

Revista Eletrônica de Sistemas de Informação

ISSN 1677-3071

Vol. 9, No 2

2010

doi:10.5329/RESI.2010.0902

Sumário

Ensino e pesquisa

INFORMATION SYSTEMS GRADUATE EDUCATION AND RESEARCH IN BRAZIL

Renata Mendes de Araújo, Márcio de Oliveira Barros

Foco nas pessoas

SOBRECARGA DE INFORMAÇÕES GERADAS PELA ADOÇÃO DE
TECNOLOGIAS DA INFORMAÇÃO MÓVEIS E SEM FIO E SUAS
DECORRÊNCIAS PARA PROFISSIONAIS DE VENDAS

Lisiane Barea Sandi, Amarolinda Zanela Saccol

A INFLUÊNCIA DOS DETERMINANTES DO TRABALHO GERENCIAL NA
PERCEPÇÃO DO AJUSTE ENTRE A TECNOLOGIA E A TAREFA: UM ESTUDO
EXPLORATÓRIO

Debora Bobsin, Monize Sâmara Visentini, Mauri Leodir Löbler

Foco nas organizações

MOTIVATION TO CREATE FREE AND OPEN SOURCE PROJECTS AND HOW
DECISIONS IMPACT SUCCESS

Carlos Denner Santos Jr., Kay M. Nelson

NAMORO OU AMIZADE? A VISÃO DE CLIENTES E FORNECEDORES SOBRE
RELACIONAMENTOS DE NEGÓCIO NO SETOR DE SOFTWARE

*Rita de Cássia de Faria Pereira, Carlo Gabriel Porto Bellini, Fernando
Bins Luce*

APLICABILIDADE DO COBIT NA GESTÃO DE ATIVIDADES DE TECNOLOGIA
DA INFORMAÇÃO TERCEIRIZADAS: UMA INVESTIGAÇÃO COM BASE EM
DUAS EMPRESAS MULTINACIONAIS

*Edimara Mezzomo Luciano, Mauricio Gregianin Testa, Leandro Pilatti,
Ionara Rech*

PROPOSIÇÃO DE UM MODELO DINÂMICO DE GESTÃO DE SEGURANÇA DA
INFORMAÇÃO PARA AMBIENTES INDUSTRIAIS

*Alexandre dos Santos Roque, Raul Ceretta Nunes, Alexandre Dias da
Silva*

OS USOS DA TI AO LONGO DA CADEIA DE SUPRIMENTOS E EM CONJUNTO
COM AS PRINCIPAIS TÉCNICAS COLABORATIVAS DE GESTÃO

Dayane Mayely Silva de Oliveira, Max Fortunato Cohen

Foco na tecnologia

EVALUATING TOOLS FOR EXECUTION AND MANAGEMENT OF
AUTHORIZATION BUSINESS RULES

*Leonardo Guerreiro Azevedo, Diego Alexandre Aranha Duarte,
Fernanda Baião, Claudia Cappelli*

REQUISITOS E ASPECTOS TÉCNICOS DESEJADOS EM FERRAMENTAS DE
TESTES DE SOFTWARE: UM ESTUDO A PARTIR DO USO DO SQFD

*Ismayle Sousa Santos, Pedro Alcântara Santos Neto, Rodolfo Sérgio
Ferreira de Resende, Clarindo Isaias Pereira da Silva e Pádua*



Esta obra está licenciada sob uma [Licença Creative Commons Attribution 3.0](http://creativecommons.org/licenses/by/3.0/).

APLICABILIDADE DO COBIT NA GESTÃO DE ATIVIDADES DE TECNOLOGIA DA INFORMAÇÃO TERCEIRIZADAS: UMA INVESTIGAÇÃO COM BASE EM DUAS EMPRESAS MULTINACIONAIS

APPLICABILITY OF COBIT IN MANAGING OUTSOURCED INFORMATION TECHNOLOGY ACTIVITIES: AN INVESTIGATION BASED ON TWO MULTINATIONAL COMPANIES

(artigo submetido em março de 2010)

Edimara Mezzomo Luciano

Programa de Pós-Graduação em
Administração (PPGAd/FACE) – Pontifícia
Universidade Católica do Rio Grande do Sul
ELuciano@puccrs.br

Maurício Gregianin Testa

Programa de Pós-Graduação em
Administração (PPGAd/FACE) – Pontifícia
Universidade Católica do Rio Grande do Sul
mauricio.testa@puccrs.br

Leandro Pilatti

Faculdade de Administração, Contabilidade e
Economia (FACE) – Pontifícia Universidade
Católica do Rio Grande do Sul
leandro_pilatti@gmail.com

Ionara Rech

Faculdade de Administração, Contabilidade
e Economia (FACE) – Pontifícia
Universidade Católica do Rio Grande do Sul
ionara@puccrs.br

ABSTRACT

When a company decides for IT outsourcing, it needs to deploy efficient control mechanisms, once the third party will be working directly with one of its most important assets, i.e., its information. Among the several sets of practices that intend to help managing IT activities, COBIT stands out for making a wide range of applicable control resources available to deal with outsourcing among other issues. In this context, the goal of this research is to analyze how the COBIT framework can help improving management processes of outsourced activities for both involved companies. Methodologically, this research was conducted through interviews with specialists and a case study, analyzing how the involved organizations can improve their relationship with each other. Data collection involved interviews with managers, document analysis and observation. The authors tried to identify which COBIT dimensions, processes and detailed control objectives are more appropriate for outsourcing situations. Improvement opportunities were identified in the studied processes, as well as actions that promote the use of COBIT. The main results involve the development of a procedure for process selection, which is directly applicable to outsourcing situations, as well as recommendations on necessary improvements in the application of each COBIT process, in order to increase the effectiveness of management of the outsourcing relationship.

Key-words: IT outsourcing; COBIT; COBIT applicability

RESUMO

Ao terceirizar operações de TI, as organizações precisam ter mecanismos de controle eficientes, uma vez que a empresa terceirizada estará atuando diretamente em um dos seus ativos mais importantes, que é a sua informação. Entre os diversos conjuntos de práticas para gestão de atividades relacionadas à TI, o COBIT disponibiliza uma ampla gama de recursos de controle aplicáveis a vários cenários, inclusive o de terceirização. Neste contexto, o objetivo desta pesquisa é analisar como o *framework* do COBIT pode auxiliar no aprimoramento dos processos de gestão das atividades terceirizadas tanto pela empresa terceirizada quanto pela que terceiriza o serviço. Metodologicamente, esta pesquisa foi operacionalizada por meio de entrevistas com especialistas e estudo de caso, analisando como uma organização (terceirizada) pode melhorar a relação com a empresa cliente (terceirizadora). No caso analisado, as técnicas de coleta de dados foram a entrevista (com gestores das empresas), análise de documentos e observação. Visando a reforçar a aplicabilidade da proposta, buscou-se identificar quais dimensões, processos e objetivos de controle detalhados são mais adequados a situações de terceirização. Os principais resultados envolvem a sistemática desenvolvida para a seleção de processos diretamente aplicáveis ao cenário de terceirização, bem como melhorias necessárias na aplicação de cada processo do COBIT estudado, visando qualificar a gestão da relação de terceirização.

Palavras-chave: terceirização de TI; COBIT; aplicabilidade do COBIT.

1 INTRODUÇÃO

Durante os últimos anos, a Tecnologia da Informação (TI) tem se tornado fundamental aos negócios de tal maneira que seria praticamente impossível para muitas organizações sobreviverem e prosperarem sem o seu auxílio. Conjuntamente, observa-se uma mudança nas organizações de Tecnologia da Informação, de um mercado local para um contexto nacional ou global de prestação de serviços de TI. Segundo Luciano, Testa e Rohde (2007), ao atuar em um mercado mais amplo, as organizações passam a fazer uso mais intensivo da terceirização de operações, já que nem sempre poderão contar com operações próprias em cada localidade onde mantêm projetos em andamento.

Ao terceirizar parte de suas operações de TI, uma empresa precisa ter mecanismos de controle eficientes, uma vez que a empresa terceirizada estará atuando diretamente em um dos ativos mais importantes da organização, que é a informação (RODA, 1999). Isto também se faz necessário para que a empresa terceirizada se mantenha alinhada com os objetivos de negócio da empresa cliente e que a auxilie no atendimento de suas metas e objetivos.

Estes dois cenários – a ampliação das fronteiras geográficas de atuação das organizações e o aumento da terceirização – fazem com que seja necessária uma boa estrutura de governança entre os parceiros, sob pena dos serviços prestados serem interrompidos e causarem perdas para as organizações envolvidas (BHATTACHARYA, BEHARA e GUNDERSEN, 2003). Estas perdas podem envolver questões financeiras, de imagem ou de oportunidade, todas elas com custos razoáveis para reversão, ou mesmo o aumento de custos diretos, indiretos e custos de transação (YANG e HUANG, 2000).

