Gerenciamento do Ambiente Físico utilizando CobiT 4.1: um estudo de caso aplicado.

Fabiano da Silva Longaray

UNIVERSIDADE DO VALE DO RIO DOS SINOS

Fabiano da Silva Longaray

Gerenciamento do Ambiente Físico utilizando CobiT 4.1: um estudo de caso aplicado.

Monografia apresentada à Universidade do Vale do Rio dos Sinos como requisito parcial para a obtenção do grau de Bacharel em MBA – Administração da Tecnologia da Informação.

Orientador: Prof. Júlio César Hilzendeger

Porto Alegre, agosto de 2010

AGRADECIMENTOS

... a Deus pela maravilhosa vida que me deu;
... a minha esposa Aline, luz da minha vida sempre presente em minha caminhada. Esta conquista é nossa!
... aos meus familiares e amigos;
... ao professor Júlio César Hilzendeger, certificado CGEIT pelo ISACA - apoio crucial para o desenvolvimento deste estudo.

“O Senhor é meu pastor e nada me faltará.”
(Salmo 22)

RESUMO

No mundo dos negócios, a estratégia - considerada de importância vital no embate da concorrência - está normalmente associada à arte da guerra. Entretanto, muito antes da estratégia, já existia a concorrência; ela surgiu com a própria vida. Com a evolução da vida, os primeiros organismos unicelulares passaram a alimentar seres mais complexos, desenvolvendo-se, com o passar do tempo, em intrincada rede de interações competitivas. Ao longo de milhões de anos, a concorrência natural não demandou qualquer estratégia; tratou-se, apenas, de seleção natural e sobrevivência do mais apto (BARCELLOS, 2002). As empresas cada vez mais investem na área de TI de forma a apoiar a estratégia da área de negócio, para assim, gerar resultado garantindo crescimento e sustentabilidade da empresa. Este trabalho visa realizar um estudo tendo por objetivo analisar o ambiente físico e gerar considerações utilizando o processo DS12 – Gerenciamento do Ambiente Físico do modelo CobiT.

Palavras-chave: Governança de TI, CobiT, Estratégia Empresarial

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1. INTRODUÇÃO

Com a crescente globalização de mercados, aumenta a competição entre as empresas e o decorrente desafio a sua sobrevivência. Empresas que sequer haviam cogitado sua exposição ao mercado externo vêem-se, repentinamente, às voltas com a disputa de seus clientes locais por experientes competidores globais (BARCELLOS, 2002).

No Brasil, são abundantes os exemplos recentes, tanto no comércio quanto na indústria. As aquisições, fusões e privatizações em curso ilustram bem o quadro atual das iniciativas estratégicas de resposta empresarial à confrontação global. O emprego cada vez maior da informática, associado às telecomunicações, está eliminando barreiras, encurtando distâncias e aproximando pessoas e organizações. Devido à substancial mudança em curso na atividade econômica, da manufatura e produção em massa para serviço e troca de informações, a economia moderna é muito diferente daquela sobre a qual foi desenvolvida grande parte da teoria econômica. Para as empresas, as implicações resultantes são imensas. A disponibilidade rápida de dados confiáveis e acurados para a tomada de decisão é um exemplo e seu valor para a gestão estratégica empresarial continuará a crescer em ritmo acelerado (BARCELLOS, 2002).

No mundo dos negócios, a estratégia - considerada de importância vital no embate da concorrência - está normalmente associada à arte da guerra. Entretanto, muito antes da estratégia, já existia a concorrência; ela surgiu com a própria vida. Com a evolução da vida, os primeiros organismos unicelulares passaram a alimentar seres mais complexos, desenvolvendo-se, com o passar do tempo, em intrincada rede de interações competitivas. Ao longo de milhões de anos, a concorrência natural não demandou qualquer estratégia; tratou-se, apenas, de seleção natural e sobrevivência do mais apto (BARCELLOS, 2002).

Conforme Barcellos (2002), como conceito, provavelmente a estratégia surgiu relacionada a operações militares, nas quais são encontrados todos os elementos que a valorizam: recursos limitados, incerteza sobre a capacidade e as intenções do adversário, comprometimento irreversível dos recursos, coordenação das ações à distância e no tempo, incerteza sobre o controle da situação e a natureza fundamental das percepções recíprocas entre os contendores.

A revolução da informação tem causado impactos marcantes em todos os aspectos da vida humana. Todos precisam adequar-se à nova realidade, que é marcada pela constante transformação e que exige flexibilidade e adaptação. Nesse cenário, a informação assume papel preponderante e essencial, principalmente no ambiente competitivo em que as organizações estão inseridas (NETO, 2004).

A essencialidade da informação para as organizações está na sua capacidade de agregação de valor, na medida em que é gerada de forma integrada, considerando as esferas extra e intra-organizacionais que a influenciam e sofrem sua influência. A tecnologia dentro das organizações é, atualmente, um dos principais recursos utilizados na geração da informação integrada, por permitir níveis de confiabilidade e rapidez exigidos para o seu uso eficaz, eficiente e efetivo (NETO, 2004).

Fica evidenciado que o caráter estratégico da TI é consubstanciado pela possibilidade que carrega de promover não apenas uma melhoria nos processos empresariais, mas também na obtenção de vantagens competitivas. O impacto da TI sobre as organizações evidencia-se por sua essencialidade em meio aos esforços organizacionais de posicionamento competitivo. A TI mostra-se útil nos principais desafios que as organizações enfrentam, quais sejam a melhoria do conhecimento sobre o mercado, o aumento da capacidade de identificação e resposta às ameaças e oportunidades, o aperfeiçoamento dos canais de comunicação e a melhoria na seleção de estratégias (NETO, 2004).

Henderson e Venkatraman (1993 apud LAURINDO, 2001) propuseram um modelo que destaca e analisa a importância estratégica do papel desempenhado pela TI dentro das empresas. O modelo proposto baseia-se em fatores internos e externos à empresa. É feita analise do impacto da TI nos negócios da empresa, como estes afetam a organização e a estratégia de TI e também quais as disponibilidades no mercado em termos de novas tecnologias. A proposta apresentada é denominada de “Modelo do Alinhamento Estratégico”. Os autores propõem que, além da amplamente reconhecida necessidade de ajuste entre a estratégia da empresa e sua estrutura interna, também deve, analogamente, haver ajuste entre a estratégia externa de TI (posicionamento no mercado de TI) e a estrutura interna de Sistemas de Informação (sua organização e administração).

Um dos desafios enfrentados pelas organizações, na exploração do potencial da TI, é a necessidade de um alinhamento entre as estratégias de negócios e de TI. Isto significa que a

TI deve ascender ao nível dos demais recursos, que constituem o conjunto de variáveis a ser analisado no processo de desenvolvimento da estratégia corporativa (NETO, 2004).

Pelas afirmações nos parágrafos anteriores, pode-se dizer que o alinhamento de TI ao negócio tende a ser ampliado de forma a sustentar, apoiar e impulsionar a estratégia adotada pelas empresas.

1.1. Definição do problema

As empresas cada vez mais investem na área de TI de forma a apoiar a estratégia da área de negócio, para assim, gerar resultados garantindo crescimento e sustentabilidade da empresa.

Este trabalho visa realizar um estudo tendo por objetivo analisar o ambiente físico e gerar considerações. Este grupo é composto de cerca de 20 empresas com forte atuação nos ramos de concessionárias de veículos e administração de consórcios. O primeiro ramo possui amplitude regionalizada, no sul do país. O segundo ramo possui atuação a nível nacional.

1.1.1. Questão de Pesquisa

Como o departamento de tecnologia da informação pode gerenciar o ambiente físico a fim de proteger os ativos de TI, seus dados, e minimizar o risco de interrupção nos negócios?

1.1.2. Objetivos

Os objetivos deste trabalho estão a seguir apresentados.

1.1.2.1. Objetivo Geral

Este trabalho visa realizar um estudo de caso aplicado tendo por objetivo analisar o ambiente físico e gerar considerações baseado no processo DS12 – Gerenciamento do Ambiente Físico do CobiT - *Control Objectives for Information and related Technology* versão 4.1.

O trabalho pode agregar valor a empresa pesquisada, contribuindo para a efetivação de ações administrativas, gerenciais ou operacionais, que viabilizem a implementação de melhorias no gerenciamento do ambiente físico.

1.1.2.2. Objetivos Específicos

Para alcançar o objetivo geral foram estabelecidos os seguintes objetivos intermediários:

- compreender a importância do alinhamento de TI a área de negócio;
- executar o estudo de caso;
- avaliar os resultados e sugerir melhorias com base no processo DS12 do CobiT.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a fundamentação teórica, partindo do conceito de Estratégia Empresarial, passando pela apresentação da importância do alinhamento da Tecnologia da Informação ao negócio, Governança de Tecnologia da Informação, seus mecanismos e o modelo CobiT.

2.1. Estratégia Empresarial

A palavra *estratégia* existe há muito tempo. Hoje os gerentes a usam livre e afetuosamente. Ela também é considerada o ponto alto da atividade dos executivos. Acontece que estratégia é uma dessas palavras que inevitavelmente definimos de uma forma, mas freqüentemente usamos de outra. Estratégia é um padrão, isto é, consistência em comportamento ao longo do tempo (MINTZBERG, 2000).

Segundo Pires e Carpinetti (2000 apud FIDELIS, 2006), a palavra *estratégia* representa o *"estabelecimento de objetivos e de planos de ação para atingi-los"*. Para cada negócio empresarial é definido um tempo para planejamento e *feedback* das estratégias e táticas traçadas. Davenport (1998 apud FIDELIS, 2006) afirma que *"a estratégia gira em torno de escolhas e de ênfases – a que tipo de negócio dedicar-se, que produtos criar, que mercados atingir"*.

Há uma grande necessidade da empresa em usar boas estratégias de competição para sua permanência no mercado (FIDELIS, 2006). *"A estratégia competitiva é um mapa de informações que responde a perguntas sobre a maneira pela qual a empresa irá operar num mundo onde a informação desempenha um papel importante"* (McGEE e PRUSAK, 1994, p. 43 apud FIDELIS, 2006).

A estratégia empresarial é definida por Oliveira (2001, p. 30 apud FIDELIS, 2006) como *"a ação básica estruturada e desenvolvida pela empresa para alcançar, de forma adequada e, preferencialmente, diferenciada, os objetivos idealizados para o futuro, no melhor posicionamento da empresa perante seu ambiente"*. Ela provém da alta administração da organização enfocando toda a empresa. Para alcançar estes objetivos, torna-se necessário a compatibilidade da empresa (correspondente aos seus recursos disponíveis, capacidades,

habilidades, compromissos e objetivos) junto ao ambiente (oportunidades de mercado com suas restrições, limitações, contingências e ameaças). É essa compatibilidade que possibilita a elaboração de estratégias competitivas e cooperativas pela organização. A preparação da estratégia empresarial requer decisões intelectuais baseadas nos objetivos, ocorrências e estimativas que passaram por avaliações sérias. Tal estratégia não se limita apenas ao planejamento das futuras decisões. Consiste também no planejamento das decisões atuais e entendimento do impacto que estas decisões poderão provocar futuramente. Este entendimento só será possível se o tomador de decisão possuir um perfeito entendimento do ambiente no qual sua organização está atuando. Este entendimento tende a melhorar à medida que este tiver acesso a informações de melhor qualidade (FIDELIS, 2006).

Ross, Weill e Robertson (2008) acreditam que algumas empresas executam melhor porque têm um alicerce de execução melhor. Elas embutiram tecnologia em seus processos para poderem executar de modo eficiente e confiável suas operações.

Empresas de todos os tipos estão chegando à conclusão de que a atenção sistemática à estratégia é uma atividade muito proveitosa. Empresas pequenas, médias e grandes, distribuidores e fabricantes, bancos e instituições sem finalidade de lucro, todos os tipos de organizações devem decidir os rumos que sejam mais adequados aos seus interesses (ALDAY, 2000).

As razões dessa atenção crescente à estratégia empresarial são muitas, algumas mais evidentes que outras. Dentre as causas mais importantes do crescimento recente do Planejamento Estratégico, pode-se citar que os ambientes de praticamente todas as empresas mudam com surpreendente rapidez. Essas mudanças ocorrem nos ambientes econômico, social, tecnológico e político (ALDAY, 2000).

2.2. A importância do alinhamento da Tecnologia da Informação ao negócio

O impacto da Tecnologia de Informação (TI) no desempenho dos negócios tem sido bastante discutido durante esta última década. Pesquisadores das áreas de negócio e de TI realizam estudos para examinar as necessidades e os benefícios do alinhamento da TI com o restante dos negócios (REICH e BENBASAT, 1996 apud BRODBECK e HOPPEN, 2003; SABHERWAL e CHAN, 2001 apud BRODBECK e HOPPEN, 2003). Os executivos de TI também têm considerado o alinhamento entre as estratégias de negócio e de TI como um dos

objetivos principais da área, pela possibilidade de identificação de novas oportunidades de negócios e pela obtenção de vantagens competitivas baseadas em soluções de TI (NIEDERMAN, BRANCHEAU e WETHERBE, 1991 apud BRODBECK e HOPPEN, 2003; PORTER, 2001 apud BRODBECK e HOPPEN, 2003).

