamento de informações;
- Novos sistemas ou funcionalidades desenvolvidos só podem ser usados pelos usuários após um teste, em ambiente de homologação, dos requisitos de segurança.

Esse controle fornece, como principal benefício, a proteção da empresa contra fraudes internas, na adoção de segregação de funções e, também o estabelecimento de controles e a revisão da delegação de autoridade e aprovações.

3.3.3 - Revisão e readequação das rotinas de *backup*

Esse controle consiste em um trabalho conjunto realizado entre gestores da aplicação e da área de operações de TI. O objetivo é validar os dados a serem copiados por parte dos gestores e a formalização do aceite, através de um termo de ambas as partes. Integram esse processo a padronização da ferramenta de agendamento das rotinas e o aprimoramento das atividades de monitoramento e correções de eventuais erros.

Como ações para subsidiar esse controle, pode-se citar:

- Elaborar procedimentos formalizados para a realização de *backups*, conforme definição de criticidade e periodicidade definida;
- Incluir os procedimentos formalizados em rotinas de execução automática de cópias de segurança nas ferramentas de *backup* da empresa, segundo os critérios definidos;
- Definir modelo de rotulagem de fitas e/ou denominação dos arquivos de segurança;
- Mapear os sistemas e dados significativos na recuperação de informações históricas;
- Identificar localidades de armazenamento de fitas mais críticas em relação à degradação dos meios de armazenamento (ex- filiais);
- Elaborar plano de teste para recuperação de dados históricos da empresa, considerando critérios para a seleção de amostras;
- Identificar falhas durante a restauração da informação, analisando a origem e a idade das fitas testadas;

- Ampliar os testes, para verificar o grau de degradação dos meios de armazenamento;
- Avaliar o grau de degradação das fitas e elaborar plano de ação para sua recuperação, caso necessário, para fins de atendimento à legislação vigente.

Há dois aspectos primordiais para a recuperação de informações e serviços chaves de uma empresa. São eles:

- A recuperação da integridade operacional do ambiente, que é definida como o conjunto de ações desencadeado pela identificação de um desvio operacional na infra-estrutura de *hardware* e de *software* e tem por objetivo a recuperação do ambiente, inclusive dados corporativos, no exato momento anterior ao desvio;
- A recuperação do fluxo de negócio da corporação e manutenção da memória legal, definida como o conjunto de ações desencadeado pela identificação de uma necessidade de negócio ou necessidade legal. Visa a obter acesso a arquivos históricos criados a partir das bases de dados operacionais e mantidos em segurança pelos procedimentos de guarda e recuperação.

A missão do *backup* corporativo da área de operações de TI da operadora é "Recuperar a integridade operacional do ambiente de TI, sempre que se fizer necessário". Cumprir essa missão requer processos bem desenhados, avaliação de risco bem elaborada, impactos quantificados e, principalmente, uma definição de quais são os dados críticos necessários para recuperação da integridade operacional do ambiente.

3.3.4 - Formalização dos processos críticos de TI

Avaliaram-se os riscos de cada área da empresa com os possíveis impactos que eles pudessem causar nas demonstrações financeiras e definiram-se os objetivos de controle para cada atividade da empresa.

Por meio de trabalhos entre os gestores das aplicações envolvidas (áreas de negócios) e a área de tecnologia da informação, houve a definição de 44 sistemas identificados como críticos para a empresa. Tratam-se de aplicações formalizadas e de todos os controles solicitados pela Sarbox, a elas aplicados. Como produtos desse controle foram feitas a revisão e publicação da política de segurança de informações; desenvolvimento e publicação de dez novas normas; revisão e publicação de 31 procedimentos e, também, a publicação de 28 novos procedimentos, no ano de 2006.

Para adequar as 44 aplicações, o banco de dados e outros componentes envolvidos nesse controle, foram elaboradas normas e criados procedimentos padrões, que também se

encontram no portal de documentos normativos da empresa. No portal, estão relacionadas todas as atividades necessárias para a solicitação, avaliação e concessão de acesso lógico aos usuários dos sistemas e recursos de informação. A figura 3.6 ilustra os processos da Sarbox, mapeados como elegíveis.

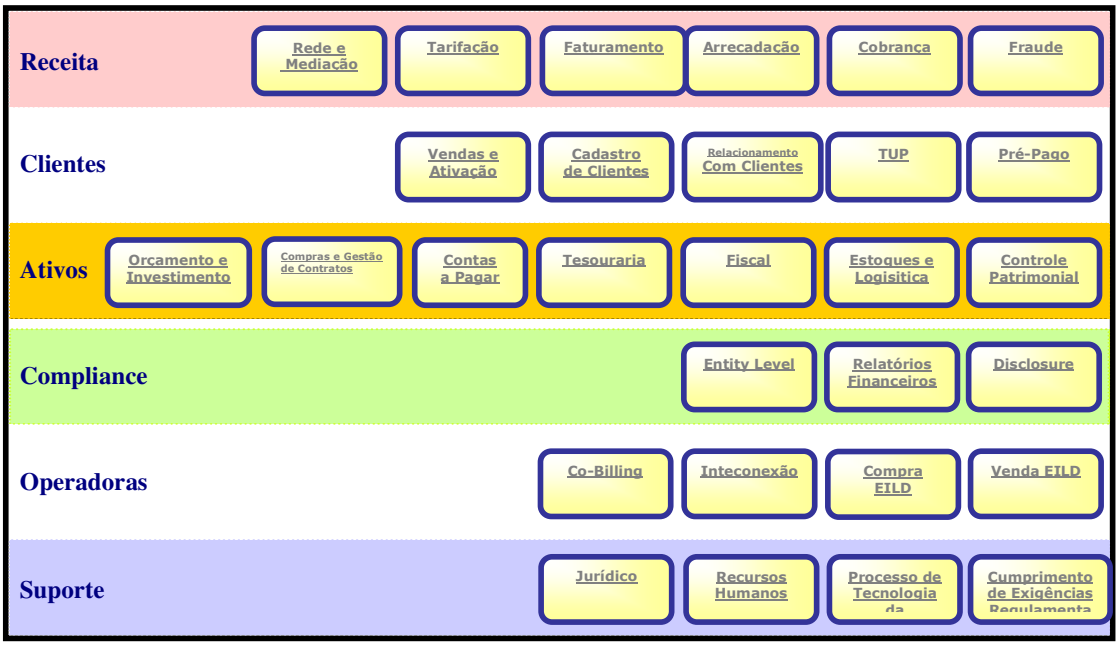

Figura 3.7: Processos mapeados na empresa
Fonte: CNASI (2007)

3.3.5 – Plano de contingência e recuperação de desastre

O plano de contingência e de recuperação de desastre refere-se ao desenvolvimento, à implementação e ao teste de um plano, envolvendo a infra-estrutura de tecnologia para as aplicações da Sarbox, que tem como objetivo principal minimizar o risco de interrupções ou de indisponibilidade dos dados processados nessas aplicações.

Uma das diretrizes do plano baseia-se na alta disponibilidade e continuidade do negócio dos sistemas de TI. Esse plano é definido como um conjunto de procedimentos previamente definidos e testados, para garantir a continuidade dos processos e serviços vitais a uma organização, mesmo sob o impacto de desastre súbito e inesperado.

O plano de contingência das 44 aplicações da Sarbox explicita os procedimentos necessários à contingência local e à recuperação de desastres para todas as aplicações priorizadas nas adequações à citada Lei. Esse plano tem o seguinte escopo: abrangência e grau de criticidade das aplicações; componentes de infra-estrutura envolvidos; procedimentos de

contingência local; procedimentos de recuperação e desastre; procedimentos de retorno à situação original; procedimentos de escalação e outros.

O escopo de contingência e de recuperação de desastres das aplicações prioritárias Sarbox devem ser tratados conforme sua criticidade. No geral, as aplicações de alta criticidade devem possuir recursos definidos para contingência local e recuperação de desastres. Já as aplicações de média e baixa criticidade apenas devem possuir infra-estrutura dedicada à contingência local. Para uma solução atender os requisitos de continuidade do negócio, quanto à infra-estrutura de TI, é necessário garantir, além da alta disponibilidade, a existência de um segundo local que suporte a operação dos sistemas, no caso de indisponibilidade do site primário.

O plano de contingência e de recuperação está integrado diretamente aos processos de negócio da organização, e seu objetivo principal é fornecer, em um período aceitável, os recursos necessários à operação dos processos críticos de negócio na ocorrência de desastres. Para que as atividades de controle estabelecidas fossem implantadas, a área de operações de TI efetuou o mapeamento da infra-estrutura relacionada às 44 aplicações eleitas pela Sarbox. O estudo contemplou os componentes básicos de cada solução, como: camada WEB, camadas de aplicações, de banco de dados e infra-estrutura de energia, ar condicionado, rede de dados, rede SAN e armazenamento que suportam estes sistemas.

3.4- MAPEAMENTOS DOS CONTROLES DA ÁREA DE OPERAÇÕES DE TI SEGUNDO O *FRAMEWORK* PCAOB x COBIT

O gerenciamento de serviços de TI é, resumidamente, o gerenciamento da integração de pessoas, processos, tecnologias e componentes de um serviço de TI. Seu objetivo é viabilizar a entrega e o suporte dos respectivos serviços, focados nos requisitos de negócio e visando ao alcance de objetivos estratégicos, a partir do estabelecimento de acordos de nível de serviço entre a área de TI e as demais áreas de negócio da organização.

A conformidade com a Sarbox tem um impacto significativo sobre a estrutura de TI da maioria das empresas com papéis na bolsa de valores. No entanto, para área de tecnologia da informação, não havia menção específica, na seção 404 dessa lei, aos controles para a estrutura de TI. Para sanar essa limitação, o comitê gestor da Sarbox consultou o PCAOB sobre o *framework* de controle de TI adequado para tal. Após estudos sobre os *frameworks* de controle existentes no mercado, o PCAOB definiu-se pelo COBIT.

O documento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting* (IT Control Objectives for Sarbanes-Oxley, 2006) mostra o elo entre a

seção 404 e o COBIT. Baseado nele, fez-se uma correlação entre os controles estabelecidos para área de operações de TI da empresa, as recomendações originadas do alinhamento do *framework* COBIT e os objetivos a serem avaliados pelo PCAOB. A figura 3.8 ilustra este mapeamento, destacando, em amarelo, objetivos de controles detalhados que se aplicam aos controles da área de operações de TI. Destaque-se que, para este estudo, foi utilizado o COBIT 4.1.

Mapeamento PCAOB - COBIT					
	COBIT	PCAOB - Controles de TI			
Controles de TI - SOX	Processos COBIT 4.0	Controle de Acesso	Segregação Ambiente Produção	Backup	Plano de contingência e recuperação
1.Adquirir e manter Software/Aplicação	AI2	AI2.3 e AI2.4	AI2.3,AI2.4 e AI2.10		
2.Adquirir e manter infra-estrutura Tecnológica	AI3	AI3.2	AI3.2		
3.Desenvolver procedimentos para operacionalização de TI	AI4	AI4.2 e AI4.4	AI4.2 e AI4.4	AI4.2	
4.Instalar e validar soluções e mudanças	AI7	AI7.6, AI7.7,	AI7.6,AI7.8,AI7.10	AI7.5 e AI7.7	
5.Gerenciar Mudanças	AI6	AI6	AI6	AI6	
6.Definir e gerenciar níveis de serviço	DS1	DS1.3	DS1.3	DS1.3	DS1.3
7.Gerenciar Serviços de Terceiros	DS2	DS2.3			
8.Garantir a segurança dos sistemas	DS5	DS5.3 e DS5.4	DS5.3 e DS5.4		
9.Gerenciar Configuração	DS9				
10.Gerenciar Problemas e Incidentes	DS8 eDS10			DS8	
11.Gerenciar dados	DS11	DS11.6	DS11.6	DS11.3,DS11.4,DS11.5,DS11.6	
12.Gerenciar o ambiente físico e gerenciar operações	DS12 e DS13		DS12.1,DS12.2,DS12.3,DS12.4, DS12.5		

Figura 3.8- Mapeamento PCAOB – COBIT e Controles de Operações de TI
Fonte: Adaptado de *IT Control Objectives for Sarbanes-Oxley* (2006)

3.4.1 Controle de acesso lógico

O controle de acesso lógico está mapeado nos objetivos de controle de alto nível AI2, AI3, AI4, AI6 e AI7, que pertencem ao domínio COBIT – Aquisição e Implementação. Em relação aos objetivos de controles detalhados do AI2, merecem destaque: controle de aplicação e de auditabilidade (AI2.3) e segurança da aplicação e disponibilidade (AI2.4). O controle de aplicação e de auditabilidade é responsável por tratar os mecanismos de autorização, integridade da informação, controle de acesso das aplicações adquiridas, cópia de segurança e esquema de rastreamento de auditoria. (ISACA, 2005). A segurança da aplicação e disponibilidade (AI2.4) aborda a questão do acesso ao *software* adquirido, de maneira que sejam seguidos os requisitos estabelecidos pela área de segurança de informações da organização.Questões a serem levadas em conta incluem direitos de acesso às aplicações e o gerenciamento de privilégios, além da proteção a dados sigilosos e da integridade de autenticação de transação (ISACA, 2005).

Para o controle adquirir e manter a arquitetura tecnológica, AI3, o objetivo de controle detalhado, relacionado com o controle de acesso lógico, é relativo aos recursos de infra-estrutura, de proteção e de disponibilidade (AI3.2). Esse controle implementa medidas de segurança e de auditabilidade durante a configuração, integração e manutenção de *hardware* e *software*. Responsabilidades para utilização de componentes de infra-estrutura que constituem as aplicações críticas da empresa devem estar bem definidas, contemplando a rastreabilidade nas operações executadas nestes recursos.

O controle AI4, nomeado por desenvolver e manter procedimentos de TI, também possui ligação com o controle de acesso lógico, através dos objetivos de controle detalhados: transferência de conhecimento e gerenciamento de negócio (AI4.2) e transferência de conhecimento ao pessoal de operações e suporte (AI4.4). É importante destacar que os dois objetivos de controle tratam de transferência de conhecimento e responsabilidade a para área de operações. Tarefas como transferência do código fonte, controle de acesso aos dados de produção e controle de acesso aos sistemas demonstram a ligação do controle de acesso lógico a este domínio.

Em relação à gerência de mudanças, AI6, o controle de acesso lógico tem como objetivo assegurar que o acesso ao ativo de informação, que está passando por manutenção, seja restrito ao perfil que esteja apto a efetuá-la. Por isso, fez-se o seu mapeamento com o objetivo de estabelecer o controle referenciado pelo PCAOB.

Complementando a ligação do controle de acesso lógico com a gerência de mudanças, esse também foi mapeado no objetivo de controle AI7, ou seja, instalar e certificar soluções e mudanças. Os controles de segurança do ambiente de produção devem ser testados e avaliados durante o processo de entrada de novos códigos, equipamentos e sistemas neste ambiente. O objetivo de controle detalhado AI7.6 ilustra essa necessidade. O Teste Final de Aceitação (AI7.7) também está relacionado com o controle de acesso lógico, pois tem como objetivo garantir que os requisitos de segurança da informação sejam satisfeitos na entrada de novos produtos no ambiente de produção.

O mapeamento do controle de acesso lógico no objetivo de controle DS2 - gerenciar serviços terceirizados - visa fortalecer a exigência de que terceiros prestadores de serviços estejam em conformidade com as regras de segurança estabelecidas pela empresa.

O controle de acesso lógico também está mapeado no objetivo de controle de alto nível DS5, que visa ao gerenciamento da segurança e à proteção de todos os recursos de TI, para minimizar o impacto sobre o negócio, quanto à vulnerabilidade na segurança e respectivos incidentes. O objetivo principal desse controle, segundo o *framework,* é garantir a segurança dos sistemas. No caso da operadora enfocada neste estudo, a finalidade é garantir plataformas, sistemas, bancos de dados e a infra-estrutura envolvida no acesso às 44 aplicações críticas. Em relação aos objetivos de controles detalhados, o controle em destaque encontra-se mapeado em dois objetivos: gerenciamento de identidade (DS5. 3) e gerenciamento de conta do usuário (DS5.4). O gerenciamento de identidade estabelece que todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, operação de sistemas, desenvolvimento e manutenção) devem ser unicamente identificáveis, ou seja, a rastreabilidade é um dos itens essenciais ao processo. Os direitos de acesso dos usuários aos sistemas e aos dados devem estar em conformidade com as necessidades dos negócios e com os requisitos de serviço. Os direitos de acesso dos usuários são solicitados pelos gestores dos recursos e são aprovados e implementados pela área de segurança. As identidades e os direitos de acesso dos usuários são mantidos em um metadiretório (ISACA, 2005).

O objetivo de controle detalhado (DS5.4) assegura que a solicitação, o estabelecimento, a publicação, a suspensão, a modificação e o bloqueio das contas dos usuários e respectivos privilégios sejam efetuados através de um procedimento de aprovação, segundo o qual a um gestor é determinada a responsabilidade pela manutenção dos usuários, por meio da formalização dessas ações. Esse controle executa a revisão gerencial regular de todas as contas e dos respectivos privilégios (ISACA, 2005).

O último mapeamento efetuado foi o do objetivo de controle detalhado DS11.6 , responsável pela aplicação dos requisitos de segurança para processamento, armazenamento, saída de dados e outras operações de manipulação de dados que possam ser efetuadas nas aplicações elencadas como críticas da empresa.