O COBIT tem se mostrado adequado ao controle de processo de negócio, pois disponibiliza uma ampla gama de recursos de controle e auditoria aplicáveis a vários cenários e organizações (HAWKINS, ALHAJJAJ e KELLEY, 2003). O COBIT, criado e mantido pelo ISACA (*Information Systems Audit and Control Association*) objetiva auxiliar os gerentes de TI no controle e no cumprimento dos objetivos de TI, mantendo estes sempre alinhados com os objetivos da organização. Este *framework* foi escolhido após uma análise prévia dos autores, por conter elementos inerentes à gestão e governança de TI fundamentais de serem gerenciados em contextos de terceirização. Segundo o ITGI (2006), a adoção do COBIT permite às empresas melhor alinhar seus investimentos em TI com um foco nos negócios e provê uma visão compreensível da TI para a gerência.

Neste contexto, o objetivo desta pesquisa é analisar como o *framework* do COBIT pode auxiliar no aprimoramento dos processos de interface entre a empresa terceirizada e aquela que terceiriza o serviço. A justificativa para o estudo é a importância e necessidade de que as organizações possam contar com mecanismos para controle da execução de processos de negócio dentro da relação de terceirização. Isso é vital para a continuidade dos negócios entre ambas as empresas, pois se uma delas

não cumpre o que foi acordado, a outra pode fazer valer o seu direito, por meio de multas, penalidades, sanções ou até mesmo rescisão de contrato, incidindo em prejuízos a ambas. De maneira mais ampla, dentro de uma perspectiva de governança corporativa, os *stakeholders* podem ser prejudicados, na medida em que os negócios entre as organizações sendo interrompidos, a comunidade que abrigava a empresa contratante tem perdas efetivas (RUSTAGI, KING e KIRSCH, 2008).

Esta pesquisa se desenvolveu por meio de um estudo de caso em uma empresa de grande porte e atuação mundial cuja principal atividade consiste em absorver áreas de negócio de TI terceirizadas por outras organizações, em geral de grande porte. O artigo procura explorar a aplicabilidade do uso do COBIT para melhorar o gerenciamento dos processos que envolvem a relação entre o cliente (empresa contratante) e a empresa terceira (contratada), tomando como foco da pesquisa o principal cliente da contratada, uma empresa de grande porte, com atuação mundial. Devido à extensão do COBIT (4 domínios divididos em 34 processos, que por sua vez se dividem em 318 objetivos de controle detalhados), definiu-se por meio de entrevistas com especialistas um conjunto de processos e objetivos de controle mais adequados aos objetivos da pesquisa, envolvendo oito processos pertencentes aos quatro domínios.

Além de auxiliar a empresa na adoção de boas práticas de gestão e governança de TI, tem-se ainda a oportunidade de transformar a obrigação de certas atividades (como a necessidade de cumprir requisitos regulatórios em áreas como privacidade de dados e relatórios financeiros) em uma vantagem competitiva, já que o COBIT é reconhecido pela sua contribuição potencial na governança de atividades relacionadas à TI.

O artigo está estruturado da seguinte forma: inicialmente apresentam-se as bases teóricas do estudo. Na sequência, os procedimentos metodológicos são detalhados. A sessão 4 apresenta a análise e interpretação dos dados com os pontos que precisam ser revistos e ações sugeridas que possibilitem a otimização dos processos identificados. Por fim, na sessão 5, são apresentadas algumas considerações finais.

2 TERCEIRIZAÇÃO E CONTROLES DE TI

A seguir, discorre-se sobre os principais temas desta pesquisa: o COBIT e a terceirização de processos de negócio.

2.1 COBIT

O mercado de TI conta com muitas metodologias, *frameworks* ou conjuntos de melhores práticas que guardam entre si similaridades e complementaridades. Desenvolvido nos Estados Unidos, o *framework* COBIT - *Control Objectives for Information and Related Technology* - foi criado pela *Information System Audit and Control Association* (ISACA) em 1996, a partir de ferramentas de auditoria, funcionando como uma espécie de guia para a gestão da TI nas empresas. O COBIT inclui uma

série de recursos como um sumário executivo, *framework*, controle de objetivos, mapas de auditoria e um conjunto de processos de trabalho já estabelecidos e empregados pelo mercado (HAWKINS, ALHAJJAJ e KELLEY, 2003).

Para Khalfan (2004), o COBIT independe das plataformas de TI adotadas pelas empresas e seu uso é orientado a negócios, no sentido de fornecer informações detalhadas para gerenciar processos. A metodologia é voltada para três níveis distintos: para gerentes que necessitam avaliar os riscos e controlar os investimentos de TI; para os usuários que precisam assegurar a qualidade dos serviços prestados para clientes internos e externos; e para auditores que necessitam avaliar o trabalho de gestão da TI e aconselhar o controle interno da organização. O foco principal é apontar onde devem ser feitas melhorias.

De acordo com a ISACA (2007), o COBIT (Figura 1) é um *framework* de governança em TI e um conjunto de ferramentas que suporta e permite que gerentes diminuam a lacuna existente entre requisitos de controle, dificuldades técnicas e riscos de negócios.

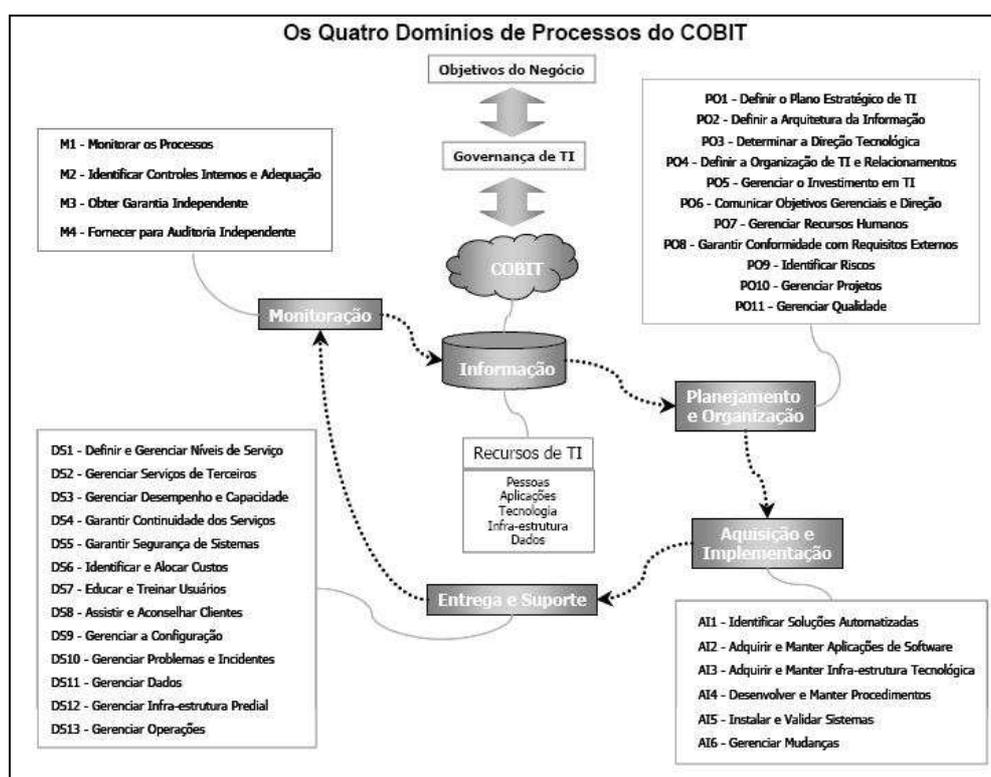


Figura 1: Domínios e Processos do COBIT

Fonte: ISACA (2010)

O COBIT se divide em quatro domínios, como pode ser visto na Figura 1:

a) Planejamento e organização: este domínio foca na identificação dos caminhos em que a TI pode melhor contribuir para a obtenção dos objetivos de negócio. Além disto, a visão estratégica necessita ser planejada, comunicada e gerenciada em diferentes perspectivas. Finalmente,

uma organização e uma infraestrutura tecnológica adequadas devem ser definidas e implementadas.

b) Aquisição e implementação: pretende identificar as soluções necessárias, utilizando o desenvolvimento ou aquisição e tê-las implementadas e integradas aos processos de negócio. Além disto, são consideradas mudanças e manutenção nos sistemas existentes, no contexto deste domínio.

c) Entrega e suporte: está focado nos produtos reais dos serviços requeridos, desde operações tradicionais de segurança e aspectos de continuidade. Este domínio inclui o processamento real de dados pelos sistemas de aplicação, normalmente classificados em controles da aplicação.

d) Monitoramento: tem como foco os processos de TI a serem avaliados, regularmente, nos aspectos de sua qualidade e conformidade com os requisitos de controle. Este domínio direciona, ainda, a vigilância da gerência nos processos de controles da organização e fornece garantia independente pela auditoria interna ou externa.

