PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

MAURICIO BECKER

AVALIAÇÃO DA APLICABILIDADE DE RECURSOS NA ÁREA DE TI PARA A CONTINUIDADE DOS SISTEMAS CRÍTICOS AO NEGÓCIO

CAMPINAS
2012

MAURICIO BECKER

AVALIAÇÃO DA APLICABILIDADE DE RECURSOS NA ÁREA DE TI PARA A CONTINUIDADE DOS SISTEMAS CRÍTICOS AO NEGÓCIO

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

Orientador: Prof. Dr. David Bianchini

PUC-CAMPINAS
2012

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

t658.4038 Becker, Mauricio.
B395a Avaliação da aplicabilidade de recursos na área de TI para a continuidade dos sistemas críticos ao negócio / Mauricio Becker. - Campinas: PUC-Campinas, 2012.
135p.

Orientador: David Bianchini.
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Ambientais e de Tecnologias, Pós-Graduação em Gestão de Redes e Telecomunicações.
Inclui bibliografia.

1. Tecnologia da informação - Administração. 2. Comunicação. 3. Governança corporativa. 4. Negócios. I. Bianchini, David. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Ambientais e de Tecnologias. Pós-Graduação em Gestão de Redes e Telecomunicações. III. Título.

19. CDD – t658.4038

MAURICIO BECKER

AVALIAÇÃO DA APLICABILIDADE DE RECURSOS NA ÁREA DE TI PARA A CONTINUIDADE DOS SISTEMAS CRÍTICOS AO NEGÓCIO

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Gestão de Redes e Serviços.
Orientador: Prof. Dr. David Bianchini

Dissertação defendida e aprovada em 03 de dezembro de 2012 pela Comissão Examinadora constituída dos seguintes professores:

Prof. Dr. David Bianchini
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof. Dr. Alexandre de Assis Mota
Pontifícia Universidade Católica de Campinas

Prof. Dr. Edson Luiz Ursini
Universidade Estadual de Campinas

Dedido este trabalho aos meus pais, Evaldo e Vera Marli pelo incentivo, à minha esposa Letuza e aos meus filhos Fábio e Gabriela por todo apoio ao longo desta jornada.

AGRADECIMENTOS

Primeiramente a Deus, nosso Senhor, por permitir a realização deste sonho.

Ao professor Dr. David Bianchini por acreditar, incentivar e efetivamente orientar a condução deste estudo tornando-o possível.

Aos professores Dra. Lia Toledo Moreira Mota e Dr. Alexandre de Assis Mota pelos ensinamentos ao longo do curso.

Ao professor coordenador do curso Dr. Marcelo Abbade pelo apoio durante este curso.

Aos gestores de TI do Estado do Ceará que participaram da pesquisa *survey* permitindo a coleta de informações fundamentais à elaboração deste estudo.

Aos colegas da turma de 2011 do Mestrado Profissional em Gestão de Redes e Telecomunicações da PUC-Campinas, colegas da Hewlett-Packard Brasil Ltda e todos amigos e familiares que incentivaram a conclusão desta importante etapa em minha vida.

“O aumento do conhecimento é como uma esfera dilatando-se no espaço: quanto maior a nossa compreensão, maior o nosso contato com o desconhecido.”

Blaise Pascal
(1623 - 1662)

RESUMO

BECKER, Mauricio, *Avaliação da Aplicabilidade de Recursos na Área de TI para a Continuidade dos Sistemas Críticos ao Negócio*, 2012. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Pontifícia Universidade Católica de Campinas, CEATEC, Programa de Pós-Graduação em Engenharia Elétrica, Campinas, 2012.

No atual contexto globalizado e conectado, as empresas e organizações dependem cada vez mais de suas infraestruturas de tecnologia da informação para a continuidade de seus negócios. Por esse motivo, tais sistemas e aplicações críticos às organizações necessitam estar disponíveis e operacionais aos usuários internos e clientes por praticamente vinte e quatro horas por dia ao longo dos trezentos e sessenta e cinco dias do ano. Diante disto, esta pesquisa buscou apreender o estado da arte em termos de tecnologias para ambientes computacionais de alta disponibilidade e como guias de melhores práticas de Governança e Gerenciamento de TI podem contribuir para manter disponíveis e operacionais os sistemas críticos ao negócio. Como complemento, buscou por meio da aplicação de um *survey* compreender a prática de TI existente em um dos três Estados do nordeste brasileiro de maior relevância econômica. O estudo foi realizado entre dezembro de 2011 e março de 2012 e teve por objetivos avaliar os atuais investimentos em recursos de TI, mensurar os impactos e identificar as principais causas das paradas não programadas. Da análise dos dados, foi possível apontar as oportunidades de melhoria no que tange infraestrutura, pessoas, processos e serviços visando minimizar a indisponibilidade dos sistemas críticos ao negócio de empresas e organizações.

Termos de Indexação: Tecnologia da Informação e Comunicação, Alta Disponibilidade, Causa das Paradas Não Programadas, Sistemas Críticos, Governança de TI.

ABSTRACT

BECKER, Mauricio, *Evaluation of Applicability in IT Resources for Business Critical Systems Continuity*, 2012. Dissertation (Professional Master Degree in Electrical Engineering) - Pontifícia Universidade Católica de Campinas, CEATEC, Programa de Pós-Graduação em Engenharia Elétrica, Campinas, 2012.

In the current globalized and connected context where companies and organizations increasingly rely on their information technology infrastructure for business continuity, such critical systems and applications need to be available and operational for end users and customers almost twenty-four hours per day over the three hundred sixty-five days of the year. In view of this, this research sought to identify the state of the art in terms of technologies for high availability computing environments and how best practice guides for IT Governance & Management can help to maintain available and operational the business critical systems. As a complement, it sought through the application of a survey research to understand the existing IT practices in one of three states with greatest economic importance in the Brazilian Northeast area. The study was conducted among December 2011 and March 2012 and aimed to evaluate current investments in IT resources, identify the main causes of unplanned downtimes and measure their impacts. From the data analysis it was possible to identify improvement opportunities regarding infrastructure, people, processes and services in order to minimize the unavailability of business critical systems for companies and organizations.

Index Terms: *Information Technology and Communication, High Availability, Causes of Unplanned Downtimes, Critical Systems, IT Governance.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANSI	=	*American National Standards Institute*
B2B	=	*Business to Business*
BCS	=	*Business Critical Systems*
BNDES	=	Banco Nacional de Desenvolvimento Econômico e Social
BSC	=	*Balanced Score Card*
CPU	=	*Central Processing Unit*
COBIT	=	*Control Objectives for Information and related Technology*
CPD	=	Centro de Processamento de Dados
CRM	=	*Customer Relationship Management*
DBA	=	*Data Base Administrator*
DRP	=	*Disaster Recovery Plan*
ECC	=	*Error Correcting Code*
ERP	=	*Enterprise Resource Planning*
FCoE	=	*Fibre Channel over Ethernet*
HA	=	*High Availability*
HBA	=	*Host Bus Adapter*
HD	=	*Hard Drive*
ISACA	=	*Systems Audit and Control Association*
ISACF	=	*Information System Audit and Control Foundation*
iSCSI	=	*Internet Small Computer Systems Interface*
ITGI	=	*Information Technology Governance Institute*
ITIL	=	*Information Technology Infrastructure Library*
ITSM	=	*Information Technology Service Management Forum*
KPI	=	*Key Performance Indicator*
LAN	=	*Local Area Network*
NAS	=	*Network Attached Storage*
NIC	=	*Network Interface Cards*
OGC	=	*Office of Government Commerce*
RAID	=	*Redundant Array of Independent Disks*
RAS	=	*Reliability, Availability and Serviceability*
SAN	=	*Storage Area Network*
SLA	=	*Service Level Agreement*
SLM	=	*Service Level Management*
SPOF	=	*Single Point of Failure*

SOX	=	*Sarbanes-Oxley Act*
TI	=	Tecnologia da Informação
TSI	=	*Telecommunications Industry Association*
UPS	=	*Uninterruptable Power Supply*
WAN	=	*Wide Area Network*

SUMÁRIO

CAPÍTULO I - INTRODUÇÃO

1.1. Contextualização do problema no cenário atual

A Tecnologia da Informação (TI) está presente em praticamente todos os setores da sociedade contemporânea tornando os indivíduos, empresas e organizações cada vez mais dependentes pela acessibilidade a sistemas e aplicações que possibilitam ou no mínimo facilitam a execução de suas atividades do dia a dia.

O conceito de sistemas críticos ao negócio surgiu a partir do nível de dependência e impacto que paradas nesses sistemas representam ao negócio de empresas e organizações. Segundo Somerville (2007), tais sistemas críticos ao negócio ou *Business Critical Systems* requerem características de alta confiabilidade, disponibilidade, segurança e proteção das informações, pois a interrupção dos mesmos normalmente resulta desde perdas financeiras diretas com a ociosidade da mão de obra aguardando o retorno do sistema, até o abalo da imagem da empresa no mercado e consequentemente a perda de clientes.

Diante desse contexto, tornou-se relevante apreender da literatura as atuais tecnologias de alta disponibilidade associadas a sistemas computacionais e identificar como os guias de melhores práticas de Governança e Gerenciamento de TI podem contribuir para manter esses sistemas críticos ao negócio disponíveis. Em complemento, buscou-se por meio de uma pesquisa *survey* com gestores de TI avaliar se as empresas e organizações conhecem as causas das paradas não programadas ocorridas em seus sistemas críticos, se dispõem de uma infraestrutura robusta, se estão investindo também na capacitação das pessoas que operam e suportam essa infraestrutura, e por fim, se adotam guias de melhores práticas de Governança e Gerenciamento de TI visando a continuidade dos negócios.

1.2. Justificativa para elaboração deste trabalho

Com o objetivo de apoiar os gestores de TI e organizações na tomada de decisão e direcionamento apropriado de seus investimentos em recursos na área de Tecnologia da Informação, institutos de pesquisa mundialmente renomados como Gartner (GARTNER, 2012) e *International Data Corporation* (IDC) (IDC, 2012) ambos com sedes nos Estados Unidos e com filiais em diversos paises, aplicam pesquisas de âmbito global com os próprios gestores de TI a respeito de temas relacionados, entre eles: buscar identificar a causa das paradas não programadas em sistemas e aplicações.

Conforme Weygant (1996), pesquisas realizadas pelo Gartner em 1993 apontavam que 40% das falhas estavam relacionadas a problemas nos equipamentos, ou seja, no *hardware*, outros 30% das paradas não planejadas associadas a falhas de *software*, 10% das indisponibilidades não previstas causadas por problemas de ambiente ou desastres naturais e 20% restantes relativas a falhas humanas como apresentado na Figura 1.

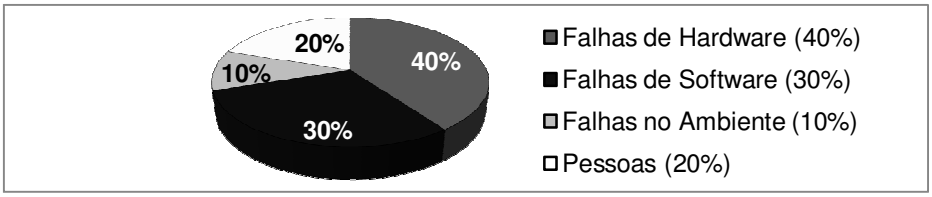

Figura 1. Causa das paradas não programadas (GARTNER,1993 *apud* WEYGANT,1996)

Entretanto, de acordo com o próprio Weygant (2001) na atualização de sua publicação, após nova pesquisa realizada pelo Gartner em 1998 reformulando as alternativas referente às causas das paradas não programadas, apresentou-se um novo cenário sendo: 40% associadas a falhas de aplicação, ou seja, nos *softwares*, 40% relacionados a erros de operação ou falha humana e apenas 20% ocasionadas por falhas da tecnologia como ilustra a Figura 2.

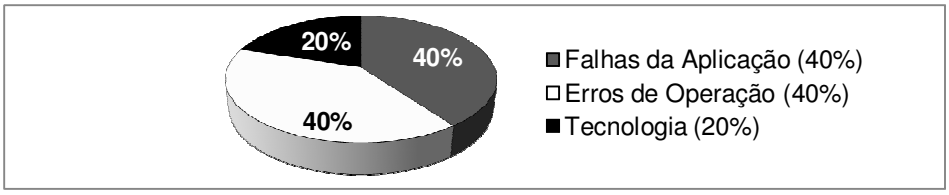

Figura 2. Causa das paradas não programadas (GARTNER,1998 *apud* WEYGANT,2001)

Com base nos resultados desta pesquisa do Gartner, Scott (1999) avalia que tanto falhas da aplicação como erros de operação podem ser considerados como falhas de pessoas e processos totalizando 80% dos incidentes enquanto apenas 20% foram relacionados a tecnologia, ou seja, aos equipamentos (*hardware*), aos sistemas operacionais (*software*), a questões de ambiente (temperatura/energia) e desastres naturais.

No melhor do conhecimento adquirido na procura por fontes de pesquisa mais atualizadas sobre o tema causa das paradas não programadas em ambientes de TI, diversas fontes pesquisadas, entre elas: (ATOS ORIGIN, 2009; NETAPP, 2006; PERTET; NARASIMHAN, 2005) atribuem 80% dessas causas a falhas de processos e pessoas e 20%, a falhas da tecnologia, conforme estudo apresentado pelo Gartner. Contudo, não foi localizado um estudo recente sobre esse assunto no Brasil ou em alguma determinada região ou Estado brasileiro.

1.3. Objetivos

Este estudo busca, por meio da revisão da literatura especializada sobre o tema, apresentar o estado da arte quanto a aplicação de tecnologias voltadas a alta disponibilidade de sistemas e adoção de guias melhores práticas para Governança e Gerenciamento de TI visando minimizar riscos de paradas não programadas em sistemas e aplicações críticos ao negócio.

Este trabalho também se propõe a desvelar a realidade praticada pelas empresas e organizações por meio de uma pesquisa *survey* com abordagem quantitativa. Para tanto, foram delimitadas uma determinada região e um período visando coletar e analisar dados válidos em relação ao momento atual, ou seja, no ano de 2012. Buscou-se aquilatar o conhecimento através dos gestores de TI referente a causa das paradas não programadas em sistemas críticos e como se configuram as infraestruturas e gestão de TI dessas empresas e organizações em relação a implementação de tecnologias de alta disponibilidade, capacitação das pessoas, relacionamento com os fornecedores e adoção de guias de melhores práticas de Governança e Gestão de TI, determinando se efetivamente podem

contribuir para evitar ou reduzir o tempo de indisponibilidade dos sistemas críticos ao negócio.