3.4.2- Segregação do ambiente de produção

O controle segregação do ambiente de produção está mapeado nos objetivos de controle de alto nível AI2, AI3, AI4, AI6 e AI7. Esse controle estabelece um processo de gerenciamento do ambiente físico para a proteção de pessoal e dos recursos de TI. Os objetivos de controle detalhados encontram-se mapeados nos seguintes objetivos:

- AI2.3, AI2.4 e AI2.10: controle de acesso aos recursos de TI, proteção à informação armazenada nestes recursos e ao desenvolvimento de um procedimento estratégico para a manutenção e entrada de novos produtos no ambiente de produção;
- AI3.2: medidas de segurança para os recursos de infra-estrutura de TI e sistemas, que são peças-chaves para o controle segregação do ambiente de produção;
- AI4.2 e AI4.4: segurança do ambiente físico e acesso aos ativos de informação, correlacionadas às necessidades da segregação do ambiente de produção;
- AI6: gerenciar mudanças está intimamente ligado ao processo de modificação de código no ambiente de produção - que restringe o acesso dos analistas desenvolvedores e programadores a este ambiente e estabelece a necessidade de procedimentos formais para realização de uma manutenção;
- AI7.6, AI7.8 e AI7.10: complementam o gerenciamento de mudanças, estabelecendo procedimentos de controle para garantir a segurança dos sistemas e efetuando testes de aceitação dos itens. Também segrega deveres, isto é, aqueles que produziram, testaram e operaram possuem perfis de acesso diferenciados.

Outro mapeamento efetuado foi o do objetivo de controle detalhado DS11.6, responsável pela aplicação dos requisitos de segurança para processamento, armazenamento físico, saída de dados e outras operações de manipulação de dados críticos que possam ser efetuadas nas principais aplicações da empresa.

O controle segregação do ambiente de produção está mapeado, também, no objetivo de controle de alto nível DS12, gerenciar a infra-estrutura de TI, no que se refere à segregação física dos ambientes. Esse controle estabelece um processo de gerenciamento do ambiente físico para a proteção de pessoal e dos recursos de TI. Em relação aos objetivos de controles detalhados, ele se encontra mapeado em quatro objetivos:

- DS12.1 - seleção do local e do leiaute: define e seleciona os locais físicos para alocação dos recursos de TI, visando à estratégia tecnológica ligada à estratégia de negócio. A seleção e o planejamento do leiaute de um local devem levar em consideração os riscos associados aos desastres naturais e à ação humana e ainda devem considerar as leis e os regulamentos relevantes, tais como aqueles que regulamentam a saúde e segurança do trabalho na área ocupacional;
- DS12.2 - medidas de segurança física: define e programa as medidas de segurança física, em alinhamento com os requisitos de negócio. As medidas devem contemplar, de forma ilimitada, o leiaute do perímetro de segurança, as zonas de segurança, a localização de equipamentos críticos e as áreas de envio e recebimento desses recursos. As responsabilidades pelo monitoramento e procedimentos de registro e resolução dos incidentes de segurança física precisam ser estabelecidas;
- DS12.3 - acesso físico: define e implementa os procedimentos para conceder, limitar e revogar o acesso aos prédios e às áreas, de acordo com as necessidades do negócio, inclusive por ocasião de emergências. O acesso aos prédios e às áreas deve ser justificado, autorizado, registrado e monitorado. Isso se aplica a todas as pessoas que acessam as áreas, incluindo o pessoal fixo, o pessoal temporário, os clientes, vendedores, visitantes ou qualquer outra parte terceirizada;
- DS12.4 - proteções contra fatores ambientais: planeja e implementa medidas para proteção contra fatores ambientais. Os equipamentos especializados e dispositivos para monitorar e controlar o ambiente devem ser instalados;
- DS12.5 - gerenciamento de ambientes físicos: gerenciar os ambientes, inclusive energia e equipamentos de comunicação, segundo as leis, regulamentos, requisitos técnicos e de negócio, especificações do fornecedor, diretrizes de segurança e saúde.

Para o segundo requisito desse controle, que é o acesso lógico ao ambiente de produção, o objetivo de alto nível DS5 engloba as necessidades, detalhando-as no gerenciamento de identidade (DS5.3) e no gerenciamento de usuários (DS5.4).

3.4.3 – Revisão das políticas de Backups

O controle de revisão das políticas de *backup* está mapeado nos objetivos de controle de alto nível AI4, AI6 e AI7. Em relação aos objetivos de controles detalhados, o controle enfocado está mapeado em quatro objetivos:

- AI4.2: no processo de transferência de conhecimento, as cópias de segurança e o processo de recuperação de dados são controles fundamentais (dados, documentação e código fonte);
- AI.6.1: estabelece procedimentos e padrões formais que devem ser contemplados no processo de mudança, seja ela corretiva, evolutiva ou emergencial. A cópia de segurança é uma das atividades-padrão responsáveis pela guarda do histórico do ativo de informação antes de efetuar uma manutenção;
- AI7.5: sistema de conversão de dados. A relação desse controle detalhado com o controle revisão das políticas de *backup* está na necessidade de fornecimento de dados para suportar a conversão;
- AI7.7: teste final de aceitação. Esses testes devem contemplar todos os componentes do sistema de informação (dados, códigos fonte, procedimentos do usuário, facilidades e equipamentos) em relação aos dados; deve ser efetuada uma cópia de segurança para fins de auditoria e para futuros testes.

Outro mapeamento efetuado para esse controle foi no objetivo de controle detalhado DS8. Apesar de ele não estar diretamente ligado ao backup, é através da central de solicitações e incidentes que são feitos os pedidos para recuperação operacional de um ambiente. Quando há um desvio operacional na infra-estrutura de hardware e de software de TI, a recuperação do ambiente é solicitada pelo cliente através dessa central e o tempo necessário para restauração do ambiente controlado pelo SLA (acordo de nível de serviço) que foi acordo entre cliente e área prestadora do serviço.

O controle de revisão das políticas de *backup* está mapeado também no objetivo de controle de alto nível DS11, que objetiva o gerenciamento de dados O objetivo principal desse controle, segundo o *framework*, é o de gerenciamento de dados, contemplando o estabelecimento de procedimentos efetivos para controlar o catálogo no qual estão armazenados os controles das mídias, a cópia de segurança (*backup*), a recuperação de dados (*restore*) e a disposição da mídia. O efetivo gerenciamento dos dados auxilia a garantia de qualidade, a otimização de tempo de recuperação e a disponibilidade dos dados de negócio (ISACA, 2005). Em relação aos objetivos de controles detalhados, o controle enfocado está mapeado em quatro objetivos:

- DS11.3: sistema de gerenciamento de biblioteca de mídia: define e implementa procedimentos, para manter um inventário de mídia local, para assegurar sua utilização e integridade. Os procedimentos devem propor revisão periódica e acompanhar qualquer discrepância apontada;

- DS11.4: define e implementa os procedimentos para prevenir o acesso aos dados e *softwares* sensíveis, de equipamentos ou de mídias, quando eles são colocados à disposição do usuário ou transferidas a outro usuário. Tais procedimentos devem assegurar que os dados apagados, ou a ser disponibilizados, não possam ser recuperados;
- DS11.5: *backup* e restauração: define e implementa procedimentos para *backup* e restauração dos sistemas, dados e documentação, em conformidade com os requisitos de negócio e do plano de continuidade. Verifica a conformidade com os procedimentos de *backup* e, ainda, a capacidade para proceder à respectiva ação e o tempo necessário para sua restauração bem sucedida e completa;
- DS11.6: requisitos de segurança para o gerenciamento de dados: estabelece mecanismos para identificar e aplicar os requisitos de segurança referentes ao recebimento, ao processamento, ao armazenamento físico, à saída de dados e às mensagens sensíveis. Isso inclui gravações físicas, transmissões de dados e quaisquer dados armazenados remotamente (*offsite*).

3.4.4 – Plano de contingência e recuperação de desastre

A operadora é altamente dependente da infra-estrutura de TI, para poder prover serviços a seus clientes com a qualidade e a eficiência necessárias. Um evento de catástrofe, com potencial que possa causar interrupções de longo período, pode comprometer todos os acordos de níveis de serviços suportados pela área de TI e a cadeia de processos de negócios vinculada a esses serviços. Cada unidade de negócio depende de uma variedade de sistemas que podem ser vulneráveis a um evento de desastre. O resultado de uma parada imprevista pode criar perdas potenciais significativas, com sérios riscos financeiros, além de problemas qualitativos na imagem da empresa no mercado.

O plano de contingência e recuperação de desastre foi elaborado pela Diretoria de Tecnologia e Planejamento Técnico Gerência de Infra-Estrutura de TI. Porém, a gerência de operações de TI possui papéis e responsabilidades bem definidos para concretizar esse plano.

O mapeamento desse controle no objetivo de controle detalhado DS1.3 e dos demais controle Sarbox da área de operações de TI visa demonstrar que a empresa reconhece a extrema importância da proteção de seus ativos para os serviços prestados a seus clientes, bem como a importância do estabelecimento de métodos que possibilitem manter a continuidade de seus negócios e serviços para seus clientes, em caso de desastres.

O objetivo de controle DS1.3 – Acordo de Nível de Serviço - define os acordos de nível de serviço para todos os serviços críticos de TI, abrangendo requisitos de suporte de serviço, métricas quantitativas e qualitativas de aferição dos avisos de suspensão dos serviços, acordos comerciais, escalonamentos e outros. Disponibilidade, confiabilidade, desempenho, capacidade de crescimento, níveis de suporte, tempo de atendimento ao incidente e à solicitação e segurança são itens que compõem esse objetivo.

Não houve mapeamento PCAOB – COBIT para o controle formalização de processos críticos, pois esse é uma avaliação dos sistemas, para garantir o processo de certificação; não é um objetivo de controle a ser trabalhado.

3.5- MAPEAMENTO DOS CONTROLES DA ÁREA DE OPERAÇÕES DE TI SEGUNDO O *FRAMEWORK* PCAOB x COBIT – CONSIDERAÇÕES FINAIS

O Caderno 21 da área de tecnologia da informação está segmentado nos subprocessos de planejamento e organização, de aquisição e de implementação, de entrega e suporte e de monitoração, conforme descrito no item 3.1. No cabeçalho da matriz de controle de cada um do subprocessos, são descritos os riscos de negócio, a probabilidade relativa a esse fator de risco e o item crítico a ser trabalhado, ou seja, o objetivo de controle detalhado a ser verificado durante o processo de certificação para cada área responsável por aquela atividade de controle.

Nesse documento, não há uma segmentação específica segundo as premissas de controle básicas estabelecidas pelo PCAOB (desenvolvimento de sistemas, mudanças em sistemas, operações computacionais e acesso a sistemas e dados) para a área de tecnologia da informação; também não há uma identificação clara em relação ao objetivo de controle detalhado do COBIT 4.1, ao qual a atividade de controle é associada. A segmentação pelos quatro itens elencados pelo PCAOB e a definição do objetivo de controle COBIT ao qual a atividade de controle está vinculada deveriam estar claramente descritos nesse documento, para fornecer uma visão específica da maturidade do processo de certificação. Com a estrutura atual, estabelecida nesse caderno, a visualização dos controles é de acordo com o *status* da atividade, contemplando a situação atual dessa, os responsáveis para efetivação desse controle e o plano de ação a ser realizado, caso necessário.

Como exemplos práticos, abaixo são descritas as atividades de controle direcionadas à área de operações de TI no ano de 2007, durante o processo de manutenção da certificação Sarbox:

- CTTI06 - Mapeamento dos dados críticos dos sistemas e manutenção de *backup* dos dados: o item relativo ao gerenciamento de dados estabelecido pelo documento do PCAOB é muito mais abrangente. O controle DS11 sugerido pelo documento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting* (IT Control Objectives for Sarbanes-Oxley , 2006) possui objetivos de controle detalhados que não estão claramente descritos nesse caderno, como: esquema de armazenamento, sistema de gerenciamento de biblioteca e mídia, requisitos de segurança para o gerenciamento de dados, testes de restauração periódica de dados, tempo de armazenamento de *logs* das cópias de segurança, dentre outros;
- CTTI061 - Restrição de acesso físico ao CPD da companhia ao pessoal autorizado: tem como objetivo (controle DS12) gerenciar o ambiente físico que referencia essa questão; possui objetivos de controles detalhados que não constam do caderno 21. A proteção contra fatores ambientais pode ser citada como um dos principais objetivos de controle detalhados que remete a um dos eventos impulsionadores da criação da Sarbox, o 11 de setembro de 2001. No caso da operadora estudada, o *Cyber Data Center* RS, *Cyber Data Center* SP; Gerência de *Cyber Data Center* PR e os *Cyber Data Center* BSB possuem um sistema de proteção contra incêndio (suspensão por gás FM-200/FE-227) para os equipamentos hospedados nos respectivos prédios. O sistema protege os ativos de informação, evitando que eles sejam atingidos pelo fogo, em pleno atendimento a tal requisito. Medidas de segurança física, gerenciamento de instalações físicas e seleção de local e leiaute para colocação dos equipamentos integram este objetivo de controle e não constam do caderno 21;
- CTTI041 - Restrição de acesso à configuração das ferramentas utilizadas na programação dos processamentos: define perfis para executar, modificar, apagar ou criar rotinas. Restringe o acesso à configuração das ferramentas de administração e de controle da produção, estabelecendo perfis para executar, modificar, apagar ou criar rotinas.

Os objetivos de controle detalhados no gerenciamento de identidade (DS5.3) e o gerenciamento de conta de usuário (DS5.4), responsáveis pelo processo de formalização, pelo procedimento de aprovação de acesso aos dados e pela outorga de privilégios a usuários das ferramentas de administração e controle de produção, complementam a atividade CTTI041, direcionada à área de operações de TI, juntamente com objetivos de controle do domínio aquisição e implementação. O caderno 21, por

ser baseado em *status* de atividades, não demonstra a intersecção dos domínios do COBIT – Entrega e Serviço e Aquisição e Implementação, verificadas nesse controle;

- CTTI039 - Concessão de acesso à criação de tabelas de banco de dados de produção apenas à área de operações da companhia. Assim como a atividade CTTI041, os objetivos de controle detalhados no gerenciamento de identidade (DS5.3) e o gerenciamento de conta de usuário (DS5.4), responsáveis pelo processo de formalização, pelo procedimento de aprovação de acesso aos dados e pela outorga de privilégios aos usuários das ferramentas de administração e controle de produção, complementam a atividade CTTI039. A intersecção dos domínios também é verificada nesse item;
- CTTI023 – Restrição de acesso dos analistas e programadores ao ambiente de produção da Companhia: essa atividade encontra-se mapeada nos objetivos de controle de alto nível AI2, AI3, AI4, AI6 e AI7 do domínio Aquisição e Implementação e no domínio Entrega e Suporte, nos objetivos gerenciamento de identidade (DS5.3) e gerenciamento de conta de usuário (DS5.4). Mais uma vez, foi identificada a intersecção dos domínios com a utilização do modelo PCAOB – COBIT, fornecendo uma visualização mais ampla do processo, a qual não pode ser verificada por meio do caderno 21.

Esse caderno 21 descreve as atividades de controle a ser efetuadas pela gerência de operações de TI, num âmbito geral, sem identificá-las segundo os objetivos de controles do *framework* COBIT. Assim, deixa margem a questionamentos no processo de auditoria.

Com a utilização do documento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting* (IT Control Objectives for Sarbanes-Oxley, 2006), que propicia a ligação entre a seção 404 da Sarbox e o COBIT, há identificação dos controles da área de operações de TI no *framework* COBIT. A identificação mapeia todos os objetivos de controle relacionados com as atividades direcionadas à gerência para o processo de certificação.

Com essa abordagem, a empresa pode otimizar o processo de certificação da gerência de operações de TI, através de medidas que estimulam a eficiência operacional, como por exemplo:

- Elaboração de um guia baseado no apêndice C do doc umento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting*"(IT Control Objectives for Sarbanes-Oxley, 2006), para orientação dos colaboradores envolvidos no processo de certificação. O guia terá os seguintes componentes: domínio do *framework* COBIT; objetivo de controle *versus* controle da área de operações de TI; exemplos de

evidências a serem solicitadas durante o processo de auditoria; relacionamento das possíveis evidências com os objetivos de controle detalhados do COBIT 4.1;

- Plano de implantação dos objetivos de controle detalhados do COBIT 4.1, que complementam os controles estabelecidos para a gerência de operações de TI, com metas trimestrais.

A companhia dá ênfase ao aumento de sua eficiência operacional, com a finalidade de atingir vários objetivos: redução de custo, alocação mais eficiente de recursos, melhoria no processo de governança corporativa, dentre outros. A adoção de um modelo suportado pelo PCAOB, para os controles estabelecidos para gerência de operações de TI, permite uma grande melhoria no processo de avaliação anual efetuado por auditorias externas, pois as diretrizes estabelecidas por essas serão utilizadas para atestar os controles internos.

4 – MODELOS ITIL e eTOM

O presente capítulo apresenta uma revisão da literatura técnica, descrevendo o modelo ITIL e o modelo eTOM, o histórico de criação desses modelos, suas gerências e disciplinas.

4.1 – MODELO ITIL

O ITIL foi criado pelo governo inglês, mais especificamente pelo *Office of Government Commerce* (OGC), no final da década de 1980. Sua filosofia adota uma estratégia orientada para processos, escalável para atender a organizações de TI de diferentes portes. Segundo ela, o gerenciamento de serviços de TI é um conjunto de processos estreitamente relacionados e altamente integrados, suportados por três "Ps": pessoas, processos e produtos, de forma eficaz, eficiente e econômica (QUINT, 2003).

O conjunto de práticas ITIL aparece no "P" de processo e propõe dois grandes grupos: um relacionado com os processos do dia-a-dia, que dão apoio às atividades de manutenção associadas ao suporte de serviços (*Service Support)* de TI, e outro relacionado com os processos de planejamento e de provimento de serviços (*Service Delivery)* com qualidade (COLIN, 2004).

O ITIL é a mais abrangente e respeitada fonte de informações sobre processos de TI. Constitui-se em uma descrição coerente e integrada de melhores práticas de gerenciamento de serviços de TI. Compreende as seguintes perspectivas: de negócio, de gerência da infra-estrutura, de gerência das aplicações, de entrega e de suportes de serviços de TI, de gerência da segurança e planejamento para implementar o gerenciamento de Serviços (OGC, 2004a).