Os quatro domínios se desdobram em um conjunto de 34 processos, e estes são compostos por atividades que necessitam ser realizadas e por 318 objetivos de controle detalhados, que servem para verificar o grau de aderência do processo (ISACA, 2007). A correta execução destas atividades permite que o processo seja executado e a necessidade do domínio, em atingir os objetivos, seja alcançada.

Segundo o ITGI (2006), o COBIT tornou-se um integrador das melhores práticas em TI e um *framework* "guarda-chuva" para a governança em TI porque ele é harmonizado com outros padrões e é continuamente atualizado. A estrutura de processos do COBIT, em conjunto com a sua abordagem em alto nível orientada aos negócios, provê uma visão ampla da TI que auxilia as organizações em conseguir o maior valor possível de seus investimentos em TI (HAWKINS, ALHAJAJ e KELLEY, 2003).

2.2 TERCEIRIZAÇÃO

De maneira geral, a terceirização consiste em repassar a uma empresa terceira um serviço, um processo de negócio ou parte de uma atividade produtiva, ou seja, procurar fora da empresa (*out*) a fonte (*source*) para a realização da atividade, de forma que o *outsourcing* envolve as tarefas não realizadas internamente à empresa. Esta pode se manifestar de diferentes formas, de acordo com a sua distribuição geográfica. O *offshore outsourcing* compreende atividades que passaram a ser realizadas por empresas em outros países, em busca, geralmente, de menores custos de produção ou transação (AUBERT, RIVARD e PATRY, 2004). Já o *offshore insourcing* consiste na realização das atividades por subsidiárias de uma mesma empresa em outros países (CHUA e PAN, 2006). Outra terminologia recentemente adotada por várias organizações é o *nearshore*, que se refere a fontes de prestação de serviços externas ao país mas próximas a ele (CARMEL e ABBOTT, 2007), tal como uma empre-

sa dos Estados Unidos terceirizando atividades para uma empresa mexicana ou canadense.

A terceirização tem sido utilizada em larga escala por médias e grandes corporações do mundo todo. A terceirização pode ter diferentes motivadores: a redução de custos, a busca de maior agilidade operacional, a necessidade de *know-how* adicional ao existente na empresa contratante e a redução de atividades que não fazem parte do *core business* de uma organização (AUBERT, RIVARD e PATRY, 2004). O objeto terceirizado pode assumir diferentes enfoques: parte do pessoal de uma equipe, de diferentes etapas de um processo produtivo ou de um serviço. Pode-se ter a terceirização da aquisição de matéria-prima, de etapas da produção ou mesmo da comercialização do produto final. Ainda, ela pode ocorrer dentro ou fora das instalações da empresa. Observa-se um aumento na terceirização da produção, por meio da qual empresas de grande porte deram início a um esforço de “enxugamento”, concentrando-se no seu *core business*, visando a responder com rapidez às necessidades e demandas do mercado (AUBERT, RIVARD e PATRY, 2004).

Na área de TI, a terceirização tem crescido rapidamente, tendo se tornado “uma realidade, e vista como uma alternativa estratégica para as empresas” (SANTOS e OLIVEIRA, 2000, p. 1).

Além dos problemas tradicionais enfrentados pela empresa quando da adoção da terceirização, novos desafios emergiram, por meio de dispositivos regulatórios com os quais a empresa precisa comprovar conformidade, tais como a Sarbanes Oxley (HALL e KIEDTKA, 2006). Há, também, dificuldade para controlar os complexos contratos de terceirização (DOMBERGER, FERNANDEZ e FIEBIG, 2000). Alguns riscos ainda associados à terceirização são a comunicação, gestão da atividade, gerenciamento de mudanças, sistemas e ferramentas, controle da qualidade, controle do gerenciamento de capacidade, fatores políticos e sociais e custos de curto e longo prazo que precisam ser considerados quando da decisão de terceirizar um serviço (LOH e VENKATRAMAN, 1995).

3 MÉTODO DE PESQUISA

Este trabalho é de natureza exploratória, adequado quando o objetivo é examinar um tema ou problema de investigação pouco estudado ou que não tenha sido abordado anteriormente (SAMPIERI, COLLADO e LUCIO, 1991, p. 59), buscando compreender o estado da arte naquelas situações em que a prática se antecipa à teoria (HOPPEN, 1997).

A Figura 2, a seguir, mostra as etapas e atividades desenvolvidas nesta pesquisa.

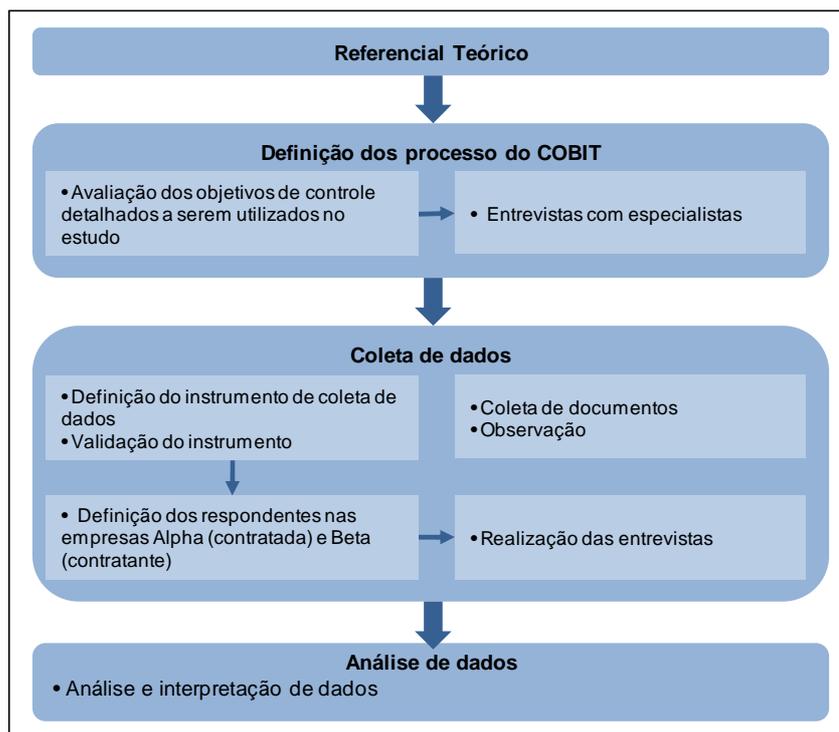


Figura 2: Desenho de pesquisa
Fonte: os autores

Quanto ao método, classifica-se como estudo de caso único. Para Yin (2001), a preferência pelo uso do estudo de caso deve ser dada quando do estudo de eventos contemporâneos, em situações onde os comportamentos relevantes não podem ser manipulados e nem observados fora de contexto, mas onde é possível se fazer observações diretas e entrevistas sistemáticas.

O caso selecionado para o estudo é a relação de terceirização entre duas empresas de grande porte, ambas com atuação na área de Tecnologia da Informação.

A empresa terceirizada, aqui chamada de empresa Alfa, detém mais de duas décadas de atuação, tendo escritórios em vários pontos do país e no exterior. Possui em torno de 3 mil funcionários e mais de uma centena de clientes em terceirização, quase que na totalidade de grande porte. É uma empresa especializada em consultoria, terceirização e integração de sistemas. A empresa desenvolve soluções para diversos segmentos de mercado e tem entre seus clientes algumas das maiores empresas do mundo. A *seleção da empresa* considerou a experiência que esta tem em atividades de terceirização. O critério de conveniência também foi considerado, já que o grupo de pesquisa tinha acesso à empresa.

Para esta pesquisa selecionou-se um de seus principais clientes, a empresa Beta, empresa da área de TI com unidades espalhadas pelo mundo, e uma das empresas destaques no seu segmento de atuação (infraestrutura de TI).

Tendo em vista a importância da terceirização para a Alfa, e por a empresa Beta ser um de seus principais clientes, justifica-se a escolha destas para este estudo. Pelo porte das empresas, representatividade no mercado de TI e mesmo sendo estas uma referência em atividades de terceirização, justifica-se o desenvolvimento de um estudo de caso único para esta pesquisa. A unidade de análise consiste na relação entre estas duas empresas, visto que o objetivo deste trabalho é analisar como o COBIT pode auxiliar o controle dos processos terceirizados.

As técnicas de coleta de dados utilizadas consistem em entrevista com especialistas, com os gestores de ambas as empresas, análise de documentos e observação.

A entrevista com especialistas foi feita visando a selecionar os processos mais adequados ao contexto analisado, para que o estudo pudesse tomar o foco necessário, de forma que os resultados fossem pertinentes ao que fora planejado, conforme exposto no início deste documento.