Com base na análise estatística descritiva dos dados, este trabalho tem por objetivo responder a seguintes perguntas: “Os gestores de TI conhecem as principais causas das paradas não programadas em seus sistemas críticos ao negócio? Estão investindo os recursos adequadamente nos quatro P’s apontados pelo guia de melhores práticas ITIL, ou seja, produtos (infraestrutura contemplando tecnologias de alta disponibilidade), pessoas (capacitação e treinamento), processos (gestão, operação, monitoração e medição de desempenho) e parceiros (suporte com os fornecedores da infraestrutura) visando a disponibilidade e continuidade dos sistemas e aplicações críticos ao negócio das empresas e organizações?”

1.4. Delimitação da pesquisa

Este trabalho apresenta tecnologias atuais de alta disponibilidade associadas a Tecnologia da Informação e como a adoção de guias de melhores práticas de Governança e Gerenciamento de TI podem contribuir para evitar indisponibilidades nos sistemas e aplicações baseado na revisão da literatura. Porém, limitou-se a pesquisa aos guias de melhores práticas COBIT 4.1 e ITIL v3 e não se visa aqui, fazer o detalhamento completo de todos seus processos nem implementá-los na prática.

Quanto a pesquisa *survey*, delimitou-se um intervalo de tempo entre Dezembro de 2011 e Março de 2012, uma população específica composta de especialistas no assunto, ou seja, gerentes e coordenadores de TI em uma determinada região do país (mais precisamente o Estado do Ceará) escolhida por ser uma das três maiores economias da região Nordeste (IBGE, 2011) e por sediar parte importante das maiores empresas da região (BANCO DO NORDESTE, 2009), bem como pela facilidade de acesso do pesquisador ao público a ser pesquisado (GROVES, 2012). A pesquisa adotou uma amostragem não probabilística intencional (RUDIO, 2010) da população pesquisada.

1.5. Organização do trabalho

Esta dissertação está organizada de forma a apresentar o Capítulo I como introdução contendo a contextualização do problema, justificativas, os objetivos do trabalho e a delimitação do estudo proposto.

O Capítulo II intitulado “Alta Disponibilidade associada a Tecnologia da Informação”, visa apresentar os conceitos de Alta Disponibilidade e Sistemas Críticos de Negócios, como também as tecnologias contemporâneas para planejar sistemas e uma infraestrutura de TI confiáveis e robustos.

O Capítulo III “Governança de TI e Guias de Melhores Práticas de TI” demonstra o conceito de governança aplicado a área de Tecnologia da Informação e dois dos principais guias de melhores práticas relacionados a governança e gerenciamento de TI adotados mundialmente.

O Capítulo IV, com base na análise dos temas Alta Disponibilidade associada a Tecnologia da Informação e Melhores Práticas de Governança e Gerenciamento de TI compartilhados nos dois capítulos anteriores, apresenta o estado da arte visando a continuidade dos sistemas críticos ao negócio.

O Capítulo V descreve a metodologia da pesquisa e o detalhamento da elaboração da pesquisa *survey* aplicada aos gestores de TI como forma de obter os dados necessários a serem analisados.

O Capítulo VI apresenta os resultados obtidos com a pesquisa *survey* e a análise estatística descritiva dos mesmos.

O Capítulo VII refere-se a conclusão deste trabalho apresentando ao leitor as conclusões finais do pesquisador e sugestões de trabalhos futuros.

E por final, as Referências e Apêndices que contém na íntegra o conteúdo do *survey* aplicado aos gestores de TI.

CAPÍTULO II - ALTA DISPONIBILIDADE ASSOCIADA A TECNOLOGIA DA INFORMAÇÃO

Com a constante demanda pelo acesso a sistemas e aplicações para execução de suas atividades diárias, tornou-se praticamente uma obrigação para empresas e organizações de manterem disponíveis seus sistemas e aplicações aos seus usuários internos e clientes, surgindo o conceito de disponibilidade e de ambientes computacionais de alta disponibilidade ou *high availability systems*.

2.1. Conceitos de Disponibilidade, Confiabilidade e Facilidade de Manutenção

O termo disponibilidade, conforme apresentado pelo dicionário Michaelis – Moderno Dicionário da Língua Portuguesa, significa: "*1. Qualidade daquele ou daquilo que é ou está disponível. 2. Coisa ou coisas disponíveis[.]*" (MICHAELIS, 2012). Verificando o significado da palavra disponível ainda no mesmo dicionário, descreve: *"[.] 3. Diz-se da mercadoria que pode ser entregue imediatamente ao comprador[.]*" (MICHAELIS, 2012).

Portanto, disponibilidade pode resumir-se na característica ou qualidade daquilo que esteja disponível ou pronto para ser imediatamente utilizado.

Trazendo o termo disponibilidade ou *availability* para a Tecnologia da Informação, os autores definem como:

> Disponibilidade é a medida de quantas vezes ou quanto tempo um serviço ou um componente do sistema está disponível para uso.
> (SCHMIDT, 2006, p.8)

> Na computação, a disponibilidade é geralmente entendida como o período de tempo em que os serviços estão disponíveis (por exemplo: 16 horas por dia, seis dias por semana).
> (WEIGANT, 2001,p.3)

Desta forma, o termo disponibilidade associado a Tecnologia da Informação caracteriza-se pelo período de tempo que um sistema é capaz de prover o serviço ao seus usuários, ou seja, é o tempo que o sistema ou aplicação

permanece disponível e pronto para utilização por seus usuários. Esse tempo de disponibilidade de um sistema também é conhecido na literatura internacional pelo termo técnico *uptime*. Já o período de tempo em que o sistema ou aplicação não está disponível a seus usuários é chamado de tempo de parada ou também pelo termo técnico *downtime*.

A disponibilidade de um sistema é uma característica que pode ser medida como a porcentagem de tempo que o sistema ou aplicação efetivamente está fornecendo um serviço de forma aceitável aos usuários. A fórmula simplificada para obter a disponibilidade ou *availability* de um sistema se dá como apresentada na Figura 3 abaixo onde *uptime* representa o tempo em que o sistema encontra-se ativo e fornecendo o serviço e *downtime* é o tempo em que o sistema esteve indisponível.

$$Disponibilidade = \frac{Tempo\ de\ uptime}{Tempo\ de\ uptime + Tempo\ de\ downtime}\ x\ 100\% \qquad (1)$$

Onde:
Tempo de *uptime*: intervalo de tempo em que o sistema encontra-se operacional e disponível
Tempo de *downtime*: intervalo de tempo em que o sistema encontra-se indisponível

Figura 3. Fórmula da disponibilidade de um sistema segundo Schmidt (2006)

Assim, aplicando-se (1) para um sistema que requer estar disponível 24 horas por dia ao longo dos 365 dias do ano, isto é, um *uptime* esperado de 365 dias e apresentar uma parada ou *downtime* de dois dias, obtem-se 99,45% de disponibilidade.

Considerando-se que a disponibilidade de um sistema pode ser medida, ela também pode ser monitorada e avaliada.

Desta forma, a disponibilidade de um sistema pode estar definida em Acordos de Nível de Serviço ou no termo em inglês, *Service Level Agreements* (SLAs). SLAs são documentos firmados entre o prestador e quem recebe tal serviço, onde se explicita quais os serviços a serem prestados bem como os níveis mínimos aceitáveis dos mesmos, formas de serem medidos e penalidades quando não são alcançados. Portanto, podem adotar a disponibilidade de um sistema como uma medida de desempenho.

A Tabela 1 representa as porcentagens de disponibilidade ou *uptime* e indisponibilidade ou *downtime* de sistemas considerando uma operação crítica em execução 24 horas por dia, sete dias por semana, 365 dias por ano.

Tabela 1. Porcentagem de *uptime/downtime* de sistemas críticos

Porcentagem *Uptime*	**Porcentagem *Downtime***	**Tempo Máximo esperado de *downtime* por ano (365x7x24)**
99%	1,0%	3,65 dias (5.256 minutos)
99,5%	0,5%	43 horas e 48 minutos (2.628 minutos)
99,9%	0,1%	8 horas e 45 minutos (525 minutos)
99,95%	0,05%	4 horas e 23 minutos (263 minutos)
99,99%	0,01%	(52 minutos)
99,999%	0,001%	(5 minutos)

Conforme demonstrado na Tabela 1, o tempo máximo esperado de indisponibilidade ou *downtime* de um sistema crítico com disponibilidade de 99,999% ou também conhecido como “cinco noves e cinco minutos”, é de apenas 5 minutos por ano.

Em resumo, quanto maior a disponibilidade ou *uptime* requerida, menor o tempo permitido para falhas e interrupções nesse sistema.

Frente a este contexto, considera-se um sistema computacional de alta disponibilidade, aquele projetado para não permitir interrupções no serviço, através do gerenciamento ou minimização de falhas, bem como do tempo das paradas programadas para manutenção (WEYGANT, 2001).

De acordo com Schmidt (2006), alta disponibilidade em sistemas de computação também pode ser descrita como:

> Alta disponibilidade é a característica de um sistema de proteger-se contra ou se recuperar de pequenas interrupções em um curto espaço de tempo através de meios amplamente automatizados.
>
> (SCHMIDT, 2006, p.7)

Buscando um conceito adicional, o dicionário de termos técnicos do *Storage Networking Industry Association* (SNIA), uma importante associação de fabricantes, revendedores e usuários finais de tecnologias de armazenamento de

dados com sede nos Estados Unidos e filiais no Brasil entre outros países, define alta disponibilidade em ambientes computacionais como:

> A capacidade de um sistema em realizar a sua função continuamente (sem interrupção), por um período de tempo muito mais longo do que a confiabilidade dos seus componentes individualmente poderia sugerir.
>
> (SNIA, 2012)

Salienta-se que, conforme mencionado por ambos autores, Weygant (2001) e Schmidt (2006), além dos sistemas computacionais de alta disponibilidade, existe um outro conceito que define os sistemas tolerantes a falhas ou *fault tolerants*, ou seja, sistemas capazes de manterem-se operacionais se um ou mais componentes falharem. Tais sistemas tem seus principais componentes de *hardware* e *software* redundantes, incluindo processadores e módulos de memória, e seu reparo também pode ser realizado sem interrupções. Portanto, *High Availability* e *Fault Tolerant* são conceitos distintos e sistemas *Fault Tolerant* não são abordados neste estudo.

De acordo com Weygant (2001), alta disponibilidade de um sistema não deve ser considerada um valor absoluto e pode variar de acordo com o conceito de criticidade do serviço, ou seja, necessidades diferentes requerem níveis de disponibilidade diferentes, pois em serviços críticos, como os que controlam o fornecimento de energia elétrica, a oferta de serviços de telefonia e comunicação de dados ou em ambientes críticos como hospitais, há a expectativa de um alto nível de disponibilidade e uma pronta resposta em caso de falhas ou indisponibilidades. Já sistemas de menor criticidade ou menor impacto, permitem um nível de disponibilidade menor.

No mundo corporativo, a disponibilidade de sistemas também é crucial para a continuidade dos negócios. Para bancos, operadoras de cartão de crédito ou corretoras que operam nas bolsas de valores, paradas representam perdas financeiras e de imagem muitas vezes irrecuperáveis.

Segundo Schmidt (2006), existem outras duas características dos sistemas que contribuiem para sua alta disponibilidade, confiabilidade ou *reliability* e sua facilidade de manutenção ou *serviceability*. As três características juntas

são representadas em inglês pelo acrônomo RAS – *Reliability, Availability and Serviceability*.

As características de confiabilidade e facilidade de manutenção contribuem para uma maior disponibilidade de um sistema. Confiabilidade é a probabilidade que um sistema permanecerá disponível em um intervalo de tempo. Normalmente é fornecida pelo fabricante do componente do sistema como o tempo médio entre falhas ou *Mean Time Between Failures* (MTBF) (SCHMIDT, 2006).

Já a característica de facilidade de manutenção ou *serviceability* representa quão prático ou quão complexo é o processo de manutenção do sistema ou equipamento desde a identificação de pré-falha ou falha de um componente, até a sua efetiva correção ou substituição. Sendo portanto, um importante atributo a ser observado durante a aquisição da solução por um gestor de TI visando a alta disponibilidade do sistema.

O tempo médio para reparo ou *Mean Time to Repair* (MTTR) pode servir como parâmetro para medir a facilidade de manutenção de um sistema ou equipamento. Não é comum os fabricantes compartilharem esse tipo de informação nos *datasheets* ou manuais de especificação dos equipamentos e sistemas.

Conhecendo o MTBF e o MTTR e os mesmos não sendo correlatos, também é possível medir a disponibilidade de um sistema como demonstra a fórmula disposta na Figura 4. (MARCUS; STERN, 2003).

$$Disponibilidade = \frac{MTBF}{MTBF + MTTR}\ x\ 100\% \qquad (2)$$

Onde:
MTBF: tempo médio entre falhas dado em horas;
MTTR: tempo médio de reparo dado em horas.

Figura 4. Fórmula da disponibilidade de um sistema conforme Marcus e Stern (2003)

Ainda sobre facilidade de manutenção, características como componentes que podem ser substituídos sem a necessidade de desligamento do equipamento, descritos na literatura como *hot-swappable,* e ferramentas de

autodiagnóstico conectadas diretamente com o suporte do fabricante ou também chamadas, *call home* (que reportam automaticamente uma falha ou pré-falha de um componente ou módulo diretamente para o fornecedor), são extremamente recomendáveis para equipamentos que farão parte de um sistema de alta disponibilidade.

2.2. Custo das paradas não programadas ou *downtimes*

Basicamente, investir em equipamentos de alta confiabilidade e de rápida recuperação para tornar alta a disponibilidade de um sistema, trata-se de uma decisão de negócios. Isso porque equipamentos com estas funcionalidades normalmente tem um custo maior que equipamentos convencionais e mantê-los operacionais em ambientes propícios ou *data centers* também custa dinheiro aos proprietários das empresas e investidores. Entretanto, quando esses sistemas, adquiridos para cumprir um determinado propósito dentro da organização, deixam de funcionar, normalmente causam um custo operacional ainda maior.

Portanto, esse tempo de inatividade ou *downtime* dos sistemas também gera um custo. E este custo de *downtime* embora variável, pois pode ser maior ou menor de acordo com o horário ao longo do dia e tempo de duração da falha em relação a carga de tarefas requeridas nesse intervalo de tempo, pode ser muitas vezes maior que o investimento ou no que seria investido para se ter um sistema de alta disponibilidade dependendo do grau de dependência e impacto que essa parada causa na continuidade dos negócios da organização.

Segundo Marcus e Stern (2003), os custos causados por uma parada não programada ou *unplanned downtime* podem ser subdivididos em custos diretos e custos indiretos. Os custos diretos referem-se principalmente a perda de produtividade, ou seja, o custo da mão de obra ociosa com a parada dos sistemas e os custos envolvidos em horas extras para a recuperação do tempo parado após o restabelecimento dos sistemas. Estas perdas financeiras dependem da área de atuação da empresa, podendo ser quantificadas em milhões de dólares por hora parada para empresas do ramo financeiro, telecomunicações ou operadoras de cartões de crédito. Já os custos indiretos estão relacionados aos

possíveis impactos na credibilidade da marca da empresa no mercado, impactos negativos no valor da ação, insatisfação e potencial perda de clientes, risco de processos judiciais e publicações negativas na mídia que, no médio prazo, podem representar um prejuízo significativamente maior que os custos diretos.