O ITIL é composto pelas seguintes publicações: *Best practice for Planning to Implement Service Management; Best practice for Service Support; Best practice for Service Delivery; Best practice for Security Management; Best practice for ICT Infrastructure Management; Best practice for Application Management; Best practice for Software Asset Management* e *Best practice for The Business Perspective.*

A figura 4.1 mostra as disciplinas do ITIL cobertas por essas publicações.

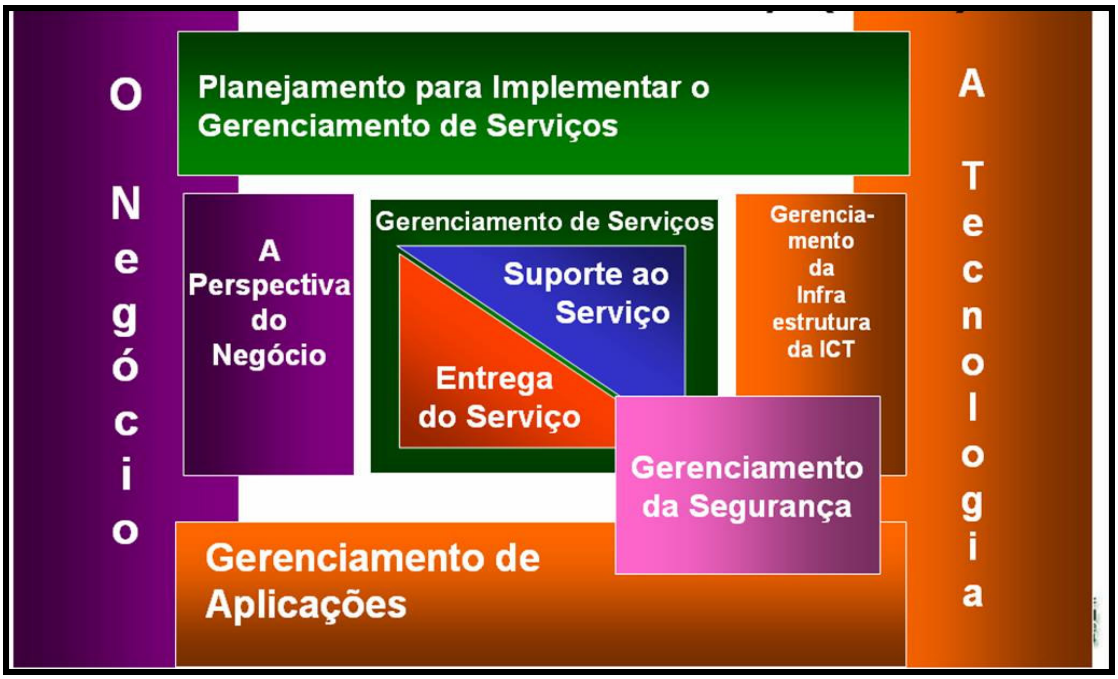

Figura 4.1: ITIL *framework* traduzido
Fonte: OGC (2005b)

Os objetivos resumidos das disciplinas do ITIL são apresentados em seguida:

4.1.1- Objetivos do ITIL

Perspectiva de negócio

Descrevem questões relacionadas com o entendimento e com a avaliação dos serviços de TI, como aspectos integrados à gestão empresarial. Entres suas seções, encontram-se: gerenciamento de continuidade dos negócios, parcerias e terceirizações, sobrevivência a mudanças e adaptação da empresa a mudanças radicais.

Gerenciamento da infra-estrutura da comunicação

O gerenciamento pró-ativo da infra-estrutura da TI e da Comunicação (*Information and Comunication Technology* - ICT) é o foco dessa disciplina. O crescente grau de dependência do negócio em relação à tecnologia, a crescente complexidade do ambiente, as necessidades de flexibilidade e satisfação do cliente, as restrições de investimentos e aos reduzidos ciclos de vida de produtos compõem os desafios do gerenciamento (OGC, 004c).

O escopo do gerenciamento da infra-estrutura de ICT engloba o desenho, o planejamento, a implantação, a operação e o suporte técnico. Essa disciplina se relaciona com as disciplinas entrega dos serviços e suporte ao serviço.

O ICT descreve questões associadas ao gerenciamento das operações de TI, quais sejam: gerenciamento de serviços de rede, gerenciamento das operações, gerenciamento de processos locais, instalação e homologação de computadores e gerenciamento de sistemas.

Gerenciamento de aplicações

Descreve o ciclo de vida do desenvolvimento de *software*: suporte ao ciclo de vida do *software* e teste de um serviço de TI para o uso operacional.

Gerenciamento da segurança

A Gestão da Segurança (*Security Management*) tem como propósito garantir a segurança do negócio e limitar os danos, através da prevenção, minimizando o impacto dos incidentes de segurança da informação. A Gestão de Segurança adota a BS 7799-1:1999 como referência de melhores práticas a serem implementadas. Referências podem ser obtidas também na norma ISO/IEC 17799:20005 e em sua equivalente nacional, da Associação Brasileira de Normas Técnicas (ABNT), NBR ISO/IEC 17799.

A informação é um ativo que tem valor para a organização e deve ser protegida contra ameaças, para garantir a continuidade dos negócios e minimizar danos. A segurança preserva o valor da informação quanto aos seguintes aspectos: confidencialidade, integridade e disponibilidade. A confidencialidade protege informações importantes de uso ou interceptação não autorizados, garantindo sua acessibilidade somente a pessoas autorizadas. A integridade salvaguarda a exatidão e a completude da informação e do *software*. A disponibilidade assegura que a informação e os serviços de TI estejam disponíveis quando necessário (OGC, 2004d).

As organizações, os sistemas de informação e as redes de computadores são colocados à prova por ameaças à segurança da informação oriundas de: fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo e inundação. Problemas causados por vírus, *hackers* e ataques de *denial of service* são cada dia mais comuns, ambiciosos e sofisticados. Essas vulnerabilidades se agravam a partir da computação distribuída, da interconexão de redes públicas e privadas e do compartilhamento de recursos.

É essencial que uma organização identifique seus requisitos de segurança, os quais derivam de três fontes principais:

- Avaliação de risco dos ativos da organização, para identificar as ameaças aos ativos, as vulnerabilidades, a probabilidade de ocorrência e o impacto potencial;
- Legislação vigente, estatutos, regulamentações e cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço devem atender;
- Conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização precisa desenvolver para apoiar suas operações.

Da norma ISO/IEC 17799:2000 e de sua equivalente nacional, a NBR ISO/IEC 17799, constam os seguintes módulos relativos à segurança e ao controle dos sistemas de TI:

- Política de segurança, cujo objetivo é fornecer a direção, uma orientação e apoio para a segurança da informação. Essa política deve ser aprovada pela direção, publicada e comunicada de forma adequada a todos os funcionários. Deve estar em conformidade com a legislação e com as cláusulas contratuais, com os requisitos de educação de segurança, com a prevenção e com a detecção de vírus e de *software* maliciosos, com a gestão de continuidade do negócio e com as conseqüências das violações na política de segurança da informação;
- Segurança organizacional, que consiste no estabelecimento de uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação na organização. Fóruns apropriados de gerenciamento, com liderança da direção, devem ser criados para aprovar a política de segurança da informação, atribuir as funções de segurança e coordenar a implementação através da organização;
- Classificação e controle dos ativos de informação, segundo os quais os ativos da organização devem ser inventariados e confiados a comodatários, assegurando-se de que cada ativo possua um responsável. As informações devem ser classificadas para indicar a importância, a prioridade e o nível de proteção. Alguns itens podem requerer um nível adicional de proteção ou tratamento especial;
- Segurança em pessoas, que objetiva reduzir riscos de erro, de roubo, de fraude ou de uso indevido das instalações. Responsabilidades de segurança devem ser atribuídas na fase de recrutamento, incluídas em contratos e monitoradas na vigência de cada contrato de trabalho. Funcionários e prestadores de serviço com acesso a informações e instalações de informática devem assinar acordo de sigilo. Os usuários devem estar cientes das ameaças e preocupações com a segurança da informação, preparando-se para apoiar a respectiva política, minimizando-se riscos. A resposta aos incidentes de

segurança e mau funcionamento visa a minimizar os danos, monitorá-los e aprender com tais incidentes. Incidentes que afetam a segurança devem ser reportados por meio dos canais apropriados, o mais rapidamente possível;

- Segurança física e do ambiente, que visa a prevenir o acesso não autorizado, danos às informações e interferência sobre elas, e instalações físicas da organização; prevenir perda, dano ou comprometimento dos ativos e a interrupção das atividades do negócio por meio da segurança dos equipamentos; implantar controles para evitar a exposição e o roubo de informações e recursos de processamento de informação;
- Gerenciamento das operações e comunicações, a qual se dá por meio do planejamento e da prevenção, para garantir a adequada disponibilidade de capacidade e recursos, minimizando o risco de falhas nos sistemas. Adota precauções para prevenir e detectar a infiltração de *softwares* maliciosos, tais como vírus de computador, a exemplo de cavalos de tróia e outros;
- Controle de acesso, processo que consiste em controlar o acesso à informação, prevenir acessos internos ou externos não autorizados, controlar o acesso aos serviços de rede internos e externos. Mecanismos especiais devem ser desenvolvidos para controlar acessos privilegiados de administradores de sistema e de banco de dados, entre outros. Requer o desenvolvimento de recursos de sistema para prevenir acessos não autorizados às aplicações e controlar acessos autorizados;
- Desenvolvimento e manutenção de sistemas, cujo foco é a garantia de que a segurança seja parte integrante dos Sistemas de Informação. Identifica e implementa requisitos de segurança e contingência, em articulação com os arquitetos de sistemas, antes do desenvolvimento das aplicações; previne perda, modificação ou uso impróprio de dados dos usuários nos sistemas aplicativos; implanta criptografia para proteger confidencialidade, autenticidade e integridade das informações;
- Gestão da continuidade do negócio, que visa reduzir, a um nível aceitável, a freqüência de interrupções causadas por desastres ou falhas de segurança, por meio de ações de prevenção e de recuperação. Planos de contingência devem ser implantados para garantir a recuperação dos processos do negócio dentro do tempo requerido. Os planos devem receber manutenção periódica e ser testados regularmente, tornando-se parte integrante dos processos gerenciais. Controles devem ser implementados para identificar e reduzir riscos, limitar os danos decorrentes de incidentes e garantir a tempestiva recuperação das operações vitais;

- Conformidade, cujo objetivo é evitar a violação de leis civis, criminais, estatutos, regulamentações, obrigações contratuais e quaisquer requisitos de segurança. Deve-se analisar criticamente a política de segurança e a conformidade técnica, mediante auditagem que assegure o cumprimento das normas implantadas.

Planejamento para implementar o gerenciamento de serviços

Descreve o planejamento e a implementação de programas destinados a otimizar o gerenciamento de serviços de TI. A parte referente ao suporte de serviços preocupa-se com a garantia de que o cliente tenha acesso aos serviços apropriados, a fim de sustentar as funções de negócio, descritas nos processos de gerenciamento de configuração; gerenciamento de incidentes; gerenciamento de problemas; gerenciamento de mudanças; gerenciamento de liberações e central de serviços (que não é processo e sim, uma função).

Em seguida, serão descritos cada um dos processos baseados nas informações de QUINT (2003), OGC (2000) e OGC (2001).

4.1.2 - Suporte a serviços

Essa disciplina do ITIL responde pelos processos operacionais a seguir (figura 4.2).

Figura 4.2: Suporte aos serviços
Fonte: Adaptado de OGC (2004e)

- Gerenciamento de incidentes: processo que tem como foco assegurar que os serviços sejam providos, em níveis predeterminados. Por isso, uma vez ocorrida falha na prestação de um serviço, seu retorno deve ser rapidamente providenciado de forma a minimizar o impacto na disponibilidade do serviço e na qualidade acordada. As interrupções ou eventos não planejados nos serviços são denominados incidentes. As principais responsabilidades dessa gerência podem ser resumidas em: detecção e

registro dos incidentes, classificação de todos os incidentes e suporte inicial, investigação e diagnóstico necessários ao pronto restabelecimento dos serviços;

- Gerenciamento de problemas: está relacionada com o tratamento de todos os tipos de serviços que falharam. Seu primeiro objetivo é minimizar o impacto dos incidentes e dos problemas no negócio, causados por erros na infra-estrutura de TI. O segundo é prevenir a recorrência de incidentes associados a esses erros. Para atingir seus objetivos, são identificadas as causas das falhas, executando-se ações para melhorar ou extinguir os problemas. Nessa gerência, as ações podem ser tanto reativas como pró-ativas, diferente da anterior, que só tem ações reativas. As responsabilidades envolvem as atividades: controle de problemas, que identifica e registra problemas; controle de erros conhecidos, de solicitações de mudanças e de administração da base de conhecimento de erros conhecidos; assistência a incidentes graves; prevenção pró-ativa; identificação de tendências para reconhecimento de problemas, além de informações gerenciais;
- Gerenciamento de configuração: processo que permite à gerência de TI um controle rígido sobre seus ativos, como equipamentos de *hardware*, programas de computador, documentação, serviços terceirizados, plantas, descrições de cargos, documentação de processos e quaisquer outros itens, chamados Itens de Configuração (IC), relacionados com a infra-estrutura de TI. A implementação da gerência de configuração oferece um modelo lógico da infra-estrutura ou de serviço, pela identificação, controle, manutenção e verificação das versões dos IC. O registro dos IC, com seus atributos de tipo, versão e fornecedor, entre outros aspectos julgados importantes, deve ser mantido em uma base de dados. Os IC e seus relacionamentos são armazenados e mantidos na Base de Dados da Gerência de Configuração (BDGC). As responsabilidades desse processo envolvem atividades básicas de planejamento, identificação, denominação, registro e histórico da situação dos IC, bem como verificação e auditoria;
- Gerenciamento de liberações: preocupa-se em manter sob controle o histórico das evoluções de *hardware* e *software*, bem como assegurar que a disponibilização de novas versões desses elementos não afete a qualidade dos serviços em andamento. Nesse sentido, é responsável pelo armazenamento do *software* controlado e autorizado, pela liberação do *software* no ambiente de produção e por sua distribuição para locais remotos, pela implementação do *software* necessário ao serviço e manutenção do *hardware* disponível, para que os incidentes possam ser tratados rapidamente. Esse processo tem as seguintes responsabilidades: política e planejamento da liberação;

projeto, construção e configuração da liberação; aceite de liberação; planejamento de *rollout* (retorno à última configuração válida no IC objeto da mudança); testes extensivos conforme o critério de aceite acordado; liberação para a implementação; comunicação, preparação e treinamento; auditoria de *hardware* e *software* antes e depois da implementação das mudanças e armazenamento de *softwares* controlados nos sistemas centralizados e distribuídos;

- Gerenciamento de mudanças: seu foco é assegurar que alterações no ambiente sejam, antes de tudo, planejadas e acordadas entre os envolvidos. Isso é feito por meio de avaliações de impacto e risco, antes da introdução de qualquer mudança que afete a estabilidade da infra-estrutura e serviços. Nesse sentido, toda alteração na situação atual de um IC se caracteriza como uma mudança. O objetivo, então, é completar, de forma sistemática, todos os ajustes na infra-estrutura de TI. Com isso, os riscos de perturbação no serviço e, conseqüentemente, a diminuição na qualidade dos serviços providos é mitigada. As responsabilidades contempladas nesse processo são: garantir que as mudanças sejam aprovadas e implementadas de forma eficiente, dentro dos custos adequados e com o risco mínimo para os serviços novos ou existentes; planejar as mudanças de forma sincronizada e disponibilizar os recursos quando necessários. Devido ao quase constante envolvimento de mais de uma área, a comunicação é fator crítico de sucesso a um processo de mudança bem sucedido, diminuindo, inclusive, incidentes provenientes de mudanças mal implementadas.

Além dos processos descritos, outra disciplina integra o suporte aos serviços, constituindo uma função: a central de serviços. Trata-se de uma disciplina que possui como missão minimizar as interrupções dos negócios causados por serviços de TI defeituoso. Isso é feito através da detecção de incidentes, dos respectivos registros e da coordenação das atividades exigidas para restauração do serviço, ao mesmo tempo registrando informações que resultarão na rápida resolução e prevenção de problemas futuros.

Essa central está associada ao monitoramento do *status* e ao progresso dos incidentes, bem como com a comunicação com o usuário, de forma a provê-lo de informações sobre a condução dos serviços. A central possui um papel-chave na gerência de incidentes, pois envolve a recepção, o registro e o rastreamento de todos os incidentes e requisições de serviços. Sua função é estar ciente das necessidades de negócio e do impacto das falhas nos negócios, maximizando a disponibilidade do serviço e assegurando que os incidentes sejam resolvidos e que o usuário esteja de volta ao trabalho normal o mais rapidamente possível.

4.1.3 Entrega de serviços

A entrega de serviços diz respeito ao serviço que o negócio exige do provedor, de forma a oferecer suporte adequado aos usuários. Suas especificações são descritas nos processos de: gerenciamento do nível de serviço; gerenciamento de capacidade; gerenciamento de continuidade; gerenciamento de disponibilidade e gerenciamento financeiro (figura 4.3).