Alguns dos conceitos mais significativos sobre alinhamento encontrados na literatura são: (1) o alinhamento entre o plano estratégico de negócio (PEN) e o plano estratégico de tecnologia de informação (PETI) é alcançado quando o conjunto de estratégias de sistemas – objetivos, obrigações e estratégias – é derivado do conjunto estratégico organizacional – missão, objetivos e estratégias (KING, 1988 apud BRODBECK e HOPPEN, 2003); (2) o elo entre PEN-PETI corresponde ao grau no qual a missão, os objetivos e os planos de TI refletem, suportam e são suportados pela missão, pelos objetivos e pelos planos de negócio (REICH e BENBASAT, 1996 apud BRODBECK e HOPPEN, 2003); (3) o alinhamento estratégico corresponde à adequação e integração funcional entre ambiente externo (mercados) e interno (estrutura administrativa e recursos financeiros, tecnológicos e humanos) para desenvolver as competências e maximizar o desempenho organizacional (HENDERSON e VENKATRAMAN, 1993 apud BRODBECK e HOPPEN, 2003); e (4) o alinhamento entre PEN-PETI é a adequação da orientação estratégica do negócio com a de TI (CHAN et al., 1997 apud BRODBECK e HOPPEN, 2003).

2.3. Governança de Tecnologia da Informação

Weill e Ross (2006) definem a Governança de Tecnologia da Informação (TI) como sendo a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização de TI.

Esta definição da Governança de TI objetiva capturar sua simplicidade – direitos decisórios e responsabilidade – e sua complexidade – comportamentos desejáveis que diferem de empresa para empresa. A governança determina quem toma decisões. A administração é o processo de tomar e implementar decisões. Por exemplo, a governança determina quem tem o direito de decidir sobre quanto a empresa investirá em TI. A administração determina a quantia efetivamente a ser investida num dado ano e as áreas em que ocorrerá o investimento. A alta gerência estabelece os direitos decisórios e a responsabilidade pela TI para estimular os comportamentos desejáveis na empresa. Se o comportamento desejável envolver unidades de negócio independentes e empreendedoras, as decisões de investimento em TI caberão

primariamente aos líderes dessas unidades. Em contraste se o comportamento desejável envolve uma visão unificada da empresa por parte do cliente, com um único ponto de contato com o cliente, um modelo mais centralizado de governança de investimento de TI funcionará melhor. Modelos mais centralizados de RH (e dos outros ativos principais) também ajudarão a criar um ponto único de contato com o cliente (WEILL e ROSS, 2006).

Weill e Ross (2006) apresentam uma grade (Figura 1) chamada de Matriz de Arranjos de Governança que ilustra as duas primeiras questões referentes à Governança de TI: quais decisões devem ser tomadas e quem deve tomá-las? Os títulos das colunas listam cinco decisões de TI inter-relacionadas:

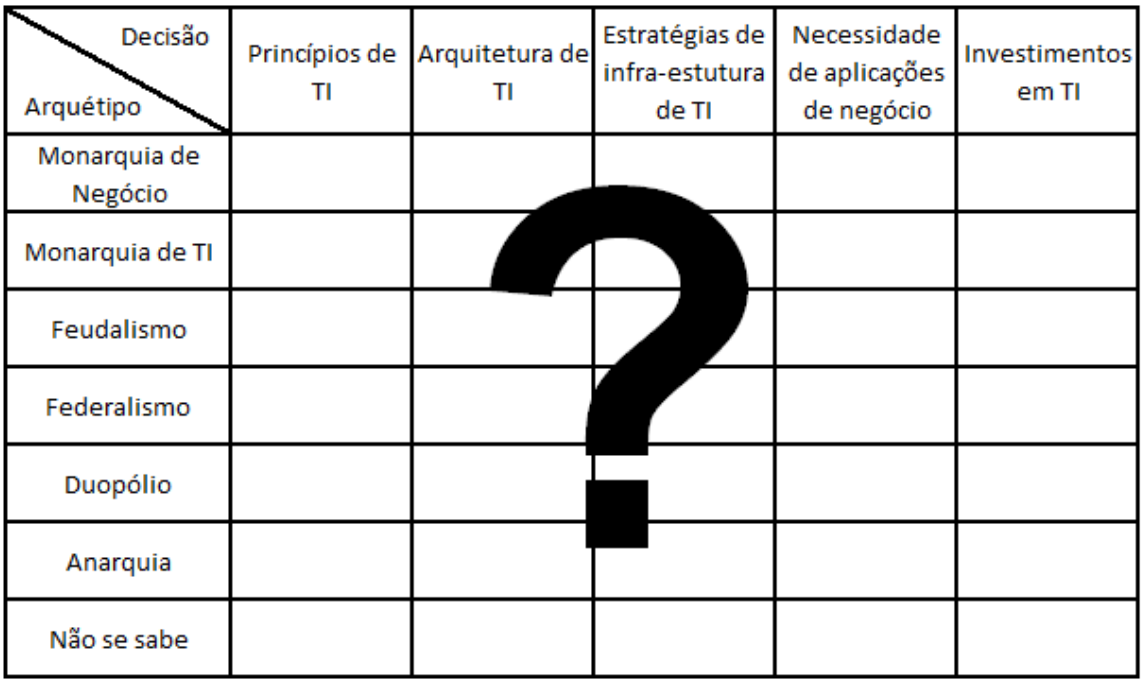
- *Princípios de TI* – esclarecendo o papel de negócio da TI;
- *Arquitetura de TI* – definindo os requisitos de integração e padronização;
- *Infra-estrutura de TI* – determinando serviços compartilhados e de suporte;
- *Necessidade de aplicações de negócio* – especificando a necessidade comercial de aplicações de TI compradas ou desenvolvidas internamente;
- *Investimentos e priorizações de TI* – escolhendo quais iniciativas financiar e quanto gastar.

Estas cinco decisões-chave estão inter-relacionadas e requerem vinculação para que haja uma governança eficaz – tipicamente fluindo da esquerda para a direita na matriz. Por exemplo, os princípios de TI motivam a arquitetura, que leva à infra-estrutura. A infra-estrutura habilita o desenvolvimento de aplicações com base nas necessidades do negócio, especificadas freqüentemente pelos detentores dos processos comerciais. Finalmente, os investimentos em TI (contração de “processos de investimento e priorização de TI”) devem ser motivados pelos princípios, pela arquitetura, pela infra-estrutura e pelas necessidades de aplicações. No entanto, cada uma dessas decisões envolve, essencialmente, um conjunto único de questões e problemas a serem discutidos (WEILL e ROSS, 2006).

Os títulos das linhas na Figura 1 listam um conjunto de arquétipos para especificar os direitos decisórios. Cada arquétipo identifica o tipo de pessoa envolvida em tomar uma decisão de TI:

- *Monarquia de negócio* – os altos gerentes;
- *Monarquia de TI* – os especialistas em TI;

- *Feudalismo* – cada unidade de negócio toma decisões independentes;
- *Federalismo* – combinação entre o centro corporativo e as unidades de negócio, com ou sem o envolvimento do pessoal de TI;
- *Duopólio de TI* – o grupo de TI e algum outro grupo (por exemplo, a alta gerência ou líderes das unidades de negócio);
- *Anarquia* – tomada de decisões individual ou por pequenos grupos de modo isolado.



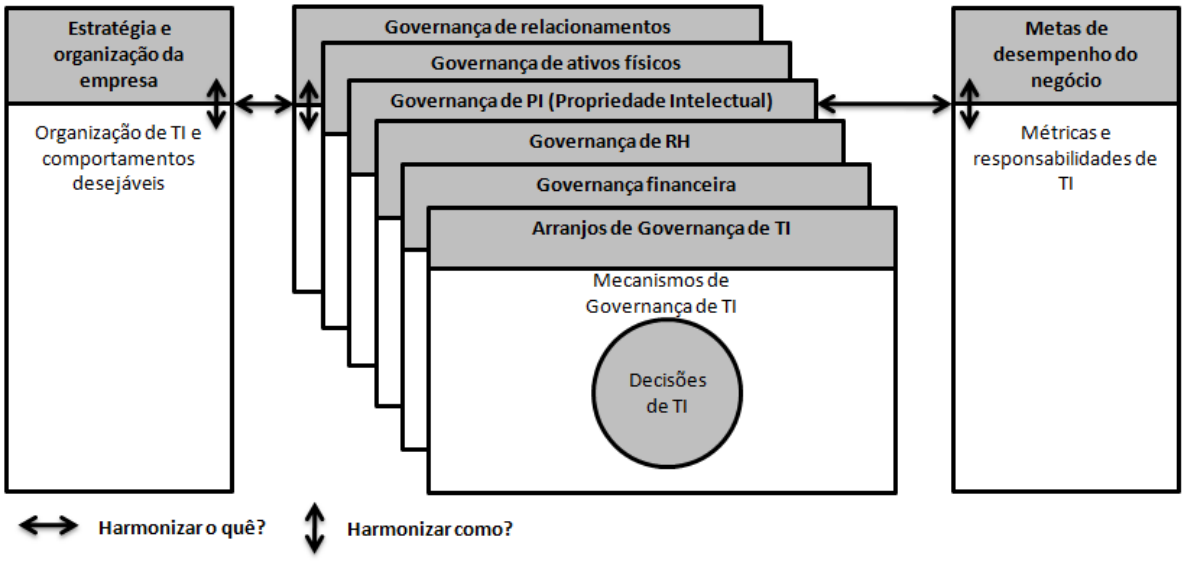
© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 1 - Matriz de Arranjos de Governança - Quais Arquétipos de Governança são usados por diferentes tipos de decisão?

O ponto de interrogação na Figura 1 representa o desafio de toda empresa para determinar quem deve ter a responsabilidade por tomar e contribuir com cada tipo de decisão de governança. Se a Matriz de Arranjos e Governança organiza os tipos de decisões e os arquétipos do processo decisório, a terceira questão – como essas decisões serão tomadas e monitoradas – requer a formulação e a implementação de mecanismos de governança, como comitês, funções e processos formais (WEILL e ROSS, 2006).

Para ajudar a entender, projetar, comunicar e sustentar uma governança eficaz, Weill e Ross (2006) propõem um *framework* de Governança de TI na Figura 2. Estes autores apresentam uma forma básica, para que os leitores possam completá-lo para qualquer

empresa. O *framework* ilustra a harmonização (setas horizontais) entre a estratégia e a organização da empresa, os arranjos de Governança de TI e as metas de desempenho do negócio. A estratégia da empresa, os arranjos de governança e as metas de desempenho são postos em prática, respectivamente, pela organização da TI e comportamentos desejáveis, por mecanismos de governança e por métricas. O *framework* ilustra, também, a necessidade de harmonizar a Governança de TI com a governança dos outros ativos principais.



© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 2 - *Framework* de Governança de TI

2.3.1. Arquétipos

Weill e Ross (2006) utilizam arquétipos políticos (monarquia, feudalismo, federalismo, duopólio e anarquia) para descrever as combinações de pessoas que têm direitos decisórios ou contribuem para a tomada de decisões de TI. Foram escolhidos deliberadamente arquétipos políticos provocativos, porque, embora exagerados, a maioria dos administradores se identifica com esses estereótipos. Um desses seis arquétipos (Figura 3) poderia descrever como sua empresa toma uma ou mais das cinco decisões-chave de TI ou contribui com os tomadores de decisão.

Estilo	Quem tem direitos decisórios ou de contribuição?
Monarquia de negócio	Um grupo de executivos de negócios ou executivos individuais (CxOs). Inclui comitês de executivos seniores de negócios (podendo incluir o CIO). Exclui os executivos de TI que atuem independentemente.
Monarquia de TI	Indivíduos ou grupos de executivos de TI.
Feudalismo	Líderes das unidades de negócio, detentores de processos-chave ou seus delegados
Federalismo	Executivos do nível de diretoria (c-*level*) e grupos de negócios (e.g., processos ou unidades de negócio); incluíndo executivos de TI como participantes adicionais. Equivalente à atuação conjunta dos governos federal e estadual
Duopólio de TI	Executivos de TI e algum outro grupo (e.g., os CxOs ou os líderes de unidades de negócio ou os líderes de processos)
Anarquia	Cada usuário individual.

© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 3 - Arquétipos de Governança de TI

2.3.1.1. Monarquia de negócio

Numa monarquia de negócio, os altos executivos de negócios tomam decisões de TI que afetam a empresa toda. A Figura 4 enumera as características distintas dos diferentes arranjos de governança e como as empresa são classificadas (WEILL e ROSS, 2006).

	Executivos de diretoria (c-*level*)	TI corporativa e/ou das unidades de negócio	Líderes das unidades de negócio ou detentores dos principais processos de negócio
Monarquia de negócio	●		
Monarquia de TI		●	
Feudalismo			●
Federalismo	●	●	●
	●		●
Duopólio de TI	●	●	
		●	●
Anarquia			

© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 4 - Principais participantes nos Arquétipos de Governança de TI

2.3.1.2. Monarquia de TI

Numa monarquia de TI, os profissionais de Tecnologia de Informação tomam as decisões de TI. As empresas implementam monarquias de TI de muitas maneiras diferentes,

freqüentemente envolvendo profissionais de TI tanto das equipes corporativas como de unidades de negócio (WEILL e ROSS, 2006).