Publicado no Jornal New York Times em 12 de Junho de 1999, a matéria entitulada "*Crash Shuts Down Ebay for Much of the Day*" ou na tradução livre "eBay fora do ar por grande parte do dia", considerou uma das piores paradas não programadas da internet. O site renomado de compra e venda de produtos pela internet chamado eBay apresentou uma indisponibilidade de seus serviços de 22 horas impactando milhões de usuários.

De acordo com Fox e Patterson (2002), essa parada não programada ou *outage* causou ao eBay uma queda de 26% nas suas ações reduzindo o valor da empresa no mercado de capitais em US$4 bilhões gerando ainda perdas financeiras diretas entre US$3 e 5 milhões.

Além deste exemplo, pode-se citar a indisponibilidade dos sistemas de reserva de passagens aéreas da Comair, uma subsidiária da Delta Air Lines que, em plena véspera de Natal em 2004, cancelou em torno de 1.100 voos impactando cerca de 30.000 passageiros. As ações da Delta Airlines na bolsa de valores cairam 1,46% após esse incidente (INTERNETNEWS.COM, 2004).

Trazendo essa situação para o mercado brasileiro, talvez uma das piores indisponibilidades que se tem notícia, foi a queda dos sistemas de transmissão de dados da empresa Telefônica que afetou quase a totalidade dos usuários de internet pessoas físicas e corporativas no Estado de São Paulo, ocorrida em Junho de 2008 e amplamente divulgada pela mídia.

> **Falha em rede atinge conexão à internet no Estado de SP**
> O Estado de São Paulo enfrenta problemas de acesso à internet nesta quinta-feira (3), com lentidão ou indisponibilidade completa na conexão. A Folha Online apurou que a rede da Telefônica apresenta problemas, gerando reflexos na banda larga, conexões dedicadas (de alta velocidade, utilizadas principalmente por empresas) e outros tipos de acesso.
> A falha começou a ser sentida na quarta-feira (2) e se intensificou durante a madrugada de hoje. Com isso, a conexão de grande parte dos internautas e das empresas que usam a rede da Telefônica no Estado está instável. Especialistas ouvidos pela

> reportagem classificaram a pane como "grave" e sem previsão de retorno.
> A instabilidade no serviço atinge não só a rede banda larga do provedor Speedy, mas também serviços de conexão dedicada utilizados principalmente por empresas e outras redes. Procurada pela reportagem, a Telefônica não se pronunciou até a publicação desta reportagem.[.]
>
> (FOLHA ONLINE, 03 de Junho de 2008)

> **Pane na Telefonica derruba *web* e para serviços pelo Estado**
> **Redes da Polícia Militar, CET, Corpo de Bombeiros, Detran, e conexão do governo e de usuários estão fora do ar**
> Uma pane no sistema de transmissão de dados da Telefonica está afetando os usuários de internet em grande parte do Estado de São Paulo. A Secretaria de Segurança Pública de São Paulo (SSP) também confirmou que a rede de comunicação que integra as polícias Civil e Militar, ao Detran, ao Corpo de Bombeiros e à Companhia de Engenharia de Trânsito (CET), por conta da pane, também estão 'fora do ar'. Segundo a assessoria da SSP, algumas delegacias estão fazendo os boletins de ocorrência manualmente. "Cada DP está agindo conforme a decisão dos delegados, não há nenhuma instrução da Secretaria sobre isso", afirmou. Foram afetados ainda a internet do governo do Estado e alguns serviços do Poupatempo."
>
> (ESTADÃO, 03 de Junho de 2008)

Frente a essa situação crítica, a imagem da empresa foi exposta pela mídia impactando sua credibilidade perante o mercado e correndo riscos, além das multas contratuais previstas com os clientes corporativos, de ressarcimentos aos usuários pessoais do serviço de internet e sanções do órgão regulador brasileiro, ANATEL – Agência Nacional de Telecomunicações.

Com o objetivo de auxiliar os gestores de empresas e organizações em especial o CIO – *Chief Information Officer* em estimar quanto custa por hora uma parada não programada (*cost of downtime*) visto que outros autores definiram fórmulas extremamente complexas para este cálculo, foi apresentado por Patterson (2002) na Conferência LISA - *Large Installation System Administration* na Califórnia, Estados Unidos, uma fórmula simplificada para estimar esse valor.

De acordo com Patterson (2002), foram definidos dois termos. O primeiro é o custo total dos funcionários por hora que é obtido através do total de salários e benefícios pagos a todos os funcionários por semana dividido pelo número médio de horas trabalhadas por semana. O segundo termo é o rendimento médio por hora definido por meio da renda total semanal da empresa dividido pelo número médio de horas semanais que a empresa está aberta para

os negócios. Importante salientar que esse segundo termo considera dois fatores: se houver rendimentos associados a vendas pela internet adicionado dos rendimentos semanais dependentes da infraestrutura de TI.

Segundo o autor, obter esses custos com pessoal e os rendimentos semanais não deve ser algo complexo tratando-se de dados para se calcular uma estimativa e que não precisam necessariamente estar expressos até os centavos. Empresas de capital aberto fornecem tais informações trimestralmente enquanto que empresas menores podem obter esses dados com os departamentos financeiros e de recursos humanos.

Após quantificar esses dois termos, para se obter o custo estimado por hora de uma parada não programada de acordo com Patterson (2002), efetua-se um cálculo que considera que: Custo Médio Estimado por Hora de *Downtime* (CMEHD) é igual ao resultado da multiplação do Custo Total dos Funcionários por hora (CTFH) pela Fração de Funcionários Afetados (FFA) pela parada somado ao resultado da multiplicação dos Rendimentos da Empresa por hora (REH) pela Fração de Rendimentos Afetados (FRA) pela parada conforme apresentado na fórmula disposta na Figura 5.

$$\mathrm{CMEHD} = (\mathrm{CTFH} * \mathrm{FFA}) + (\mathrm{REH} * \mathrm{FRA}) \quad (3)$$

Onde:
CTFH: dado em moeda corrente (R$);
FFA: dado em percentual de funcionários impactados onde 1,0 representa 100%;
REH: dado em moeda corrente (R$);
FRA: dado em percentual de rendimentos horários afetados onde 1,0 representa 100%.

Figura 5. Fórmula para cálculo do custo médio estimado de *downtime* segundo definido por Patterson, 2002

Aplicando hipoteticamente (3) em uma empresa de médio porte de vendas por telefone, com os seguintes parâmetros: custo total dos funcionários por hora: R$7.500,00 (estimado); rendimentos por hora: R$13.636,00 considerando que a empresa fatura anualmente R$36 milhões, ou seja, R$3 milhões por mês trabalhando em regime 10x5, ou seja 2ª à 6ªfeira das 08:00hs às 18:00hs (R$3.000.000,00 divididos por 22 dias e o resultado dividido por 10 horas); se houver a parada do sistema responsável pela colocação das ordens de

venda por uma hora, impactando 90% dos funcionários em horário comercial e 100% dos rendimentos que dependem totalmente desse sistema, o custo estimado de *downtime* por hora seria de R$20.386,00 conforme demonstra a Figura 6.

$$\text{CMEHD} = (\text{R\$}7.500{,}00 * 0.9) + (\text{R\$}13.636{,}00 * 1{,}0) = \text{R\$}20.386{,}00 \qquad (3)$$

Figura 6. Exemplo da aplicação da fórmula para cálculo do custo médio estimado de *downtime* seguindo a fórmula apresentada por Patterson, 2002

Desta forma, este valor, mesmo que estimado, pode auxiliar o CIO e dirigentes da organização na tomada de decisão para investimentos em TI buscando um sistema de alta disponibilidade. Como demonstrado com a aplicação de (3), se houver uma parada não programada por um dia útil ou 10 horas, apenas de custos diretos, ou seja, sem considerar os custos indiretos de insatisfação dos clientes, impacto na marca e vendas futuras, pode representar mais de duzentos mil reais de perdas. Este valor possivelmente seria suficiente para adquirir um sistema robusto com níveis de serviço de suporte adequados com o fornecedor que evitariam ou minimizariam o risco de paradas não programadas e consequentemente impactos na continuidade dos negócios dessa empresa.

2.3. Níveis de Alta Disponibilidade para sistemas de TI

Empresas e organizações tem uma gama de sistemas e aplicações em uso no seu dia a dia. Cabe aos gestores de negócio alinhados com os gestores de TI mapearem qual é a criticidade de cada uma dessas aplicações para a continuidade das operações da organização. De acordo com o impacto ao negócio gerado pela parada não programada de cada sistema ou aplicação, devem ser definidos quais serão os sistemas configurados em alta disponibilidade e que nível de disponibilidade será adotado nos mesmos sempre balanceando o valor investido na solução de TI com a importância desse sistema ao negócio.

Como forma de apoiar os gestores e as empresas, o *International Data Corporation* (IDC), outro instituto de pesquisa e avaliação de soluções de TI com sede nos EUA fundado em 1964, qualificou a seguinte distribuição de níveis de disponibilidade conforme apresentado no Quadro 1, denominada *IDC's Availability Spectrum* (IDC, 2010a).

Quadro 1. Níveis de Disponibilidade de Sistemas de acordo com IDC (2010a)

Nível de Disponibilidade *(Availability Level)*	**Impacto da falha de um componente aos usuários prioritários**	**Características de Proteção do Sistema**
AL4	- É transparente aos usuários não havendo interrupções, perda de transações nem perda de desempenho.	- Componentes e funções 100% redundantes.
AL3	- Usuários permanacem *online*. - Talvez a transação corrente tenha que ser refeita. - Pode haver perda de desempenho.	- Processo automático de *failover* transferindo os usuários e suas sessões de trabalho para componentes reserva. - Múltiplos sistemas com acesso aos dados armazenados.
AL2	- Interrupção do usuário mas pode rapidamente se reconectar ao sistema. - Pode haver a necessidade de refazer a última transação. - Pode apresentar impacto no desempenho do sistema.	- Usuários transferidos para componentes reserva (*backup*). - Múltiplos sistemas com acesso aos dados armazenados.
AL1	- Trabalho impactado. - Desligamento não controlado do sistema. - Integridade dos dados garantida.	- Redundância no armazenamento de dados com espelhamento de discos ou tecnologia RAID (*Redundant Array of Independent Disks)*. - Sistemas de arquivos com identificação e recuperação de transações incompletas.

A tecnologia RAID (*Redundant Array of Independent Disks*), será abordada com mais detalhes na seção 2.4.2 deste Capítulo.

Como apresentado no Quadro 1, o IDC classifica o nível mais alto de disponibilidade (AL4) como sistemas *fault tolerant* considerados para um número muito reduzido de necessidades críticas como o controle de tráfego aéreo nos Estados Unidos por exemplo. Tais sistemas não serão tratados neste estudo.

A grande maioria das aplicações críticas de negócio de empresas e organizações enquadram-se nos níveis AL2 e AL3 contemplando sistemas com características de *failover* e *cluster*, ou seja, com a capacidade de migração da aplicação ou banco de dados entre servidores alternativos compartilhando o acesso aos mesmos dados armazenados permitindo restabelecer a operação e acessibilidade dos usuários em um breve espaço de tempo (IDC, 2010a).

Segundo a tradução livre do dicionário de termos técnicos do SNIA (2012), pois não foi encontrada uma única palavra na Língua Portuguesa que possa definir *failover* em ambientes computacionais, trata-se da substituição automática de um componente do sistema que falhou por outro com funcionalidades equivalentes.

Um *cluster* em ambientes computacionais é um grupo de servidores ou nós interconectados e trabalhando em conjunto como se fossem um único servidor ou sistema respondendo as requisições dos usuários. Os servidores que compõe um *cluster* necessitam ser da mesma plataforma de *hardware* e mesmo tipo e versão de sistema operacional possibilitando que o serviço ou aplicação permaneça disponível em caso de falha de um desses servidores configurados no *cluster* (GOPALAKRISHNAN, 2007).

Os autores Marcus e Stern (2003) e Zhu *et al.* (2009), também subdividem os níveis de alta disponibilidade dos sistemas de acordo com as formas de proteção a falhas aplicados em cada camada ou componente do sistema.

Como forma de proteção do sistema para sua continuidade de operação quando ocorre uma falha, a redundância é uma característica chave tratando-se de alta disponibilidade e é definida como:

> Redundância é a inclusão de componentes adicionais de um dado tipo de sistema (além dos requeridos para o sistema desempenhar sua função) com a finalidade de permitir a operação contínua, no caso de uma falha de um componente.
>
> (SNIA, 2012)

Segundo Zhu *et al.* (2009), os níveis de alta disponibilidade são subdivididos em cinco, conforme apresenta a Figura 7, que também permite

demonstrar a relação direta de quanto maior o nível de alta disponibilidade desejado, maior será o investimento na infraestrutura de TI.

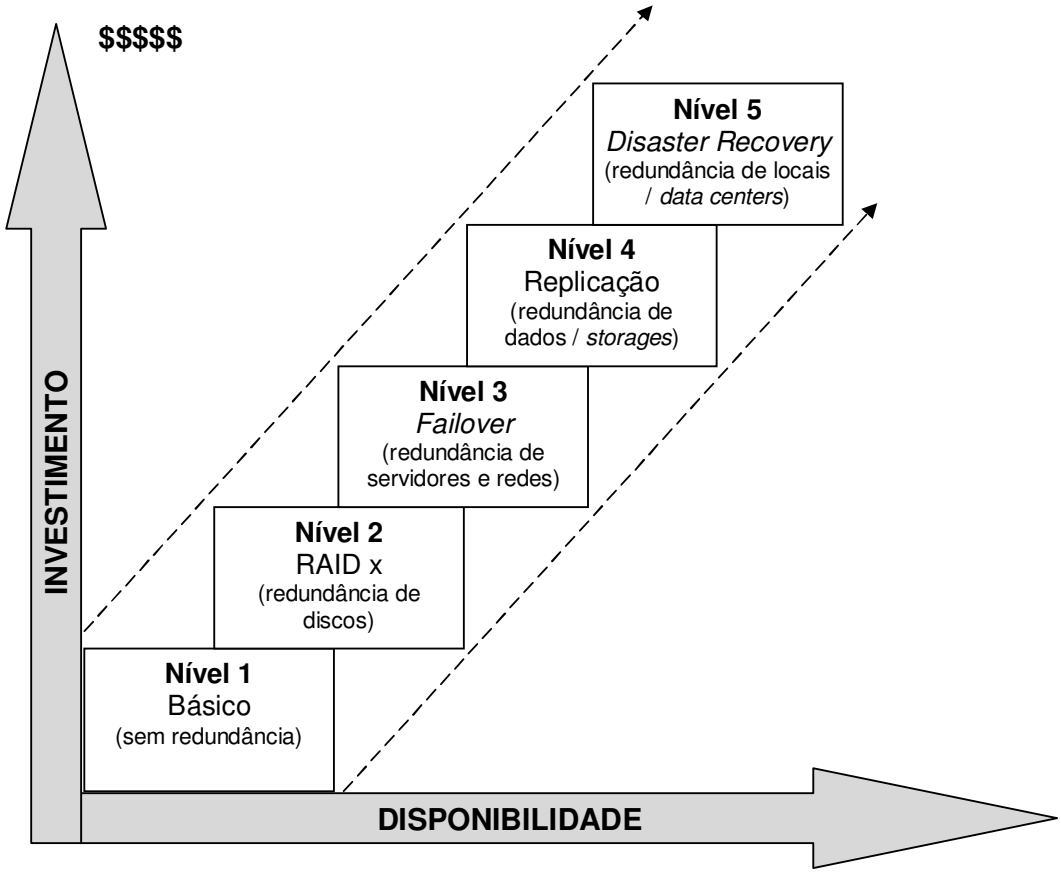

Figura 7. Níveis de Disponibilidade de sistemas adaptado de Zhu *et al*.(2009)

Fazendo uma analogia entre a divisão definida pelo IDC e a apresentada por Zhu, o nível de disponibilidade AL1 do IDC equivale-se ao Nível 2 de Zhu, AL2 e AL3 aos Níveis 3 e 4. Já o nível AL4 do IDC *(fault tolerant)* seria acima da distribuição definida por Zhu enquanto o Nível 5 de Zhu seria um AL3 avançado do IDC mas ainda dentro do conceito de alta disponibilidade.