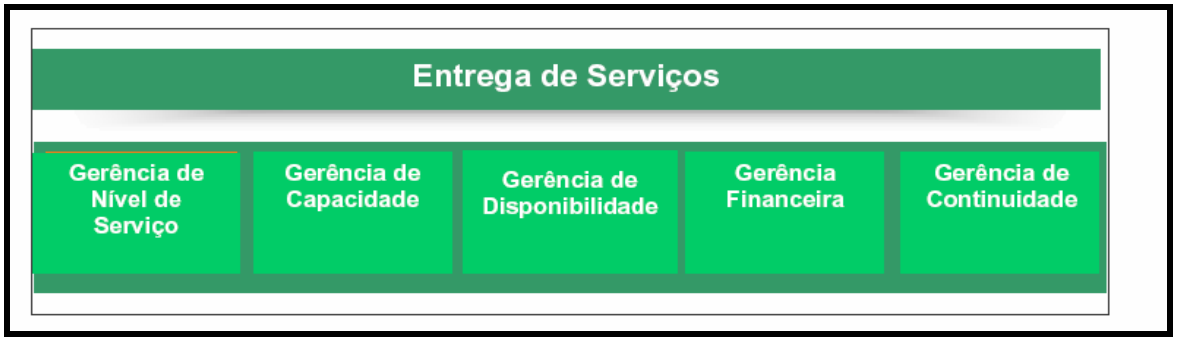

Figura 4.3: Entrega de serviços
Fonte: Adaptado de OGC (2004e)

Essa disciplina do ITIL é responsável pelos processos táticos, detalhados abaixo.

- Gerenciamento dos Níveis de Serviços (GNS): essa disciplina garante a administração da qualidade e da quantidade de serviços fornecidos aos clientes pela organização dos serviços de TI. A essência do GNS é o Acordo do Nível do Serviço (ANS), que é, geralmente um contrato entre a organização de TI e seus clientes, descrevendo em detalhes os serviços fornecidos, com características de quantidade e qualidade, tais como desempenho e disponibilidade desses serviços. Assegura o melhoramento contínuo da qualidade do serviço e a redução da ocorrência de ruptura no seu fornecimento. As atividades principais do GNS são: observar o gerenciamento das relações com o cliente; manter o catálogo de serviços; detalhar o conjunto de serviços que o departamento de TI pode fornecer e os diferentes níveis de serviços que estão disponíveis, negociar e monitorar os contratos de serviços quanto ao aperfeiçoamento e à qualidade dos serviços prestados;
- Gerenciamento de capacidade: responsável pela garantia de que a capacidade de processamento e de armazenamento da TI acompanha as crescentes demandas do negócio da maneira mais efetiva em custo e tempo. O processo em questão trata do monitoramento do desempenho e da produtividade dos serviços de TI e seus

componentes, dos ajustes para tornar mais eficiente o uso dos recursos existentes, a compreensão das atuais demandas sobre os recursos de TI, a criação das previsões para futuras solicitações e a elaboração de um plano de capacidade que permita ao fornecedor de serviços de TI oferecerem serviços na qualidade definida nos ANS. Pode-se dizer que o gerenciamento de capacidade é, essencialmente, um ato de equilíbrio do custo contra a capacidade e da oferta contra a demanda;

- Gerenciamento da disponibilidade: processo relacionado com as ações necessárias para evitar falhas no provimento do serviço ou, caso elas ocorram, seu rápido restabelecimento, incluindo segurança, , capacidade de recuperação, sustentabilidade e resiliência dos recursos de TI. O principal objetivo é garantir que todos os serviços sejam suportados em todos os níveis, por IC suficientes e confiáveis, ou seja, com manutenção adequada, no tempo certo, e disponível. Um serviço é considerado disponível, quando o cliente recebe o serviço como acordado no ANS. Na versão 2, o ITIL trata o gerenciamento da segurança como um processo independente, responsável pela administração de um nível predefinido de segurança para um serviço, incluindo a gerência de reação a incidentes de segurança e aumentando a disponibilidade dos serviços com a diminuição dos incidentes relacionados com a segurança, devido à proteção das informações do serviço e seus usuários. Os aspectos de segurança envolvem proteção de informações sensíveis à divulgação, à interceptação não autorizada/confidencialidade, à salvaguarda da exatidão e completude da informação e do *software/*integridade e à garantia de que as informações e os serviços estarão disponíveis, quando necessários/disponibilidade;
- Gerenciamento financeiro: preocupa-se em mapear e gerenciar os custos do aparato de TI (infra-estrutura e serviços), necessário ao atendimento das demandas. Está ligada aos processos internos de previsão orçamentária, contabilidade e cobrança. Com a previsão orçamentária, deve-se garantir que a TI tenha recursos para garantir o provimento e a manutenção dos serviços prestados. A contabilidade viabiliza a análise de custos e benefícios, de maneira a subsidiar as decisões contratuais mais adequadas, fornecer informações para justificar as despesas e investimentos com TI, entre outros aspectos. O benefício fundamental para a cobrança é que se instale, na empresa, um procedimento com foco mais comercial, de equilíbrio entre a forma e a quantidade de serviços de TI e as necessidades e recursos dos clientes. Com a cobrança, os clientes adquirem o direito de influenciar nas decisões, quanto à provisão desses serviços, de modo que a TI passe a ser encarada, de fato, como provedora de serviços alinhados à real necessidade de

negócio. Embora muitas organizações não efetuem a cobrança formal efetiva dos serviços de TI, seus custos devem ser amplamente divulgados;

- Gerenciamento de continuidade do serviço: tem como missão suportar todo o processo de continuidade dos negócios, garantindo que todo o aparato técnico de TI e seus serviços possam ser recuperados dentro dos prazos de negócio necessários e acordados, durante e depois da ocorrência de um incidente maior. As dependências entre negócio e TI determinam que o gerenciamento da respectiva continuidade seja um subconjunto do gerenciamento de continuidade dos negócios, de acordo com a natureza do negócio e da extensão da penetração da tecnologia na organização.

4.1.4 – ITIL: Considerações

Como se pode perceber, o ITIL tem como preocupação essencial garantir que os serviços de TI estejam sempre disponíveis e em grau de qualidade condizente com as expectativas dos usuários. Para prover esses serviços com a qualidade requerida, a empresa pode montar uma estrutura de TI própria, assumindo os riscos de sua manutenção, ou pode terceirizar, no todo ou em parte, sua operacionalização.

O ITIL é eficiente na descrição de como implantar as melhores práticas em processos de TI, mas limitado em métricas e auditoria. Uma característica do modelo é sua flexibilidade, uma vez que a recomendação principal é “adote e adapte”.

O espírito inerente à biblioteca ITIL é o reconhecimento de que as organizações estão se tornando cada vez mais dependentes de TI, para atingir seus objetivos corporativos e satisfazer as necessidades de negócio. Como códigos de prática, a biblioteca tem a finalidade de auxiliar as organizações na manipulação da crescente complexidade de sistemas, de atender as exigências dos clientes por flexibilidade e a sempre presente necessidade de mudanças. As disciplinas ITIL podem ser usadas por organizações de qualquer tipo e porte. As melhores práticas representam um conjunto de orientações baseadas nas melhores experiências em um determinado campo.

4.2 - MODELO ETOM

4.2.1 - Modelo ETOM: origem e definições

Toda empresa tem um plano estratégico do negócio, seja esse divulgado implicitamente ou explicitamente. Metas, visão, missão, clientes alvo e objetivo fazem parte do plano de negócio de qualquer empresa e são responsáveis pelo processo de estruturação da

companhia. As prestadoras de serviço de telecomunicações perseguem a excelência operacional, sempre buscando oferecer um serviço confiável com o menor custo (MARCONDES, 2006).

O *Telemanagement Forum* (TMForum) é um consórcio internacional de provedores de serviços de telecomunicações e fornecedores de equipamentos e sistemas. Sua missão consiste em ajudar os provedores de serviço a automatizar seus processos, incluindo os seguintes tópicos: especificação dos processos de negócios; padronização da informação que flui entre os processos (modelo de informação); especificações de ambientes e arquiteturas que propiciem a integração dos Sistemas de Suporte à Operação (OSS - *Operating Support Systems*); apoio ao desenvolvimento de mercado e produtos para integração e automatização dos processos.

O TMForum é um consórcio de aproximadamente 400 operadoras, fornecedores e integradores de produtos e serviços, que têm como foco de atuação o gerenciamento da automação operacional e de processos de negócios.

Entre as iniciativas do TMForum, está o sistema *New Generation Operations Systems and Software* (NGOSS) que, junto com o modelo eTOM, permite a conexão entre vários sistemas. Ele fornece o mapa de negócios para o NGOSS e funciona como primeiro direcionador de requisitos de negócios para alimentar a respectiva visão de negócios.

O primeiro *framework Telecommunications Operations Map* (TOM) foi desenvolvido entre 1995 e 1998, estabilizando-se em 1999. Entre 2000 e 2001, evoluiu para o modelo *Enhanced Telecommunications Operations Map* (eTOM) e, desde então, vem sofrendo evoluções, sempre direcionadas e gerenciadas pelo TMForum, estando hoje na versão 6.0.

O eTOM é uma estrutura de processos de negócios de classe mundial, que serve de guia a provedores de serviços de telecomunicações, fornecedores de *hardware*, *software* e de integradores, de forma a contribuir para o sucesso dos seus empreendimentos. É reconhecido como ferramenta estratégica que permite estabelecer uma linguagem única nas empresas, possibilitando que todo o setor trabalhe de forma harmonizada. Tamanha é sua importância para as telecomunicações mundiais, que o eTOM tornou-se recomendação da União Internacional de Telecomunicações (ITU-T), organismo da Organização das Nações Unidas (ONU), voltado para os assuntos do setor.

O eTOM utiliza-se de decomposição hierárquica para estruturar os processos de negócios, possibilitando a decomposição em diversos níveis, sucessivamente. A modelagem de processos do eTOM descreve um fluxo de processos numa abordagem de "raias", vertical, direcionado a processos fim-a-fim. Esses tendem a superar as fronteiras das organizações,

integrando clientes, empresas, parceiros e fornecedores, de forma a constituir os processos necessários à descrição do fluxo de atividades, que visam a resolver um determinado problema. Um exemplo disso é o macro processo de aprovisionamento, ou seja, tudo que envolve o fluxo de aprovisionamento de um serviço para o cliente. Na abordagem horizontal, direciona processos com a visão de funcionalidade entre todas as unidades organizacionais internas à empresa, como a gestão de relacionamento com o cliente. Porém, essa estrutura do eTOM é definida de forma o mais genérica possível, para garantir uma aplicação independente de organização, tecnologia e serviços.

O modelo eTOM é um conjunto de processos de negócios utilizados por provedores de serviço, no uso de informações de clientes, serviços, recursos, fornecedores/parceiros e outros. Opera por múltiplos processos, procurando posicionar a empresa em questão dentro de um contexto geral de sua área de negócio, isto é, fazendo com que seus negócios estejam alinhados com outras organizações.

4.2.2 - Modelo ETOM – nível 0

O quadro de processos do eTOM procura posicionar a empresa operadora de serviços dentro em um contexto geral de sua área de negócio, isto é, fazendo que seus negócios estejam alinhados com outras organizações. O quadro de processos representa o ambiente global da empresa, descrito na figura 4.4.

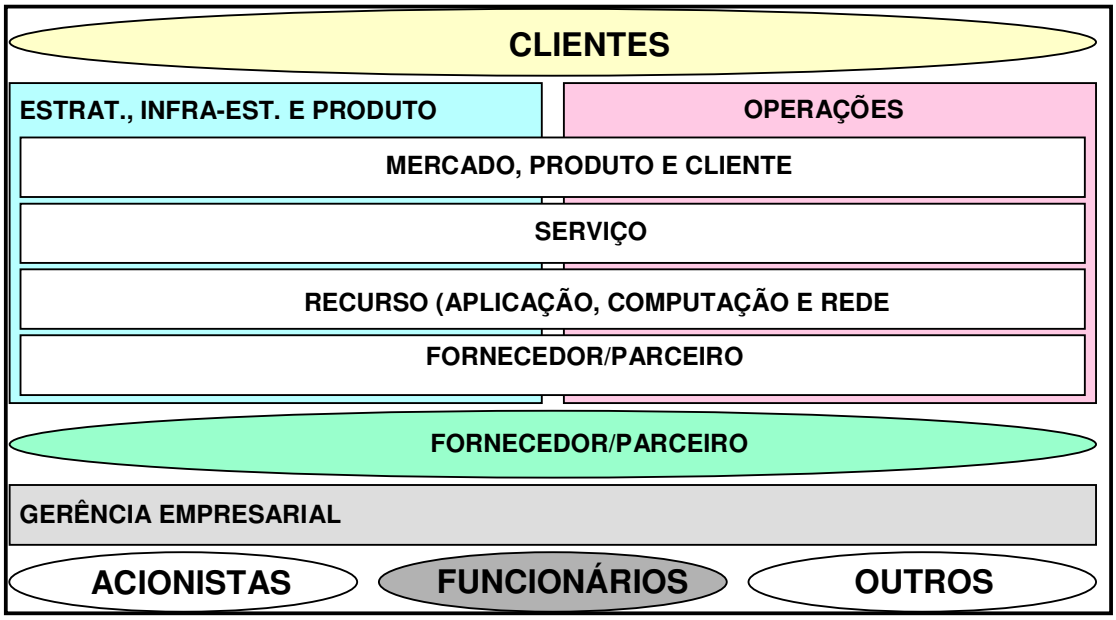

Figura 4.4: Quadro de Processos do eTOM – nível 0
Fonte: Marcondes (2006)

No nível conceitual, o eTOM pode ser visto como três grandes áreas de processo: estratégia, infra-estrutura e produto; operações e gerência da empresa.

- Estratégia, infra-estrutura e produto: área voltada para os objetivos estratégicos, planejamento e gerenciamento do ciclo de vida do negócio, infra-estrutura e produto. Os processos incluem o desenvolvimento de estratégias para o estabelecimento de compromissos para com o cumprimento desses objetivos; gerenciamento da entrega de serviços; melhoria de produtos, da infra-estrutura e da cadeia de suprimentos;
- Operações: é o coração do modelo, focado no núcleo da gerência operacional. Seus processos incluem o suporte a clientes, a operações e ao gerenciamento delas no dia-a-dia. Área composta por atividades de ciclo de vida curto, que não exigem grandes mudanças; porém executa atividades que impactam diretamente o cliente, garantindo a continuidade do negócio a curto e médio prazo;
- Gerência empresarial: refere-se, basicamente, aos processos gerenciais da empresa, necessários em qualquer negócio. Esses processos estão focados no nível empresarial, em suas metas e objetivos.

As duas maiores áreas, apresentadas na figura 4.4, dão suporte aos processos das áreas funcionais da empresa, dispostos em blocos horizontais. São elas:

- Processos de mercado, produto e cliente: referem-se àquilo que se relaciona com o gerenciamento vendas, distribuição, marketing, propostas, produtos, *Customer Relantionship* (CRM), ordens de serviço, solução de problemas, SLA e faturamento;
- Processos de serviços: incluem todas as ações relacionadas com o desenvolvimento e a configuração dos serviços, gestão dos problemas, análise de qualidade e preços;
- Processos de recursos: tudo que é feito relacionado ao desenvolvimento de gerenciamento de infra-estrutura da empresa, relacionado aos produtos e serviços ou para suportar a empresa como um todo;
- Processos de parcerias: interações da empresa com fornecedores e parceiros.

Essa representação é nomeada como nível 0 ou nível conceitual. Para fechá-lo, o diagrama apresenta as primeiras entidades que interagem com a empresa, são elas: clientes, para quem o serviço é vendido; fornecedores, quem provê recursos ou produtos usados pela empresa; parceiros, com quem a empresa opera conjuntamente com a área de negócio; empregados, quem trabalha para a empresa com o propósito de atingir objetivos; acionistas, os que investem na empresa e são proprietários das ações; e interessados, os que têm, de certa forma, compromissos com a empresa.

4.2.3 - Modelo eTOM: nível 1

Abaixo do nível conceitual, o modelo eTOM é decomposto em um conjunto de processos que provê o primeiro nível de detalhe. Essa visão é considerada como sendo o nível do *Chief Executive Officer* (CEO) Diretor Presidente ou nível 1, em que o desempenho irá determinar o sucesso da empresa.

Para representar melhor esse nível, os processos podem ser divididos em dois agrupamentos:

- Agrupamento vertical dos processos: representa uma visão dos processos fim-a-fim dentro de um negócio como, por exemplo, tudo que estiver envolvido num fluxo de bilhetagem para um cliente;
- Agrupamento horizontal dos processos: representa a visão funcional dentro de um negócio como, por exemplo, a gestão de canais de fornecimento (figura 4.5).