A *seleção dos especialistas* considerou o seu conhecimento em COBIT, em *frameworks* correlatos e em terceirização, além da sua experiência e escolaridade. Foram entrevistados cinco especialistas, sendo que dois atuam como pesquisadores em universidades e três como consultores em empresas de grande porte. O tempo de experiência variou entre 8 e 22 anos (média de 14 anos). Dos três consultores, dois atuam em posição sênior e um como consultor pleno. As entrevistas foram conduzidas presencialmente, tiveram duração entre 40 minutos e 100 minutos, e foram precedidas por uma explicação dos objetivos da pesquisa e da entrevista. As entrevistas foram gravadas, posteriormente transcritas e revisadas pelos pesquisadores.

Nesta entrevista, os especialistas foram convidados a analisar os 34 processos do COBIT, indicando em cada processo a importância percebida no controle de uma relação de terceirização. O roteiro de entrevista se constituiu em uma grade, tendo na primeira coluna o domínio (quatro domínios), na segunda coluna os processos (34), e na terceira, quarta e quinta colunas a opção para o grau de importância (baixa, intermediária ou alta). O entrevistador mantinha consigo uma lista dos 318 objetivos de controle detalhados, caso o especialista quisesse consultá-los antes de indicar a sua opinião. A aplicação do instrumento foi feita em duas etapas: a primeira foi focada na aplicabilidade (sim/não) dos processos e na segunda foi solicitado ao entrevistado que comentasse aspectos relacionados ao processo e sua aplicação.

Procedeu-se também uma *entrevista com os gestores* de Tecnologia da Informação das duas empresas, responsáveis pela definição e acompanhamento dos processos terceirizados (um gestor de cada empresa). Elaborou-se um quadro de dimensões e variáveis, baseado no referencial teórico, e que visava a analisar principalmente a percepção de aplicabilidade dos processos do COBIT a aspectos relativos à terceirização e à relação entre as empresas. Da mesma forma como acontecera na entrevista com os especialistas, a aplicação do instrumento foi feita em duas

etapas: a primeira foi focada na aplicabilidade (sim/não) dos processos e na segunda foi solicitado ao entrevistado que comentasse sobre aspectos relacionados ao processo e sua aplicação.

A entrevista abordou aspectos sobre Alinhamento entre TI e negócio, cultura organizacional, desafios do *outsourcing* (necessidades, existência de indicadores de acompanhamento e métricas), além de questões relativas a “se” e “como” se manifestam na relação entre as empresas os oito processos do COBIT selecionados. As entrevistas foram conduzidas presencialmente, tiveram duração entre 50 minutos e 1h20 minutos, e foram precedidas por uma explicação dos objetivos da pesquisa e da entrevista. As entrevistas foram gravadas, posteriormente transcritas e revisadas pelos pesquisadores.

A observação foi utilizada no intuito de verificar aspectos intrínsecos à relação de terceirização, mas não aparentes de forma tão clara quando se adotam outras técnicas de coleta de dados. Ocorreu em reuniões entre as duas empresas ocorridas durante o segundo semestre de 2007 (seis reuniões), de forma parcialmente aberta: os gestores da Alfa e da Beta tinham conhecimento que as reuniões estavam sendo acompanhadas com o intuito da pesquisa, mas os demais participantes da reunião não foram informados.

Os aspectos analisados na observação envolveram a busca por evidências de: a) acompanhamento e controle das atividades (se surgiam pontos em que uma das partes mostrava desconhecimento); b) relacionamento (animosidade ou gentileza, irritação ou aceitabilidade), proximidade (cooperação/conflicto iminente), entre outros. A análise de documentos utilizou contratos e registros de reuniões para estabelecimento da parceria e procurou identificar situações em que os controles do COBIT poderiam ser úteis para manter e aprimorar aspectos de gestão e mesmo para evitar contratemplos e situações diferentes das combinadas entre as partes.

A análise dos dados provenientes das entrevistas ocorreu por meio de análise de conteúdo para as questões abertas, seguindo sobretudo as recomendações de Bardin (1977). Para as questões de avaliação da aplicabilidade do COBIT, fez-se um agrupamento de respostas em cada item da escala.

A triangulação de fontes de dados e o cuidado na coleta e análise de dados, fundamentais para o rigor científico, foram medidas tomadas durante a realização desta pesquisa.

4 RESULTADOS

A seguir, discorre-se sobre a análise dos dados. Primeiramente, procede-se à análise dos dados coletados por meio das entrevistas com especialistas. Em seguida, segue a análise das entrevistas com os gestores das organizações envolvidas (Alfa e Beta), bem como uma comparação da realidade da empresa com os preceitos do COBIT.

4.1 ENTREVISTA COM ESPECIALISTAS: IDENTIFICAÇÃO DOS PROCESSOS ADEQUADOS AO CONTEXTO

Primeiramente, procedeu-se à análise das entrevistas com os especialistas, visando a selecionar o conjunto de processos mais adequados ao controle da atividade de terceirização de atividades de TI. Agrupados nos quatro domínios do COBIT há 34 processos a serem verificados pelos gestores de TI quando da implementação completa do *framework*. Para cada processo existem objetivos de controle detalhados (OCDs) que auxiliam o gestor de TI na verificação da conformidade da empresa com o processo em estudo. Conforme exposto na Figura 2, foram escolhidos pelos pesquisadores oito processos aparentemente pertinentes ao controle e acompanhamento de uma relação de terceirização, sendo que a opção por estes oito processos foi avaliada com a empresa Alfa. Procedeu-se então a uma avaliação com os cinco especialistas para a escolha dos OCD a serem usados como base para a etapa seguinte do estudo. Os oito processos foram mantidos pelos especialistas, que selecionaram 39 OCD. Naturalmente, a opinião dos especialistas não era totalmente convergente, de forma que quando não havia uma clara preferência em relação a determinado objetivo estar adequado ou não, os pesquisadores tomaram a decisão final, baseada nos comentários dos especialistas ao indicar ou não o objetivo.

Na Figura 3, está detalhada a sequência de passos executados até serem escolhidos os processos a serem analisados na empresa.

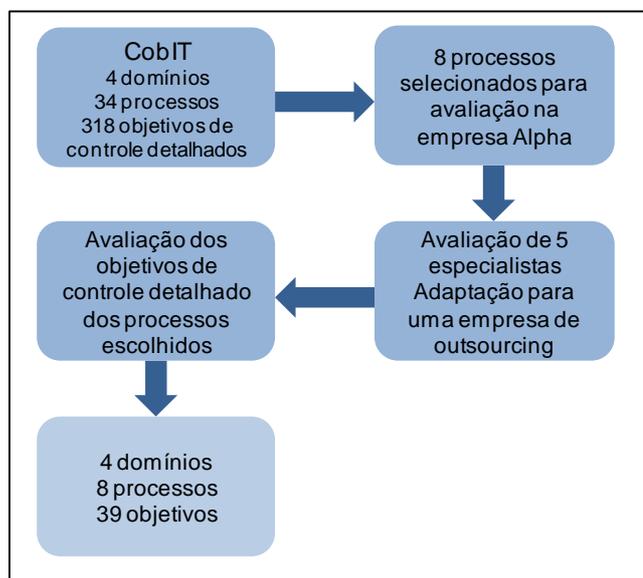


Figura 3: Etapas da validação dos processos e objetivos
Fonte: os autores

Os oito processos e os 39 OCD selecionados pelos especialistas estão expostos abaixo, no Quadro 1.

Domínio	Processo	Objetivo de controle detalhado
Planejamento e organização	PO 04 – Definir a organização e relacionamentos de TI	PO4.1 <i>Framework</i> de processos de TI PO4.4 Colocação organizacional e função da TI PO4.6 Papéis e responsabilidades PO4.9 Responsabilidade dos dados e sistema PO4.10 Supervisão PO4.11 Segregação dos deveres PO4.12 Equipe de funcionários de TI PO4.13 Pessoas chave da TI PO4.14 Procedimentos e políticas para funcionários contratados PO4.15 Relacionamentos
	PO 06 – Comunicar objetivos e diretrizes da administração	PO6.1 Política de TI e controle de ambiente PO6.3 Gerenciamento de políticas de TI PO6.4 Aplicação de políticas PO6.5 Comunicação da direção e dos objetivos de TI
	PO 07 – Gerenciar recursos humanos	PO7.1 Recrutamento e retenção de pessoal PO7.2 Competências pessoais PO7.3 Supervisão de papéis PO7.4 Treinamento de pessoal PO7.5 Dependência de indivíduos PO7.6 Procedimentos de verificação de pessoal PO7.7 Avaliação de desempenho do funcionários PO7.8 Mudança de cargo e desligamento
Aquisição e implementação	AI 06 – Gerenciar mudanças	AI6.1 Procedimentos e padrões de mudança AI6.2 Avaliação de impacto, priorização e autorização AI6.3 Mudanças emergenciais AI6.5 Fechamento e documentação de mudança
Entrega e suporte	ES 01 – Definir níveis de serviço	ES1.1 <i>Framework</i> de nível de serviço ES1.2 Definição de serviços ES1.3 Acordo de nível de serviço (SLA) ES1.5 Monitoramento e relato do atingimento dos SLAs ES1.6 Revisão dos SLAs e dos contratos
	ES 02 – Gerenciar serviços de terceiros	ES2.1 Identificação do relacionamento de todos os fornecedores ES2.2 Gerenciamento de riscos de fornecedores ES2.4 Monitoramento de desempenho de fornecedores
	ES 13 – Gerenciamento de operações	ES13.1 Instruções e procedimentos de operações ES13.2 Programação do trabalho ES13.4 Dispositivos de saída de documentos confidenciais
Monitoramento	ME 02 – Avaliar a adequação do controle interno	ME 2.1 Monitoramento do <i>framework</i> de controle interno