Dada sua importância, os conceitos técnicos de Replicação e *Disaster Recovery* apresentados na Figura 7 serão abordados com mais detalhes na seção 2.4.3 deste Capítulo.

2.4. Identificando as possíveis vulnerabilidades e apontando as principais técnicas de Alta Disponibilidade aplicadas a ambientes de TI

Com base no alinhamento estratégico dos objetivos de negócio da organização com a área de TI, definindo quais são os sistemas críticos de negócio que requerem maior robustez e disponibilidade e consequentemente um maior investimento financeiro, os profissionais técnicos da área de TI, apoiados em muitos casos por consultorias externas e pelos próprios fabricantes, definem a infraestrutura de TI e níveis de suporte e assitência técnica necessários para atender essa demanda do negócio.

Portanto, conhecer as principais vulnerabilidades, bem como as técnicas e tecnologias capazes de evitar as paradas não programadas dos sistemas críticos é uma premissa para planejar e implementar um ambiente computacional de alta disponibilidade.

Segundo Gartner (1998) *apud* Weygant (2001) e IDC (2003), as causas das paradas não programadas ou *outages* estão relacionadas principalmente por:

a) Falhas na tecnologia que englobam a infraestrutura de TI como um todo, ou seja, o local ou *data center* onde os equipamentos encontram-se instalados e possíveis desastres naturais como fogo ou inundações, os equipamentos (*hardware*) e o sistema operacional (*software*);

b) Falhas das aplicações (*softwares*) relacionadas as aplicações desenvolvidas e customizadas especificamente para a organização e as padrão de mercado como banco de dados, CRM – *Customer Relationship Management* e ERP – *Enterprise Resource Planning*;

c) Falhas operacionais envolvendo erros humanos ou processos ineficazes ou inexistentes de operação e administração do ambiente de TI.

Com o objetivo de minimizar ou inclusive evitar que falhas na tecnologia gerem a indisponibilidade de sistemas críticos, uma das principais

características é a adoção de redundâncias no sistema visando eliminar os pontos únicos de falha ou *Single Point of Failures* (SPOFs).

Um ponto único de falha ou SPOF é um componente de *hardware* ou de *software* que não possui um segundo componente redundante ou como espera (*standby*) e cuja falha nesse componente causa a indisponibilidade de todo o sistema (WEYGANT, 2001).

2.4.1. Data Center

Os *data centers,* ou anteriormente conhecidos como centros de processamento de dados (CPDs), consistem na infraestrutura básica onde os equipamentos serão instalados. Os *data centers* devem prover desde o local como também a alimentação elétrica, os equipamentos de ar condicionado para controle de temperatura e umidade ambiente, o cabeamento estruturado elétrico e lógico até o controle de acesso e a proteção contra incêndio.

Não havendo mecanismos de proteção e redundância, a simples queda ou oscilação de energia da distribuidora pode desligar abruptamente todos os equipamentos, incluindo os sistemas críticos ao negócio. Segundo a empresa especialista em data centers Emerson Network Power, a simples falha do sistema de ar condicionado pode elevar a temperatura da sala de 20ºC para 35ºC em cerca de apenas 6 minutos, também causando um *outage* e desligamento de todos os equipamentos por sobretemperatura ou *overtemp* (EMERSON NETWORK POWER, 2008).

Portanto, subestações de energia redundantes na alimentação do *data center*, instalação de *nobreaks* ou UPS – *uninterruptable power supplies*, que mantém a alimentação por alguns minutos através de baterias mesmo com a queda de energia no fornecimento associados à instalação de geradores de energia sincronizados que sejam acionados automaticamente e sistemas de ar condicionado redundantes, são requisitos para abrigar sistemas de alta disponibilidade.

A definição do local do prédio do *data center,* evitando riscos de catástrofes naturais como inundações ou deslizamentos ou riscos causadas pelo homem como proximidade de aeroportos, devem ser avaliados. Exemplos reais como *tsunami* no Japão em 2009 ou o furacão Katrina em 2004, afetando a cidade de Nova Orleans e outras no sul dos Estados Unidos, não impactaram apenas residências mas também empresas e consequentemente suas infraestruturas de TI.

Outras questões também importantes a serem consideradas são: o controle de acesso à sala e o monitoramento com circuitos internos de TV, evitando a entrada de pessoas não autorizadas, bem como a proteção contra incêndios com a instalação de sistemas de deteção e contenção de incêndios .

A *Telecommunications Industry Association* (TIA), uma associação comercial credenciada pelo *American National Standards Institute* (ANSI), publicou o padrão ANSI/TIA-942 denominado *Telecommunications Infrastructure Standard for Data Centers* em 2005. Atualizado em 2008 e 2010, o ANSI/TIA942 qualifica os *data centers* em quatro níveis ou *tiers* de acordo com sua infraestrutura, sendo o *Tier* 1 o mais básico e o *Tier* 4 o mais robusto, planejado para ambientes missão crítica.

O Instituto Uptime com sede nos EUA e recentemente também com sede no Brasil, definiu sua própria escala de certificação dos *data centers* chamada *Tier Performance Standards* também com quatro níveis ou *tiers*, são eles:

a) *Tier I* - Infraestrutura Básica: *data centers* que não possuem redundância de caminhos de distribuição de energia nem tão pouco de componentes de capacidade como *nobreaks* ou UPS's; falhas ou manutenções programadas tanto na UPS como no caminho de distribuição de energia afetarão todo o *data center;*

b) *Tier II* – Redundância de Componentes de Capacidade: são *data centers* com UPS's (componentes de capacidade) redundantes mas permanecendo com um único caminho de distribuição, assim, falhas

de distribuição indisponibilizam todo o *data center* e falhas de UPS podem ou não afetar todo o ambiente;

c) *Tier III* – Manutenção sustentável: contém caminhos de distribuição independentes e componentes de capacidade (UPS's) redundantes, permitindo manutenções sem impactos na operação do *data center*;

d) *Tier IV* – Tolerante a Falha: contém todas as características do *Tier III* além de fontes primárias de energia redundantes, que podem ser considerados geradores elétricos próprios ou subestações externas garantindo a continuidade de operação em caso de falhas de energia, distriuição ou componentes de capacidade.

A certificação de um *data center* por uma empresa ou instituto especializado é um passo importante na gestão da infraestrutura de TI sendo capaz de auxiliar os gestores na implementação de melhores práticas visando a alta disponibilidade do ambiente.

2.4.2. Equipamentos *(hardware)*

A escolha dos equipamentos, ou seja, dos servidores, dispositivos de armazenamento de dados ou *storages*, equipamentos de infraestrutura de redes avaliando as características de confiabilidade, facilidade de manutenção (*serviceability*) e principalmente de redundância de componentes, também é de extrema importância em sistemas de alta disponibilidade.

Fontes de alimentação e ventiladores são os componentes dos equipamentos com os piores índices de MTBF, isto é, mais sucetíveis a falhas segundo Marcus e Stern (2003).

Desta forma, é fundamental para sistemas de alta disponibilidade que os servidores, equipamentos de armazenamento de dados (*storages*) e equipamentos da infraestrutura de redes como *switches* e roteadores tenham fontes e ventiladores reduntantes e *hot-swappable,* capazes de manter os

equipamentos operacionais, mesmo em caso de uma falha de fonte ou ventilador, bem como capazes de facilitar o processo de manutenção no momento de sua substituição sem gerar parada programada do equipamento.

O código interno ou *firmware* é também um componente que requer atenção. Pode ser considerado um ponto único de falha tendo como principal ação a ser adotada no intuito de evitar problemas, a manutenção da versão de *firmware* atualizada conforme as novas versões disponibilizadas pelo fabricante, visando garantir que as correções e melhorias conhecidas mais recentes sejam aplicadas (BECKER, *et al.* 2012).

Os processadores ou CPUs – *Central Processing Units*, por terem sua interação direta com o Sistema Operacional, não possuem níveis de redundância de componentes em sistemas de alta disponibilidade que possam evitar que a falha de um desses componentes cause a reinicialização abrupta do equipamento.

Entretanto, alguns fabricantes em determinadas plataformas de servidores de missão crítica, adicionaram um monitoramento interno via *firmware* que é capaz de isolar o processador que apresentou a falha reiniciando o servidor com esse processador desativado. Desta forma, o sistema reiniciará em modo degradado, sem esse processador ativo, reduzindo o risco de novas reinicializações pelo mesmo motivo até que o processador seja substituído (SCHMIDT, 2006).

Com relação a módulos de memórias, determinadas plataformas de servidores permitem o espelhamento físico dos módulos, ou seja, redundância de componentes, permitindo que uma falha de *hardware* em um módulo de memória ocorra sem a interrupção do sistema. Porém, com a grande capacidade de memória utilizada nos atuais sistemas e o fato do investimento ser exatamente o dobro (pois será necessário ter o dobro da memória no sistema como redundância), tal prática não tem sido observada com frequência na prática. Normalmente os sistemas de alta disponibilidade utilizam módulos de memória com a tecnologia *Error Correcting Code* (ECC) que autocorrige erros mais simples

(também conhecidos como *single bit errors*) reduzindo a ocorrência de paradas não programadas por falha de memória.

As falhas das interfaces de entrada e saída como as *Network Interface Cards* (NICs) que interligam os servidores e *storages* tipo NAS – *Network Attached Storage* à rede LAN – *Local Area Network* e as *Host Bus Adapters* (HBAs) que interligam os servidores e *storages* via a rede SAN – *Storage Area Network* necessitam ser redundantes e configuradas via *software* com a funcionalidade de *failover* para também não se tornarem um ponto único de falha (BENDER; JOSHI, 2004).

No caso da infraestrutura de redes, seja ela LAN, SAN ou WAN – *Wide Area Network,* um cabeamento estruturado dentro das especificações, bem identificado e documentado, a utilização de equipamentos como *switches* e roteadores com fontes de alimentação e ventiladores internos reduntantes bem como ter os próprios equipamentos e cabeamentos duplicados, permitindo que tanto os servidores como *storages* sejam acessados por caminhos diferentes, elimina os próprios equipamentos e cabos de rede ou fibra ótica como SPOFs.

O mesmo se aplica às conexões externas da rede WAN contendo *links* de comunicação entre os *data centers* ou filiais das empresas e organizações duplicados, preferencialmente utilizando caminhos físicos diferentes e mais de um provedor do serviço de telecomunicações, buscando evitar a indisponibilidade da comunicação com ambiente externo, como ocorreu com empresas e organizações impactadas em 2008 com a parada não programada do serviço provido pela empresa Telefônica no Estado de São Paulo.

Outro ponto de atenção fundamental, é a proteção dos dados armazenados nos discos rígidos ou *hard drives* (HDs) pois, segundo os autores Marcus e Stern (2003), as falhas de *hardware* mais frequentes estão relacionadas a discos rígidos ou HDs, devido à complexibilidade dos seus mecanismos com componentes eletromecânicos e altas taxas de rotação.

Para evitar que a simples falha de um disco gere a perda ou a corrupção de dados, implementa-se nas controladoras internas de discos nos servidores e nas controladoras dos *storages* a tecnologia RAID – *Redundant*

Array of Independent Disks que habilita um grupo de discos operarem em conjunto como uma única unidade lógica também chamada de LUN – *logical unit* apresentada ao sistema operacional. Os níveis de RAID (salvo o RAID0) utilizam algoritmos de espelhamento ou paridade que mantém a integridade e disponibilidade de acesso aos dados mesmo que ocorra a falha de um dos discos rígidos que compõe a LUN.

Os níveis de RAID atualmente adotados em ambientes de alta disponibilidade por proverem redundância de dados em caso de falha de um disco são: RAID1 (espelhamento utilizando sempre dois discos, ambos contendo a mesma cópia dos dados), RAID4 (disco de paridade), RAID5 (paridade distribuída), RAID6 ou RAIDDP (dupla paridade distribuída) e RAID10 ou RAID0+1(espelhamento distribuído por meio da combinação de RAID0 e RAID1 utilizando quantidades pares de discos por grupo). Apenas o nível de RAID0 não prove redundância de dados e não deve ser considerado na configuração de ambientes de alta disponibilidade (TROPPENS *et al.*, 2009; BECKER, 2012).

O gestor de TI na tomada de decisão pelo investimento na infraestrutura necessita considerar os prós e os contras para cada nível de RAID a ser aplicado a para cada tipo de dado das aplicações, pois existem diferenças consideráveis quanto ao desempenho de escrita e leitura bem como de valores investidos por *byte* armazenado. No Quadro 2 é apresentado a comparação entre os níveis de RAID e suas características de tolerância a falha de discos e desempenho conforme o autor Schmidt, 2006.

Quadro 2. Comparação entre os níveis de RAID adaptado de TROPPENS *et al.*(2009)

Nível de RAID	Tolerância a falha de discos	Desempenho de leitura	Desempenho de escrita	Espaço Requerido
RAID 0	Não tem	Bom	Muito Bom	n
RAID 1	Alta	Baixo	Bom	n/2
RAID 4	Alta	Bom	Muito Baixo	(n – 1)/n
RAID 5	Alta	Bom	Baixo	(n – 1)/n
RAID 6 (DP)	Muito Alta	Bom	Muito Baixo	(n – 1)/n
RAID 10	Muito Alta	Muito Bom	Bom	n/2

No campo espaço requirido, *n* representa a quantidade de discos em cada unidade lógica (LUN) sendo os RAIDs 4, 5 e 6(DP) mais eficientes que os

RAID 1 e 10 mas o RAID 10 apresenta um melhor desempenho tanto para escrita como para leitura de dados.