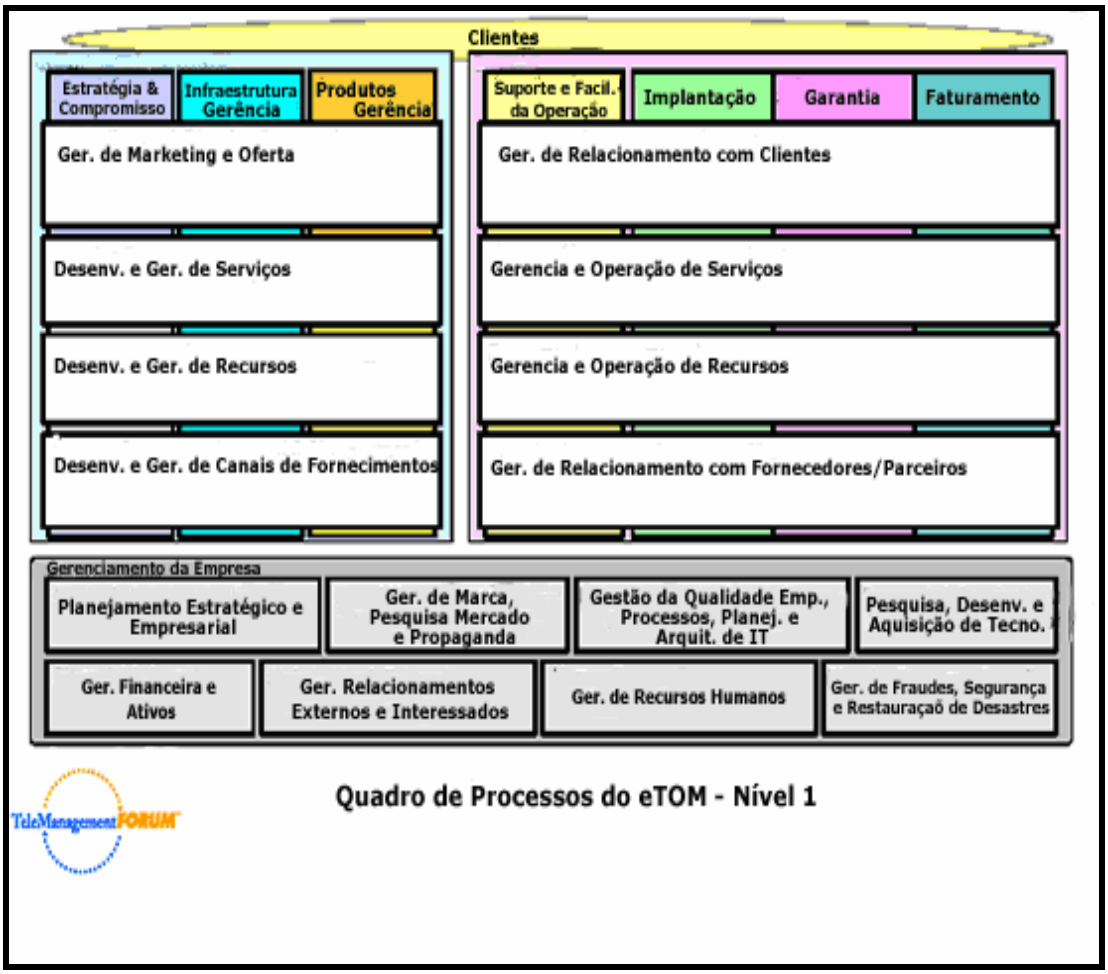

Figura 4.5: Quadro de processos do eTOM – nível 1
Fonte: Teleco (2007)

Agrupamento vertical dos processos da área de operações

Os processos da área de operações contêm quatro agrupamentos gerais:

- Implantação: esse processo é responsável pela entrega dos produtos desejados pelo cliente. Informa ao cliente o status de seu pedido, garantindo a sua execução a tempo, atendendo a sua satisfação;
- Garantia: esse processo é responsável pela execução de atividades de manutenção preventiva e corretiva, de forma que os serviços estejam continuamente disponíveis e nos níveis de performance estabelecidos pelo SLA ou *Quality of Service* (QoS);
- Faturamento: esse processo é responsável pela produção de faturas precisas e no tempo correto;
- Suporte a facilidades da operação: processo que responde pelo suporte aos três outros processos do grupo IGF e garantia a facilidades operacionais das áreas de implantação, garantia e faturamento. As atividades desse processo não estão na mesma velocidade daqueles presentes no IGF; portanto, o modelo eTOM dá um tratamento em separado. No entanto, no mundo real, é possível encontrar nas empresas uma mistura destes processos com os IGF.

Agrupamento horizontal dos processos da área de operações

Os processos da área de operações que estão representados horizontalmente podem ser agrupados em quatro partes:

- Gerência de relacionamento com o cliente (CRM): esse processo considera fundamental o conhecimento das necessidades dos clientes e inclui todas as funcionalidades necessárias à aquisição, ganho e retenção do relacionamento com um cliente. Responde pela garantia de um serviço e um suporte ao cliente com qualidade, seja pelo atendimento direto ou telefone, pela WEB ou através de serviços em campo. O CRM também inclui a coleta de informações do cliente para aplicação em serviços personalizados e identificação de oportunidades para incrementar o valor dos clientes para a empresa;
- Gerência e operações de serviços: agrupamento focado nas funcionalidades necessárias ao gerenciamento e operação dos serviços de comunicação e informação. Seu ponto principal é a entrega e o gerenciamento do serviço. Possui processos mensuráveis para avaliar a qualidade do serviço, o desempenho dos processos, a satisfação do cliente, custos, entre outros;

- Desenvolvimento e gerenciamento de recursos: esse agrupamento de processos mantém o conhecimento dos serviços e inclui todas as funcionalidades necessárias ao gerenciamento e operação dos serviços de comunicações e informações, para atendimento aos propósitos dos clientes. Tem a responsabilidade de garantir à infra-estrutura condições de suportar a entrega fim-a-fim dos serviços;
- Gerenciamento do relacionamento com fornecedores/parceiros: esse processo está fortemente alinhado com os de gerenciamento do relacionamento com clientes, incluindo: requisições, acompanhamentos até a entrega, tratamento de problemas, validação de faturas, autorização e pagamentos e gerenciamento da qualidade dos fornecedores/parceiros.

Processos estratégicos, infra-estrutura e produtos – SIP

Esse agrupamento manteve a sigla baseada no seu nome em inglês *Strategy, Infrastructure and Product* (SIP). A seguir, são descritos os grupos de processos verticais:

- Estratégia e compromissos: grupo de processos responsável pela definição das estratégias no suporte à infra-estrutura e ciclo de vida dos produtos da empresa. É também responsável pelo estabelecimento de compromissos que dêem suporte às estratégias dentro da organização. Acompanha o sucesso e a efetividade das estratégias e faz ajustes quando necessário;
- Gerenciamento do ciclo de vida: esse grupo permite aos processos principais, com foco em operações e clientes, atender às demandas de mercado e às expectativas dos clientes. O desempenho desses processos é acompanhado pelo mais alto nível da empresa, dado seu impacto na competitividade e retenção dos clientes. Há dois conjuntos de processos relacionados com a gerência de ciclo de vida: infra-estrutura e produto. Ambos possuem um ciclo de desenvolvimento e entrega;
- Gerenciamento do ciclo de vida das infra-estruturas: responsável pela definição, planejamento e implantação de toda infra-estrutura necessária. Identifica novos requisitos e capacidades; projeta e desenvolve nova infra-estrutura ou melhorias;
- Gerenciamento do ciclo de vida dos produtos: responsável pela definição, planejamento, projeto e implantação de todos os novos produtos na empresa.Visa a atender as margens de lucro, satisfação dos clientes e atendimento da qualidade. É responsável também por entender o mercado, o ambiente do negócio, necessidades dos clientes e competidores.

A seguir, são descritos os grupos de processos horizontais do SIP:

- Gerenciamento de marketing e oferta: engloba a definição de estratégias, o desenvolvimento de novos produtos, o gerenciamento dos produtos em funcionamento e acompanhamento do mercado. Definem também estratégias de canais, vendas, preços, comunicações de marketing e promoções;
- Gerenciamento e desenvolvimento de serviço: tem seu foco no planejamento, desenvolvimento e entrega dos serviços para o domínio de operações. Deve garantir que a capacidade tem condições de suportar as demandas de serviços futuros;
- Gerenciamento e desenvolvimento de recursos: engloba o planejamento, o desenvolvimento e a entrega dos recursos necessários para suportar os serviços e produtos. Inclui os processos necessários à definição do desenvolvimento da rede e outros recursos, físicos ou não, à introdução de novas tecnologias e interconexão com as redes em funcionamento e à garantia de atendimento das demandas futuras;
- Gerenciamento e desenvolvimento de canais de fornecimento: ajuda a garantir que os melhores parceiros/fornecedores sejam escolhidos para a operação conjunta. Gerencia o fluxo de informações técnicas, de acompanhamento e financeiras.

Finalmente, na estrutura conceitual do quadro de processos do eTOM – nível 1, há os processos de gestão empresarial, localizados na parte inferior desse. Tal grupo envolve o conhecimento de ações e necessidades no nível da empresa, englobando todos os processos de gerenciamento do negócio necessários ao devido suporte das demais partes da empresa. Os processos de gestão da empresa são:

- Planejamento estratégico empresarial: responsável pelo planejamento da empresa. Incluem focos de negócio, mercado alvo, objetivos financeiros, aquisições que possam melhorar posicionamento financeiro e de mercado, entre outros. Define a missão e a visão da empresa, sua estrutura gerencial, guias e políticas de TI;
- Gerenciamento de marca, pesquisa de mercado e propaganda: voltada para o marketing corporativo;
- Gerência de qualidade da empresa, planejamento e arquitetura de processos de TI: diz respeito ao desenvolvimento e à melhoria das arquiteturas da empresa;
- Gerência de pesquisa e aquisição de tecnologia: gerencia o conhecimento, a pesquisa tecnológica e a avaliação de potenciais aquisições de tecnologia;
- Gestão financeira e de ativos: inclui contas a pagar e a receber, relatórios de despesas, fluxo de caixa, impostos e recolhimentos, pagamentos e outros. Define a política de ativos, o controle do inventário e o gerenciamento do balanço;

- Gerência de relacionamentos externos: envolve o relacionamento com acionistas, órgãos reguladores, comunidade, associações, entidades de classe, governo e outros;
- Gerência de recursos humanos: define políticas salariais e de premiação, programas de benefícios e de comunicação, treinamento, contratações e demissões, processos de aposentadoria e outros;
- Gestão de fraudes, segurança e restauração dos desastres: agrupamento que garante à empresa manter suas operações, processos, aplicações e comunicações críticas em face de um desastre, de ameaças, à segurança e tentativas de fraude.

4.2.4 – ETOM: considerações finais

A utilização do modelo eTOM promove a identificação individual de cada um dos processos da empresa, sua aplicabilidade, valor, custo e performance, posicionamento e categorização, de acordo com um padrão mundial estabelecido para empresas do setor. Esse padrão apesar de mais aplicável a empresas de Telecomunicação também vem sendo utilizado por empresas de prestação de serviço entre outras

Na última década, as operadoras de telecomunicações sofreram uma mudança no conceito de prestação de serviço. O mercado tornou-se altamente dinâmico e dependente do uso de TI, para a disponibilização de produtos e serviços no mercado. A prestação de serviço fim-a-fim a um cliente, de forma verticalizada e numa rede inteiramente sua, está se tornando mandatório entre os provedores de serviço de telecomunicações.

Diante dessa realidade, o eTOM definiu um modelo para o contexto em que estão inseridas as operadoras de telecomunicações. Esse modelo está representado, de modo simplificado, na figura 4.6

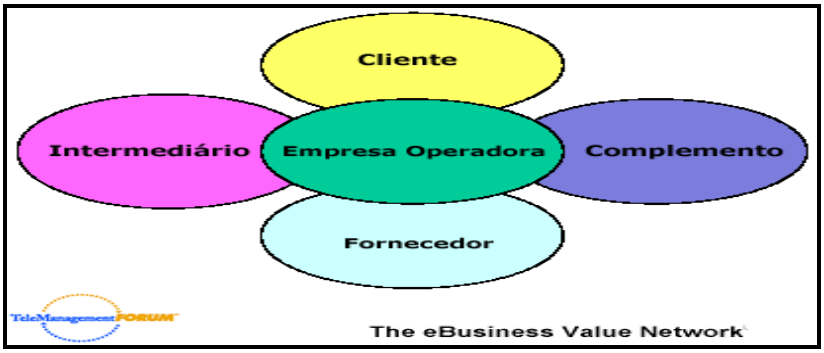

Figura 4.6- Estrutura e-TOM para uma empresa de telecomunicações
Fonte: Teleco (2007)

A figura representa um conjunto de elementos que compõem uma rede, cujo objetivo é fornecer serviço ou produto que tenha valor para o cliente. Esses elementos são:

- Cliente: a rede existe para servir às necessidades do cliente. Esse pode ser um indivíduo ou outra empresa. Dependendo das atividades que executa, o cliente pode ser um assinante (responsável por firmar e pagar o contrato), um usuário final (usa os produtos e serviços) ou ambos;
- Empresa operadora: o operador é o núcleo desta rede de valor. É o ponto central de execução e responsável pela rede de valor. Estão sob sua responsabilidade a plataforma operacional e a infra-estrutura através da qual outros parceiros podem colaborar para fornecer produtos e serviços ao cliente;
- Fornecedor: grupo que interage com a empresa, fornecendo produtos e serviços integrados pelo prestador de serviços, de modo a que ele possa fornecer seus produtos e serviços ao cliente. Estão aí incluídos tanto os *vendors*, que fornecem equipamentos, *software* e soluções para o operador, como prestadores de serviço, para os quais são terceirizadas funções do operador e outros operadores. Desses, são contratados infra-estrutura e/ou serviços de conectividade, circuito ou rede;
- Intermediário: executa uma função em nome da empresa junto a clientes ou fornecedores. Há, tipicamente, três categorias de intermediários: vendas, implantação e serviços de informação;
- Complemento: fornece produtos e serviços adicionais para estender as capilaridades da rede de valor. Geralmente, os produtos e serviços complementares são construídos a partir da infra-estrutura fornecida pela empresa. Um exemplo disso são os provedores de serviço de valor adicionado.

Para os provedores de serviço de telecomunicações, esse modelo de processos provê uma referência que pode ser utilizada para a reengenharia de seus processos internos, assim como dos processos de relacionamento com o ambiente externo da organização, em especial com seus parceiros, fornecedores, clientes e demais empresas operadoras de telecom. Para os fornecedores de soluções ao mercado de telecomunicações, o eTOM é uma boa referência para o desenvolvimento de seus produtos. Há uma tendência mundial no mercado de telecomunicações para utilizar essa metodologia. Mais de 25 empresas utilizam o modelo eTOM, entre elas: a VIVO, a TIM, a Vodafone, a Telefônica, China Telecom, França Telecom, Coréia Telecom e Deutsche Telecom.

As empresas de telecomunicações necessitam de metodologias cada vez mais alinhadas às metas e estratégias de negócios, objetivando fortalecer sua marca, mantê-la competitiva,

rentável. Para alcançar esses objetivos, as empresas de Telecom têm desafios, como por exemplo, conhecer, com base em suas metas estratégicas de negócio, o que será impactado, quanto tempo levará para implantar essa nova meta estratégica, o que deve ser mudado e quanto custará essa implantação. Além desses, há o desafio de conhecer suas operações para, mais rapidamente, saber como otimizá-las, retroalimentando seus portfolios de projetos, que implantarão soluções otimizadas, padronizadas e de menor custo, proporcionando uma operação mais ágil e focada no negócio. Torna-se o canal desejado para fidelização, retenção e captação de novos clientes, atingindo, assim, os seguintes objetivos: competitividade, rentabilidade, fortalecimento da marca, minimização das taxas de *churn* de clientes e perda de *market share*. Para tanto, as empresas de telecom precisam ter seus clientes - Complementos (URAs, TAVs - Terminais de Auto Atendimento)– Fornecedores – Intermediários (*Call-Centers*) cada vez mais integrados e com crescente melhoria na qualidade do tempo de resposta, para que essa seja rápida e padronizada, garantindo a satisfação do cliente e suportando as entradas de novos produtos, serviços e soluções.

5–AVALIAÇÃO DA CONFORMIDADE SARBOX DE UM MODELO CONVERGENTE ETOM – ITIL

O presente capítulo realiza um comparativo macro entre o modelo eTOM e o modelo ITIL e realiza a identificação dos controles Sarbox para área de operações de TI nos dois modelos. O estudo é baseado no documento GB921V do eTOM.

5.1- MODELO CONVERGENTE ETOM – ITIL

A efetividade da estratégia de marketing em um ambiente de alta tecnologia e de grandes mudanças na relação empresa-mercado demanda novas habilidades das empresas quanto à gestão sistemática da experiência do cliente, à capacidade de criar valores junto com ele, na medida de suas necessidades, e, finalmente, quanto à construção de relacionamentos que favoreçam a lealdade pró-ativa, ou seja, o cliente tornar-se um verdadeiro promotor da empresa.

Mas, na realidade, verifica-se claramente que não é fácil obter agilidade e muitas empresas, em momentos de turbulência, encontram várias barreiras nesse sentido. Para que o sucesso no atendimento das demandas ocorra, é necessário um alinhamento das áreas de negócio com a área de TI, a fim de estabelecer-se uma sincronia entre seus objetivos.

Muitas empresas passam por mudanças necessárias e imprescindíveis para sua sobrevivência no mercado e devem estar preparadas para explorar novas oportunidades. Podem-se destacar algumas situações que demandam e estimulam essa sincronia entre as áreas de negócio e as áreas de TI, em particular nas empresas de telecomunicações: convergência dos serviços de telefonia fixa e móvel; fusão de operadoras; tempo mais curto para o desenvolvimento de novos serviços e para colocação de um novo produto no mercado; melhorias identificadas pelos sistemas de relacionamento com o cliente para sua fidelização; e adequação à legislação.

Há algum tempo, os departamentos de TI das empresas de telecomunicações mudaram seu papel na organização; eles passaram a ser visualizados como ponto estratégico na entrega de um serviço e como parceiros para área de negócio, deixando de ser meros coadjuvantes. A infra-estrutura de rede, a infra-estrutura de TI e os sistemas de informação encontram-se no mesmo patamar de relevância, visando ao alcance das metas e objetivos estabelecidos pela empresa.

Para que um novo produto ou serviço seja implementado, necessita-se de infra-estrutura de rede e também que o serviço oferecido seja aprovisionado, medido e faturado. Os sistemas de informação têm um papel fundamental nesse aspecto.

A adoção de *frameworks* como eTOM e ITIL é uma necessidade cada vez maior nas organizações, seja por pressões financeiras, de eficiência, de regulação (Sarbox) ou por transparência nas operações de TI. Nesse caso, verifica-se a necessidade de se compatibilizarem as disciplinas oferecidas pelo ITIL com os processos estabelecidos pelo eTOM, como o objetivo de esclarecer como um *framework* pode apoiar ou servir de obstáculos a outros, bem como se há ganhos na adoção conjunta de dois *frameworks*. No quadro a seguir, comparam-se os dois modelos, sumarizando diferenças e similaridades, conforme o artigo GB921 do eTOM (Quadro 5.1).