Quadro 1: Domínios, processos e objetivos de controle
detalhado selecionados pelos especialistas
Fonte: os autores

Este aspecto por si só já representa uma contribuição, uma vez que outras empresas que tenham a intenção de utilizar o COBIT para o controle de uma relação de terceirização podem fazer uso prioritário dos processos acima, deixando os demais processos para uma segunda etapa.

4.2 ENTREVISTA COM OS PRINCIPAIS GESTORES: APLICABILIDADE DOS PROCESSOS SELECIONADOS PELOS ESPECIALISTAS

A partir das entrevistas realizadas com os gestores (da Alfa e Beta, responsáveis pela relação de terceirização) foram obtidas informações fundamentais para a análise e o entendimento da relação entre a empresa que terceiriza e o terceirizado e também dos processos existentes.

Pode-se dizer que as entrevistas com os gestores tiveram duas etapas. A primeira estava focada em aspectos mais gerais da relação de terceirização e a segunda mais focada na aplicabilidade dos processos do COBIT.

Na primeira parte da entrevista, foi possível perceber deficiências no alinhamento entre a TI e o negócio da Alfa, o que faz a equipe que atende a empresa terceira se sentir, por vezes, deslocada *entre* as duas empresas (sem se sentir parte de nenhuma delas). Acerca da cultura organizacional, percebeu-se bom nível de aceitação de mudanças nas duas empresas, possivelmente pelo fato delas trabalharem em contato com equipes em diferentes locais do mundo e diferentes culturas.

Ainda sob a ótica de cultura organizacional, a área de TI é percebida de diferentes formas. O ponto de vista do principal cliente da empresa é que a TI é uma prestadora de serviços. Mas não é assim que ela é vista pela própria empresa. Isso pode gerar algumas desavenças, já que no dia-a-dia as equipes da Alfa e da Beta se misturam no mesmo ambiente. Se não estiver claro o papel de cada uma, a convivência pode acarretar alguns percalços.

Percebeu-se, igualmente, que não existe um processo formal de identificação e revisão de necessidades para manter o objeto terceirizado em funcionamento. Há reuniões periódicas entre os gestores de cada equipe, mas nem sempre os resultados são formalizados. O impacto disto possivelmente é minimizado pela existência de métricas e indicadores bem definidos e rigorosos quanto ao nível de serviço.

Apesar de nem todas as métricas estarem satisfatórias perante o cliente, a empresa tem conhecimento de todas as métricas exigidas. Os indicadores internos auxiliam o gestor a gerenciar efetivamente as operações ao passo que os indicadores externos (exigidos e cobrados pelo cliente) garantem ao cliente que a empresa está prestando o serviço dentro dos padrões exigidos.

A métrica de *turnover* (rotatividade) é um exemplo de ponto a ser melhorado. Na entrevista, surgiu que o processo de acompanhamento dos indicadores é satisfatório, mas em algumas das reuniões percebeu-se que ele ainda precisa de melhorias, já que houve dissonâncias em relação a dados de dois indicadores (tempo de preenchimento das vagas e tarefas entregues *on-time*).

A segunda parte da entrevista, focada na aplicabilidade dos processos e OCD, teve como base os objetivos identificados como principais pelos especialistas. Os oito processos indicados pelos especialistas originam 39 objetivos de controle detalhados, o que ainda é um número significativo de elementos para análise. Sendo assim, a entrevista com os gestores teve como objetivo refinar a lista de objetivos de controle detalhados aplicáveis às relações de terceirização (definida pelos especialistas). A base para a entrevista foi a relação de terceirização entre as empresas objeto do estudo, mas sem deixar de considerar a vivência dos gestores em outras situações de terceirização, já que sua experiência nesta área é significativa.

Para os objetivos identificados como aplicáveis, os gestores foram convidados a identificar uma ordem de prioridade (alta, média ou baixa). Isso foi feito com o intuito de orientar outras empresas em relação ao que deve receber atenção prioritária da empresa, já que a adoção de qualquer conjunto de melhores práticas é gradativa, seja pelo custo da adoção em recursos e pessoas, seja pelo esforço de equipe consumido. As entrevistas tinham um objetivo adicional de identificar a satisfação percebida em cada um dos aspectos analisados (objetivos de controle detalhados). Esta análise de satisfação teve o intuito de identificar itens mais complexos ou que deveriam potencialmente exigir um olhar mais apurado em outros processos de adoção.

Os objetivos de controle detalhados dos processos que tinham baixa importância recebiam um peso 1, os de média importância recebiam um peso 2 e os de alta importância recebiam um peso 3. Para o grau de satisfação, se o gestor estava totalmente insatisfeito com o processo existente dentro da empresa, então o objetivo de controle recebia um peso 4, caso estivesse insatisfeito, o peso era 3, se estivesse satisfeito o peso atribuído era 2 e caso estivesse totalmente satisfeito o peso era 1.

A partir disso, procedeu-se à comparação entre importância e satisfação percebida pelos gestores em relação a como ocorre na prática o que preconiza cada OCD. Com isso foi possível gerar um escore e priorizar os objetivos e os processos de uma maneira que se pudesse destacar processos de alta importância e maior insatisfação. Desta forma, foi possível montar um quadro que auxilie as organizações na identificação de processos prioritários para endereçar esforços, visando ao aprimoramento. O conjunto de 39 elementos foi dividido em tercias, visando à classificação em três faixas de prioridade de ação: alta, média e baixa.

4.3 PRIORIZAÇÃO DOS OBJETIVOS DO COBIT DO ADEQUADA PARA ATIVIDADES DE TERCEIRIZAÇÃO

A seguir, procede-se a análise da opinião dos gestores acerca da aplicabilidade e importância de cada OCD analisado. Algumas das recomendações são aplicáveis a apenas um dos lados do processo (contratada ou contratante), mas a maioria se aplica a ambas, já que o foco de análise foi a relação de terceirização. Tanto a empresa que contrata o serviço como a contratada precisam saber qual é a sua responsabilidade no processo, visando a alcançar o que se espera daquela relação de terceirização.

4.3.1 Prioridade alta

Os OCD classificados como de prioridade alta estão organizados em ordem decrescente de score (ou seja, os primeiros a serem citados são os indicados como mais importantes (e com menor satisfação no atendimento). Para cada OCD, faz-se uma comparação da situação encontrada com as premissas do COBIT, sugerindo ações (possivelmente também aplicáveis a outras situações de terceirização) para o seu atendimento.

No processo PO 07 (Gerenciar recursos humanos), o COBIT estabelece que a gestão de TI deva contratar e treinar pessoal, motivando por meio de sólidos planos de carreira, designando papéis que correspondam às competências, estabelecendo um processo definido de revisão destes papéis, criando descrições de posições e garantindo a consciência da dependência de indivíduos.

Desta forma, para o OCD PO 7.4 (Treinamento de pessoal), é importante prover aos funcionários de TI uma orientação apropriada quando contratados e um treinamento contínuo para manter o conhecimento, técnica e habilidades, controles internos e consciência de segurança no nível requerido para atingir os objetivos organizacionais.

No processo ME 02 (Avaliar a adequação do controle interno), deve-se assegurar a realização dos objetivos de controle internos previstos para os processos de TI. Isso é possível por meio do compromisso de monitorar os processos de controles internos para atividades de TI e identificar ações de melhoria.

Desta forma, para o objetivo de controle ME 2.1 (Monitoramento do *framework* de controle interno), sugere-se monitorar continuamente o *framework* de controle do ambiente de TI, tanto em aspectos de governança de TI, gerenciamento de riscos e segurança da informação como na aplicação do próprio COBIT. Esta avaliação pode ser feita usando melhores práticas da indústria e *benchmarking*, visando a aprimorar o ambiente de controle de TI e o *framework* de controle.