Os autores reforçam que trata-se de uma comparação teórica pois os fabricantes de *storages* implementam técnicas complementares nos produtos como aumento do tamanho de memória *cache* nas controladoras, adição de mais controladoras e mais canais de acesso aos discos, virtualização dos níveis de RAID e algorítmos que identificam pré-falhas de discos, entre outras características adicionais que melhoram os desempenhos apresentados no Quadro 2 (TROPPENS *et al.*, 2009).

Atualmente os *storages* também contemplam as funcionalidades de cópias de segurança instantâneas dos volumes lógicos, ou LUNs, denominados *snapshots,* que criam apenas a cópia dos ponteiros onde os dados estão armazenados naquele determinado instante, ou *snapclones,* que consistem de uma cópia completa da estrutura do volume lógico e consequentemente todos os dados armazenados nesse volume. Tais funcionalidades normalmente são adotadas para a execução de rotinas de cópia de segurança dos dados ou também *backups* de forma *online,* sem a necessidade de parada programada das aplicações.

Entretanto, os *storages* tornaram-se centralizados através de redes SAN ou na própria rede LAN via protocolos iSCSI (SNIA, 2012) ou FCoE (SNIA, 2012) e consequentemente um ponto único de falha. Mesmo com as diversas aplicações sendo configuradas em servidores, virtualizados ou físicos em *cluster,* com acessos redundantes ao *storage* armazenando dados em volumes virtuais em RAID, uma falha completa no *storage* indisponibiliza todas as aplicações com dados armazenados nesse *storage*.

Portanto, além das rotinas mandatórias de *backup* dos dados armazenados nos *storages,* para unidades de fita magnética ou outro meio que permita a restauração dos dados em caso de necessidade, surgiu o conceito de replicação dos dados ou *data replication,* conforme mencionado no nível de alta disponibilidade 4 pelos autores Zhu *et al.*, 2009.

A replicação dos dados consiste da duplicidade de *storages* e um aplicativo (*software*) específico, normalmente fornecido pelo próprio fabricante do *storage,* capaz de replicar de forma simultânea os dados armazenados em dois volumes dispostos em dois *storages* fisicamente distintos, aumentando consideravelmente o nível de alta disponibilidade, pelo fato de permitir a parada completa de um dos *storages* enquanto que o outro *storage,* com os dados replicados, permanece operacional (TROPPENS *et al*., 2009).

Esses dois *storages* replicando os dados podem estar fisicamente locados em *data centers* diferentes, instalados em prédios, bairros ou até em cidades distintas, dependendo logicamente de *links* de alta velocidade entre os mesmos.

Estendendo o conceito de replicação de dados entre *data centers* distintos, além dos próprios dados serem replicados, pode-se adicionar nós ou servidores aos *clusters* conectados aos *storages* de ambos *data centers,* elevando a alta disponibilidade dos sistemas ao nível mais alto denominado recuperação de desastres ou *disaster recovery* (MARCUS; STERN, 2003).

O próprio nome desse nível de alta disponibilidade caracteriza que se ocorrer um desastre natural ou provocado pelo homem em um dos locais, como a queda das torres gêmeas no ataque de 11 de setembro de 2001 por exemplo, os sistemas críticos podem ser migrados para o *data center* remanescente com o mínimo de impacto para os usuários.

Normalmente esse *failover* do *site* principal para o *site* réplica não é feito de forma automática e requer intervenção humana da equipe de TI. Portanto, há necessidade de documentação dos procedimentos, testes prévios de validação e equipe capacitada para operacionalizar esse processo. O documento contendo todas estas informações é chamado de Plano de Recuperação de Desastres ou *Disaster Recovery Plan* (DOLEWSKI, 2008).

Concluíndo a descrição das características de alta disponibilidade dos equipamentos *(hardware)*, também é relevante que tais equipamentos contemplem uma automonitoração interna via *firmware* capaz de efetuar um autodiagnóstico e fornecer informações de falhas, ou pré-falhas dos componentes

internos, como também alterações na alimentação elétrica e temperatura interna para uma ferramenta de monitoração e gerenciamento da infraestrutura, permitindo identificar e preventivamente corrigir falhas ou pré-falhas ou alterações do ambiente antes que possam provocar uma parada não programada.

2.4.3. Sistema Operacional (software)

Tomando os sistemas operacionais Microsoft Windows 2008 Server, Red Hat Enterprise Linux 6.3 ou VMware ESX 5.0 como exemplos, verifica-se que os mesmos também podem apresentar erros ou falhas que causem a indisponibilidade do sistema ou da aplicação crítica ao negócio.

O sistema operacional pode ser definido como a parte do *software* que controla e gerencia os recursos de *hardware* do servidor fornecendo uma *interface* abstrata para outros serviços e aplicações serem executados. Inclui também componentes de gestão padronizados e *drivers* providos pelos fornecedores do *hardware* (SCHMIDT, 2006).

Como boas práticas, é recomendado manter os sistemas operacionais e demais componentes que interagem diretamente com o *hardware,* como os *drivers,* atualizados com as versões mais recentes disponibilizadas pelos fabricantes, garantindo que as correções e melhorias conhecidas pelas engenharias desses fabricantes estejam aplicadas, agindo pró-ativamente e evitando a ocorrência de problemas ou *bugs*, falhas de *software,* já conhecidas.

No nível de sistema operacional é possível criar acessos redundantes (*multipath*) e balanceamento de carga (*loadbalancing*) entre as placas de rede NICs ou entre as controladoras de acesso aos storages HBAs. Entretanto, a única forma de evitar que o sistema operacional torne-se um SPOF e cause a parada indesejada do sistema, é aplicando uma camada adicional de *software,* chamada de *cluster,* que torna os sistemas operacionais de servidores físicos ou virtuais redundantes, migrando a aplicação automaticamente entre os servidores via um processo denominado *failover*.

Segundo a SNIA (2012), *cluster* em computação é definido como:

> Um conjunto de computadores que estão interligados (normalmente em altas velocidades) com a finalidade de melhorar a confiabilidade, disponibilidade, facilidade de manutenção, balanceamento de carga e/ou desempenho. Muitas vezes, os computadores em cluster têm acesso a um dispositivo de armazenamento de dados comum e executam um software especial para coordenar as atividades entre esses computadores.
>
> (SNIA, 2012)

Desta forma, um sistema de alta disponibilidade em *cluster* consiste de sistemas operacionais em cada nó ou servidor do *cluster* com um componente de *software* adicional (o *software* de *cluster*), atuando de forma distribuída, compartilhando os recursos de *storage* e redes. Esses nós compartlham o acesso aos mesmos volumes lógicos ou LUNs em um *storage* externo, mas é a camada do *software* de *cluster* que controla esse acesso aos dados evitando corrupções ou inconsistências.

Como exemplos de *software*s de *clusters* de mercado, podemos citar: Oracle RAC - Real Application Clusters, Microsoft Cluster Service, HP MC Service Guard ou IBM Cluster Systems Management for AIX.

2.4.4. Aplicações (software)

Neste contexto, considera-se aplicações todos os demais componentes de *software* além do sistema operacional. Portanto, embora alguns autores façam a distinção entre aplicações comerciais como banco de dados Oracle ou Microsoft SQL, aplicações de ERP como Oracle Applications ou SAP R3, servidores *web* Apache ou servidores de *email* como Microsoft Exchange, aplicações *middleware* e aplicações proprietárias customizados de acordo com a necessidade de negócio de cada organização, neste estudo, aplicação será considerada todos os componentes de *software* além do sistema operacional que possam também gerar paradas não programadas nos sistemas críticos.

Portanto, as mesmas melhores práticas sugeridas a sistemas operacionais no que tange a instalação de atualizações ou correções específicas

também chamadas de *patches* fornecidas periodicamente pelos fornecedores, também aplicam-se a camada de *software* das aplicações.

Contudo, quanto aos incidentes de falhas de *software,* Pertet e Narasimhan (2005) salientam que um número considerável ocorre durante manutenções de rotina, atualizações de versões do *software* ou na integração de sistemas. Tais incidentes sugerem que possam estar relacionadas simplesmente a complexidade dos sistemas ou com testes inadequados ou insatisfatorios ou falha na compreensão das dependências na fase de análise de sistemas. A sobrecarga do sistema, o esgotamento dos recursos ou a inexistência de rotinas de recuperação para falhas complexas também são causas importantes de falha de *software*.

Schmidt (2006) sugere às organizações ter um ambiente de desenvolvimento e testes de qualidade ou também conhecido como Q&A *(Quality and Assurance)* distinto do ambiente de produção buscando testar e identificar as falhas de aplicação ou de novas versões da aplicação antes que ela entre em operação no ambiente produção.

De acordo com Bender e Joshi (2004), os times de desenvolvedores das aplicações, DBAs – *Data Base Administrators* e responsáveis pela administração e operação da infraestrutura de TI, necessitam trabalhar muito próximos em *teamwork* no planejamento e implantação de atualizações de versão das aplicações ou de novas aplicações.

Portanto, contar com profissionais treinados e capacitados no processo de desenvolvimento e implantação dessas aplicações bem como ter processos definidos que garantam a execução exaustiva de baterias de testes de qualidade antes das aplicações ou novas versões dessas aplicações customizadas entrarem em produção na organização é de suma importância para aumentar a estabilidade dos sistemas.

2.4.5. Operações / Fator Humano

Conforme Weygant (2001), a intervenção humana nos sistemas é sempre passível de erros e imprevisível. Portanto, para o autor, uma das abordagens para mitigar falhas humanas ou erros operacionais é automatizar os processos reduzindo a interação humana com os sistemas críticos em alta disponibilidade.

Pertet e Narasimmhan (2005), em sua pesquisa sobre as causas das falhas de aplicações *web*, buscaram classificar os erros de operação em três categorias: erros de configuração, erros processuais e acidentes diversos.

Como erros de configuração podem ser citados: definição incorreta de parâmetros críticos de utilização de recursos do sistema limitando indevidamente a utilização dos mesmos e consequentemente gerando um travamento do sistema crítico ou causar a corrupção dos arquivos de configuração ou retornar os parâmetros para o padrão de fábrica (*default*) durante uma alteração de configuração.

Já os erros processuais, podem ser considerados quando os operadores ou adminstradores dos sistemas se esquecem de executar uma ação crítica como por exemplo executar a rotina diária de *backup*, isto é, a cópia de segurança dos dados de uma base de dados fundamental para um sistema crítico. Também quando deixam de controlar o espaço ocupado em um sistema de arquivos permitindo que o mesmo exceda o espaço disponível e cause a parada do sistema. Falhas durante a execução de um plano de ação em uma manutenção agendada digitando caracteres indevidos em um arquivo de configuração ou se esquecendo de reiniciar o serviço ao término da manutenção são também consideradas falhas operacionais.

Os acidentes diversos causados por falha humana podem ser considerados quando arquivos são apagados indevidamente por descuido do operador ou algum técnico de *hardware* ou eletricista instala um equipamento incorretamente na alimentação elétrica do *data center* causando um desligamento abrupto da alimentação AC parcial ou de todo o *data center*.

Pertet e Narasimmhan (2005) mencionam em seu estudo que os relatórios posteriores ao incidente do eBay de 1999 que causou um prejuízo de milhões de dólares, ocorreu quando um eletricista durante a instalação de um equipamento de monitoração esbarrou acidentalmente em um cabo de força desconectando-o da alimentação elétrica.

Ainda dentro desse contexto, o Instituto Uptime, especialista em certificação de *data centers,* categorizou mais de 5.000 incidentes anormais em ambientes de TI através de pesquisas com empresas e fabricantes da tecnologia apontando que nos últimos anos, parte importante desses incidentes anormais foram causados pela equipe de operação. Segundo o Instituto Uptime, 34% em 2009, 41% em 2010 e 40% em 2011 de tais incidentes nos ambientes de TI foram causados pelas pessoas que operam ou prestam serviços no ambiente de TI. (COMPUTERWORLD, 2012a).

Em resumo, considerando a avaliação dos autores Weygant, 2001, Marcus e Stern 2003, IDC, 2012 e 2011, Bender e Joshi, 2004, Schmidt, 2006 entre outros pesquisados, a principais recomendações visando mitigar as falhas humanas, embora seja sabido que não possam ser totalmente evitadas, são:

a) Maximizar a automatização das atividades como rotinas de *backup*, ferramentas de monitoração, controle de atualizações de *softwares* e *firmwares* e processos de recuperação após uma falha reduzindo a interação da equipe de operação com os sistemas e consequentemente o risco de falha humana;

b) Capacitar e manter a equipe atualizada não apenas sob o aspecto técnico com treinamentos e certificações providos pelos fornecedores da tecnologia mas também nos processos de operação, administração e suporte da infraestrutura;

c) Avaliar os níveis de serviço contratados com os fornecedores da tecnologia buscando serviços diferenciados chamados de serviços de missão crítica que contemplem pró-atividade e equipes dedicadas como uma extensão e suporte à equipe de operações de TI;

d) Orientar a equipe técnica e a própria gestão da TI a processos estruturados e documentados definindo desde o planejamento e implantação de novos projetos, atividades cotiadianos de operação, suporte a incidentes e lições aprendidas até processos de recuperação de desastres e escalação entendendo o que deve ser feito e quem deve ser envolvido dependendo de cada situação e sua criticidade.

O Capítulo III desta dissertação tratará com mais detalhes a questão de orientação a processos estruturados de governança e gestão de TI, os principais guias de melhores práticas como ITIL e COBIT bem como seus benefícios a continuidade dos negócios que dependem dos sistemas críticos em operação na infraestrutura de TI.

CAPÍTULO III – GOVERNANÇA DE TI E GUIAS DE MELHORES PRÁTICAS

Torna-se importante compreender o termo Governança Corporativa antes de atribuir este conceito à área de Tecnologia da Informação.

3.1. Governança Corporativa

A Governança Corporativa trata da gestão de empresas e organizações e sua relação com os acionistas e investidores, bem como com as demais partes interessadas ou *stakeholders*, ou seja, colaboradores, clientes, fornecedores, governo e sociedade.

O conceito de Governança Corporativa começou a ser adotado a partir do ínicio da década de 1990, originando-se com o objetivo de garantir a relação entre os investidores e os gestores de empresas e organizações, isto é, visando a transparência e sincronia das decisões tomadas por quem gere tais organizações (os executivos e quadro diretivo da empresa) com quem investe e apoia essas organizações (os investidores e acionistas que buscam a lucratividade e continuidade dos capitais investidos).

Com os escândalos financeiros de grandes corporações norte-americanas, como a Worldcom e Enron, ocorridos 2002, a Governança Corporativa entrou ainda mais em evidência devido a necessidade de transparência e monitoração da gestão das empresas.