	ETOM	**ITIL**
Abrangência	Contexto global na organização com foco para a indústria de provimento de serviços de comunicação e telecomunicações.	Contexto focado em TI.
Padronização	Padrão internacional do ITU.	Incluído no padrão ISO 20.000.
Objetivo	Permitir automação de processos fim a fim com uma linguagem comum. Padronização de processos.	Constitui-se de uma descrição coerente e integrada de melhores práticas de Gerenciamento de Serviços de TI.
Conteúdo	Fornece uma visão hierárquica do processo de negócio versus uma visão de toda a empresa. Foco em clientes externos.	Fornece uma padronização para suportar os níveis de serviços oferecidos e métodos para atingi-los. Possui um foco voltado mais para clientes internos.
Implementação	Implementação se diferencia de empresa para empresa. Suportado pelo TMF/especificação NGOSS.	Implementação se diferencia de empresa para empresa.
Áreas fortes	Cadeia de fornecimento, faturamento, suporte de operações e disponibilidade .	Central de serviços Gerenciamento de continuidade Gerenciamento de Capacidade Gerenciamento de disponibilidade

Tabela 5.1: Quadro comparativo eTOM x ITIL
Fonte: Adaptado artigo eTOM and ITIL – Jenny Huang (2005)

5.1.1 Vantagens de uma visão integrada

Segundo o citado artigo, a vantagem de uma visão integrada pode ser vista sob dois aspectos: na visão do cliente e na visão interna do provedor de serviços, como segue:

- Visão do cliente, que implica uma comunicação focada no cliente, através: da utilização de uma linguagem única em toda a cadeia de provisão de um serviço, por meio da qual o cliente terá a comunicação melhorada e facilitada com o provedor de serviço, refletindo uma percepção de melhor serviço; da melhor oferta de serviços, compreendendo todas as demandas de um cliente, sejam de telecomunicações ou TI e tendo um método padronizado para lidar com tais demandas. É possível oferecer um melhor conjunto de soluções que atendam suas necessidades de satisfação do cliente, pois se fala um vocabulário padrão, unificado internamente, alinhado aos processos de negócio e apto a entregar os serviços de que o cliente necessita. Assim a organização verá os níveis de satisfação dos clientes se elevarem;
- Visão interna do provedor de serviços, que representa um valor incremental e de complementaridade; os dois *frameworks,* apresentam uma abordagem comum e complementar na revisão dos processos. Os recursos empregados em iniciativas de melhorias de processos podem ser otimizados, economizando tempos de projeto e recursos e maximizando os resultados. Os benefícios do provedor são:
  a- Otimização de *Operational Expenditure* (OPEX), através da consolidação de funções redundantes: uma estratégia consolidada eTOM/ITIL pode dinamizar e consolidar ambientes de processos separados, criando oportunidades para identificar áreas redundantes e oportunidades para melhorias de processos;
  b- Clareza na estratégia de processos: a integração dos dois processos em um único ambiente pode eliminar interfaces desnecessárias e prover ganhos através da reutilização de "blocos de atividades padrão" nos processos. Evita também disputas internas na adoção de *frameworks* ou na criação de metodologias não aderentes ou interconectadas, que acarretariam mais custos e complexidade;
  c- Comunicação clara: através da simplificação dos processos e da redução dos pontos de medidas, a comunicação com o gerenciamento dos serviços fica mais fácil e clara.

A convergência tecnológica está transformando o modelo de negócios do setor de telecomunicações, gerando impacto no desempenho das empresas provedoras de serviços.

Para garantir a competitividade no mercado, há necessidade de revisão dos processos operacionais e de adequação a um modelo unificado.

Por meio da confiança nos controles internos e da evolução da cultura da importância em adotá-los na organização, tornou-se possível elaborar relatórios com informações e demonstrações condizentes com a realidade da empresa. Isso assegura a tomada das melhores decisões e a transparência da confiabilidade para o mercado

Outros desafios são vislumbrados, como a necessidade de alinhamento constante entre a tecnologia ofertada e o objetivo de negócio. Essencialmente, o alinhamento das estratégias significa aderência dos investimentos e gastos à tecnologia, em face do valor que eles agregam aos negócios da instituição. A partir disso, o sucesso das atividades tecnológicas passa a ser avaliado pela contribuição que os gastos e investimentos realizados dão à empresa.

No ambiente de redes, tal como no ambiente de TI, as mudanças na produção são constantes, tanto para a expansão como para a correção de problemas, as evoluções tecnológicas, o aprovisionamento de serviços e outros. Os negócios de grandes empresas de telecomunicações são, de algum modo, dependentes da tecnologia (redes ou TI). Mas, apesar dessa dependência, não se pode esquecer que existem pessoas envolvidas no processo global do negócio, as quais operam e tomam decisões, desenham processos para o cumprimento dos procedimentos operacionais e para a organização das ações e tarefas.

5.2 – MAPEAMENTO DOS CONTROLES SARBOX DA GERÊNCIA DE OPERAÇÕES DE TI NO MODELO CONVERGENTE

O processo de avaliação do modelo convergente para os controles estabelecidos pela Sarbox, para o ambiente de operações de TI, aborda a localização do controle segundo o *framework* ITIL e a localização do controle segundo o eTOM. Avalia-se a aderência dos processos, segundo o documento GB929 do eTOM para os controles descritos: controle de acesso lógico; segregação do ambiente de produção; revisão e adequação das políticas de *backup;* plano de contingência e recuperação de desastre.

5.2.1 Controle de acesso lógico

O controle de acesso lógico promove a mitigação de possíveis fraudes, elimina a solicitação de acessos desnecessários e de transações conflitantes, permitindo a identificação de responsáveis pelas solicitações através da formalização do processo. A importância do controle de acesso para os sistemas e recursos de informação em um ambiente convergente

deve ser estendida a todas as tecnologias envolvidas e determinadas pela organização, como parte crítica da garantia de certificação e continuidade do negócio.

Controle de acesso segundo ITIL

O controle Sarbox de acesso lógico está relacionado com uma das disciplinas do ITIL: o gerenciamento de segurança. Esse gerenciamento é um processo que tem por finalidade controlar um nível definido de segurança para a informação e para os serviços e infra-estrutura de TI. Utiliza como referência a norma ABNT NBR ISO/IEC 17799:2005.

Controle de acesso segundo eTOM

O processo de gestão da empresa no eTOM contempla o controle Sarbox de acesso lógico também na gerência de segurança, que é responsável pelo estabelecimento de políticas e diretrizes corporativas e melhores práticas de gerência de segurança e auditoria para conformidade com as práticas internas da empresa.

Aderência dos processos segundo o documento GB929 do eTOM

Baseado no documento citado, tem-se o controle Sarbox de acesso lógico, apontando para gerência de segurança nos *frameworks* ITIL e eTOM. Na matemática, diz-se que as duas gerências são congruentes, considerando-se "Congruência como a propriedade atribuída a duas figuras que são geometricamente iguais".

O processo relacionado com o controle de acesso lógico não é tratado particularmente como uma disciplina do ITIL e sim como componente da norma na qual este se baseia. No eTOM, a gerência de segurança também contempla o controle de acesso. Empresas de telecomunicações adotam a norma ABNT NBR ISO/IEC 18028 de gestão de segurança em redes, em conjunto com a norma ABNT NBR ISO/IEC 27001:2005, que se refere ao sistema de segurança da informação, para subsidiar a gerência de segurança relacionada com equipamentos de telecomunicações, como: roteadores, DSLAMs, gerências e outros.

Na figura 5.1, encontra-se representada a gerência de segurança relativa ao eTOM, relacionada com a gerência de disponibilidade do ITIL. Não há representação gráfica da gerência de segurança do ITIL devido ao documento enfocar, especificamente, o gerenciamento de serviços.

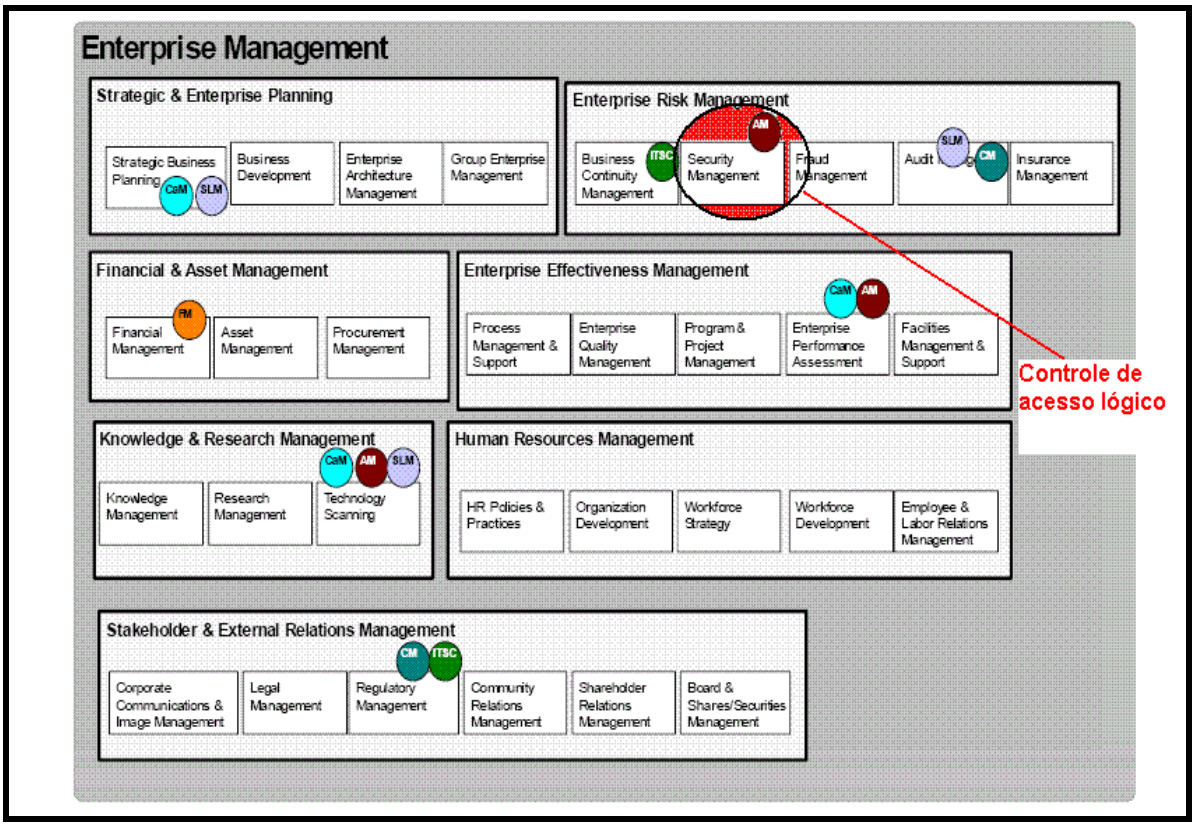

Figura 5.1 –eTOM nível 2 processos de gerência empresarial – Controle de acesso lógico
Fonte: GB921V – Tmforum (2005)

5.2.2 Processos de segregação

Segregação do ambiente de produção

A segregação é definida como a separação de diferentes ambientes. Esse controle engloba a separação dos ambientes de produção de infra-estrutura da tecnologia da informação em relação aos ambientes de homologação, testes e desenvolvimento que suportam as aplicações, banco de dados e todos os recursos envolvidos.

A informação seja da instituição, pessoal, física ou lógica, possui um valor intrínseco, mas um conjunto delas possui potencial capaz de causar prejuízo, se for disponibilizada de maneira inadequada.

Segregação do ambiente de produção segundo o ITIL

O ITIL, como já definido, é um conjunto de padrões que provê os fundamentos para o processo de gerenciamento dos recursos tecnológicos da TI, fornecendo uma abordagem

prática da produção, baseada na experiência. O controle Sarbox segregação do ambiente de produção, assim como o controle de acesso lógico, está relacionado com a gestão de segurança. Essa, no ITIL, possui um processo específico, que enfatiza a importância do adequado gerenciamento da segurança da informação e considera os SLAs entre os processos do negócio e os da TI.

Segregação do ambiente de produção segundo eTOM

O controle segregação do ambiente de produção também é encontrado na gerência de segurança do *framework* eTOM. A gerência de segurança, como já citado, é responsável por todos os aspectos relacionados com a segurança dos equipamentos, com as gerências e com outras tecnologias envolvidas

Aderência dos processos segundo o documento GB929 do eTOM

Utilizando como referência o documento GB929 do eTOM, há o controle Sarbox de segregação do ambiente de produção, que aponta para a gerência de segurança nos dois *frameworks*, ITIL e eTOM.

O processo associado ao controle de segregação de ambiente também não é tratado particularmente por uma disciplina do ITIL e sim como parte integrante de duas seções da norma ABNT NBR ISO/IEC 17999, a Segurança Física e do Ambiente e a Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação, nas quais se baseia. No *framework* eTOM, esse controle é contemplado pela gerência de segurança, como uma das principais recomendações da norma adotada pela empresa para proteger suas informações sensíveis e críticas.

A figura 5.2. representa a gerência de segurança relativa ao eTOM, na qual se encontra o controle de segregação do ambiente de produção.

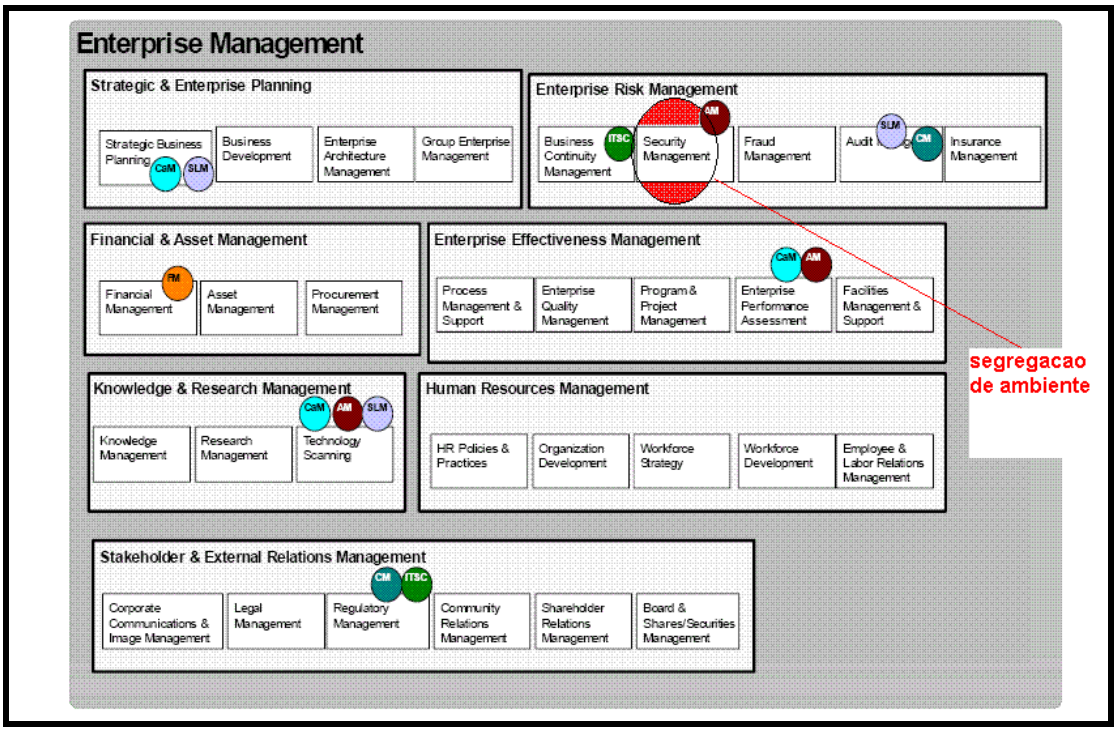

Figura 5.2. –eTOM nível 2 processos de gerência empresarial – segregação de ambiente
Fonte: GB921V (2005)

Atualmente, os sistemas e serviços de telecomunicações desempenham um papel vital na coleta, análise, produção e distribuição da informação indispensável à execução do negócio das organizações. Com a convergência, a diretriz do TMForum de utilização complementar do ITIL aplica-se a esse controle, pois as gerências são complementares.

5.2.3 Revisão e adequação das políticas de *backup*

Em um ambiente convergente, há a necessidade de que o fluxo de negócio da corporação e a manutenção da memória legal estejam ligados à recuperação da integridade operacional do ambiente, contemplando todas as tecnologias e variáveis envolvidas no processo de negócio. O controle de adequação das políticas de *backup* possui um papel fundamental nesse processo.

***Backup* segundo o ITIL**

A versão 2 do ITIL é organizada em cinco módulos principais: 1) perspectiva de negócios; 2) gerenciamento de aplicações; 3) entrega de serviços; 4) suporte a serviços; 5) gerenciamento de infra-estrutura. O controle Sarbox de adequação das políticas de *backup* baseado no ITIL está relacionado com o processo operacional gerência de continuidade, pertencente ao módulo entrega de serviços.

O objetivo principal desse processo é dar suporte à continuidade de serviços de TI que suportam os processos de negócio da organização, garantindo que tais serviços possam ser recuperados no menor intervalo de tempo possível e de acordo com as prioridades de negócio, após a ocorrência de desastres.

Estudos sobre o planejamento de continuidade de negócio mostraram que praticamente um terço das organizações não possui planos de proteção contra desastres provocados por terrorismo, casos fortuitos, força maior ou falhas de sistemas.

O *backup* de informações é uma peça chave no plano de recuperação do ambiente ou das informações legais das empresas, e é um subprocesso da gerência de continuidade de serviços do ITIL.

A figura 5.3 ilustra a associação entre os processos principais dessa gerência.