2.3.1.3. Feudalismo

O modelo feudal é baseado nas tradições da “antiga e alegre Inglaterra”, onde príncipes e princesas, ou os cavaleiros por eles escolhidos, tomavam suas próprias decisões, otimizando suas necessidades locais. No caso da Governança de TI, a entidade feudal é tipicamente a unidade de negócio, a região ou a função (WEILL e ROSS, 2006).

2.3.1.4. Federalismo

O modelo decisório federalista tem uma longa tradição nos governos. Arranjos federalistas tentam equilibrar as responsabilidades e cobranças de múltiplos órgãos de governo, como país e estados. Charles Handy[1], entre outros, identificou a utilidade do modelo federalista em negociar os interesses tanto da organização central (tipicamente a sede) como das unidades individuais. Definimos o modelo federalista como a tomada de decisões coordenadas que envolve tanto o centro como as unidades de negócio. Os representantes das unidades no modelo federalista podem ser os seus líderes ou os detentores de processo de negócio. Líderes de TI em nível corporativo e/ou das unidades de negócio podem, também, envolver-se na governança federalista como participantes adicionais (WEILL e ROSS, 2006).

O modelo federalista é sem dúvida o mais difícil arquétipo para a tomada de decisões, pois os líderes da empresa têm preocupações diferentes das dos líderes das unidades de negócio. Os membros de uma organização federalista representam suas próprias responsabilidades exclusivas. Além disso, os sistemas de incentivo levam os administradores a focarem com freqüência nos resultados das áreas de negócio, e não da empresa. O impacto dos recursos compartilhados no desempenho das unidades de negócio – e especificamente as taxas de transferência cobradas pelos recursos – costuma suscitar preocupações quanto a justiça (WEILL e ROSS, 2006).

Nos modelos federalistas, as unidades de negócio maiores e mais poderosas com freqüência ganham mais atenção e têm maior influência sobre as decisões. Conseqüentemente, as unidade menores estão sempre insatisfeitas e por vezes se separam da união para atender a suas próprias necessidades. As empresas que adotam estruturas de

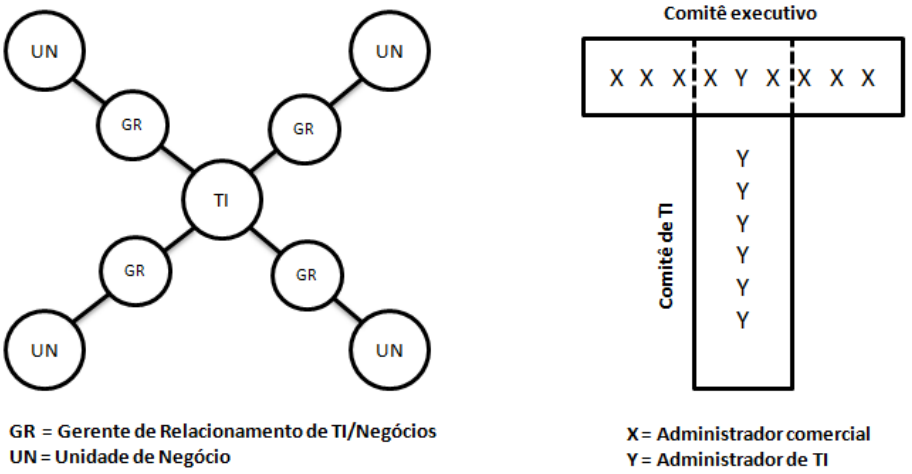
[1] Charles Handy: autor e filósofo.

governança federalistas costumam fazer uso de equipes administrativas e comitês executivos para resolver conflitos inerentes (WEILL e ROSS, 2006).

2.3.1.5. Duopólio de TI

O duopólio de TI é um arranjo entre duas partes em que as decisões representam o consenso bilateral entre executivos de TI e algum outro grupo. Os executivos de TI podem ser um grupo central de TI ou uma equipe composta por organizações de TI centrais e das unidades de negócio. O outro grupo pode ser constituído de CxOs, líderes das unidades de negócio ou detentores de processos de negócios, ou, ainda, grupos dos principais usuários de sistemas (Figura 4). O duopólio difere do modelo federalista no sentido de que o arranjo federalista tem sempre representação tanto corporativa como local, ao passo que o duopólio tem uma ou outra, mas nunca ambas, e inclui invariavelmente profissionais de TI (WEILL e ROSS, 2006).

Os duopólios de TI assumem, freqüentemente, uma de duas formas: a "roda de bicicleta" ou a estrutura de comitê em forma de T (Figura 5). A roda de bicicleta ilustra o duopólio que envolve o grupo central de TI e as unidades de negócio. O grupo de TI encontra-se no cubo central e as unidades de negócio em volta do aro. Os raios são a série de relacionamentos bilaterais entre o grupo de TI e as várias unidades de negócio. Cada unidade de negócio ganha atenção individual ao longo dos raios, mas o mesmo cubo suporta toda a empresa (WEILL e ROSS, 2006).



© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 5 - Duopólio da Roda de Bicicleta e em Forma de T

Um duopólio que envolva o grupo central de TI e a equipe da alta gerência (os CxOs e os líderes das unidades de negócio) é muitas vezes implementado por dois comitês sobrepostos. O comitê executivo (a parte horizontal do T) é composto predominantemente de administradores da área comercial. A parte vertical do T é um comitê de TI constituído em sua maioria por administradores técnicos. Um pequeno grupo de pessoas participa de ambos os comitês para coordenar e garantia a sobreposição. Para melhorar a coordenação, os comitês podem se reunir no mesmo dia – digamos que o comitê executivo se reúna pela manhã e o de TI pela tarde – com algum período de reunião conjunta (WEILL e ROSS, 2006).

Weill e Ross (2006) indicam que o arquétipo de duopólio é popular em parte porque envolve somente dois grupos decisórios – podendo atingir muitos dos objetivos do modelo federalista usando uma estrutura administrativa mais simples. Similarmente, os duopólios têm uma vantagem sobre os modelos feudais, no sentido de que o grupo central de TI é, em muitos casos, um dos poucos grupos que vêm a empresa como um todo e podem procurar oportunidades de compartilhamento e reutilização. Os profissionais de TI podem, também, gerenciar a adesão, abertamente ou não, à arquitetura de TI da empresa. Os duopólios empregam usualmente gerentes de relacionamento ou os CIOs das unidades de negócio para representar as necessidades destas últimas. O grupo de TI pode ter uma série de duopólios, com diferentes unidades de negócio habilitando decisões mais customizadas em menos tempo. Esses duopólios têm a vantagem de se concentrarem diretamente nas necessidades das unidades de negócio, o que resulta em maior satisfação por parte dessas unidades. Mas tais duopólios de unidades de negócio podem ser caros e ineficazes quando se está decidindo problemas da organização em geral.

2.3.1.6. Anarquia

Numa anarquia, indivíduos ou pequenos grupos tomam suas próprias decisões com base somente em suas necessidades locais. As anarquias são a ruína de muitos grupos de TI, sendo caras de sustentar e preservar. Anarquias formalmente sancionadas são raras, sendo adotadas nos casos em que se requer uma reponsividade muito rápida a necessidades locais ou de clientes individuais.

2.3.2. Principais decisões sobre a Governança de TI

Toda empresa precisa tomar cinco decisões inter-relacionadas sobre a TI: os princípios, a arquitetura, a infra-estrutura, as necessidades de aplicações do negócio e os investimentos e a priorização da TI. A Figura 6 organiza essas decisões enfatizando suas interconexões críticas. A decisão referente aos princípios de TI fica na parte superior do diagrama, uma vez que ela, por explicitar os objetivos empresariais de TI, estabelece diretrizes para todas as outras decisões. Se os princípios não estiverem claros, é improvável que as outras decisões sejam aderidas de maneira significativa. As decisões sobre a arquitetura de TI convertem os princípios de TI em requisitos de integração e padronização e, então, delineiam um guia técnico para prover as capacidades necessárias. As decisões relativas aos investimentos e à priorização da TI mobilizam recursos para converter princípios em sistemas (WEILL e ROSS, 2006).

<table>
<tr><th colspan="3">Decisões sobre os princípios de TI</th></tr>
<tr><td colspan="3">Declarações de alto nível sobre como a TI é utilizada ao negócio</td></tr>
<tr><th>Decisões sobre a arquitetura de TI</th><th>Decisões sobre a infra-estrutura de TI</th><th>Decisões sobre os investimentos e a priorização da TI</th></tr>
<tr><td rowspan="3">Organização lógica de dados, aplicações e infra-estruturas, definida a partir de um conjunto de políticas, relacionamentos e opções técnicas adotadas para obter a padronização e a integração técnica e de negócio desejadas.</td><td>Serviços de TI coordenados de maneira centralizada e compartilhados, que provêm a base para a capacidade de TI da empresa.</td><td rowspan="3">Decisões sobre quanto e onde investir em TI, incluindo a aprovação de projetos e as técnicas de justificação.</td></tr>
<tr><th>Necessidades de aplicações de negócio</th></tr>
<tr><td>Especificação da necessidade de negócio de aplicações de TI adquiridas no mercado ou desenvolvidas internamente</td></tr>
</table>

© 2003 Center for Information Systems Research (CISR) da MIT Sloan School. Adaptado de Weill e Ross (2006).

Figura 6 - Principais Decisões sobre a Governança de TI

Decisões sobre infra-estrutura e aplicações podem fluir de cima para baixo (abordagem *top-down*) – dos princípios, da arquitetura e dos critérios de investimento. Nesse caso, a infra-estrutura gera as capacidades necessárias de TI e as aplicações fazem uso dessas capacidades. Com a mesma freqüência, necessidades e oportunidades de negócio identificam a necessidade

de aplicações de TI, que “borbulham” da base (abordagem *bottom-up*) para gerar novos requisitos de infra-estrutura. Por fim, as decisões de investimento selecionam e financiam as iniciativas de infra-estrutura e aplicações, que implementam uma arquitetura projetada para incorporar os princípios de TI – e em última instância os princípios do negócio (WEILL e ROSS, 2006).

2.3.2.1. Decisão 1: Princípios de TI

Os princípios de TI são um conjunto relacionado de declarações de alto nível sobre como a Tecnologia da Informação é utilizada no negócio. Uma vez articulados, os princípios de TI ternam-se parto do léxico administrativo da empresa e podem ser discutidos, debatidos, apoiados, recusados e aprimorados (WEILL e ROSS, 2006).

2.3.2.2. Decisão 2: Arquitetura de TI

A arquitetura de TI é a *organização lógica dos dados, aplicações e infra-estruturas, definida a partir de um conjunto de políticas, relacionamentos e opções técnicas adotadas para obter a padronização e a integração técnicas e de negócio desejadas.* Por prover o direcionamento para a infra-estrutura e as aplicações (e, por conseguinte, para as decisões de investimento), as decisões arquitetônicas são cruciais para uma gestão e utilização eficazes da Tecnologia da Informação (WEILL e ROSS, 2006).

2.3.2.3. Decisão 3: Infra-estrutura de TI

A infra-estrutura é a base da capacidade planejada de TI (tanto técnica como humana) disponível em todo o negócio, na forma de serviços compartilhados e confiáveis, e utilizada por aplicações múltiplas. Os serviços de infra-estrutura de uma empresa incluem, freqüentemente, serviços de rede de telecomunicação; a provisão e o gerenciamento de computadores em larga escala; o gerenciamento da base de dados compartilhada de cliente; a *expertise* em pesquisa e desenvolvimento, com o fim de identificar a utilidade de tecnologias emergentes para o negócio; e uma *intranet* para toda a empresa (WEILL e ROSS, 2006).

O conceito de serviços da infra-estrutura de TI é muito poderoso, uma vez que os administradores podem valorizar mais prontamente um serviço, do que um componente técnico como um servidor ou um pacote de *software* (WEILL e ROSS, 2006).

2.3.2.4. Decisão 4: As necessidades de aplicações de negócio

Segundo Weill e Ross (2006), a identificação da necessidade de negócios de aplicações de TI costuma ter dois objetivos conflitantes – a criatividade e a disciplina. A criatividade consiste em identificar maneiras novas e mais eficazes de gerar valor para os clientes por meio da TI e envolve a identificação de aplicações de negócio que dêem suporte a objetivos de negócio estratégicos e facilitem experimentos de negócios. A disciplina consiste na integridade arquitetônica – assegurando que as aplicações aproveitem e amplifiquem a arquitetura da empresa, ao invés de solapar seus princípios. A disciplina envolve, também, foco – comprometendo os recursos necessários para concretizar metas de projetos e negócios.

2.3.2.5. Decisão 5: Investimentos e priorização de TI

A decisão de investimento em TI é freqüentemente a mais visível e controversa das cinco decisões-chave de TI. Alguns projetos são aprovados, outros são repelidos e o restante passa pelo equivalente organizacional da animação suspensa, com a temida solicitação dos tomadores de decisão de “refazer o plano de negócio” ou “prover mais informações”. As empresas que obtêm valor superior da TI concentram seus investimentos em suas prioridades estratégicas, cientes da distinção entre capacidades de TI que “precisamos ter” e que “seria bem se tivéssemos” (WEILL e ROSS, 2006).