Diante deste contexto, a Lei Sarbanes-Oxley (Sarbanes-Oxley Act), abreviada como SOX, criada em 30 Julho de 2002 nos Estados Unidos visando dar maior transparência à gestão das empresas e restabelecer a confiança dos investidores nos balanços financeiros apresentados pelos gestores. É considerada um marco evolutivo na Governança Corporativa (MASUR, 2009).

No Brasil, o primeiro código de Governança Corporativa foi elaborado pelo IBGC – Instituto Brasileiro de Governança Corporativa em 1999. Segundo este instituto, Governança Corporativa é definida como:

> Governança Corportiva é o sitema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para sua longevidade.
>
> (IBGC, 2012)

Em resumo, a Governança Corporativa não trata apenas da adequação às normas e regulamentações, em prover relatórios financeiros e garantir os direitos dos acionistas minoritários, mas abrange uma visão mais ampla da gestão e da tomada de decisão por investimentos de forma transparente a todas as partes interessadas no processo (STEINBERG *et al.*, 2003).

3.2. Governança de TI

Trazendo o conceito de Governança para a área de TI, percebe-se que a Governança de TI não se resume apenas em implementar guias de melhores práticas de governança e gestão de TI mundialmente conhecidos como ITIL e COBIT que serão apresentados neste estudo, mas uma forma de alinhar a gestão dos recursos e a infraestrutura da área de Tecnologia da Informação com as estratégias e objetivos corporativos.

Os autores Weill e Ross (2004) definem Governança de TI como:

> A especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI.
>
> (WEILL e ROSS, 2004, p.8)

Os principais fatores que motivam a implantação da Governança na área de TI de empresas e organizações, além basicamente da transparência da adminstração, estão dispostos na Figura 8 (FERNANDES; ABREU, 2008).

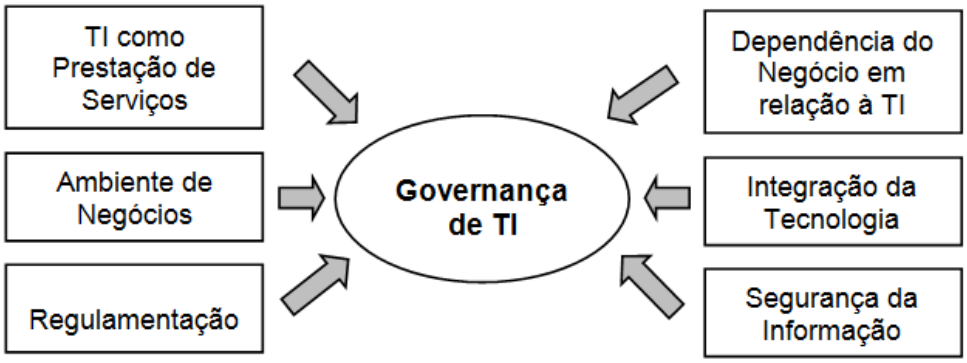

Figura 8. Principais Motivos para Adoção da Governança de TI adaptado de Fernandes e Abreu (2008).

Aprofundando o entendimento de cada um destes principais fatores que motivam a adoção da Governança de TI, os autores detalham que:

a) TI como Prestação de Serviços – adotando uma postura orientada à prestação de serviços entendendo o que os usuários esperam da área de TI, com relação a atender os requisitos do negócio, disponibilidade das aplicações e infraestrutura, capacidade de crescimento do negócio e resolução de incidentes;

b) Ambiente de Negócios – entendimento da agressiva competição com novos concorrentes globais de baixo custo, ciclos de vida de produtos e serviços sendo reduzidos, maior transparência nos negócios, clientes mais exigentes e ameaças macroeconômicas em um mercado globalizado;

c) Regulamentação – estar em concordância com marcos de regulamentação como o Sarbanes-Oxley Act (SOX), para empresas de capital aberto, ou Basiléia II (MASUR, 2009), para bancos e instituições financeiras que exigem controles, gestão de riscos e relatórios financeiros diretamente relacionados com a área de TI, no que tange à disponibilidade e confiabilidade dos dados armazenados e exatidão das informações fornecidas pelas aplicações relacionadas;

d) Dependência do Negócio em Relação à TI – a relação de dependência é diretamente proporcional ao papel da TI no apoio a execução das estratégias corporativas e operações do dia a dia da empresa; quanto maior o impacto de TI nessas atividades, maior será essa dependência;

e) Integração da Tecnologia – com a integração da gestão da organização e processos produtivos com aplicações ERP – *Enterprise Resource Planning*, *softwares* de gestão do relacionamento com clientes, chamados CRM – *Customer Relationship Management,* gestão das cadeias de suprimento e integração das redes de distribuição bem como das aplicações que auxiliam na gestão estratégica e planejamento como BI – *Business Intelligence* ou *Data Warehouse*, demonstram a importância da Tecnologia da Informação para a continuidade dos negócios;

f) Segurança da Informação – proteção dos sistemas e dados corporativos contra invasão e roubo de informações privilegiadas, considerando a interconexão dos sistemas com a Internet, passando não apenas pela adoção de aplicações de segurança, como antivírus e controle de acesso à rede (*firewalls*), mas também da educação de todos os colaboradores quanto a segurança da informação (FERNANDES; ABREU, 2008).

Para Grembergen e Haes (2008), não é tão simples distinguir os conceitos de Governança de TI e Gerenciamento de TI.

Contudo, no entendimento de Weill e Ross (2004), a diferença entre o gerenciamento e a governança é que o gerenciamento está mais relacionado com as tomadas de decisões diárias relacionadas à operação e administração da empresa. Já a governança busca um maior afastamento do dia a dia da organização visando uma abordagem mais ampla sobre quais são as decisões de negócio fundamentais a serem tomadas e quem tem as melhores condições de tomar tais decisões tão importantes.

Dentro deste contexto, governança pode ser definida como a criação de um ambiente onde outros possam gerenciar de forma eficaz, enquanto gerenciamento compreende as tomadas de decisão diárias na operação (SOHAL; FITZPATRICK (2002) *apud* GREMBERGEN; HAES (2008)).

Peterson (2003) *apud* Grembergen e Haes (2008) simplifica o entendimento quanto a diferença entre Governança de TI e Gerenciamento de TI conforme demonstra a Figura 9, descrevendo que a Governança de TI tem um foco no futuro e externo a área de TI, buscando o alinhamento com as estratégias futuras de negócio da organização e clientes, enquanto o Gerenciamento de TI está focado no presente e em gerir as questões internas da área de TI.

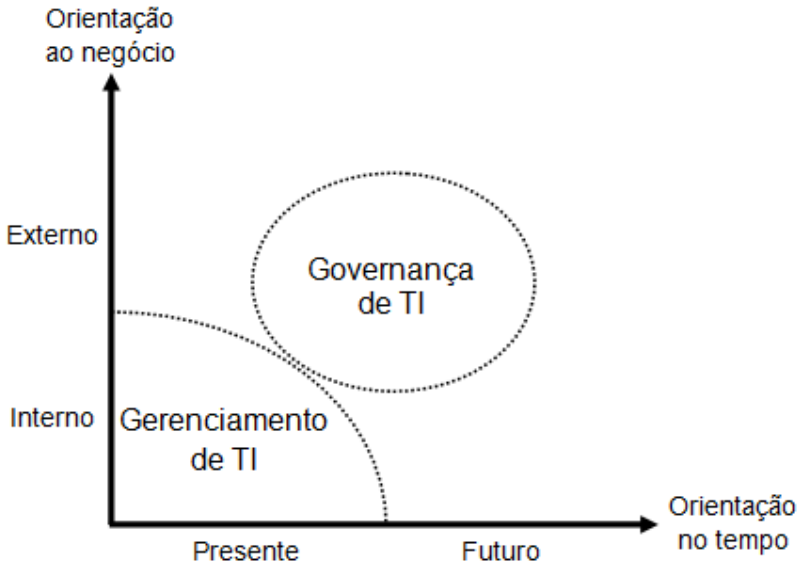

Figura 9. Governança de TI x Gerenciamento de TI adaptado de (PETERSON (2003) *apud* GREMBERGEN; HAES (2008)).

Destaca-se que nas traduções da literatura da Língua Inglesa para a Língua Portuguesa, o termo *management* aparece como gerenciamento, gestão e administração causando dúvidas de interpretação. Neste estudo, os termos gerenciamento de TI e gestão de TI foram considerados como equivalentes para descrever as atividades diárias de monitoramento, controle e tomada de decisão das operações e serviços de TI nos níveis táticos e operacionais das empresas e organizações.

De acorco com Weill e Ross (2004), uma governança eficiente busca tratar basicamente três questões: entender que decisões devem ser tomadas, quem estaria mais preparado para tomá-las e após tomadas, como monitorar seus resultados.

Diante deste prisma, os autores Weill e Ross (2004) citam cinco principais decisões de TI inter-relacionadas e seis modelos ou arquétipos políticos que descrevem dentro da organização, as pessoas que contribuem ou tem o direito a tomada de decisão. Estas cinco decisões de TI são:

a) Princípios de TI, que esclarecem o papel da TI no negócio;

b) Arquitetura de TI, que determina os requisitos de integração e padronização;

c) Infraestrutura de TI, que definem as bases da capacidade da TI e os serviços a serem oferecidos;

d) Necessidade de aplicações de negócio, que definem as aplicações de TI padrão de mercado ou customizadas internamente a serem adotadas de acordo com as necessidades do negócio

e) Investimentos e priorização de TI que basicamente optam por quais serão as iniciativas e projetos na área de TI e quanto será investido.

Ainda segundo os autores, essas cinco principais decisões na área de TI normalmente estão fortemenre interconectadas iniciando-se pelos princípios de TI que determinam a arquitetura que por sua vez, levam à definição da infraestrutura. Com a infraestrutura definida, são desenvolvidas as aplicações de acordo com as necessidades do negócio. A partir desse ponto, ou seja, tendo definidos os princípios, arquitetura, infraestrutura e necessidades de negócio, é que serão priorizados os investimentos de TI (WEILL; ROSS, 2004).

Cada uma dessas cinco áreas de decisão em Tecnologia da Informação possui suas características e questões específicas a serem abordadas requerendo uma ou um grupo de pessoas responsáveis por tomar a decisão ou influenciar na decisão a ser tomada (WEILL; ROSS, 2004).

Segundo Weill e Ross (2004), esses grupos de pessoas responsáveis pela tomada da decisão pela TI de empresas e organizações foram subdivididos em seis modelos ou arquétipos sendo eles: 1. Monarquia de negócios, onde os executivos incluindo os executivos seniors tomam a decisão; 2. Monarquia de TI, onde o executivo da TI (CIO) e os profissionais da área de TI são os responsáveis pela tomada de decisão; 3. Feudalismo, que considera que as tomadas de decisão ocorrem pelos líderes das unidades de negócio; 4. Federalismo, que reune os executivos das áreas de negócio e os executivos da área de TI na tomada de decisão conjunta; 5. Duopólio de TI, quando os executivos da área de TI unem-se aos líderes de processos ou a executivos das áreas de negócio para a tomada de decisão em um consenso bilateral, e por fim, como sexto arquétipo, a Anarquia, onde cada usuário toma a decisão individualmente sendo considerado o pior cenário.

Com base em pesquisas de mercado no cenário brasileiro, Masur (2009) propõe a alteração da nomenclatura dos arquétipos anteriormente definidos por Weill e Ross (2004) para melhor se adequar ao mercado local, estabelecendo: 1. Orientada ao Negócio, em vez de Monarquia de Negócios pois há um maior envolvimento da TI da tomada de decisão; 2. Orientada a TI, contra a Monarquia de TI, pois no mercado local também há um maior envolvimento dos demais executivos da empresa na tomada de decisões da TI; Feudalismo, Federalismo e Duopólio permanecem inalteradas e a substituição da Anarquia pela Orientada ao Usuário, levando em consideração principalmente os aspectos do usuário e perdendo um pouco da padronização e integração mas não sendo uma anarquia propriamente dita.

Para Fernandes e Abreu (2008), a Governança de TI objetiva compartilhar as decisões da área de TI com os demais gestores da organização definindo as regras e processos do uso da tecnologia pelos usuários internos, departamentos, clientes e fornecedores estabelecendo como os serviços de tecnologia da informação serão providos.

Portanto, ainda dentro do entendimento dos autores Fernandes e Abreu (2008), o escopo da Governança de TI necessita:

a) Garantir que a área de TI esteja alinhada ao negócio, ou seja, aos objetivos estratégicos da organização;

b) Garantir que a área de TI esteja em conformidade com as atuais regulamentações externas como Sarbanes-Oxley (SOX) para empresas que negociam na bolsa de valores norte-americana ou Basiléia II para instituições financeiras entre outras regulamentações e normas vigentes;

c) Garantir a continuidade do negócio evitando falhas e paradas não programadas nos serviços providos pela área de TI, ou seja, evitar interrupções em aplicações e sistemas críticos ao negócio.

Este último requisito da Governança de TI, ou seja, a continuidade do negócio de empresas e organizações através da disponibilidade de aplicações e sistemas críticos, é avaliado neste estudo.

A partir da década de 80, surgiram guias de melhores práticas de TI visando apoiar a gestão, estruturação de processos de operação, medição e controle (MANSUR, 2009; FERNANDES; ABREU, 2008).

Como exemplos de guias de melhores práticas relacionados a Governança e Gerenciamento de TI, podem ser citados: *Control Objectives for Information and related Technology* (COBIT) (ISACA, 2012a), *Information Technology Infrastructure Library* (ITIL) (APMG, 2012a), IT Value Delivery (Val IT) (ISACA, 2012b), *Balanced Scorecard* (BSC) (BALANCED SCORECARD INSTITUTE, 2012) e *The Open Group Architecture Framework* (TOGAF) (OPEN GROUP, 2012) entre outros.

Em adição a estes guias de melhores práticas voltados a Governança de TI e Gerenciamento de TI, também podem ser mencionados os guias de melhores práticas focados no gerenciamento de projetos como *Project management Body of Knowledge* (PMBOK) (PMI, 2012) ou *Projetc in Controlled Environments* (PRINCE2) (APMG, 2012).

Conforme estudo realizado por Masur (2009) e também descrito por Assis (2011), O ITIL e o COBIT são guias de melhores práticas ou *frameworks* complementares. O ITIL tem um maior foco nos processos de gerenciamento de serviços, ou seja, em como executar os serviços da TI, enquanto o COBIT tem como fortalezas, os controles, as métricas e a segurança da informação.

Considerando os resultados da pesquisa aplicada com os executivos de TI das cem maiores empresas do Brasil, publicado em 2009, demonstrando ITIL e COBIT como preferência no mercado brasileiro (RODRIGUES *et al.*, 2009), esta revisão da literatura aprofunda o detalhamento desses dois guias de melhores práticas avaliando sua relação com a disponibilidade dos sistemas e a continuidade dos negócios.