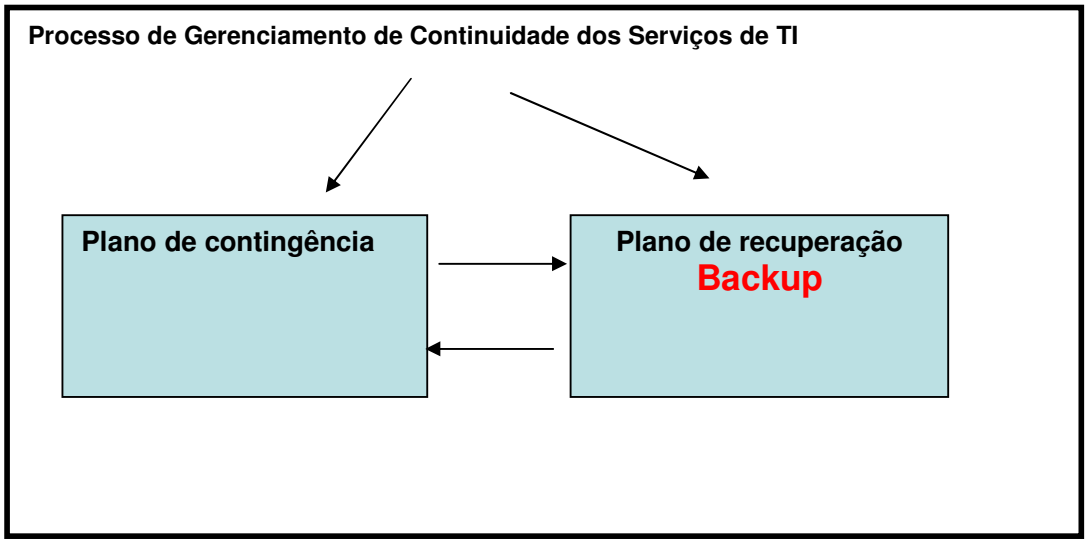

Figura 5.3.–Associação entre processos da gerência de continuidade
Fonte: Autora desta pesquisa

A missão do processo de gerenciamento de continuidade dos serviços de TI é assegurar que a infra-estrutura e os serviços de TI (incluindo, sistemas, redes de comunicação de dados, servidores, bancos de dados e outros) possam ser recuperados nos prazos requeridos e acordados no negócio.

Backup segundo o eTOM

Os processos que tratam da gerência de continuidade de serviços, de *backup* e de recuperação no eTOM são contemplados pela Gestão da Empresa, que se refere ao conhecimento de ações e das necessidades no nível da empresa; envolve todos os processos de gerenciamento do negócio, necessários ao devido suporte às demais partes da empresa. Os processos de Gestão da Empresa são: Gerenciamento de Relacionamentos Externos e colaboradores e Gestão de Fraudes, Segurança e Restauração de Desastres.

O processo de Gerenciamento de Relacionamentos Externos e colaboradores enfoca o relacionamento da empresa com os colaboradores e entidades externas. É representado no nível 3 do eTOM pelas seguintes gerências:

- Gerência de Relações Públicas, responsável pela comunicação de mensagens para o público em geral e com a comunidade;
- Gerência de Relações com os Acionistas, voltada para o relacionamento da empresa com seus acionistas, envolvendo todos os requisitos de negócio, financeiro, legal e regulatório;
- Gerência Regulatória: garante o atendimento de todos os regulamentos governamentais vigentes na empresa;
- Gerência Jurídica: é responsável pela garantia de que a empresa está cumprindo todos os requisitos legais relevantes.

O processo de Gestão de Fraudes, Segurança e Restauração está representado no nível 3 do eTOM pela gerências :

- Gerência de Recuperação de Desastres e Planejamento de Contingências, que estabelece políticas e diretrizes corporativas e melhores práticas de recuperação de desastres e auditoria para conformidade com as práticas internas da empresa;
- Gerência de Segurança, responsável pelo estabelecimento de políticas e diretrizes corporativas e por melhores práticas de gerência de segurança e auditoria, visando à conformidade com as práticas internas da empresa;

- Gerência de Fraudes, voltada para o estabelecimento de políticas e de diretrizes corporativas, bem como para melhores práticas de gerência de fraude e auditoria para conformidade com as práticas internas da empresa.

Aderência dos processos de *backup* segundo o documento GB929 do eTOM

No documento GB929 do eTOM, propõe-se a utilização complementar do ITIL nos processos de Gerenciamento do Serviço de telecomunicações. A figura 5.4 é parte desse documento e ilustra a convergência entre as gerências dos *frameworks*. A avaliação de aderência tem como principal objetivo mostrar a proximidade entre as gerências de continuidade definidas pelo ITIL, as gerências de recuperação de desastres e planejamento de contingências e a gerência regulatória, na qual se encontra o controle de adequação de políticas de *backup* definido pela Sarbox para a área de operações de TI. O *backup* também não é tratado como disciplina particular no eTOM, nem como uma gerência específica no ITIL; é um subprocesso que suporta as gerências dos dois *frameworks.*

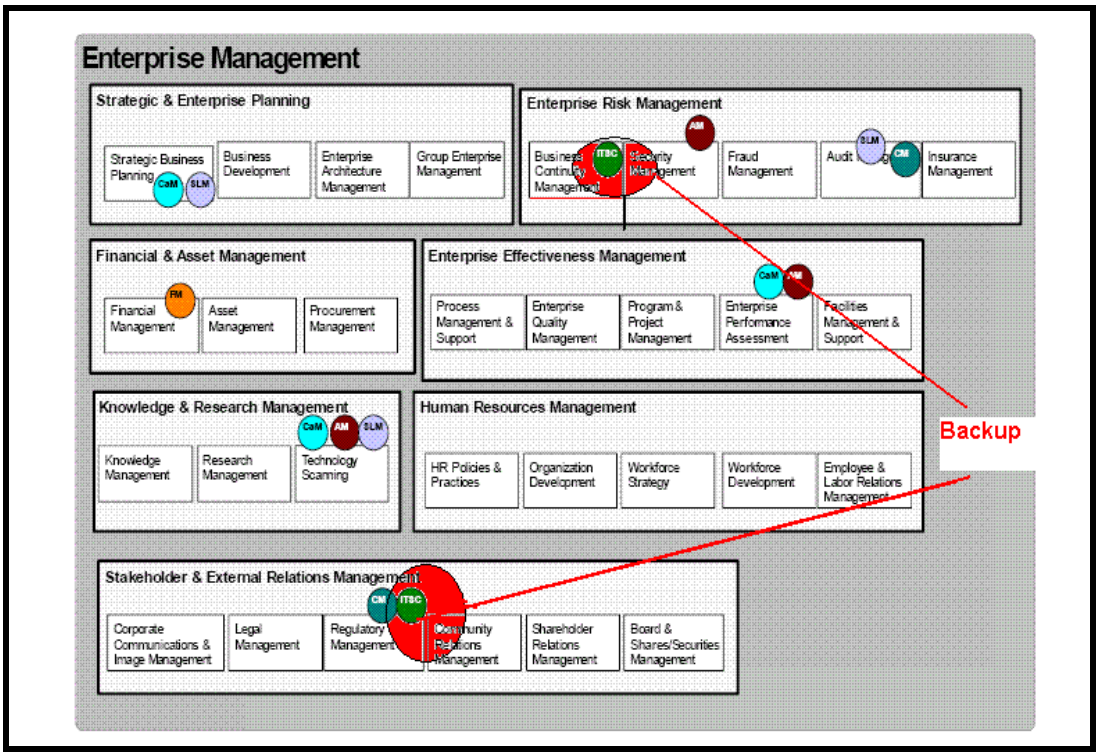

Figura 5.4 –eTOM nível 2 processos de gerência empresarial - Backup
Fonte: GB921V – Tmforum (2005)

Os círculos em verde nessa figura representam a Gerência de Continuidade do ITIL, na qual o controle *backup* está contemplado, mostrando a aderência dos processos ao eTOM. Quanto mais próximo do retângulo de processo do eTOM, mais aderente é o processo ITIL. Observa-se que essa Gerência é mais aderente à Gerência de Recuperação de Desastres e Planejamento de Contingências, em relação à Gerência Regulatória.

Avaliando o controle relativo ao *backup* no *framework* eTOM, verifica-se que o processo de recuperação de informações ou serviços está contemplado na Gerência Regulatória e também na Gerência de Continuidade de Negócio. A diretriz do TMForum é a utilização complementar do ITIL em alguns processos. No caso do controle de adequação das políticas de *backup,* essa diretriz é aplicável, pois o eTOM contempla a fusão das necessidades.

5.2.5 Planos de contigência e de recuperação

As interrupções nos serviços, sejam suportadas pela infra-estrutura de tecnologia de informação ou por plataformas ou equipamentos de rede, sempre afetam os negócios, provocando impactos muitas vezes irreversíveis. Segundo o *Disaster Recovery Institute* (DRI), de cada cinco organizações que sofrem interrupção em suas operações por uma semana, duas fecham as portas em menos de três anos. Esses dados são justificados no mercado, pois um dos maiores desafios dos executivos é garantir a continuidade de seus negócios, independentemente do tipo de evento que possa ocorrer. Em um mundo convergente, esse desafio se torna maior ainda, pois muitas variáveis estarão interligadas.

Plano de contingência e recuperação de desastre segundo o ITIL

O controle Sarbox do plano de contingência e recuperação de desastre, assim como o controle de adequação das políticas de *backup*, é associado ao processo operacional gerência de continuidade pertencente ao módulo entrega de serviços. A meta do gerenciamento de continuidade dos serviços de TI é assegurar que os recursos técnicos e os serviços de TI requeridos pelo negócio sejam recuperados no tempo necessário e acordado.

Gerenciar os riscos de falhas em serviços-chave de TI, através da prevenção de riscos identificados e do planejamento de recuperação desses serviços em uma contingência, é um dos objetivos desse módulo.

O Gerenciamento de Continuidade dos Serviços de TI se concentra em todos os serviços de TI necessários à manutenção dos processos de negócios críticos em funcionamento; também é responsável por identificar e minimizar impactos nesses processos de negócio.

O plano de contingência lista os procedimentos de recuperação da infra-estrutura e os técnicos/gerentes escaláveis, em caso de indisponibilidade do serviço, direcionando as ações técnicas a serem adotadas.

Plano de contingência e recuperação de desastre segundo eTOM

Assim como o controle relacionado com o *backup,* o plano de contingência e recuperação de desastre no *framework* eTOM é associado ao Grupo Gestão da empresa, que trata dos processos de Gerenciamento de Relacionamentos Externos e Colaboradores, Gestão de Fraudes, Segurança e Restauração de Desastres.

Aderência dos processos segundo o documento GB929 do eTOM

Utilizando como referência o documento GB929 do eTOM, verifica-se a similaridade entre a Gerência de Continuidade do ITIL, a Gerência de Recuperação de Desastres e Planejamento de Contingências e a Gerência Regulatória.

O plano de contingência faz parte da Gerência de Recuperação de Desastres e Planejamento de Contingências do eTOM. Também é parte integrante da Gerência de Continuidade de Serviços de TI do ITIL.

No *framework* eTOM, esse controle está mais relacionado com a Gerência de Recuperação de Desastres, que estabelece as políticas e diretrizes corporativas e as melhores práticas de recuperação de desastres, apesar de a aderência da Gerência de Continuidade também estar relacionada com a Gerência Regulatória.

A figura 5.5 representa os processos de gerência empresarial do eTOM nível 2.

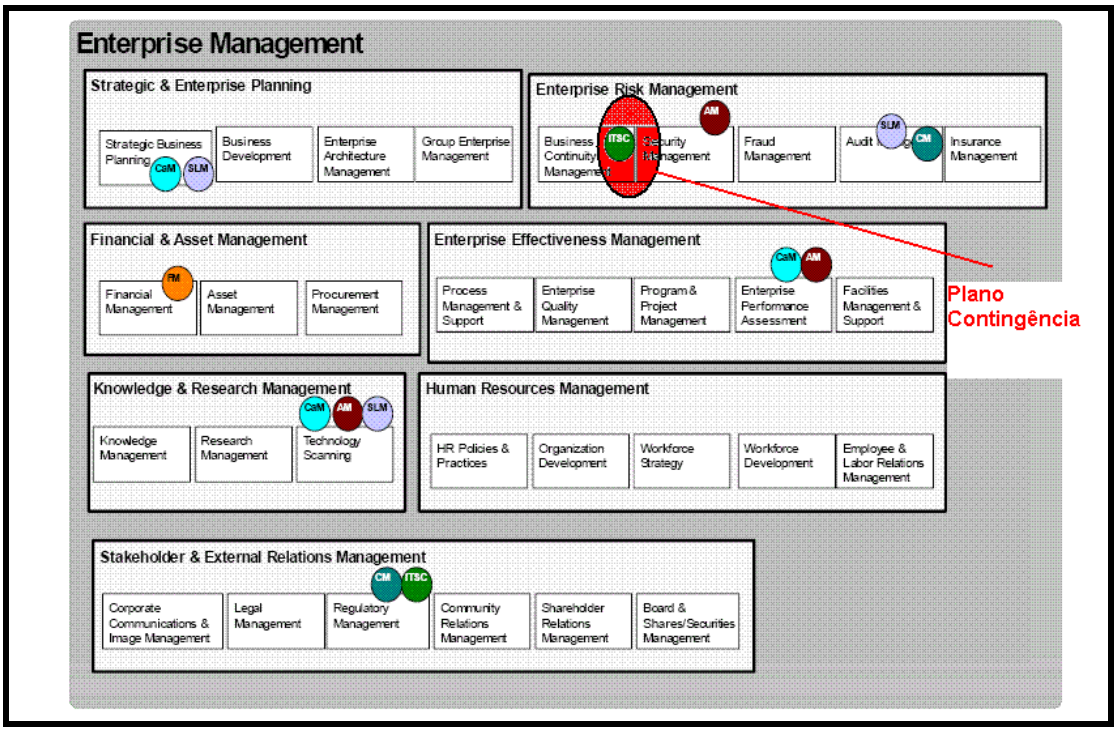

Figura 5.5 –eTOM nível 2 processos de gerência empresarial – Plano de Contingência
Fonte: GB921V – Tmforum (2005)

O círculo vermelho representa a localização do plano de contingência em relação às gerências que o contemplam, nos *frameworks* eTOM e ITIL. Quanto mais próximo do retângulo de processo do eTOM, mais é aderente o processo ITIL. Observa-se que a Gerência de Continuidade ITIL é mais aderente à Gerência de Recuperação de Desastres e Planejamento de Contingências.

Seguindo a diretriz do TMForum, é pertinente a utilização complementar entre as duas gerências dos *frameworks*, para idealização de um plano de contingência que contemplo todos os processos, componentes de infra-estrutura, equipes, plano de recuperação, grau de criticidade do serviço para um ambiente convergente .

5.3 – MAPEAMENTO DOS CONTROLES SARBOX DA GERÊNCIA DE OPERAÇÕES DE TI NO MODELO CONVERGENTE – Considerações Finais

O cenário atual das empresas prestadoras de serviço demonstra que o crescimento e o sucesso das organizações estão diretamente relacionadas com necessidade de se manter uma infra-estrutura de tecnologia de informação e telecomunicações segura e confiável. A dependência dessa infra-estrutura, associada às oportunidades, aos benefícios e aos riscos inerentes à área, exige que essas organizações não só considerem a convergência uma exigência do tempo, como também um processo que necessita de gerenciamento adequado, para que elas possam cumprir os objetivos a que se destinam com a competitividade que o mercado requer. Esse cenário levou ao desenvolvimento de melhores práticas para se obter um modelo adequado para o provimento de serviços.

O projeto de convergência dos mundos de TI e de telecomunicações da empresa foi iniciado em 2006, na Diretoria de Tecnologia e Planejamento Técnico. A abrangência de sua primeira fase incluía: Gerência de Falhas, Gerência de Incidentes e *Trouble Ticketing*, Gerência de Problemas, Gerência de Mudanças,Gerência de Liberações, Gerência de Configurações,Gerência de Força de Trabalho e de Relacionamento com o cliente.

Posteriormente, com a ampliação do projeto de convergência na área de Operações para manter a conformidade com os controles da Sarbox, surgiria a necessidade de criação de um modelo único, com a combinação dos *frameworks* eTOM e ITIL.

O modelo ideal para atender o controle de acesso lógico convergente demandaria um estudo do ambiente tecnológico da empresa (comunicação de dados, plataformas, centrais de comutação e planta de tecnologia da informação), objetivando a elaboração de uma política de controle de acesso unificada, baseada na ISO/IEC-17799, nos objetivos de controle COBIT pertinentes e nas normas da ABNT para tecnologia da informação e planta de telecomunicações. Após a elaboração e implementação dessa política, seria necessária a divulgação dos novos procedimentos, normas e objetivos, na estrutura normativa da empresa.

No contexto dos sistemas de informação, a definição básica de implantação é: “a fase do ciclo de vida de um sistema, que corresponde textualmente à passagem do software/aplicação para a produção, ou seja, a fase de entrega ao cliente final”. Sob a perspectiva de um mundo convergente, a definição de ambiente de produção não estaria atrelada especificamente aos sistemas de informação, mas contemplaria, também, toda a tecnologia (equipamentos de rede, centrais telefônicas, hardware e outros) implantada para provimento de serviços a um cliente. Os requisitos para o desenvolvimento de sistemas seriam

aplicados a um universo num nível macro, visando ao controle de alterações nos ambientes críticos e à proteção de dados reais da empresa.

Da mesma maneira que o controle Sarbox de acesso lógico, a adequação desse controle ao mundo convergente demandaria um estudo amplo de organização e um projeto que vise a adequar a implantação de novas tecnologias a esse modelo.

Os novos procedimentos e normas de segregação de ambiente de produção seguiriam a norma da ABNT e as premissas de controle estabelecidas pelo PCAOB, contemplando os objetivos detalhados do COBIT para recursos de tecnologia da informação. Mas haveria a necessidade de adicionar componentes de segurança da norma específica para planta de telecomunicações, criando-se assim uma política geral para entrada de novas tecnologias no ambiente de produção.