2.4. Segurança da Informação – NBR ISO/IEC 27002

A norma NBR ISO/IEC 27002 - *Código de Prática para a Gestão de Segurança da Informação*, tem por objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. A segurança da informação visa proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização (ABNT, 2005 apud FARIA, 2010a).

É preciso esclarecer que anteriormente esta norma era conhecida como NBR ISO/IEC 17799, mas a partir de 2007 a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002 (ABNT, 2005 apud FARIA, 2010a).

A norma está distribuída em 11 seções que correspondem a controles de segurança da informação, conforme apresentado a seguir:

2.4.1. Política de Segurança da Informação

Deve ser criado um documento sobre a política de segurança da informação da organização, que deveria conter, entre outros, os conceitos de segurança da informação, o comprometimento da direção com a política, uma estrutura para estabelecer os objetivos de controle e os controles, a estrutura de análise e avaliação e gerenciamento de riscos, as políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização. Essa política também deve ser comunicada a todos, bem como analisada e revisada criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias (ABNT, 2005 apud FARIA, 2010a).

2.4.2. Organizando a Segurança da Informação

Para implementar a segurança da informação em uma organização, é necessária que seja estabelecida uma estrutura para gerenciá-la. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes de diversas partes da organização, com funções e papéis relevantes. Todas as responsabilidades pela segurança da informação também devem estar claramente definidas. É importante ainda que sejam estabelecidos acordos de confidencialidade para proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes (ABNT, 2005 apud FARIA, 2010a).

2.4.3. Gestão de Ativos

Ativo, de acordo com a norma, “é qualquer coisa que tenha valor para a organização”. Gestão de Ativos, portanto, significa proteger e manter os ativos da organização. Para que eles sejam devidamente protegidos, devem ser primeiramente identificados e levantados, com proprietários também identificados e designados, de tal forma que um inventário de ativos possa ser estruturado e posteriormente mantido. As informações e os ativos ainda devem ser classificados, conforme o nível de proteção recomendado para cada um deles, e seguir regras documentadas, que definem qual o tipo de uso é permitido fazer com esses ativos (ABNT, 2005 apud FARIA, 2010a).

2.4.4. Segurança em Recursos Humanos

Antes de realizar a contratação de um funcionário ou mesmo de fornecedores e terceiros, é importante que cada um deles entenda suas responsabilidades e esteja de acordo com o papel que desempenhará. Portanto, as descrições de cargo e os termos e condições de contratação devem ser explícitos, especialmente no que tange às responsabilidades de segurança da informação. É importante também que quaisquer candidatos sejam devidamente analisados, principalmente se forem lidar com informações de caráter sigiloso. A intenção aqui é mitigar o risco de roubo, fraude ou mau uso dos recursos (ABNT, 2005 apud FARIA, 2010a).

Durante todo o tempo em que funcionários, fornecedores e terceiros estiverem trabalhando na empresa, eles devem estar conscientes sobre as ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações, de tal maneira que estejam preparados para apoiar a política de segurança da informação da organização. Eles também devem ser educados e treinados nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação. É fundamental ainda que um processo disciplinar formal seja estabelecido para tratar das violações de segurança da informação. No momento em que ocorrer o encerramento ou uma mudança na contratação, a saída de funcionários, fornecedores e terceiros deve ser feita de modo ordenado e controlado, para que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso sejam concluídas (ABNT, 2005 apud FARIA, 2010a).

2.4.5. Segurança Física e do Ambiente

As instalações de processamento de informação críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física. Essa proteção deve ser compatível com os riscos previamente identificados. Os equipamentos também devem ser protegidos contra ameaças físicas e ambientais, incluindo aqueles utilizados fora do local (ABNT, 2005 apud FARIA, 2010a).

2.4.6. Gestão das Operações e Comunicações

É importante que estejam definidos os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Além disso, deve-se utilizar sempre que necessária a segregação de funções (recomenda-se que uma pessoa realize

uma ou algumas partes de um processo, mas não todas), visando reduzir o risco de mau uso ou uso indevido dos sistemas. Para o gerenciamento de serviços terceirizados, deve-se implementar e manter o nível apropriado de segurança da informação e em conformidade com acordos de entrega de serviços terceirizados. É fundamental planejar e preparar a disponibilidade e os recursos dos sistemas para minimizar o risco de falhas, bem como prever a capacidade futura dos sistemas, de forma a reduzir os riscos de sobrecarga. Também deve-se prevenir e detectar a introdução de códigos maliciosos e os usuários devem estar conscientes sobre isso. Procedimentos para a geração de cópias de segurança e sua recuperação também devem ser estabelecidos. Deve-se garantir ainda o gerenciamento seguro de redes. Controles adicionais podem até mesmo ser necessários para proteger informações confidenciais que trafegam em redes públicas (ABNT, 2005 apud FARIA, 2010b).

As trocas de informações entre organizações devem ser baseadas em uma política formal específica, devendo ser efetuadas a partir de acordos entre as partes e sempre em conformidade com toda a legislação pertinente. Deve-se ainda implementar mecanismos de monitoração de atividades não autorizadas de processamento da informação. Os eventos de segurança da informação devem ser registrados, lembrando que as organizações devem estar aderentes aos requisitos legais aplicáveis para suas atividades de registro e monitoramento (ABNT, 2005 apud FARIA, 2010b).

2.4.7. Controle de Acesso

O acesso a informação, aos recursos de processamento das informações e aos processos de negócios devem ser controlados com base nos requisitos de negócio e na segurança da informação. Portanto, deve ser assegurado o acesso de usuário autorizado e prevenido o acesso não autorizado a sistemas de informação. Para isso, deve haver procedimentos que englobem desde o cadastro inicial de um novo usuário até o cancelamento final do seu registro, garantindo assim que já não possuem mais acesso a sistemas de informação e serviços. Os usuários sempre devem estar conscientes de suas responsabilidades, particularmente no que se refere ao uso de senhas e de segurança dos equipamentos de usuários. Nesse sentido, sugere-se ainda a adoção da “política de mesa e tela limpa”, para reduzir o risco de acessos não autorizados ou danos a documentos, papéis, mídias e recursos de processamento da informação que estejam ao alcance de qualquer um (ABNT, 2005 apud FARIA, 2010b).

2.4.8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Segundo a norma, “Sistemas de informação incluem sistemas operacionais, infra-estrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário”. Por essa razão, os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação. As informações devem ser protegidas visando a manutenção de sua confidencialidade, autenticidade ou integridade por meios criptográficos (ABNT, 2005 apud FARIA, 2010b).

2.4.9. Gestão de Incidentes de Segurança da Informação

Deve-se assegurar que eventos de segurança da informação sejam o mais rápido possível comunicados, de tal forma que a tomada de ação corretiva ocorra em tempo hábil. Para isso, devem ser estabelecidos procedimentos formais de registro e escalonamento, bem como todos os funcionários, fornecedores e terceiros devem estar conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos (ABNT, 2005 apud FARIA, 2010b).

2.4.10. Gestão da Continuidade do Negócio

Deve-se impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar que a sua retomada ocorra em tempo hábil. Para isso, planos de continuidade do negócio, incluindo controles para identificar e reduzir riscos, devem ser desenvolvidos e implementados, visando assegurar que as operações essenciais sejam rapidamente recuperadas (ABNT, 2005 apud FARIA, 2010b).

2.4.11. Conformidade

Deve-se garantir e evitar a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Para isso, é conveniente contratar, caso necessário, consultoria especializada, bem como analisar criticamente a segurança dos sistemas de informação em intervalos regulares, verificando, sobretudo, sua conformidade e aderência a requisitos legais e regulamentares (ABNT, 2005 apud FARIA, 2010b).

2.5. CobiT

O modelo CobiT (*Control Objectives for Information and related Technology*) foi criado pelo ISACA – *Information Systems Audit and Control Association* – através do *IT Governance Institute*, organização independente que desenvolveu a metodologia considerada a base da governança tecnológica. O CobiT funciona como uma entidade de padronização e estabelece métodos documentados para nortear a área de tecnologia das empresas, incluindo qualidade de software, níveis de maturidade e segurança da informação (SORTICA, CLEMENTI, CARVALHO; 2004). Este modelo tem por missão pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação (ISACA, 2007).

Os documentos do CobiT definem Governança Tecnológica como sendo "uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa de modo a atingir objetivos corporativos, através da agregação de valor e risco controlado pelo uso da tecnologia da informação e de seus processos" (SORTICA, CLEMENTI, CARVALHO; 2004).

A governança de TI habilita a organização a obter todas as vantagens de sua informação, maximizando os benefícios, capitalizando as oportunidades e ganhando em poder competitivo. Esses resultados requerem um modelo para controle de TI que se adéqüe e dê suporte ao COSO *("Committe of Sponsoring Organisations of the Treadway Commission's Internal Control – Integrated Framework"*), um modelo para controles internos amplamente aceito para governança e gerenciamento de riscos empresariais, e outros modelos similares. O CobiT fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. As boas práticas do CobiT representam o consenso de especialistas. Elas são fortemente focadas mais nos controles e menos na execução. Essas práticas irão ajudar a otimizar os investimentos em TI, assegurar a entrega dos serviços e prover métricas para julgar quando as coisas saem erradas (ISACA, 2007).

O foco em processos do CobiT é ilustrado por um modelo de processos de TI subdivididos em quatro domínios e 34 processos em linha com as áreas responsáveis por planejar, construir, executar e monitorar, provendo assim uma visão total da área de TI. Conceitos de arquitetura corporativa ajudam a identificar os recursos essenciais para o sucesso dos processos, ou seja, aplicativos, informações, infraestrutura e pessoas (ISACA 2007).

O CobiT é um modelo e uma ferramenta de suporte que permite aos gerentes suprir as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. O CobiT habilita o desenvolvimento de políticas claras e boas práticas para controles de TI em toda a empresa. O CobiT é atualizado continuamente e harmonizado com outros padrões e guias. Assim, o CobiT tornou-se o integrador de boas práticas de TI e a metodologia de governança de TI que ajuda no entendimento e gerenciamento dos riscos e benefícios associados com TI. A estrutura de processos do CobiT e o seu enfoque de alto nível orientado aos negócios fornece uma visão geral de TI e das decisões a serem tomadas sobre o assunto (ISACA, 2007).

Segundo ISACA (2007), os benefícios de implementar o CobiT como um modelo de governança de TI incluem:

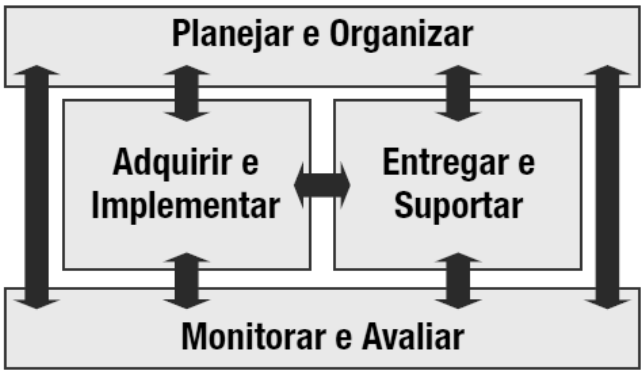
- um melhor alinhamento baseado no foco do negócio;
- uma visão clara para os executivos sobre o que TI faz;
- uma clara divisão das responsabilidades baseada na orientação para processos;
- aceitação geral por terceiros e órgãos reguladores;
- entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum;
- cumprimento dos requisitos do COSO para controle do ambiente de TI.

2.5.1. Domínios

O CobiT define as atividades de TI em um modelo de processos genéricos com quatro domínios. Esses domínios são Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar e Monitorar e Avaliar. Esses domínios mapeiam as tradicionais áreas de responsabilidade de TI de planejamento, construção, processamento e monitoramento (ISACA, 2007).

O modelo CobiT fornece um modelo de processo de referência e uma linguagem comum para que todos na organização possam visualizar e gerenciar as atividades de TI. Incorporar o modelo operacional e a linguagem comum para todas as áreas de negócios envolvidas em TI é um dos mais importantes passos e ações preliminares para uma boa governança. Isto também fornece uma metodologia para medição e monitoramento da performance de TI, comunicação com provedores de serviços e integração das melhores práticas de gerenciamento. Um modelo de processos incentiva a determinação de

proprietários dos processos, o que possibilita a definição de responsabilidades (ISACA, 2007).



(ISACA, 2007)
Figura 7 - Os quatro domínios inter-relacionados do CobiT

Dentro desses quatro domínios o CobiT identificou 34 processos de TI geralmente utilizados. Embora a maioria das organizações tenha definido as responsabilidades de TI de planejar, construir, processar e monitorar, e muitas delas tenham os mesmos processos-chave, poucas terão a mesma estrutura de processos ou aplicarão todos os 34 processos do CobiT. O CobiT fornece uma completa lista de processos que podem ser utilizados para verificar a totalidade das atividade e responsabilidades. No entanto, nem todos precisam ser aplicados e podem ser combinados conforme as necessidades de cada empresa (ISACA, 2007).