3.3. Guias de Melhores Práticas de TI - COBIT 4.1

3.3.1. A Evolução do COBIT

O *Control Objectives for information and related Technology* ou simplesmente COBIT, na sua primeira versão, desenvolvida pelo *Information System Audit and Control Foundation* (ISACF), uma fundação ligada ao *Information Systems Audit and Control Association* (ISACA) nos Estados Unidos, teve foco nos objetivos de controle e foi lançado em 1994 (FERNANDES; ABREU, 2008).

Já em 1998 foi disponibilizado COBIT 2ªedição, tendo a revisão e maior detalhamentos dos objetivos de controle, porém, ainda, com maior foco na auditoria e controleTI.

Em 2000, a 3ª edição do COBIT foi publicada pelo *IT Governance Institute* (ITGI), uma extensão do ISACA criado com o objetivo de dissiminar a adoção dos objetivos de Governança de TI. Nessa versão, além dos objetivos de controle, foram também adicionados orientações da gestão de TI.

A evolução desse modelo de melhores práticas ou *framework*, se deu com o lançamento da versão COBIT 4.0 em 2005 como foco maior na Governança de TI alinhando as práticas e processos com outros guias de melhores práticas, como o ITIL. O COBIT 4.0 também adicionou a conformidade com regulamentações como o SOX e Basiléia II e aumentou a abrangência do público alvo incluindo gestores, técnicos, especialistas e auditores de TI (FERNANDES; ABREU, 2008).

O COBIT 4.1, lançado em 2007, buscou amadurecer os objetivos de controle, revendo suas definições como diretrizes de práticas de gestão e melhorando também os processos de verificação e divulgação dos resultados. O COBIT 4.1 manteve-se como versão recomendada e em uso até meados de 2012, quando a versão COBIT 5 foi disponibilizada, consolidando e atualizando os *framewoks* COBIT 4.1, Val IT e Risk IT em um único guia de melhores práticas. Porém, como o lançamento do COBIT 5 ainda é muito recente, a literatura revisada neste trabalho mantém-se focada na versão 4.1, foi adicionado apenas um item deste capítulo com a principais diferenças do COBIT 5 em relação ao COBIT 4.1, com base nas informações disponibilizadas pelo ISACA.

3.3.2. Os Princípios Básicos e Objetivos do COBIT 4.1

Segundo o ITGI (2007), a Governança de TI está sustentada basicamente em cinco pilares:

a) Alinhamento Estratégico: assegura a conexão entre os planos de negócio e da TI, alinhando as operações de TI com as operações da organização e definindo e mantendo o valor da TI;

b) Entrega de Valor: garantir que os benefícios prometidos pela área de TI sejam entregues à organização, otimizando custos e demonstrando o valor da TI inerente ao negócio;

c) Gestão de Recursos: otimização dos investimentos e gestão dos quatro recursos críticos de TI (aplicativos, informações, infraestrutura e pessoas);

d) Gestão de Risco: entendimento dos riscos pelo nível executivo, transparência sobre os riscos identificados e introdução do gerenciamento de riscos na organização;

e) Mensuração de Desempenho: por meio do acompanhamento e monitoramento da estratégia, execução de projetos, uso de recursos, desempenho e entrega dos serviços através de *balanced scorecards* para traduzir a estratégia em ações objetivas capazes de serem medidas.

O COBIT 4.1 foi desenvolvido tendo como objetivos o foco nos negócios e a orientação a processos baseando-se em controles e medições. Portanto, como o principal tema do COBIT é a necessidade do negócio, possibilita sua utilização por executivos e responsáveis pelos processos de negócio e não apenas pelos prestadores de serviço de TI e auditores (ITGI, 2007).

O COBIT 4.1 está baseado nos seguintes princípios (ITGI, 2007):

> Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.
>
> (ITGI, 2007)

A Figura 10 demonstra esses quatro princípios do COBIT definidos pelo ITGI e suas inter-relações com foco no negócio da empresa ou organização, onde os requisitos de negócio direcionam os investimentos em recursos de TI que, por sua vez, são utilizados pelos processos de TI que fornecem as informações organizacionais para atender os requisitos de negócio, concluíndo o ciclo.

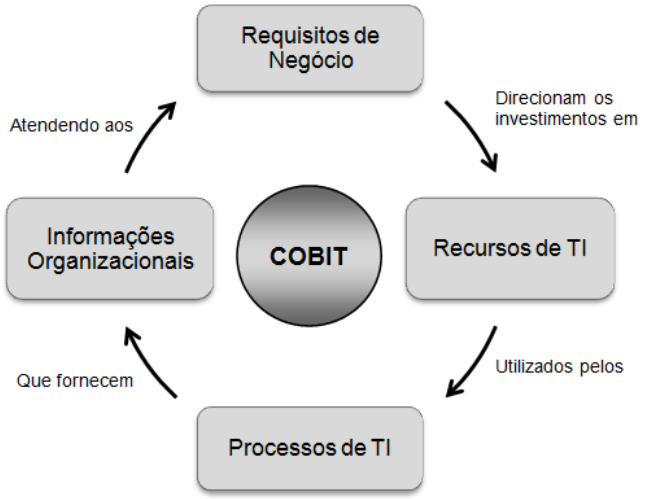

Figura 10. Princípio Básico do COBIT adaptado do ITGI (2007)

Como o principal objetivo do COBIT é atender as necessidades de negócio, as informações providas devem estabelecer alguns importantes critérios de controle, sendo eles: Efetividade, Eficiência, Confidencialidade, Integridade, Disponibilidade, Conformidade e Confiabilidade.

Tais informações são fornecidas por meio de processos de TI que por sua vez utilizam os recursos de TI. Esses recursos de TI, segundo o COBIT (ITGI, 2007), são divididos em:

a) Pessoas: requerem capacitação e conhecimento para desempenhar suas funções;

b) Infraestrutura: equipamentos (*hardware*), infraestrutura de redes, sistemas operacionais e bancos de dados para executarem as aplicações;

c) Aplicações: processam os dados e fornecem as informações ao negócio.

Desta forma, os investimentos são direcionados para que os recursos de TI (pessoas, infraestrutura e aplicações) tenham a capacidade técnica de suportar as demandas do negócio.

3.3.3. A Estrutura do COBIT 4.1

O COBIT 4.1 é composto de 34 processos de TI distribuídos em quatro domínios, utilizando o tradicional ciclo de melhoria contínua composto de: planejar, executar, monitorar e atuar (FERNANDES; ABREU, 2008).

Esses quatro domínios do COBIT estão divididos como: Planejamento e Organização (PO), Aquisição e Implementação (AI), Entrega e Suporte ou *Delivery and Support* (DS) e Monitoração e Avaliação ou *Monitor and Evaluate* (ME), tendo cada um desses quatro domínios seus respectivos processos associados.

Os autores Fernandes e Abreu (2008) adaptaram em uma tabela, com dados do próprio ITGI (2007), a relação das principais questões gerenciais e como são tratadas nos 34 processos de TI do COBIT. Adaptando tal relação apenas com o foco na escolha da tecnologia da infraestrutura, relacionamento com fornecedores, gestão das pessoas e infraestrutura bem como da disponibilidade dos sistemas que contribuem para a continuidade dos negócios, temos a redução para algumas questões gerenciais importantes e processos associados conforme apresentado na Quadro 3.

Quadro 3. Relação de Questões Gerenciais e Processos de TI do COBIT associados a disponibilidade dos sistemas adaptado de Fernandes e Abreu (2008)

Domínio	Questões Gerenciais	Processos de TI
PO	Os riscos da área de TI estão entendidos e sendo gerenciados? A qualidade dos sistemas de TI se adequa as necessidades do negócio?	PO-3 → Determinar a direção tecnológica; PO-5 → Gerenciar o investimento em TI; PO-7 → Gerenciar os recursos humanos; PO-8 → Gerenciar a qualidade; PO-9 → Avaliar e gerenciar riscos de TI.
AI	Os novos sistemas funcionam corretamente após implementados? A condução das mudanças realizadas gera baixos impactos nas operações de negócio em execução?	AI-1 → Identificar soluções automatizadas; AI-3 → Adquirir e manter a infraestrutura tecnológica; AI-6 → Gerenciar mudanças; AI-7 → Instalar e aprovar soluções e mudanças;

Quadro 3. Relação de Questões Gerenciais e Processos de TI do COBIT associados a disponibilidade dos sistemas adaptado de Fernandes e Abreu (2008) (continuação)

Domínio	Questões Gerenciais	Processos de TI
DS	Os serviços de TI são entregues de acorco com as prioridades de negócio? As equipes de trabalho são capazes de operar os sistemas de TI com segurança e produtividade? Características como confidencialidade, integridade e disponibilidade estão implementados adequadamente?	DS-1 → Definir e gerenciar níveis de serviço; DS-2 → Gerenciar serviços terceirizados; DS-3 → Gerenciar o desempenho e capacidade; DS-4 → **Garantir a continuidade dos serviços**; DS-7 → Educar e treinar usuários; DS-8 → Gerenciar central de serviços e incidentes; DS-10 → Gerenciar problemas; DS-12 → Gerenciar o ambiente físico;
ME	As medições de desempenho da TI são capazes de detectar preventimente os problemas antes que aconteçam? Exitem controles de integridade, disponibilidade e confiabilidade para assegurar segurança da informação?	ME-1 → Monitorar e avaliar o desempenho da TI

Em resumo, o Quadro 3 demonstra a preocupação do *framework* COBIT 4.1 com a gestão dos recursos de TI, visando a disponibilidade dos serviços e aplicações atendendo aos requisitos de negócio, bem como a adoção de tais melhores práticas pode auxiliar as empresas e organizações na continuidade de seus negócios dependentes da Tecnologia da Informação.

Um dos pontos fortes do COBIT está no controle e medição dos processos pois implementa modelos de maturidade para avaliar os processos de TI existentes, conceituando-os nos seguintes níveis: nível 0 (processo inexistente), nível 1 (inicial), nível 2 (repetitivo mas dependente das pessoas), nível 3 (definido e documentado), nível 4 (gerenciado e mensurável) e nível 5 (otimizado e automatizado) (FERNANDES; ABREU, 2008).

3.3.4. Os Benefícios da Adoção do COBIT

Conforme citado pelo próprio ITGI (2007), a adoção e implementação do COBIT como modelo Governança de TI proporciona os seguintes benefícios:

a) Melhor alinhamento da organização com base nas necessidades do negócio;

b) Possibilita uma visão mais apurada do nível executivo em relação as atividades que TI desempenha;

c) Atribuição e clareza das responsabilidades com base em uma orientação a processos;

d) É um modelo difundido e aceito pelo mercado e por órgãos regulamentadores;

e) Facilidade de entendimento e compreensão por todas as partes interessadas por apresentar uma linguagem comum.

Os autores Fernandes e Abreu (2008), complementam os benefícios do COBIT como:

a) Redução dos custos operacionais e de propriedade da infraestrutura de TI;

b) Identificação dos pontos de vulnerabilidades dos atuais processos de TI;

c) Diminuição dos riscos de negócio se forem adotadas as melhorias identificadas nos processos;

Em suma, a implementação do COBIT, como uma guia de melhores práticas de Governança de TI, pode proporcionar a empresas e organizações melhores serviços recebidos e bases sólidas para um melhor retorno dos investimentos de TI.

3.3.5. As diferenças entre COBIT 4.1 e o novo COBIT 5

A recente atualização do COBIT 5 disponibilizada em meados de 2012 pelo ISACA, busca apresentar um modelo de referência revisado com uma nova

abordagem de Governança de TI, atualizando e adicionando processos com o objetivo de atender as atividades fim a fim de empresas e organizações, desde as áreas de negócio até as áreas funcionais da TI. O COBIT 5 consolida o COBIT 4.1, Val IT e Risk IT em um único guia de melhores práticas, ou *framework,* estando atualizado e alinhado a outros guias de melhores práticas como o ITIL V3 2011 e TOGAF (ISACA, 2012a).

COBIT 5, em comparação com a versão COBIT 4.1, apresenta um quadro de responsabilidades e funções mais bem detalhado e completo para cada prática gerenciada, possibilitando uma melhor definição de funções, responsabilidades e níveis de envolvimento no desenvolvimento e implementação de processos (ISACA, 2012a).

O COBIT 5 implementa também um novo conceito de gerenciamento das expectativas das partes interessadas, ou seja, as pessoas e entidades envolvidas com a organização, buscando o alinhamento dessas expectativas com as estratégias da empresa ou organização.

Conforme mencionado pelo ISACA, diversos processos foram revisados e alguns adicionados no COBIT 5 atendendo a nova abordagem, sendo eles:

- APO03 *Manage enterprise architecture;*
- APO04 *Manage innovation;*
- APO05 *Manage portfolio;*
- APO06 *Manage budget and costs;*
- APO08 *Manage relationships;*
- APO13 *Manage security;*
- BAI05 *Manage organizational change enablement;*
- BAI08 *Manage knowledge;*
- BAI09 *Manage assets;*
- DSS05 *Manage security service;*
- DSS06 *Manage business process controls.*

3.4. Guias de Melhores Práticas de TI – ITIL v3

3.4.1. A Evolução do ITIL

O *Information Technology Infrastructure Library* (ITIL) foi desenvolvido no final da década de 80, a partir de uma solicitação do governo britânico por um guia de melhores práticas de gerenciamento da TI que pudesse ser utilizado independentemente de fornecedor, devido a estarem insatisfeitos com serviços de TI recebidos (FERNANDES; ABREU, 2008).

A atualização do ITIL, chamado ITIL v2, foi disponibilizada em 2000, baseando-se em sete livros: Perspectiva de Negócio, Entrega de Serviços, Suporte a Serviços, Gerenciamento da Segurança, Gerenciamento da Infraestrutura, Gerenciamento de Aplicações e Planejamento da Implementação do Gerenciamento de Serviços. A versão ITIL v2 vislumbrava a melhora na qualidade dos serviços prestados pela área de TI, através da orientação dos processos com redução de tempo e distribuição dos serviços, bem como na redução da indisponibilidade dos serviços (RODRIGUES, 2006).

A versão mais recente chamado ITIL v3 foi apresentada em 2007 pelo Office of Government Commerce (OGC) da Inglaterra. É considerada uma grande evolução em relação a versão anterior, pois estruturou os processos de gerenciamento dos serviços de TI com base no ciclo de vida do serviço integrando a TI ao negócio. (FERNANDES; ABREU, 2008).

3.4.2. Os Objetivos do ITIL v3

O ITIL v3 tem por objetivo principal propor um conjunto de melhores práticas de gerenciamento de serviços de TI através da abordagem do ciclo de vida do serviço, ou seja, da perspectiva da gestão dos serviços pelos próprios serviços em vez de cada processo (CARTLIDGE *et al.*, 2007).