No processo PO 04 (Definir a organização e relacionamentos de TI), o COBIT ressalta que é necessário estabelecer estruturas organizacionais de TI transparentes, flexíveis e receptivas, bem como definir e implementar

processos de TI com responsáveis, papéis e responsabilidades integrados com o negócio e com o processo de decisão.

Desta forma, para o objetivo de controle PO 4.12 (Acompanhamento permanente da equipe de TI), é importante avaliar requisitos da equipe de funcionários com uma frequência regular ou quando houver grandes mudanças no negócio e também a avaliação do ambiente de TI para garantir que se tenha um número suficiente de pessoas com competência no que está sendo trabalhado. Este objetivo leva em consideração a colocação do negócio/equipe de funcionários de TI, treinamento funcional cruzado, mudança de cargo e oportunidades de *outsourcing*.

Para o objetivo de controle PO 7.1 (Recrutamento e retenção de pessoal), é necessário garantir que os processos de recrutamento de pessoal de TI estejam sincronizados com a política e os procedimentos de recrutamento de pessoal da organização como um todo. A gerência deve implementar processos que garantam que a organização tenha uma força de trabalho apropriada com as competências necessárias para atingir os objetivos organizacionais.

Já para o objetivo de controle PO 7.2 (Competências pessoais), sugere-se verificar regularmente se a equipe possui as competências para cumprir seus papéis com base em sua educação formal, capacitações ou experiência. Torna-se fundamental definir requisitos chave de competências de TI e verificar se estão sendo mantidos, usando programas de qualificação e de certificação quando apropriado.

No objetivo de controle PO 7.7 (Avaliação do desempenho do funcionário), sugere-se que as organizações realizem avaliações regulares, procurando identificar se a atuação profissional do funcionário coaduna os seus objetivos pessoais com os da organização. Sempre que isto estiver dissociado, deverão ser planejadas medidas, visando a evitar que uma das partes (ou o funcionário ou a empresa) esteja em dissonância com os seus objetivos. Deverão ser estabelecidos mecanismos para que os funcionários solicitem capacitação sempre que necessário.

Para o objetivo de controle PO 7.8 (Mudança de cargos e desligamento), sugerem-se ações referentes à adequação da atividade dos profissionais ao seu cargo. Dificilmente um profissional que recebe remuneração ou vantagens (e eventualmente reconhecimento e status) menores do que o conjunto de responsabilidades a ele atribuído estará satisfeito, e profissionais não satisfeitos contribuem para aumentar os riscos relacionados à terceirização.

No processo ES 13 (Gerenciamento de operações), o COBIT ressalta a importância da gerência eficaz do processamento de dados e a manutenção de *hardware*. Este processo inclui definir políticas e procedimentos das operações, proteção da saída de dados sensíveis, monitoria da infraestrutura e manutenção preventiva do *hardware*. O objetivo em relação a este aspecto é manter a integridade de dados, reduzir os atrasos no negócio e os custos operacionais de TI.

Para o objetivo de controle ES 13.2 (Programação do trabalho), é importante observar o planejamento das atividades e projetos na sequência mais eficiente. As programações iniciais, bem como as mudanças destas programações, devem ser autorizadas. Os procedimentos devem ser levados em conta para identificar, investigar e aprovar partidas das programações padrão do trabalho.

Para o objetivo de controle ES 13.4 (Dispositivos de saída e documentos confidenciais), deve-se estabelecer as proteções físicas apropriadas, práticas da contabilidade e inventário de patrimônio de recursos sensíveis de TI tais como formulários especiais, instrumentos de negociação e equipamentos para fins específicos.

No processo PO 06, a gerência deve desenvolver uma estrutura para definir e comunicar políticas. Um programa contínuo de comunicação deve ser executado para articular a missão, os objetivos do serviço, as políticas e os procedimentos, sendo aprovado e suportado pela gerência. A comunicação suporta o atendimento de objetivos e assegura a consciência e a compreensão do negócio e dos riscos de TI, objetivos e direção. O processo deve assegurar a conformidade com as leis e regulamentos relevantes.

Para o objetivo de controle PO 6.1 (Política de TI e controle do ambiente), sugere-se definir os elementos de um ambiente do controle para TI, alinhado com a filosofia de gerenciamento e estilo de operar da empresa. Estes elementos incluem expectativas e requisitos a respeito da entrega do valor dos investimentos em TI, risco tolerado, integridade, valores éticos, competência da equipe de funcionários e responsabilidade. O ambiente de controle deve ser baseado em uma cultura que suporte a entrega do valor ao controlar riscos significativos, incentivar a cooperação e o trabalho de equipe cruzado (com equipes do contratante e do contratado), promovendo a conformidade e a melhoria contínua dos processos, e ainda evitando desvios e falhas nos processos. Desta forma, a riqueza da experiência obtida na operação pode ser compartilhada entre as equipes do contratado e do contratante.

Para o objetivo de controle PO 6.3 (Gerenciamento de políticas de TI), sugere-se desenvolver e manter um conjunto de políticas para suportar a estratégia da TI. Estas políticas devem incluir a intenção da política, os papéis e as responsabilidades, o processo de exceção, a aproximação da conformidade e as referências aos procedimentos, aos padrões e às guias. As políticas devem endereçar tópicos chave tais como a qualidade, a segurança, a confidencialidade, controles internos e a propriedade intelectual. Sua relevância deve ser confirmada e aprovada regularmente.

Já para o objetivo de controle PO 6.5 (Comunicação da direção e dos objetivos de TI), é importante assegurar-se de que a consciência e a compreensão do negócio e dos objetivos de TI e a direção sejam comunicadas por toda empresa. A informação comunicada deve abranger uma missão claramente articulada, objetivos do serviço, segurança, controles internos, qualidade, um código de ética/conduita, políticas e

procedimentos etc., e deve ser incluída dentro de um programa contínuo de comunicação, suportado pela gerência superior na ação e nas palavras. A gerência deve dar atenção específica para comunicar a consciência da segurança e a mensagem de que segurança é responsabilidade de todos.

4.3.2 Prioridade intermediária

No processo ES 01 (Definir níveis de serviço), uma comunicação eficaz entre gerência de TI e clientes de negócio a respeito dos serviços requeridos é permitida por uma definição documentada e por um acordo dos serviços de TI e níveis de serviço. Este processo inclui também o monitoramento e o relato oportuno às partes interessadas na realização de níveis de serviço. Este processo permite o alinhamento entre os serviços de TI e as exigências relacionadas do negócio.

Para o objetivo de controle ES 1.1 (*Framework* de gerenciamento de nível de serviço), sugere-se que seja definida uma estrutura que forneça um processo formalizado da gerência do nível de serviço entre o cliente e o fornecedor de serviço. Esta estrutura mantém o alinhamento contínuo com exigências e prioridades do negócio e facilita a compreensão comum entre o cliente e o provedor de serviço. A estrutura inclui processos para a criação de requisitos do serviço, definições do serviço, acordos de nível de serviço (SLAs), acordos de níveis operacionais (OLAs) e fontes financiadoras. Estes atributos são organizados em um catálogo do serviço. A estrutura define a estrutura organizacional para a gerência do nível de serviço, cobrindo os papéis, as tarefas e as responsabilidades de fornecedores de serviço e de clientes internos e externos.

Para o objetivo de controle ES 1.3 (Acordo de nível de serviço), é fundamental definir acordos do nível de serviço para todos os serviços críticos de TI baseados nos requisitos do cliente e das capacidades de TI. Isto cobre compromissos do cliente, requisitos de suporte de serviço, métricas quantitativas e qualitativas para medir o serviço assinado pelas partes interessadas, financiamento e arranjos comerciais, quando isto se aplicar, e papéis e responsabilidades, incluindo a supervisão do SLA. Os itens a serem considerados são a disponibilidade, confiabilidade, desempenho, capacidade do crescimento, níveis de suporte, do planejamento da continuidade, da segurança e de restrições de demanda.

Já para o objetivo de controle ES 1.6 (Revisão dos SLAs e dos contratos), os acordos de nível de serviço e contratos com os fornecedores de serviço internos e externos precisam ser revistos periodicamente, para assegurar que sejam eficazes, atualizados e que as mudanças nas exigências tenham sido explicadas.

No objetivo de controle PO 4.6 (Definição de papéis e responsabilidades), deve-se proceder à definição e comunicação de papéis e responsabilidades para todo o pessoal na organização com relação aos sistemas de informação para permitir a autoridade suficiente para exercer os papéis e responsabilidades atribuídos. É necessário criar descrições dos cargos e atualizá-las regularmente. Estas descrições delineiam a autoridade e a

responsabilidade, incluindo definições das habilidades e experiência necessárias na posição relevante, apropriadas para o uso na avaliação de desempenho. As descrições dos papéis devem conter a responsabilidade para o controle interno.