Para cada um desses 34 processos, uma ligação foi feita com os objetivos de negócios e de TI suportados. Também são fornecidas informações sobre como os objetivos podem ser medidos, quais são as atividades-chave, as principais entregas e quem é responsável por elas (ISACA, 2007).

2.5.1.1. Planejar e Organizar (PO)

Este domínio cobre a estratégia e as táticas, preocupando-se com a identificação da maneira em que TI pode melhor contribuir para atingir os objetivos de negócios. O sucesso da visão estratégica precisa ser planejado, comunicado e gerenciado por diferentes perspectivas (ISACA, 2007).

ISACA (2007) indica que uma apropriada organização bem como uma adequada infra-estrutura tecnológica devem ser colocadas em funcionamento. Este domínio tipicamente ajuda a responder as seguintes questões gerenciais:

- As estratégias de TI e de negócios estão alinhadas?
- A empresa está obtendo um ótimo uso dos seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são entendidos e estão sendo gerenciados?
- A qualidade dos sistemas de TI é adequada às necessidades de negócios?

2.5.1.2. Adquirir e Implementar (AI)

Segundo ISACA (2007), para executar a estratégia de TI, as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, implementadas e integradas ao processo de negócios. Além disso, alterações e manutenções nos sistemas existentes são cobertas por esse domínio para assegurar que as soluções continuem a atender aos objetivos de negócios. Este domínio tipicamente trata das seguintes questões de gerenciamento:

- Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
- Os novos projetos serão entregues no tempo e orçamento previstos?
- Os novos sistemas ocorreram apropriadamente quando implementado?
- As alterações ocorrerão sem afetar as operações de negócios atuais?

2.5.1.3. Entregar e Suportar (DS)

Este domínio, segundo ISACA (2007), trata da entrega dos serviços solicitados, o que inclui entrega de serviço, gerenciamento da segurança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais. Trata geralmente das seguintes questões de gerenciamento:

- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
- Os custos de TI estão otimizados?
- A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?

- Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?

2.5.1.3.1. DS12 – Gerenciamento do Ambiente Físico

A seguir o processo DS12 – Gerenciamento do Ambiente Físico, será apresentado de acordo com o modelo CobiT 4.1 (ISACA, 2007).

A proteção de pessoas e equipamento de informática requer instalações físicas bem planejadas e gerenciadas. O processo de gerenciamento do ambiente físico inclui a definição dos requisitos do local físico, a escolha de instalações apropriadas, o projeto de processos eficazes de monitoramento dos fatores ambientais e o gerenciamento de acessos físicos. O gerenciamento eficaz do ambiente físico reduz as interrupções nos negócios provocadas por danos causados a equipamentos ou pessoas.

- **Controle sobre o seguinte processo de TI:** Gerenciar o ambiente físico;
- **Que satisfaça aos seguintes requisitos do negócio para a TI:** Proteger os ativos de TI e os dados do negócio e minimizar o risco de interrupção nos negócios;
- **Com foco em:** Prover e manter um ambiente físico adequado que proteja os recursos de TI contra acesso indevido, danos ou roubo;
- **É alcançado por:** Implementação de medidas de segurança física – seleção e gerenciamento de instalações físicas;
- **E medido por:** Tempo de indisponibilidade devido a incidentes no ambiente físico – quantidade de incidentes causados por falhas ou violação da segurança física – freqüência das avaliações e revisões de riscos físicos.

2.5.1.3.1.1 Objetivos de Controle Detalhados

- **DS12.1 Seleção do Local e Layout:** Definir e selecionar o local para os equipamentos de TI, considerando o alinhamento da estratégia de tecnológica com a estratégia de negócio. A seleção e o planejamento do layout de uma instalação física devem levar em consideração os riscos associados a possíveis desastres naturais e não naturais, bem como as leis e regulamentações relevantes, tais como regulamentações de saúde ocupacional e segurança do trabalho;
- **DS12.2 Medidas de Segurança Física:** Definir e implementar medidas de segurança física alinhadas com os requisitos de negócio para proteger o local e os ativos físicos. As medidas de segurança física devem ser capazes de

efetivamente prevenir, detectar e mitigar riscos relacionados a roubo, temperatura, fogo, fumaça, água, vibração, terrorismo, vandalismo, quedas de energia, produtos químicos ou explosivos;

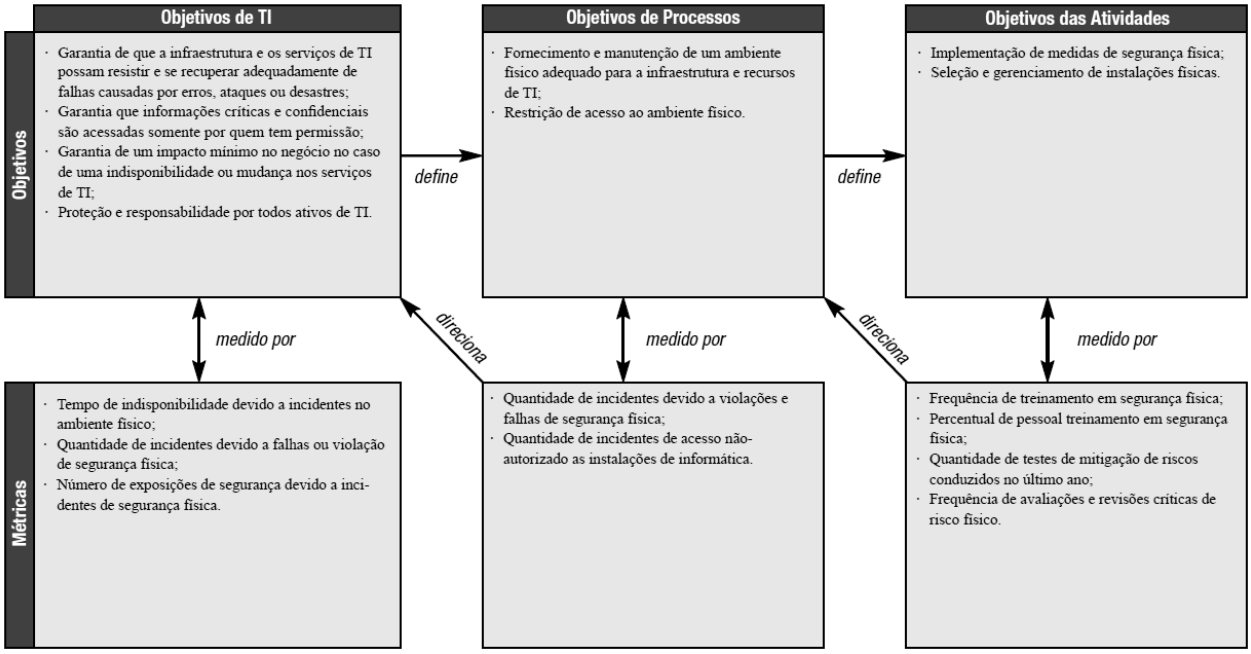
- **DS12.3 Acesso Físico:** Definir e implementar procedimentos para conceder, limitar e revogar o acesso a instalações, prédios e áreas de acordo com as necessidades do negócio, inclusive em situações de emergências. Os acessos a instalações, prédios e áreas devem ser justificados, autorizados, registrados e monitorados. Isso se aplica a todas as pessoas que acessam as instalações, inclusive ao pessoal fixo, funcionários temporários, clientes, vendedores, visitantes ou outros terceiros;
- **DS12.4 Proteção contra Fatores Ambientais:** Projetar e implementar medidas de proteção contra fatores ambientais. Equipamentos e dispositivos especializados para monitorar e controlar o ambiente devem ser instalado;
- **DS12.5 Gerenciamento de Instalações Físicas:** Gerenciar as instalações físicas, incluindo equipamentos de energia e comunicação, em alinhamento com leis e regulamentações, requisitos técnicos e de negócio, especificações dos fabricantes e distribuidores de equipamentos e diretrizes de segurança e saúde ocupacional.

A Figura 8 apresenta a tabela RACI do processo DS12, esta tabela identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado (I).

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Definir o nível necessário de proteção física;					C	A/R	C				C
Selecionar e comissionar instalações físicas (data, center, escritório, etc);	I	C	C	C	C	A/R	C		C	C	C
Implementar medidas no ambiente físico;					I	A/R	I	I			C
Gerenciar o ambiente físico (manutenção, monitoração e relatórios incluídos);						A/R	C				
Definir e implementar procedimentos para autorização e manutenção de acesso físico				C	I	A/R	I	I	I		C

(ISACA, 2007)
Figura 8 - Tabela RACI - DS12 Gerenciar o Ambiente Físico

A Figura 9 ilustra os objetivos e métricas do processo.



(ISACA, 2007)

Figura 9 - Objetivos e Métricas - DS12 Gerenciar o Ambiente Físico

2.5.1.4. Monitorar e Avaliar (ME)

Segundo ISACA (2007), todos os processos de TI precisam ser regularmente avaliados com o passar do tempo para assegurar a qualidade e a aderência aos requisitos de controle. Este domínio aborda o gerenciamento de performance, o monitoramento do controle interno, a aderência regulatória e a governança. Trata geralmente das seguintes questões de gerenciamento:

- A performance de TI é mensurada para detectar problemas antes que seja muito tarde?
- O gerenciamento assegura que os controles internos sejam efetivos e eficientes?
- O desempenho da TI pode ser associado aos objetivos de negócio?
- Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

3. METODOLOGIA DE PESQUISA

Seguindo a metodologia adotada na pesquisa intitulada "*Análise do uso de Padrões de Projeto em empresas de Tecnologia da Informação: um estudo de caso com empresas da UNITEC*" (LONGARAY, 2008), o presente capítulo tem por objetivo apresentar a metodologia de pesquisa utilizada para a realização do trabalho. Este capítulo está dividido na apresentação da técnica de estudo de caso, descrição dos passos metodológicos e elaboração do protocolo de pesquisa.

3.1. Estudo de caso

O estudo de caso deve ser a estratégia escolhida ao se examinarem acontecimentos contemporâneos, mas quando não se podem manipular comportamentos relevantes. Este método conta com muitas das técnicas utilizadas pelas pesquisas históricas[2], mas acrescenta duas fontes de evidências que usualmente não são incluídas no repertório de um historiador: observação direta dos acontecimentos que estão sendo estudados e entrevistas com as pessoas neles envolvidas. Embora os estudos de casos e as pesquisas históricas possam se sobrepor, o poder diferenciador do primeiro é sua capacidade de lidar com uma ampla variedade de evidências - documentos, artefatos, entrevistas e observações – além do que pode estar disponível no estudo histórico convencional (YIN, 2005).

O estudo de caso como estratégia de pesquisa compreende um método que abrange lógica de planejamento, técnicas de coleta de dados e abordagens específicas para sua análise. Nesse sentido, esta técnica não é nem tática para a coleta de dados nem meramente uma característica do planejamento em si, mas uma estratégia de pesquisa abrangente (STOECKER, 1991, apud YIN, 2005, p.33).

O estudo de caso é circunscrito a uma ou poucas unidades, entendidas como pessoa, família, produto, empresa, órgão público, comunidade ou país. Ele tem caráter de profundidade e detalhamento. Pode ou não ser realizada no campo (VERGARA, 2007).

[2] Pesquisa histórica: estratégia de pesquisa baseada em fatos históricos (YIN, 2005).

Conforme o método escolhido, utiliza-se tal ou qual procedimento de coleta de dados no campo. Questionários, entrevistas, formulários, observação são procedimentos gerais (VERGARA, 2007).

Segundo Yin (2005), os estudos de caso representam a estratégia preferida quando se colocam questões do tipo ‘como’ e ‘por que’; quando o pesquisador tem pouco controle sobre os acontecimentos; quando o foco encontra-se em fenômenos contemporâneos inseridos em algum contexto da vida real.

Um estudo de caso é uma pesquisa empírica em que:

- investiga-se um fenômeno contemporâneo dentro de seu contexto real;
- as fronteiras entre o fenômeno e o contexto não são claramente evidentes;
- múltiplas fontes de evidências são utilizadas.

Estudos de caso podem ser aplicados para:

- explicar ligações causais em intervenções ou situações da vida real que são complexas demais para tratamento através de estratégias experimentais ou de levantamento de dados;
- descrever um contexto de vida real no qual uma intervenção ocorreu;
- avaliar uma intervenção em curso e modificá-la com base em um estudo de caso ilustrativo;
- explorar aquelas situações nas quais a intervenção não tem clareza no conjunto de resultados.

3.2. Descrição dos passos metodológicos

A pesquisa foi divida nas seguintes etapas:

- Levantamento teórico sobre Estratégia Empresarial e Governança de Tecnologia da Informação;
- Levantamento do processo DS12 Gerenciar o Ambiente Físico do modelo CobiT;
- Identificação da empresa estudada;
- Execução do estudo de caso.

3.2.1. Levantamento teórico sobre Estratégia Empresarial e Governança de Tecnologia da Informação

Para que fosse possível executar o estudo de caso, foi necessária a elaboração de levantamento teórico sobre Estratégia Empresarial, a importância do alinhamento da Tecnologia da Informação ao negócio, Governança de Tecnologia da Informação e seus mecanismos de implementação, e, o modelo CobiT, utilizado como base para processo de gerenciamento do ambiente físico.