Nesse cenário, o controle de adequação das políticas de *backup* poderia ser classificado como insuficiente. Essa avaliação baseia-se em pesquisas no ambiente da empresa pesquisada, realizadas por colaboradores responsáveis pelos ambientes, e também em pesquisa no repositório de documentos normativos da empresa. Se a estrutura atual não for modificada, a documentação será insuficiente para suportar a certificação e a garantia da administração.

Para início do processo de adequação do controle convergente relativo ao *backup,* seria necessário o ajuste do processo da cópia de segurança, implementado nas diversas áreas da empresa (comutação, dados, plataformas e outros), à estrutura normativa da empresa, disponibilizando políticas, normas e procedimentos dos equipamentos da planta de telecomunicações.

A figura 5.6 ilustra a diretriz de estrutura normativa da companhia adotada atualmente pela área de operações de TI, para o controle relativo a *backup*, dentre outros.

Figura 5.6 - Estrutura normativa da operadora
Fonte: Intranet da operadora (2007)

Com base na necessidade da empresa de recuperar a informação legal para fins de regulação, de recuperação do ambiente operacional para continuidade de negócio e também de aderência aos processos ITL e eTOM estudados, visualizou-se um hiato no atendimento desses interesses. A criação de uma área englobando as gerências de continuidade ITIL, a gerência de recuperação de desastres e o planejamento de contingências e gerência regulatória garantiria que as informações relativas à recuperação de integridade operacional e do fluxo de negócio da empresa estariam alinhadas, promovendo-se, assim, uma visão única em toda a cadeia de provimento de serviço. A integração dos dois ambientes poderia eliminar interfaces desnecessárias, sobreposições de esforços, duplicação de cópias de dados e redundâncias de informações, otimizando os recursos utilizados.

Em resumo, as políticas de *backup* seriam padronizadas, segundo uma diretriz única da empresa, tanto para os equipamentos de telecomunicações considerados críticos (centrais, roteadores, *switches*, e outros.), quanto para os equipamentos e serviços de TI. O foco da recuperação de informações da empresa faria um balanceamento das necessidades operacionais e legais e dos recursos que poderiam ser compartilhados, de acordo com as intenções e com as diretrizes globais da organização, visando aos processos de negócio.

O sucesso de um plano convergente de contingência e de recuperação de desastres é diretamente proporcional à identificação dos processos de negócio. Um processo de negócio compreende um conjunto de atividades realizadas na organização, associadas às informações

que manipula, utilizando os recursos e a estrutura da organização. Em um ambiente convergente, entende-se por recursos as técnicas, os métodos, as ferramentas, sistemas de informação, planta de telecomunicações, recursos financeiros e todo o conhecimento envolvido na respectiva utilização.

Da mesma forma que o controle Sarbox de acesso lógico e o controle de segregação de ambiente de produção, a adequação do controle ao mundo convergente demandaria um estudo amplo da organização. O plano de contingência é imprescindível para a continuidade do negócio da empresa, pois a interrupção no fornecimento de alguns serviços, muitas vezes representa riscos, perdas financeiras, degradação da imagem no mercado e insatisfação do seu maior patrimônio, seus clientes.

A identificação dos pontos mais críticos para a empresa, em conjunto com toda tecnologia envolvida no processo, seja ele de telecomunicações ou de tecnologia da informação, seria o passo inicial desse plano.

O plano de contingência e de recuperação de desastres elaborado em 2007 não estaria apto ao mundo convergente, pois seu foco é a recuperação das 44 aplicações, baseada na infra-estrutura de tecnologia da informação. Seu propósito é minimizar o impacto de uma interrupção nos processos de negócios das unidades de vendas de telefonia fixa, vendas de telefonia móvel e *service assurance.* Esse plano está segmentado por plataformas de infra-estrutura de TI, as quais fazem parte dos processos de negócio, não contemplando os ativos da rede de telecomunicações que também integram esse universo. Ter uma clara visão dos objetivos de recuperação previstos no plano de contingência convergente é fundamental para se poder alcançar o entendimento das funções críticas de negócios e executar atividades para a melhoria contínua dos serviços prestados.

Para atendimento dos requisitos necessários a um modelo convergente, este trabalho propõe a combinação das potencialidades dos modelos COBIT e ITIL, da norma ISO 17799 e ISO 18028 e do *framework* eTOM como estrutura de referência para a categorização das atividades de negócio e suporte aos controles Sarbox. A combinação das respectivas metodologias permitirá a utilização das potencialidades de cada um para desenvolvimento de um modelo único que facilite identificar: o quê, quem, como e que recursos tecnológicos estão envolvidos no provimento de um determinado serviço.

6–CONSIDERAÇÕES FINAIS

A adequação aos dispositivos do ato Sarbanes-Oxley é imperiosa para que as empresas possam manter suas as ações nas bolsas de valores norte-americanas, contribuindo com a valorização do seu patrimônio e a melhoria da imagem no mercado Isso requer a apresentação de informações transparentes e respeito aos requisitos de certificação e de divulgação.

A companhia, no dia 20 de junho de 2007, comunicou ao mercado ter cumprido com sucesso os dispositivos exigidos pela seção 404 da Sarbox. Com isso, ela se obriga a manter os requisitos da referida Lei, no que diz respeito à transparência das informações dos relatórios anuais divulgados no mercado, bem como na forma de divulgação dessas informações. A transparência das informações dos relatórios, por sua vez, exige a adoção de práticas transparentes e de governança para atender os usuários dessas informações.

Dois itens do regimento interno do Conselho da Administração da empresa, publicado em setembro de 2007, devem ser destacados:

- a necessidade de aderência às normas legais e regulamentares, que é uma responsabilidade da administração;
- a revisão da qualidade e da efetividade dos controles internos da companhia e a eliminação ou mitigação de quaisquer deficiências significativas ou fraquezas relevantes nos controles internos pela Diretoria, pelo Conselho de Administração e pelos Auditores independentes.

Neste trabalho, foram verificadas inadequações na seleção dos controles Sarbox estabelecidos para gerência de operações de TI, mapeados e discutidos no capítulo 3, com base em regras oficiais, segundo o PCAOB no documento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting* (IT Control Objectives for Sarbanes-Oxley, 2006).

O PCAOB é um órgão não governamental, independente, sem fins lucrativos, constituído por membros em período integral, de diversas atividades profissionais, interessados nos relatórios contábeis. Tem como principal função interferir diretamente em práticas adotadas pelos auditores independentes, na qualidade dos controles internos das companhias e regulamentação de questões éticas e normas contábeis. As empresas de auditoria que prestam serviço às companhias que têm ações ou títulos negociados nos Estados Unidos possuem registro no PCAOB e estão sujeitas a processos de fiscalização, que avaliam a aplicação dos preceitos técnicos estabelecidos pelo referido órgão.

A revisão da qualidade dos controles internos é parte integrante do regimento interno do Conselho da Administração. Como contribuição para essa deliberação, o presente trabalho fornece o mapeamento dos controles da gerência de operações de TI, segundo os controles básicos estabelecidos pelo PCAOB para área de tecnologia da informação: ambiente de TI, operações computacionais, acesso a sistemas e dados, mudança na infra-estrutura de TI e em sistemas e desenvolvimento de sistemas.

Apesar de os controles Sarbox estabelecidos para gerência de operações de TI estarem formulados a partir do *framework* COBIT, não há nenhuma referência aos quatro controles que fazem o elo entre a seção 404 da referida Lei e a área de tecnologia de informação. Como exemplos práticos, já desenvolvidos no capítulo 3, citam-se:

- Gerenciar dados (DS11): foi trabalhado, apenas, em relação ao mapeamento de dados críticos e à manutenção de *backup* de dados; mas esse demanda uma abordagem mais ampla, contendo desde o gerenciamento da biblioteca de mídia, o tempo de armazenamento de *logs* dessas cópias e testes de restauração periódica que não estavam documentados adequadamente no caderno 21;
- Gerenciar ambiente físico (DS12): possui objetivos de controles detalhados que não foram citados no caderno 21; proteção contra fatores ambientais, medidas de segurança física e leiaute para colocação de equipamentos integram este objetivo e não foram abordados explicitamente.

A materialização do que foi proposto neste trabalho iniciou-se pelo mapeamento dos controles da gerência de operações de TI segundo o *framework* PCAOB *versus* COBIT. Seu efetivo resultado ocorrerá após a implantação dos objetivos de controle detalhados do COBIT 4.1, que complementam os controles Sarbox para a gerência de operações de TI.

Ao término das etapas propostas, a gerência de operações de TI estará alinhada com as quatro diretrizes estabelecidas pelo PCAOB, servindo de alicerce para suportar os questionamentos e o processo de geração de evidências solicitadas pelos auditores independentes, durante o processo de manutenção da certificação Sarbox.

Além da contribuição da adequação dos controles Sarbox da gerência de operações de TI aos procedimentos e *frameworks* regulamentados pelo PCAOB, no capítulo 5, fez-se uma avaliação da conformidade Sarbox em relação ao modelo convergente eTOM *versus* ITIL , que já é uma realidade para algumas disciplinas desta gerência .

A convergência, sem dúvida, é uma forte tendência da organização e trata de um processo que envolve a oferta de pacotes integrados e a disponibilização de serviços novos que exijam

uma infra-estrutura única. Somente uma infra-estrutura convergente, flexível e conforme aos aspectos legais exigidos permitirão a oferta rápida e eficaz de novos serviços.

7- SUGESTÕES PARA TRABALHOS FUTUROS

O cumprimento dos objetivos deste trabalho ressaltou necessidades que são aqui apresentadas como sugestão para trabalhos futuros:

- Elaboração de um projeto para adequação dos controles Sarbox da gerência de operações de TI ao modelo convergente eTOM versus ITIL;
- Elaboração de um guia Sarbox para a gerência de operações de TI, baseado no apêndice C do documento *The Role of IT in the Design and Implementation of Internal Control Over Finacial Reporting (IT Control Objectives for Sarbanes-Oxley, 2006)*, com a seguinte estrutura:
    1) Introdução á Lei Sarbanes – Oxley;
    2) O papel da gerência de operações de TI na certificação;
    3) Aplicações críticas listadas para o processo de certificação;
    4) Tabela para cada controle da gerência de operações de TI, seguindo mapeamento COBIT *versus* PCAOB, segundo figura 7.1;
    5) Exemplo de evidências solicitadas durante o processo de certificação;
    6) Resultado das últimas auditorias com os pontos a serem trabalhados.

Gerenciar Dados (DS11)		
Objetivo de Controle - gerencia os dados; define o modelo de dados e o ciclo de vida da informação, especificando prazos para sua manutenção, segundo os requisitos do negócio e a legislação pertinente;esquema de armazenamento, gerenciamento de bibliotecas de mídias, testes de restauração.		
Exemplos de Controles a serem auditados	**Exemplos de Testes a serem solicitados pela Auditoria**	**Referência COBIT 4.0**
Políticas de retenção versus log de execução das cópias de segurança	Avaliação das políticas de backup implantadas versus o log de execução.	DS11.1
	Solicitação de evidências de proteção aos dados das aplicações críticas, com acesso restrito a estes.	DS11.2 e DS11.6
Gerenciamento das mídias físicas e dados lógicos somente por profissionais autorizados.	Evidências de acesso restrito a equipe responsável por manipular estes dados.	DS11.6
Retenção e políticas de armazenamento definidos em documento oficiais, contendo os responsáveis pela solicitação.	Confirmação através de evidências que os períodos de retenção para as aplicações críticas estão de acordo com o demandado pela SOX	DS11.2
	Seleção de uma amostragem relacionadas as aplicações SOX a serem auditadas.	
Validação da política de backup como um todo, Retenção, dados a serem copiados , frequência da cópia , janela acordada.	Seleção de uma amostragem relacionada as aplicações SOX para geração de evidências.	DS11.5
Teste de restauração e validação de mídia de backup.	Seleção de uma amostragem relacionada as aplicações SOX para geração de evidências, ou seja log de testes periódicos de restauração de mídia.	DS11.5
Mudança na política de backup	Seleção de uma amostragem relacionada as aplicações SOX e validação se as alterações são efetuadas pelo processo de gerência de mudanças.	AI6

Figura 7.1:Guia Objetivos de controle PCAOB x COBIT
Fonte: Adaptado de *IT Control Objectives for Sarbanes-Oxley* (2006)

BIBLIOGRAFIA

ACADEMY, Quint W. Redwood. (2003). **Conceitos Básicos ITIL para Gerenciamento de Serviços em TI.** São Paulo: Quint.

ABNT NBR ISO/IEC 17799 (2005). Tecnologia da Informação – Técnicas de Segurança – Códigos de Prática para a gestão de segurança da informação.

ANDRADE, A. (2006). **Governança Corporativa: Fundamentos, desenvolvimento e tendências**. 2 ed. São Paulo: Atlas.

ASTI VERA, A. **Metodologia da pesquisa científica**. (1979) 5. ed. Porto Alegre: Globo.

BRAMBILA, Gustavo Roberto; DAMÁZIO, Layany; SILVA, Ranério *et al.* (2007). **Gerência de Mudanças:** um Modelo Convergente para Empresas de Telecomunicações. Disponível em < http://www.teleco.com.br/ tutoriais/tutorialgermud/Default.asp> Acesso em 05/10/2007.

CADERNO 21. (2007) Tecnologia de Informações.

COEN, G; RUBINATO FILHO, S. (2007) itSMF no Brasil. In: **IT Service Management Fórum**. Disponível em <http://www.itsmf.com.br>. Acesso em 07/10/2007

COLARES DE OLIVEIRA, Marcelle; SILVA LINHARES Juliana (2007). A implantação de controle interno adequado às exigências da Lei Sarbanes-Oxley em empresas brasileiras – Um estudo de caso. Disponível em < http://www.congressoaec.locaweb. com.br/artigos 62006/38.pdf> Acesso em 12/07/2007.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. (2004) Enterprise Risk Management Framework,USA. Disponível em: <http://www.COSO.org>.

DELOITTE. (2003) **Lei Sarbanes – Oxley**. Guia para melhorar a governança corporativa através de eficazes controles internos.

GB921D TMForum (2005) . The Business Process Framework for the information and Comunications Services Industry Enhanced Telecom Operation Map (Etom) – Release 6 **The Telemanagement Forum November**.

GB921V TMForum (2005). An Interium View of an Interpreter´s Guide for eTOM and ITIL Practitioners – **Release 6** , November.

HP®. (2005) Modelo de referência HP ITSM. Disponível em <http://hp.com.br/itsm>. Acesso em 12/08/2007.

HUANG, J. (2005). eTOM and ITIL: Should you be Bi-lingual as TI Outsourcing Service Provider? **BPTrends**, January.

IBM, Bruce Anthony (2007) Convergence — driving profound change in the Telecommunications Industry. IBM Systems & Technology Group.

IT (2005) Governance Institute CobiT 4.0,USA. Disponível em <http://www.itgi.org>. Acesso em 12/07/2007.

IT (2006) Governance Institute. IT Control Objectives for Sarbanes-Oxley – The Role of IT in The Implementation of Internal Control Over Financial Reporting 2 ed,USA. Disponível em <http://www.itgi.org>.

IT (2004) Service Management Forum. **ITIL Service Delivery**.

IT (2004) Service Management Forum. **ITIL Service Support**.

IT (2004) Service Management Forum. **ITIL Planning to Implement Service Management**.

ITU-T (2004) Recommendation M.3050 Supplement 1: Enhanced Telecom Operations Map® (eTOM) – ITIL **Application Note**.

LEI SARBANES-OXLEY (2002). Resumo das principais cláusulas de interesse para auditores internos. Disponível em <http://www.ipai.pt/files/A_Lei_Sarbanes_Oxley_ 2002. pdf>. Acesso em 12/08/2007

MAGALHÃES, I.; PINHEIRO W. B (2007). **Gerenciamento de Serviços de TI na Prática**. Rio de Janeiro: Novatec.

MARCONDES, G. (2006) Gestão de serviços. **Enfoque ITIL e TMN e-TOM**. Brasília.

MONROY RODRIGUES , Carlos; ARIAS ALMARCHA Carlos (2007). **Agilidad Empresarial y tendências em los sistemas de informacion de los operadores de telecomunicaciones** . Disponível em <

MONTEIRO, C. (2005). **Implementando governança de TI utilizando framework COBIT®**. São Paulo: IT Partners.

OFFICE OF GOVERNMENT COMMERCE (OGC). (2007). **About ITIL®**. Disponível em: <http://www.ogc.gov.uk>. Acesso em 12/10/2007.

OFFICE OF GOVERNMENT COMMERCE (OGC). (2005). **Best practice for application management. ITIL®**. London: TSO.

OGC. OFFICE OF GOVERNMENT COMMERCE. (2004a). **An introduction to ITIL®.** London: TSO.

OFFICE OF GOVERNMENT COMMERCE (OGC). (2004b). **Best practice for business perspective:** the IS view on delivering services to the business. ITIL®. London: TSO,

RUDD, Colin. (2004). An Introductory Overview of ITIL**. Earley, Inglaterra: The IT Service Management Forum**.

SARBANES-OXLEY ACT. Congress of the United States of America. Washington: 2002.

SYSTEM AUDIT & CONTROL ASSOCIATION (ISACA). (2005). Control Objectives for Information and related Technology – **CobiT 4.0 Framework**. Ilinois: IT Governance Institute.

TELEMANAGEMENT Forum. (2002). **GB921 e-TOM** The Business Process Framework.

TMF, GB921V (2005). An Interim View of an Interpreter's Guide for eTOM and ITIL Practitioners. **Release 6**, November.

TUDE, Eduardo; MARTINS, Vergílio Antonio (2003). **Mapa de Processos de uma Operadora de Telecomunicações (eTOM)** Disponível em <http://www.teleco.com.br/ tutoriais/ tutorialetom/Default.asp> Acesso em 10/11/2007

WEILL, Peter; ROSS, Jeanne (2004) **Governança de Tecnologia da Informação**. São Paulo: M. Books.