Quanto ao objetivo de controle PO 4.9 (Responsabilidade dos dados e do sistema), sugere-se que a organização contratante forneça à contratada detalhes documentados acerca da estrutura de dados e dos sistemas, bem como acesso a ferramentas de acompanhamento do impacto nos sistemas das ações desenvolvidas. Isso permitirá que a contratada enderece as suas responsabilidades para a posse de dados e de sistemas de informação. Os proprietários tomam decisões sobre como classificar a informação e os sistemas e como protegê-los de acordo com esta classificação.

Já para o objetivo de controle PO 4.10 (Supervisão), a supervisão na função de TI deve ser realizada, para assegurar-se que os papéis e as responsabilidades estejam sendo exercidos corretamente, a fim de avaliar se todo o pessoal tem a autoridade e os recursos suficientes para executar seus papéis e responsabilidades, e para rever os indicadores chave do desempenho.

Para o objetivo de controle PO 4.14 (Procedimentos e políticas para contratação de funcionários), devem ser definidas e implementadas políticas e procedimentos, visando a controlar as atividades dos consultores e de pessoal contratado pela TI para assegurar a proteção dos recursos de informação da organização e para atender exigências contratuais.

Para o OCD PO 4.15 (Relacionamentos), é importante desenvolver e manter uma coordenação e uma estrutura de comunicação, visando à ligação entre a TI da contratante, a área de TI da contratada e as áreas de negócio de ambas. Por exemplo, informações sobre equipe gestora da contratante, unidades de negócio, usuários individuais, fornecedores, pessoal de segurança, gerentes de risco, *outsourcers* e gerência *offsite* são fundamentais para a tomada de decisão tática e operacional da contratada.

Quanto ao objetivo de controle PO 7.3 (Supervisão de papéis), deve-se definir, monitorar e supervisionar papéis, responsabilidades e estruturas da recompensa para o pessoal, incluindo a exigência de aderir às políticas e aos procedimentos de gerência e ao código de ética e de prática profissional. Os termos e as condições de emprego devem ressaltar a responsabilidade do empregado com a segurança da informação, o controle interno e a aderência aos regulamentos. O nível da supervisão deve estar alinhado com o que as empresas esperam em termos de desempenho e comportamento de cada papel.

Para o objetivo de controle PO 7.5 (Dependência de indivíduos), sugere-se que a organização minimize a exposição à dependência crítica de indivíduos chave por meio da captação do conhecimento (documen-

tação), de compartilhamento do conhecimento, de planejamento de sucessão e de apoio da equipe de funcionários.

Já para o objetivo de controle ES 13.1 (Instruções e procedimentos de operações), sugere-se que a organização defina, execute e mantenha procedimentos para as operações de TI e assegure-se de que a equipe de funcionários das operações esteja familiarizada com todas as tarefas que deve executar. Os procedimentos operacionais devem prever deslocamento formal da atividade, atualização de status, problemas operacionais, procedimentos de escalonamento e de relatórios das responsabilidades, assegurando a continuidade das operações.

Para o objetivo de controle PO 6.4 (Aplicação de políticas), sugere-se assegurar que políticas de TI estejam implementadas e sejam respeitadas por toda a equipe. Os métodos de implementação dessas políticas devem estar alinhados às necessidades das organizações e às implicações da política em cada atividade terceirizada.

Quanto ao objetivo de controle ES 1.2 (Definição de serviços), deve-se definir uma base de serviços de TI em características do serviço e em exigências do negócio, organizadas e armazenadas centralmente por meio da execução de uma aproximação do catálogo/portfólio de serviços.

Para o objetivo de controle ES 1.5 (Monitoria e relato do atingimento dos SLAs), sugere-se que a contratante monitore continuamente critérios especificados de desempenho do nível de serviço. Os relatórios são fornecidos em um formato adequado às partes interessadas na realização de níveis de serviço. As estatísticas de monitoração são analisadas e servem para identificar tendências negativas e positivas para serviços locais ou globais.

No objetivo de controle PO 4.4 (Colocação organizacional da função da TI), sugere-se prever a função da TI na estrutura organizacional, refletindo a importância da TI dentro da empresa, principalmente a sua criticidade à estratégia de negócio e o nível da dependência operacional da TI. A posição do CIO é proporcional à importância da TI dentro da empresa.

Para o objetivo de controle PO 4.11 (Segregação dos deveres), sugere-se executar uma divisão dos papéis e das responsabilidades que reduza a possibilidade de que um único indivíduo tenha conhecimento de um processo crítico. A gerência deve certificar-se também de que o pessoal está executando somente atividades autorizadas relevantes para seus respectivos trabalhos e posições.

Já para o objetivo de controle PO 7.6 (Procedimentos de verificação de pessoal), sugere-se incluir verificações pessoais dentro do processo de recrutamento. A extensão e a frequência da revisão do período destas verificações dependem da sensibilidade e/ou da criticidade da função e devem ser aplicadas a empregados, contratantes e vendedores.

Quanto ao objetivo de controle PO 4.1 (*Framework* de processos de TI), deve-se prever uma estrutura de processos de TI para executar o

plano estratégico. Inclui a estrutura do processo e relacionamentos, posse, maturidade, medida de desempenho, melhoria, conformidade, alvos da qualidade e planos para atingi-los. Fornece a integração entre os processos que são específicos da TI, gerência de portfólio da empresa, processos do negócio e processos da mudança do negócio. Esta estrutura de processo deve ser integrada em um sistema de gerência da qualidade e na estrutura interna do controle.

No processo ES 2 (Gerenciar serviços de terceiros), o COBIT ressalta a necessidade de assegurar que os serviços providenciados por terceiros atinjam as exigências do negócio e requer um efetivo processo de gerenciamento de terceiros. Este processo é realizado ao definir claramente os papéis, as responsabilidades e as expectativas em acordos com terceiros, bem como ao rever e monitorar tais acordos para garantir sua eficácia e conformidade com os mecanismos regulatórios da contratante. A gerência eficaz de serviços terceirizados minimiza o risco do negócio associado com os fornecedores.

Para o objetivo de controle ES 2.3 (Gerenciamento de riscos de fornecedores), deve-se identificar e mitigar os riscos que se relacionam à habilidade dos fornecedores de continuar a entrega eficaz do serviço, de uma maneira segura e eficiente, regularmente. Deve-se assegurar que os contratos se ajustem aos padrões universais do negócio e atendam a exigências legais e regulatórias.

4.3.3 Prioridade baixa

Mesmo sendo de menor prioridade, considera-se necessário listar as recomendações sugeridas. O fato de estes objetivos de controle serem de baixa prioridade indica que eles são os últimos a serem adotados, mas, ainda assim, precisam ser adotados a fim de continuar o processo de melhoria contínua das atividades relacionadas à terceirização.

Para o objetivo de controle PO 4.13 (Identificação de pessoas-chave na TI), sugere-se definir e identificar pessoal chave de TI, prevendo a possibilidade de substituição em caso de saída não programada.

Para o objetivo de controle ES 2.2 (Gerenciamento do relacionamento com os fornecedores), deve-se formalizar o processo de gerenciamento do relacionamento com o fornecedor para cada fornecedor. Os proprietários do relacionamento devem embasar-se em problemas do cliente e do fornecedor e assegurar a qualidade do relacionamento baseado na confiança e na transparência (por exemplo, com os acordos do nível de serviço).

Para ES 2.4 (Monitoramento do desempenho de fornecedores), sugere-se que a organização contratante estabeleça um processo para monitorar a entrega do serviço, visando a assegurar que a contratada atinja as exigências do negócio e mantenha aderência aos acordos do contrato e aos acordos de nível de serviço. É importante que seu desempenho seja compatível com o de fornecedores alternativos e as condições de mercado.

Quanto ao objetivo de controle ES 2.1 (Identificação do relacionamento com todos fornecedores), sugere-se identificar todos os serviços fornecidos por fornecedores externos e categorizá-los de acordo com o tipo, significado e a criticidade. Deve-se manter a documentação formal dos relacionamentos técnicos e organizacionais cobrindo os papéis e as responsabilidades, objetivos, *deliverables* previstos e credenciais dos representantes destes fornecedores.

No processo AI 06 (Gerenciar mudanças), o COBIT ressalta que todas as mudanças, incluindo manutenções emergenciais e *patches* relacionados à infraestrutura e às aplicações dentro do ambiente da produção devem ser gerenciados formalmente de maneira controlada. As mudanças (incluindo procedimentos, processos, parâmetros de sistema e de serviço) devem ser registradas, avaliadas e autorizadas antes da execução e devem ser revistas, comparando os resultados ao planejamento, depois da implementação. Isto assegura a mitigação dos riscos de impactar negativamente a estabilidade ou a integridade do ambiente da produção.