3.2.2. Levantamento do processo DS12 Gerenciar o Ambiente Físico do modelo CobiT

O processo DS12 – Gerenciar o Ambiente Físico, existente no modelo CobiT, foi utilizado no processo de avaliação e geração de considerações sobre a coleta de dados.

3.2.3. Identificação da empresa estudada

O grupo de empresa estudado é composto de cerca de 20 empresas com forte atuação nos ramos de concessionárias de veículos e administração de consórcios. O primeiro ramo possui amplitude regionalizada, no sul do país. O segundo ramo possui atuação a nível nacional.

3.2.4. Execução do estudo de caso

O estudo de caso foi executado através da observação direta do autor deste estudo por três meses durante a execução da melhoria do controle do ambiente físico da empresa estudada. Após a observação, foram geradas considerações apresentadas neste estudo.

3.3. Elaboração do protocolo de pesquisa

Os passos que guiaram a pesquisa realizada foram:

- título da pesquisa;
- questão de pesquisa;
- objetivo geral;
- objetivos específicos;
- escolha da empresa;

- procedimentos de coleta de dados.

Estes passos estão descritos no Apêndice A deste trabalho.

O protocolo de pesquisa detalha os itens que direcionaram o pesquisador durante o estudo de caso. Segundo Yin (2005), este trabalho deve conter as seguintes sessões:

- visão geral do projeto do estudo de caso;
- procedimentos de campo;
- questões do estudo de caso;
- guia para o relatório do estudo de caso.

4. ESTUDO DE CASO APLICADO

O estudo de caso realizado teve por objetivo analisar o ambiente físico e gerar considerações baseado no processo DS12 – Gerenciamento do Ambiente Físico do CobiT - *Control Objectives for Information and related Technology* versão 4.1 no ambiente físico centralizado de um grupo de empresas. Os dados foram coletados por observação direta do autor e os resultados apresentados a área de TI do grupo de empresas estudado.

4.1. Avaliação do nível de maturidade

O modelo de maturidade é uma forma de medir quão bom os processos de gerenciamento são, ou seja, quão capazes eles são. O quanto devem ser desenvolvidos ou capacitados deveria primariamente depender dos objetivos de TI e sua conexão como as necessidades de negócios que eles suportam. O quanto dessa capacidade é realmente entregue depende largamente do retorno que a organização deseja do investimento. Os modelos de maturidade do CobiT enfocam a maturidade mas não necessariamente a abrangência e profundidade dos controles. Eles não são um número para ser atingido, tampouco são desenhados para ser uma base formal de certificação com níveis que criam requisitos mínimos difíceis de atingir. No entanto, são desenhados para serem sempre aplicáveis, fornecendo níveis com descrições que uma empresa pode reconhecer como os que melhor se adéquam aos seus processos. O nível correto é determinado pelo tipo de organização, ambiente e estratégia (ISACA, 2007).

O estudo foi realizado a partir da definição dos níveis de maturidade apresentados pelo processo DS12 – Gerenciar o Ambiente Físico do CobiT, a seguir descritos:

- **0 – Inexistente:** Não há consciência da necessidade de proteger as instalações ou os investimentos em recursos de computação. Fatores ambientais, como proteção contra incêndios, poeira ou sujeira, energia elétrica, calor e umidade excessivos, não são monitorados nem controlados;
- **1 - Inicial/Ad hoc:** A organização reconhece como requisito de negócio ter um ambiente físico adequado que proteja os recursos e as pessoas

contra desastres naturais e não naturais. O gerenciamento de instalações e equipamentos é dependente das habilidades e capacidades técnicas de pessoas-chave. As pessoas podem transitar nas instalações sem qualquer restrição. Os responsáveis pelo gerenciamento não monitoram os controles ambientais das instalações ou o trânsito de pessoas;

- **2 - Repetível, porém Intuitivo:** Os controles ambientais são implementados e monitorados pela equipe de operações. A segurança física é um processo informal conduzido por um pequeno grupo de funcionários com alto nível de preocupação com a proteção das instalações físicas. Os procedimentos de manutenção das instalações não estão bem documentados e se baseiam em boas práticas de poucos indivíduos. Os objetivos da segurança física não são baseados em quaisquer padrões formais, e os responsáveis pelo gerenciamento não garantem que os objetivos da segurança sejam alcançados.

- **3 - Processo Definido:** A necessidade de controlar um ambiente de computação é compreendida e aceita dentro da organização. Os controles ambientais, a manutenção preventiva e a segurança física são itens orçados, aprovados e acompanhados pela Direção. Restrições de acesso são aplicadas e apenas pessoal aprovado tem acesso autorizado às instalações computacionais. Os visitantes são registrados e acompanhados sob a responsabilidade de alguém. As instalações físicas são discretas e não são facilmente identificáveis. As autoridades civis monitoram a conformidade com as regulamentações de segurança e de saúde. Os riscos são considerados de mínimo valor otimizando os custos de seguros.

- **4 - Gerenciado e Mensurável:** A necessidade para manter um ambiente computacional controlado é totalmente compreendida, o que pode ser evidenciado pela estrutura organizacional e a alocação de orçamentos. Os requisitos de segurança física e ambientais são documentados e o acesso físico é rigorosamente controlado e monitorado. O proprietário desse processo e sua responsabilidade foram estabelecidos e comunicados. A equipe responsável pelas instalações computacionais está completamente treinada em situações de emergência, bem como nas práticas de segurança

e saúde do trabalho. Mecanismos de controle padronizados são estabelecidos para restringir o acesso físico às instalações e consideram fatores ambientais e de segurança. Os responsáveis pelo gerenciamento monitoram a efetividade dos controles e a conformidade com os padrões estabelecidos. Os responsáveis pelo gerenciamento estabeleceram objetivos e métricas para avaliar o gerenciamento do ambiente computacional. A capacidade de recuperação dos recursos computacionais está incorporada ao processo de gerenciamento de riscos organizacionais. A informação integrada é utilizada para otimizar a cobertura de seguros e custos associados.

- **5 – Otimizado:** Existe um plano de longo prazo aprovado para as instalações físicas do ambiente computacional da organização. Padrões são definidos para todas as instalações, envolvendo escolha de local, construção, vigilância, segurança do pessoal, sistemas elétricos e mecânicos, proteção contra fatores ambientais (incêndios, raios, inundações). Todas as instalações são inventariadas e classificadas de acordo com o processo vigente de gerenciamento de riscos da organização. O acesso físico é controlado rigorosamente de acordo com a necessidade do cargo e monitorado continuamente e todos os visitantes são acompanhados em tempo integral. O ambiente é monitorado e controlado por equipamentos especializados, e as salas de equipamentos não têm identificação pública. Os objetivos e métricas são consistentemente avaliados. Os programas de manutenção preventiva seguem os cronogramas rigorosamente, e testes periódicos são realizados nos equipamentos críticos. Os padrões e a estratégia de gerenciamento das instalações estão alinhados com as metas de disponibilidade de serviços de TI e integrados ao planejamento de continuidade de negócio e gerenciamento de crises. Os responsáveis pelo gerenciamento examinam e otimizam as instalações de TI utilizando continuamente as medições, capitalizando oportunidades para melhorar a contribuição com o negócio.

4.1.1. DS12.1 Seleção do Local e *Layout*

Definir e selecionar o local para os equipamentos de TI, considerando o alinhamento da estratégia de tecnológica com a estratégia de negócio. A seleção e o planejamento do layout de uma instalação física devem levar em consideração os riscos associados a possíveis desastres naturais e não naturais, bem como as leis e regulamentações relevantes, tais como regulamentações de saúde ocupacional e segurança do trabalho (ISACA, 2007).

Atributo	Avaliação	Nível de Maturidade
Consciência e Comunicação	Existe o entendimento da necessidade de alinhamento para definição e seleção do local adequado para os equipamentos de TI. Os custos necessários são comunicados e compartilhados com a direção para a tomada de decisão.	3
Políticas, Planos e Procedimentos	Não existe processo, plano ou política para seleção de local e *layout*.	1
Ferramentas e Automação	Não existe ferramenta para seleção de local e *layout*.	1
Habilidades e Especialização	Habilidades mínimas requeridas para áreas críticas são identificadas e o processo de especialização ocorre por necessidade, não planejamento.	2
Responsabilidade e Responsabilização	A responsabilidade e responsabilização por processos estão definidas e proprietários de processos são identificados.	3
Definição de Objetivos e Métricas	Não existem objetivos e métricas.	1

Tabela 1- Avaliação de Maturidade – DS12.1 Seleção do Local e *Layout*

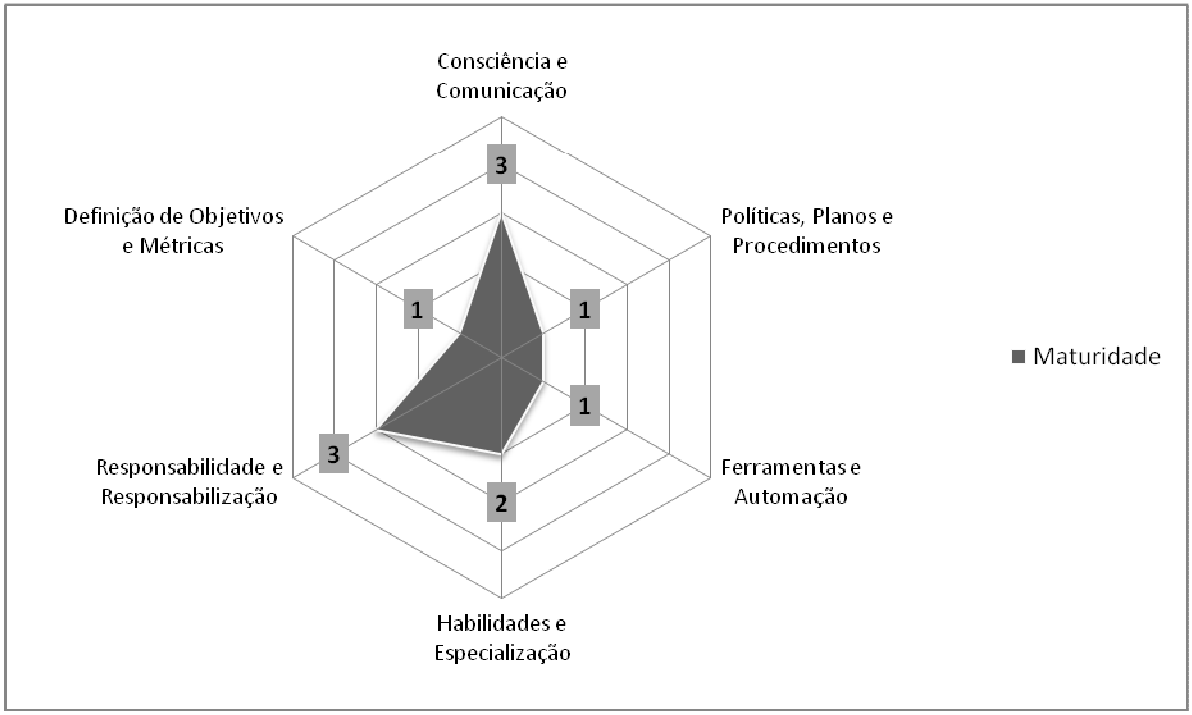


Gráfico 1 - Nível de Maturidade por Atributo - DS12.1 Seleção do Local e *Layout*

4.1.2. DS12.2 Medidas de Segurança Física

Definir e implementar medidas de segurança física alinhadas com os requisitos de negócio para proteger o local e os ativos físicos. As medidas de segurança física devem ser capazes de efetivamente prevenir, detectar e mitigar riscos relacionados a roubo, temperatura, fogo, fumaça, água, vibração, terrorismo, vandalismo, quedas de energia, produtos químicos ou explosivos (ISACA, 2007).