Para o objetivo de controle AI 6.1 (Definição de procedimentos e padrões para a mudança), sugere-se ajustar os procedimentos formais da gerência da mudança para lidar de uma maneira padronizada com todos os pedidos (incluindo manutenção e *patches*) para mudanças nas aplicações, procedimentos, processos, parâmetros de sistema e plataformas subjacentes.

Para o objetivo de controle AI 6.2 (Avaliação de impacto, priorização e autorização), a organização fornecedora deve assegurar-se de que todos os pedidos de mudança sejam avaliados de uma maneira estruturada com relação a impactos no sistema operacional e em sua funcionalidade. Esta avaliação deve incluir a categorização e a priorização das mudanças. Antes da migração para produção, as mudanças devem ser autorizadas pela parte interessada.

Já para o objetivo de controle AI 6.3 (Mudanças emergenciais), um processo deve ser estabelecido, visando a definir, levantar, avaliar e autorizar as mudanças emergenciais, que não seguem o processo estabelecido para mudanças regulares. A documentação e o teste devem ser executados, possivelmente depois da execução da mudança de emergência.

Quanto ao objetivo de controle AI 6.5 (Fechamento e documentação da mudança), a organização deve atualizar o sistema, a documentação e os procedimentos associados do usuário sempre que mudanças de sistema sejam executadas. Deve-se estabelecer um processo de revisão para assegurar a execução completa das mudanças.

5 CONSIDERAÇÕES FINAIS

O estudo procurou, ao longo de seu desenvolvimento, obter subsídios que pudessem avaliar a aplicabilidade do COBIT à gestão da relação de terceirização. Este objetivo foi atingido, por meio da sistemática para

seleção de processos adequados ao contexto de terceirização, tendo em vista a necessidade de customização dos 318 objetivos de controle detalhados. Procedeu-se, ainda, uma extensa análise de que ações as organizações envolvidas em terceirização podem realizar, visando a estarem mais aderentes ao que preconiza o COBIT. Considera-se que estes dois aspectos constituem a contribuição deste estudo.

Por meio das entrevistas e da observação foi possível analisar em detalhes o funcionamento da relação entre a empresa Alfa e o seu principal cliente, a empresa Beta. Também se pôde comparar os processos de terceirização utilizados com o que preconiza o COBIT. Isto permitiu identificar a aplicabilidade dos processos do COBIT, selecionando aqueles mais adequados ao contexto. Embora a pesquisa tenha feito uso do estudo de caso, a análise procurou extrapolar os achados para o contexto de terceirização, não ficando limitada à realidade das duas empresas.

De maneira geral, a gerência de TI deve se preocupar principalmente com o domínio *Planejamento e organização*, mais especificamente com o processo PO 07 (Gerenciar Recursos Humanos), pois na terceirização de serviços a qualidade obtida é diretamente proporcional à qualidade das pessoas e ao alinhamento entre os saberes e competências destas com o conjunto de papéis e responsabilidades. Neste aspecto amplo estão envolvidos o recrutamento, a seleção, a capacitação, a definição de papéis e responsabilidades, o controle do índice de *turnover*, a constante revisão do desempenho da equipe de funcionários da TI e a satisfação dos *stakeholders* com a experiência e a competência do pessoal de TI. Entretanto, é importante ressaltar que existem métricas, indicadores e relatórios gerenciais que auxiliam os gestores no acompanhamento e no controle dos processos existentes, relacionados ao processo analisado do COBIT. Isto demonstra o uso intrínseco dos processos e atividades já mencionados.

No que diz respeito ao processo ME 02 (Avaliar a adequação do controle interno), é importante monitorar de uma forma regular a estrutura de processos internos, a fim de que seja possível ter um controle mais efetivo e identificar melhorias. Uma forma de se mensurar esta sugestão de aprimoramento no processo é através do número de iniciativas de melhorias no controle interno.

Já no processo ES 13 (Gerenciamento de operações), é importante destacar a necessidade de práticas e processos consistentes, operando de acordo com níveis de serviço acordados e instruções definidas e também mantendo a infraestrutura de TI.

No processo PO 06 (Comunicar diretrizes e objetivos da administração), é necessário definir políticas e processos de comunicação, bem como guias e outros documentos atualizados, compreensíveis e claros para os *stakeholders*. Isto pode ser atingido ao se definir o *framework* de controle de TI, desenvolvendo e implementando políticas de TI e garantindo a aderência a estas políticas por parte dos *stakeholders*.

Para estudos futuros, pretende-se aplicar a sistemática aqui desenvolvida em outro estudo de caso, que envolva a relação entre uma empresa de TI e outra de segmento distinto, visando a complementar os achados.

REFERÊNCIAS

- AUBERT, Benoit, RIVARD, Suzanne, PATRY, Michel. A transaction cost model of IT outsourcing. *Information & Management*, v. 41, p. 921-932, 2004. doi:10.1016/j.im.2003.09.001
- BARDIN, Laurence. *Análise de conteúdo*. Lisboa: Edições 70, 1977.
- BHATTACHARYA, Somnath, BEHARA, Ravi S., GUNDERSEN, David E. Business risk perspectives on information systems outsourcing. *International Journal of Accounting Information Systems*, v. 4, p. 75-93, 2003. doi:10.1016/S1467-0895(03)00004-6
- CARMEL, Erran, ABBOTT, Pamela. Why 'nearshore' means that distance matters. *Communications of the ACM*, v. 50, n. 10, p.40-46, 2007. doi:10.1145/1290958.1290959
- CHUA, Ai Ling, PAN, Shan L. Knowledge transfer in offshore insourcing. In.: International Conference on Information Systems, 27, Wisconsin. *Anais... AIS*, 2006.
- DOMBERGER, Simon, FERNANDEZ, Patrick, FIEBIG, Denzil G. Modelling the price, performance and contract characteristics of IT outsourcing. *Journal of Information Technology*, v. 15, p. 107-118, 2000. doi:10.1080/026839600344302
- HALL, James A., LIEDTKA, Stephen L. The Sarbanes-Oxley Act: implications for large-scale IT outsourcing. *Communications of the ACM*, v. 50, n. 3, p. 95-100, 2007.
- HAWKINS, Kyleen W., ALHAJJAJ, Stephany, KELLEY, Sharon. S: Using COBIT to secure information assets. *The Journal of Government Financial Management*, v. 52, n. 2, p. 22-33, 2003.
- HOPPEN, Norberto et al. Avaliação de artigos de pesquisa em sistemas de informação: proposta de um guia. In.: Encontro Nacional da Associação Nacional de Programas de Pós-Graduação em Administração, 21, Rio das Pedras. *Anais... ANPAD*, 1997, 1 CD-ROM.
- ISACA - Information Systems Audit and Control Association. COBIT model. 2007. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit>. Acesso em: 10 de setembro de 2010.
- ITGI, IT Governance Institute. Board briefing on IT Governance, 2001. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/> Acesso em: 10 de setembro de 2010.
- KHALFAN, Abdulwahed. Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, v. 24, p. 29-42, 2004. doi:10.1016/j.ijinfomgt.2003.12.001

LOH, Lawrence, VENKATRAMAN, N. An empirical study of information technology outsourcing: benefits, risks and performance implications. In.: International Conference on Information Systems, 16, Amsterdam. *Anais... AIS*, 1995.

LUCIANO, Edimara M., TESTA, Maurício G., ROHDE, Leonardo R. Gestão de serviços de Tecnologia da Informação: identificando a percepção de benefícios e dificuldades para a sua adoção. In.: Encontro Nacional da Associação Nacional de Programas de Pós-Graduação em Administração, 31, Rio de Janeiro. *Anais... ANPAD*, 2007, 1 CD-ROM.

RODA, Roy. IT skills standards. *Communications of the ACM*. v. 42, n. 4, p. 21-26. April, 1999. doi:10.1145/299157.299162

RUSTAGI, Sandeep, KING, William R., KIRSCH, Laurie J. Predictors of formal control usage in IT outsourcing partnerships. *Information Systems Research*, 19, 2, p. 126–143, 2008. doi:10.1287/isre.1080.0169

SAMPIERI, Roberto H., COLLADO, Carlos F., LUCIO, Pilar B. *Metodología de la investigación*. México: McGraw-Hill, 1991.

SANTOS, Carlos A. P. N., OLIVEIRA, Francisco C. Terceirização no processo de desenvolvimento de sistemas de informações. In: Encontro Nacional da Associação Nacional de Programas de Pós-Graduação em Administração, 24, Florianópolis. *Anais... ANPAD*, 2000, 1 CD-ROM.

YANG, Chyan, HUANG, Jen-Bor. A decision model for IS outsourcing. *International Journal of Information Management*, v. 20, p. 225-239, 2000. doi:10.1016/S0268-4012(00)00007-4

YIN, R. *Estudo de caso: planejamento e métodos*. 2. ed. Porto Alegre: Bookman, 2001.