Atributo	Avaliação	Nível de Maturidade
Consciência e Comunicação	Existe o entendimento da necessidade de adotar medidas de segurança física. Os custos são compartilhados e aprovados pela alta direção.	3
Políticas, Planos e Procedimentos	Os processos são amplamente intuitivos devido a habilidades individuais. Medidas de segurança contra incidentes são adotados.	2
Ferramentas e Automação	Existem ferramentas adquiridas de terceiros para monitoramento do ambiente.	2
Habilidades e Especialização	Habilidades mínimas requeridas para áreas críticas são identificadas e o processo de especialização ocorre por necessidade.	2

Responsabilidade e Responsabilização	A responsabilidade e responsabilização é de um pequeno grupo de funcionários, sem formalização.	2
Definição de Objetivos e Métricas	Não existem objetivos e métricas.	1

Tabela 2- Avaliação de Maturidade – DS12.2 Medidas de Segurança Física

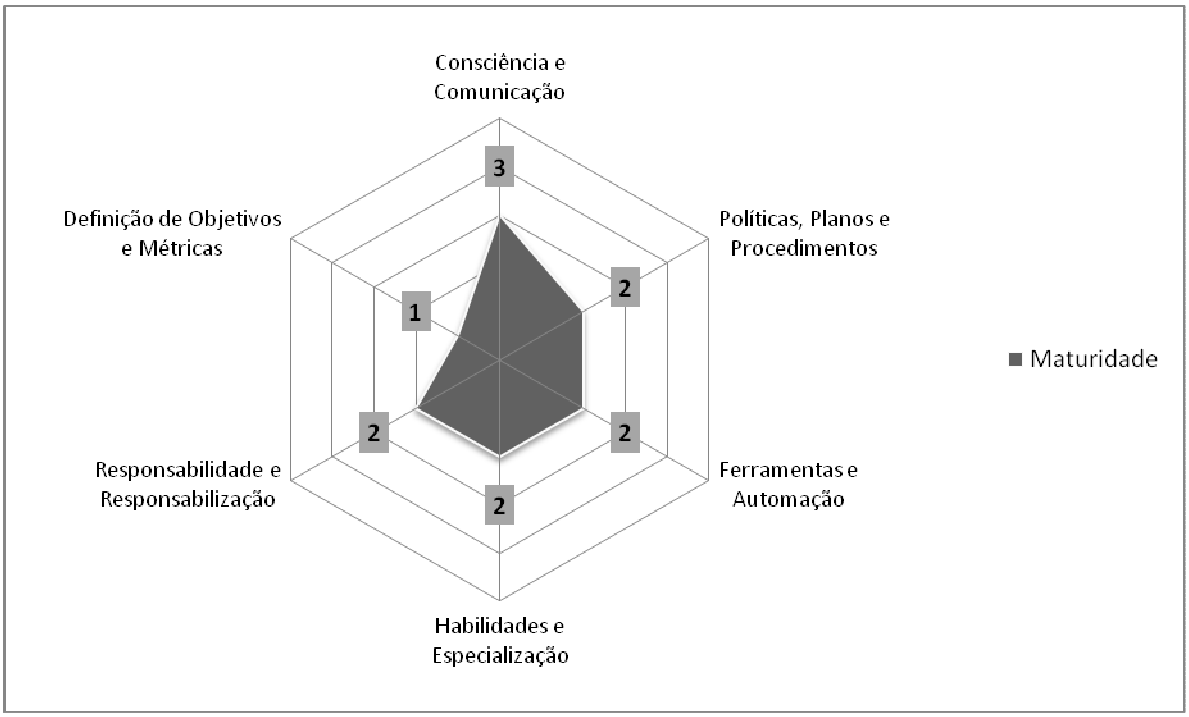


Gráfico 2 - Nível de Maturidade por Atributo - DS12.2 Medidas de Segurança Física

4.1.3. DS12.3 Acesso Físico

Definir e implementar procedimentos para conceder, limitar e revogar o acesso a instalações, prédios e áreas de acordo com as necessidades do negócio, inclusive em situações de emergências. Os acessos a instalações, prédios e áreas devem ser justificados, autorizados, registrados e monitorados. Isso se aplica a todas as pessoas que acessam as instalações, inclusive ao pessoal fixo, funcionários temporários, clientes, vendedores, visitantes ou outros terceiros (ISACA, 2007).

Atributo	Avaliação	Nível de Maturidade
Consciência e Comunicação	Existe consciência da necessidade de definir um plano para manutenção de acessos as instalações.	2
Políticas, Planos e Procedimentos	Não existe padrão formal e os responsáveis não garantem que os objetivos de segurança sejam atendidos.	2
Ferramentas e Automação	Existem ferramentas adquiridas de terceiros para manutenção do acesso físico.	2
Habilidades e Especialização	Habilidades mínimas requeridas para áreas críticas são identificadas e o processo de especialização ocorre por necessidade, não planejamento.	2
Responsabilidade e Responsabilização	A responsabilidade e responsabilização é de um pequeno grupo de funcionários, sem formalização.	2
Definição de Objetivos e Métricas	Não existem objetivos e métricas.	1

Tabela 3- Avaliação de Maturidade – DS12.3 Acesso Físico

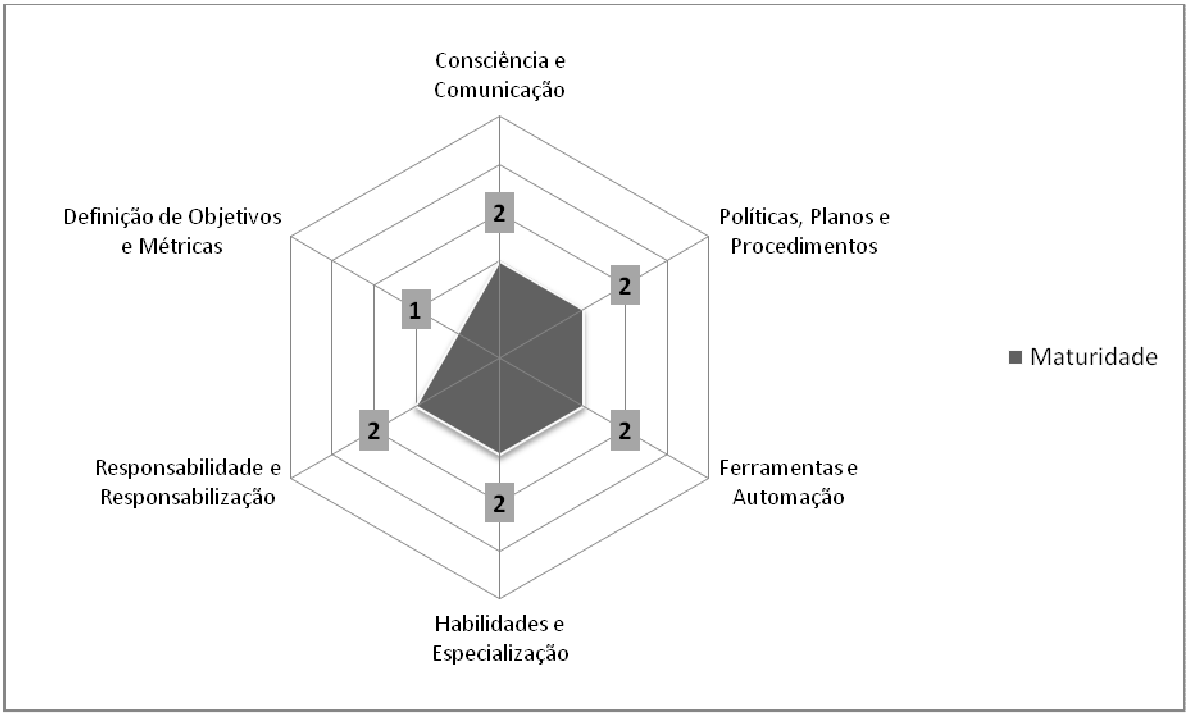


Gráfico 3 - Nível de Maturidade por Atributo - DS12.3 Acesso Físico

4.1.4. DS12.4 Proteção contra Fatores Ambientais

Projetar e implementar medidas de proteção contra fatores ambientais. Equipamentos e dispositivos especializados para monitorar e controlar o ambiente devem ser instalados (ISACA, 2007).

Atributo	Avaliação	Nível de Maturidade
Consciência e Comunicação	Existe o entendimento da necessidade de controle ambiental a fim de assegurar a alta disponibilidade do ambiente computacional.	3
Políticas, Planos e Procedimentos	Os processos de proteção são intuitivos.	2
Ferramentas e Automação	Existem ferramentas adquiridas de terceiros para monitoramento do ambiente.	2
Habilidades e Especialização	Habilidades mínimas requeridas para áreas críticas são identificadas e o processo de especialização ocorre por necessidade, não planejamento.	2
Responsabilidade e Responsabilização	A responsabilidade e responsabilização é de um pequeno grupo de funcionários, sem formalização.	2
Definição de Objetivos e Métricas	Não existem objetivos e métricas.	1

Tabela 4- Avaliação de Maturidade – DS12.4 Proteção contra Fatores Ambientais

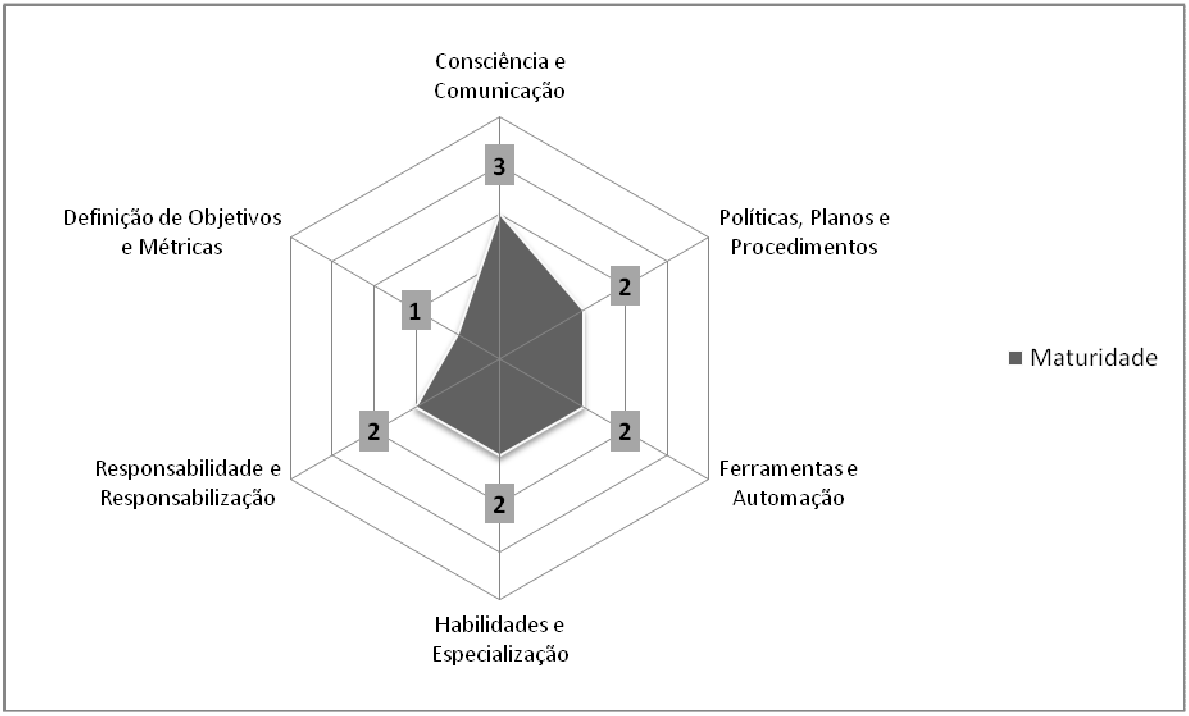


Gráfico 4 - Nível de Maturidade por Atributo - DS12.4 Proteção contra Fatores Ambientais

4.1.5. DS12.5 Gerenciamento de Instalações Físicas

Gerenciar as instalações físicas, incluindo equipamentos de energia e comunicação, em alinhamento com leis e regulamentações, requisitos técnicos e de negócio, especificações dos fabricantes e distribuidores de equipamentos e diretrizes de segurança e saúde ocupacional (ISACA, 2007).

Atributo	Avaliação	Nível de Maturidade
Consciência e Comunicação	Existe o entendimento da necessidade de gerenciamento das instalações físicas, incluindo os equipamentos de energia e comunicação.	3
Políticas, Planos e Procedimentos	Os procedimentos de manutenção das instalações não estão bem documentados.	2
Ferramentas e Automação	Existem ferramentas adquiridas de terceiros para monitoramento do ambiente.	2
Habilidades e Especialização	Habilidades mínimas requeridas para áreas críticas são identificadas e o processo de especialização ocorre por necessidade, não planejamento. A habilidade baseia-se em boas práticas de poucos indivíduos.	2

Responsabilidade e Responsabilização	A responsabilidade e responsabilização é de um pequeno grupo de funcionários, sem formalização.	2
Definição de Objetivos e Métricas	Não existem objetivos e métricas.	1

Tabela 5- Avaliação de Maturidade – DS12.5 Gerenciamento de Instalações Físicas

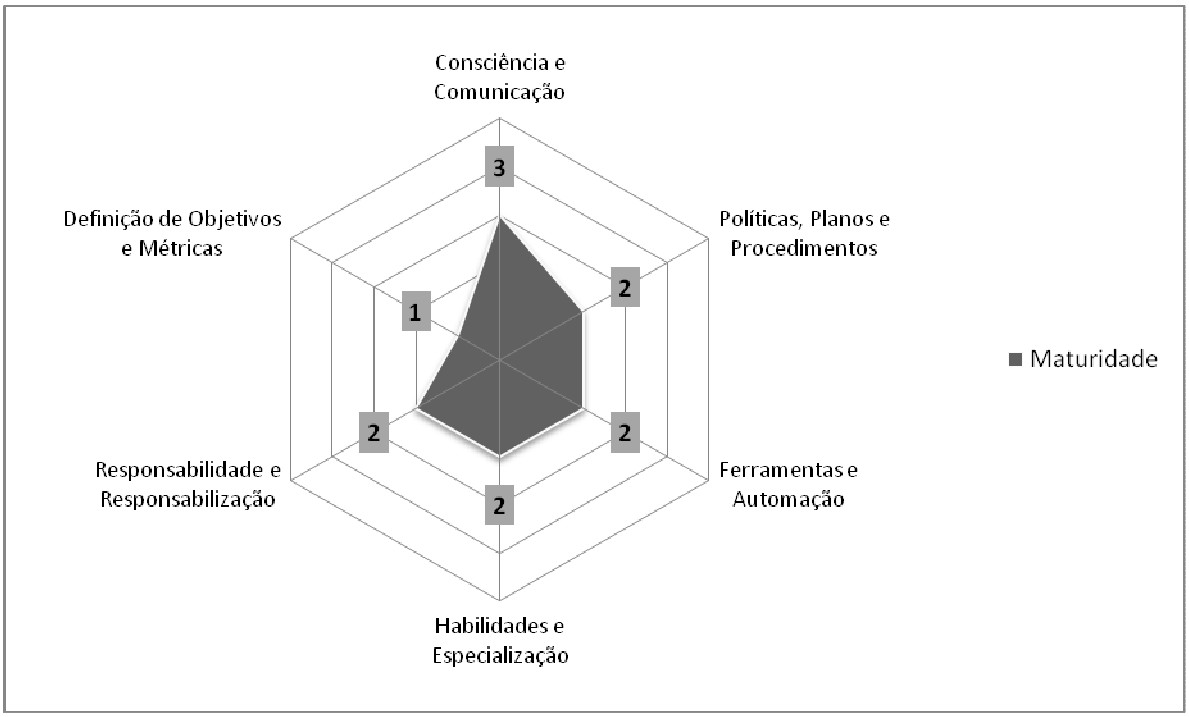


Gráfico 5 - Nível de Maturidade por Atributo - DS12.5 Gerenciamento de Instalações Físicas

4.2. Nível de maturidade atual

A empresa possui um *datacenter* próprio que está localizado estrategicamente por diretrizes definidas pela área de negócio. O local escolhido para abrigar o *datacenter* possui prevenção, detecção e mitigação de riscos relacionados a roubo – através do controle de acesso, temperatura – através da redundância de condicionadores de ar, fogo e fumaça – através do uso de sensores e gás anti-chamas apropriado para ambientes de *datacenters*, água – através do uso de sensores de umidade, quedas de energia – através do contingenciamento de duas redes elétricas auxiliadas por um equipamento no-break e um gerador de energia elétrica movido a combustível, vibração, vandalismo e terrorismo, produtos químicos e explosivos – através da ativação de um *datacenter* secundário.

O acesso ao *datacenter* é controlado através de biometria. O cadastramento e manutenção da impressão digital são feito por pessoal autorizado da área de TI. Sempre que

alguma pessoa necessita entrar no *datacenter*, estará acompanhada de um funcionário autorizado.

A empresa possui monitoramento do ambiente tecnológico através de sensores de temperatura e umidade. O *datacenter* está isolado das alterações climáticas externas por não possuir nenhum tipo de abertura ou qualquer acesso externo, exceto pela porta principal. As instalações físicas e equipamentos de energia e comunicação seguem especificação dos fabricantes e distribuidores.

Cada objetivo de controle foi analisado individualmente a fim de identificar de forma clara o nível de maturidade atual da empresa estudada e apresentar se a empresa está próxima de atingir o nível superior.

O gráfico abaixo (gráfico 6) representa o nível médio de cada atributo de maturidade:

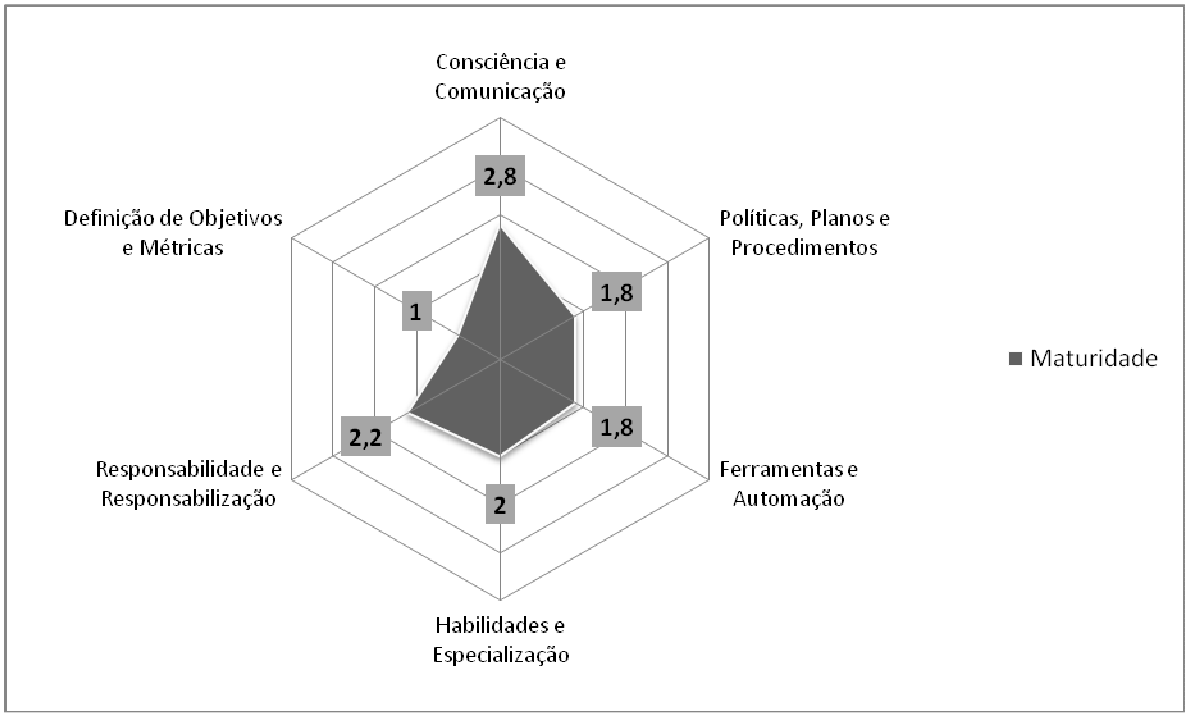


Gráfico 6 - Nível Médio de Maturidade por Atributo

4.3. Sugestão de melhoria

Através dos resultados obtidos durante a execução da pesquisa, foi possível identificar o claro entendimento e conscientização da necessidade de gerenciamento do ambiente físico, da mesma forma que identificou-se a falta evidente da definição de objetivos e métricas. Os demais atributos obtiveram pontuação média.

Sugere-se como trabalho futuro a formalização dos processos e a criação de uma comunicação efetiva, clara, de entendimento e participação comum a todos os indivíduos participantes do processo de gerenciamento do ambiente físico. Após a formalização do processo deve-se criar objetivos e métricas, juntamente com a definição de responsáveis pelo monitoramento, compreensão e gerenciamento do processo como um todo.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. ABNT, 2005.

ALDAY, Hernan E. C. O Planejamento Estratégico dentro do Conceito de Administração Estratégica. **Revista da FAE**, Curitiba, v.3, n.2, p.9-16, maio/ago. 2000.

BARCELLOS, Paulo F. P. Estratégia empresarial. In: SCHMIDT, Paulo. (Org.). **Controladoria: agregando valor para a empresa**. Porto Alegra: Bookman, 2002.

BRODBECK A. F.; HOPPEN N. Alinhamento Estratégico entre os Planos de Negócio e de Tecnologia de Informação: um Modelo Operacional para Implementação. **RAC**, v. 7, n. 3, P. 9-33, Jul./Set. 2003.

CHAN, Y. E. et al. Business strategic orientation, information system strategic orientation, and strategic alignment. **Information Systems Research**, v. 8, n. 2, p. 125-150, June 1997.

DAVENPORT, T. H. **Ecologia da informação: porque só a tecnologia não basta para o sucesso na era da informação**. São Paulo: Futura, 1998.

FARIA, A. L. **Conheça a NBR ISO/IEC 27002 – Parte 1**. Acessado em 14 de agosto de 2010. Disponível em <http://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1/>, 2010a.

FARIA, A. L. **Conheça a NBR ISO/IEC 27002 – Parte 2**. Acessado em 14 de agosto de 2010. Disponível em <http://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-2/>, 2010b.

FIDELIS, Joubert R. F.; CANDIDO, Cristiane M. **A administração da informação integrada às estratégias empresariais**. *Perspect. ciênc. inf.* [online]. 2006, vol.11, n.3, pp. 424-432. ISSN 1413-9936.

HENDERSON, J. C.; VENKATRAMAN, N. Strategic alignment: leveraging information technology for transforming organizations. **IBM System Journal**, v. 32, n. 1, p. 4-16, 1993.

ISACA; **Control Objectives for Information and related Technology (COBIT) – Framework, Control Objectives, Management Guidelines, and Maturity Models**. IT Governance Institute, USA, 2007.

KING, W. R. How effective is your IS planning? **Long Range Planning**, v. 21, n. 5, p. 103-112, Oct. 1988.

LAURINDO, F. J. B.; SHIMIZU, T.; CARVALHO, M. M.; RABECHINI Jr., R. O papel da Tecnologia da Informação (TI) na estratégia das organizações. **Revista G&P: Gestão e Produção**, v. 8, n. 2, p. 160-179, São Carlos, agosto. 2001.

LONGARAY, F. S. **Análise do uso de Padrões de Projeto em empresas de Tecnologia da Informação: um estudo de caso com empresas da UNITEC**. Monografia apresentada à Universidade do Vale do Rio dos Sinos como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação. São Leopoldo, 2008.

MCGEE, J. V.; PRUSAK, L. **Gerenciamento estratégico da informação: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica**. Rio de Janeiro: Campus, 1994.

MINTZBERG, Henry; AHLSTRAND, Bruce; LAMPEL, Joseph. **Safári de Estratégia: um roteiro pela selva do planejamento estratégico**. Tradução Nivaldo Montingelli Jr. Porto Alegre: Bookman, 2000.

NETO, A. N. S; **Modelo Conceitual de Verificação do Alinhamento Entre as Estratégias de Negócios, de TI e de Comércio Eletrônico por Meio do Perfil do *Site Web* da Organização**. Dissertação apresentada à Universidade Federal de Santa Catarina como um dos pré–requisitos para a obtenção de título de Mestre em Engenharia de Produção. Florianópolis, 2004.

NIEDERMAN, F.; BRANCHEAU, J. C.; WETHERBE, J. C. Information systems management issues for the 1990s. **MIS Quarterly**, v. 15, n. 4, p. 475-500, Dec. 1991.

OLIVEIRA, D. P. R. **Estratégia empresarial e vantagem competitiva**. São Paulo: Atlas, 2001. 456 p.

PIRES, S. R. I.; CARPINETTE, L. C. **Fábrica do Futuro**. [S. l.]: Elizabetha Banas, 2000. Apostila.

PORTER, M. E. Strategy in the Internet. **Harvard Business Review**, p. 62-78, Mar. 2001.

REICH, B. H.; BENBASAT, I. Measuring the linkage between business and information technology objectives. **MIS Quarterly**, v. 20, n. 1, p. 55-81, Mar. 1996.

ROSS, Jeanne W.; WEILL, Peter; ROBERTSON, David C. **Arquitetura de TI como Estratégia Empresarial**. São Paulo: M.Books, 2008.

SABHERWAL, R.; CHAN, Y. E. Alignment between business and IS strategies: a study of prospectors, analyzers and defenders. **Information Systems Research**, v. 12, n. 1, p. 1-33, Mar. 2001.

SORTICA, E. A.; CLEMENTI, S.; CARVALHO, T. C. M. B. Governança de TI: comparativo entre COBIT e ITIL. **Congresso Anual de Tecnologia da Informação - CATI**. 2004.

STOECKER, R. Evaluating and rethinking the case study**. The Sociological Review**, 1991.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 2007.

WEILL P., ROSS J. W. **Governança de TI. Tecnologia da Informação**. São Paulo: M. Books do Brasil Editora Ltda, 2006

YIN, Robert K**. Estudo de Caso – Planejamento e Métodos**. Tradução Daniel Grassi. Porto Alegre: Bookman, 2005.

APÊNDICE A – Protocolo de Pesquisa

Título da pesquisa: Gerenciamento do Ambiente Físico utilizando CobiT 4.1: um estudo de caso aplicado.

Questão de pesquisa: Como o departamento de tecnologia da informação pode gerenciar o ambiente físico a fim de proteger os ativos de TI, seus dados, e minimizar o risco de interrupção nos negócios?

Objetivo geral: Este trabalho visa realizar um estudo de caso aplicado tendo por objetivo analisar o ambiente físico e gerar considerações baseado no processo DS12 – Gerenciamento do Ambiente Físico do CobiT - *Control Objectives for Information and related Technology* versão 4.1.

Objetivos específicos:

- compreender a importância do alinhamento de TI a área de negócio;
- executar o estudo de caso;
- avaliar os resultados e sugerir melhorias com base no processo DS12 do CobiT.

Escolha da empresa: O grupo de empresa estudado é composto de cerca de 20 empresas com forte atuação nos ramos de concessionárias de veículos e administração de consórcios. O primeiro ramo possui amplitude regionalizada, no sul do país. O segundo ramo possui atuação a nível nacional.

Procedimentos de coleta de dados: Observação direta.