Para Fernandes e Abreu (2008), o ITIL tem como principal objetivo ser guia de melhores práticas de gerenciamento de TI, contendo um conjunto de práticas de gerenciamento de TI já testadas e comprovadas seguindo o ciclo de vida do serviço e aprimoramento contínuo, a ser adotado por empresas e organizações independentemente de tamanho como forma de buscar a eficência e qualidade do uso dos recursos de TI alinhados às necessidades do negócio.

3.4.3. A Estrutura do ITIL v3

O chamado núcleo do ITIL na versão 3, é composto por cinco livros aplicáveis a qualquer organização de serviços como guia de melhores práticas. Estes livros são: Estratégia de Serviço, Desenho do Serviço, Transição do Serviço, Operação de Serviço e Melhoria de Continuada (KNELLER, 2010).

Além destes cinco livros que compõem o núcleo do ITIL v3, existe um conjunto de publicações complementares para determinados setores empresariais denominados Orientação Complementar à ITIL (MASUR, 2009).

A seguir, tem-se a descrição de cada um dos cinco livros que compõem o núcleo do ITIL v3 de acordo com os autores (CARTLIDGE *et al.*, 2007, FERNANDES; ABREU, 2008, KNELLER, 2010 e OGC, 2010):

a) Estratégia de Serviço: busca o alinhamento estratégico entre o negócio e a TI para desenvolver uma estratégia de serviço de como as políticas e processos de gerenciamento de serviços podem ser planejados, desenvolvidos e implementados para atender as necessidades de negócio da organização;

b) Desenho do Serviço: projeta a arquitetura de TI e cada tipo de serviço de TI necessário visando atender os objetivos de negócio da organização ou clientes, quando se trata de um empresa especialista que apenas fornece os serviços de TI, detalhando características fundamentais como: capacidade, disponibilidade, continuidade, segurança da informação e níveis de serviços (SLAs);

c) Transição do Serviço: gestão e controle de mudanças dos serviços no ambiente de TI, sendo responsável pelo planejamento e implantação de alterações ou novos serviços; desta forma, o gerenciamento de mudanças, da configuração, dos ativos de TI, de testes e validação do serviço de TI e a gerência do conhecimento, estão inclusas nesta publicação;

d) Operação de Serviço: trata da entrega e suporte operacional dos serviços de TI, ou seja, das atividades diárias do gerenciamento dos serviços, detalhando o tratamento de eventos, incidentes, problemas e implantação das requisições de mudanças e melhorias;

e) Melhoria de Serviço Continuada: orienta por meio de métodos de gerenciamento da qualidade visando medir e melhorar a entrega dos serviços de TI, aprendendo através da experiência em um ciclo de melhoria contínua com base no modelo PDCA (Planejar, Executar, Verificar e Atuar corretivamente ou do original em inglês *plan, do, check and action*) (CAMPOS, 1992).

Estes cinco livros que compõe as bases do guia de melhores práticas de Gerenciamento de TI ITIL v3 estão inter-relacionados possibilitando auxiliar desde o alinhamento das necessidades de negócio, definição dos serviços a serem prestados por TI até os processos de colocação dos mesmos em operação e seu monitoramento e avaliação de desempenho.

A Figura 11 ilustra as cinco publicações que compõe o núcleo do ITIL v3, exemplificando o conceito do ciclo de vida do serviço; ou seja, a Estratégia do Serviço define o serviço, alinhando-o com a necessidade de negócio; no Desenho do Serviço o serviço é desenvolvido e especificado; na Transição do Serviço o serviço é testado e validado solicitando a mudança para entrar em operação; na Operação do Serviço o serviço entra propriamente em uso, sendo gerenciado e monitorado buscando a melhoria contínua na Melhoria de Serviço Continuada.

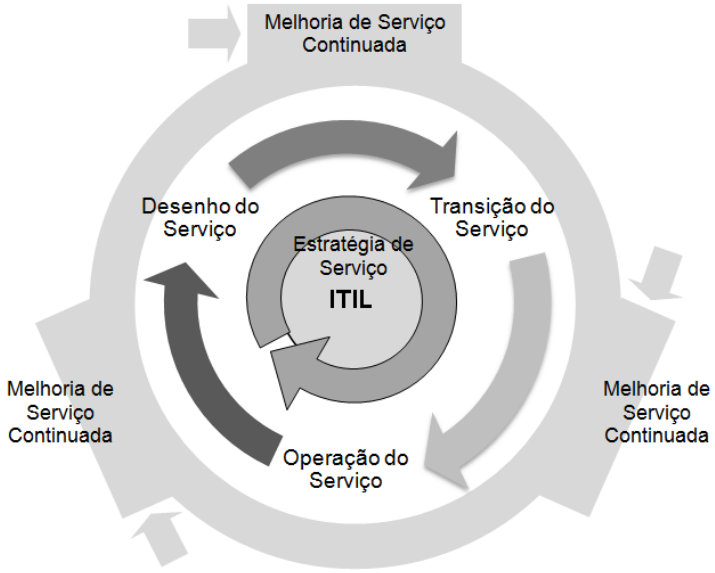

Figura 11. Núcleo do ITIL v3 adaptado de APMG (2012)

Segundo Cartlidge *et al.* (2007) em uma publicação do *The IT Service Management Forum* (ITSM), referente ao ITIL v3, recomenda uma abordagem holística no estágio do Desenho do Serviço, visando garantir a qualidade, consistência e integração de todas as atividades e processos de TI com o negócio. Portanto, um bom projeto de serviço, seguindo essa ótica, depende de identificar e utilizar de forma eficiente e eficaz os quatro P's relacionados à prestação de serviços de TI, ou seja: produtos, pessoas, processos e parceiros.

Os produtos referem-se aos equipamentos, infraestrutura, aplicações e *softwares* necessários para a operação da TI. Os processos norteam as funções e atividades na prestação de serviços de TI buscando padronização, qualidade e métricas de desempenho. As pessoas devem possuir competências e as habilidades para possibilitar serviços de TI prestados com eficiência e qualidade no tempo de resposta adequado. Já os parceiros representam os terceiros, ou seja, os fabricantes e fornecedores utilizados para auxiliar e apoiar a entrega dos serviços de TI (CARTLIDGE *et al.*, 2007).

O Quadro 4 apresenta as cinco publicações que compõem o núcleo do ITIL v3 e seus 23 processos e as quatro funções associados (FERNANDES; ABREU, 2008; APMG, 2012a).

Quadro 4. Divisão dos Processos ITIL v3 adaptado de Fernandes e Abreu (2008)

Núcleo do ITIL v3 Publicações	Processos	Funções
Estratégia do Serviço	Gerenciamento Financeiro de TI Gerenciamento do *Portfolio* de Serviços Gerenciamento da Demanda	
Desenho do Serviço	Gerenciamento do Catálogo de Serviços Gerenciamento do Nível de Serviço Gerenciamento da Capacidade **Gerenciamento da Disponibilidade** **Gerenciamento da Continuidade do Serviço** Gerenciamento da Segurança da Informação Gerenciamento do Fornecedor	
Transição de Serviço	Gerenciamento da Mudança Gerenciamento da Configuração e de Ativo de Serviço Gerenciamento da Liberação e Implantação Validação e Teste de Serviço Avaliação Gerenciamento do Conhecimento	
Operação de Serviço	Gerenciamento do Evento Gerenciamento do Incidente Gerenciamento de Problema Gerenciamento de Requisição Gerenciamento de Acesso	Central de Serviço Gerenciamento das Operações de TI Gerenciamento Técnico Gerenciamento de Aplicativo
Melhoria de Serviço Continuada	Medição de Serviço Relatório de Serviço	

Semelhante à análise realizada com os processos do COBIT 4.1, este estudo também efetua uma análise dos processos dispostos no ITIL v3, identificando e focando nos processos relacionados com a escolha da tecnologia da infraestrutura, relação com os fornecedores, gestão das pessoas e infraestrutura, bem como da disponibilidade dos sistemas que consequentemente contribuem para a continuidade dos negócios, buscando evitar paradas não programadas nos sistemas críticos.

O Gerenciamento da Disponibilidade no estágio de Desenho de Serviço busca assegurar que os serviços de TI sejam planejados e desenvolvidos

com os niveis de disponibilidade e confiabilidade exigidos pelo negócio, reduzindo riscos de paradas por meio de monitoração, solução rápida de incidentes e melhoria contínua a equipe e infraestrutura de TI (FERNANDES; ABREU, 2008).

Ainda sobre o Gerenciamento da Disponibilidade, Cartlidge *et al.* (2007) reforça:

> Gerenciamento de Disponibilidade deve ocorrer em dois níveis inter-relacionados que visam otimizar continuamente e de forma pró-ativa melhorar a disponibilidade do serviços de TI e sua organização de suporte. Existem dois aspectos fundamentais:
> - atividades reativas: monitoramento, medição, análise e gestão de eventos, incidentes e problemas envolvendo indisponibilidade do serviço;
> - atividades pró-ativas: planejamento e desenvolvimento pró-ativo, recomendações e melhorias da disponibilidade.
>
> (CARTLIDGE *et al.*, 2007)

Portanto, o Gerenciamento de Disponibilidade como parte de suas atividades, necessita considerar as características de confiabilidade, disponibilidade e facilidade de manutenção não apenas do serviço em si mas de seus demais componentes incluindo a infraestrutura de TI e aplicações (CARTLIDGE *et al.*, 2007; ADDY, 2007).

O Gerenciamento da Continuidade do Serviço de TI é outro processo diretamente relacionado à continuidade dos serviços de TI, buscando assegurar que os serviços de TI que envolvem infraestrutura, redes, sistemas e aplicações sejam restabelecidos dentro dos prazos preestabelecidos por SLAs.

De acordo com Cartlidge *et at* (2007), a Tecnologia da Informação é um componente crucial na maioria dos processos de negócio e alta disponibilidade dos sistemas críticos, alcançada através da redução de riscos, e medidas de rápida recuperação são essencias para a continuidade dos negócios.

O Gerenciamento da Segurança da Informação alinha a segurança da TI com a segurança do negócio através de procedimentos, documentação e infraestrutura de TI, buscando a confidencialidade, integridade e disponibilidade dos dados. (FERNANDES; ABREU, 2008).

Os autores Cartlidge *et at* (2007), complementam que confidencialidade significa que uma informação é acessada ou divulgada apenas para aqueles que tem o direito de ter conhecer seu conteúdo. A disponibilidade dos dados caracteriza-se pela informação estar acessível sempre que necessário. A integridade dos dados considera que os mesmos estejam precisos, completos e protegidos contra modificações. Também consideram um fator adicional relacionado à verificação da autenticidade na troca das informações e transações comerciais.

Portanto, além dos processos relacionados a gerência da disponibilidade, continuidade de serviço e segurança da informação contidos na publicação do Desenho de Serviço do ITIL v3, outros cinco processos (um ainda no Desenho de Serviço e os outros quatro na Operação de Serviço) podem também ser mencionados como importantes na busca da alta disponibilidade dos sistemas críticos; são eles:

a) Gerenciamento de Fornecedor (Desenho de Serviço): trata do gerenciamento dos serviços e contratos de suporte prestados pelos fornecedores, incluindo os fabricantes de *hardware* e *software* da infraestrutura de TI;

b) Gerenciamento de Evento (Operação de Serviço): mantém a monitoração dos eventos, buscando validar constantemente a operacionalidade da infraestrutura de TI tendo um processo de escalonamento pré-definido para resolução de condições de exceção (incidentes, problemas e mudanças);

c) Gerenciamento de Incidente (Operação de Serviço): tem como principal objetivo restaurar o serviço de TI o mais rápido possível, assegurando os níveis de disponibilidades acordados em SLA e minimizando o impacto ao negócio; porém trata apenas o efeito e não a causa;

d) Gerenciamento de Problema (Operação de Serviço): busca endereçar os incidentes e problemas relacionados a falhas de infraestrutura, bem como evitar a reincidência dos mesmos, reduzindo os impactos ao

negócio, agindo tanto pró-ativamente na identificação e endereçamento de problemas conhecidos e documentados como reativamente, resolvendo problemas e incidentes que já ocorreram e estão impactando as operações de TI (FERNANDES; ABREU, 2008; MASUR, 2009).

Além dos processos, o ITIL v3 define quatro funções na Operação de Serviço. A função, segundo a definição do ITIL, refere-se a pessoas ou alguma forma automatizada que executa determinado processo, atividade ou a comunicação entre processos e atividades (OGC, 2010).

Segue a descrição das quatro funções na Operação de Serviço segundo os autores (CARTLIDGE *et at,* 2007 e FERNANDES; ABREU, 2008):

a) Central de Serviço ou *Service Desk*: fornece o ponto central de contato para atendimento das necessidades dos usuários pela TI. A sua função é receber, registrar e gerenciar todos os incidentes e requisições, fazendo a interface entre os usuários e as demais funções e processos da Operação de Serviço;

b) Gerenciamento Técnico: relacionado às áreas e equipes de especialistas que detém a experiência e conhecimento técnico para prestar suporte à operação, sendo também responsável em assegurar a capacitação técnica dos recursos para a definição, planejamento e melhoria da tecnologia da informação utilizada;

c) Gerenciamento das Operações de TI: trata das áreas e equipes que mantém as operações e serviços de TI do dia a dia (também chamadas na literatura técnica de *ongoing*);

d) Gerenciamento de Aplicativo: relacionado às equipes que gerenciam as aplicações ao longo de seu ciclo de vida, ou seja, desde a definição, levantamento de requisitos, desenvolvimento, testes de validação, implantação, operação e suporte bem como as possíveis melhorias aplicadas ao longo do ciclo de vida.

A Melhoria de Serviço Continuada, apresentada pelo ITIL v3, busca assegurar que os serviços de TI estarão sendo continuamente avaliados e melhorados com o objetivo de manterem-se alinhados com o negócio ao longo do tempo. Com base em pesquisas de satisfação dos usuários, métricas de cumprimento de SLAs e de tendências, é possível aplicar as ferramentas de qualidade, também utilizadas em outros *frameworks* como COBIT, PMBOK e PRINCE2, visando identificar as oportunidades de melhoria e lições aprendidas ao longo o ciclo de vida dos serviços.

Portanto, a Melhoria de Serviço Continuada contida neste guia de melhores práticas pode contribuir para identificar e reduzir quantidade de falhas ou avaliar o valor da TI através de conceitos como o retorno sobre investimento (ROI) (FERNANDES; ABREU, 2008).

3.4.4. Os Benefícios da Adoção do ITIL v3

Segundo Masur (2009), a adoção do ITIL por empresas e organizações, com base em resultados de pesquisas em âmbito internacional publicadas pelo ITSM forum em 2005, apresenta resultados extremamente benéficos para a disponibilidade dos sistemas e continuidade dos negócios, entre eles: diminuição das falhas operacionais em 35%, significativa redução do tempo de reparo em 70%, diagnóstico 50% mais rápido e aumento da disponibilidade do ambiente de TI em 10%.

Complementando esses resultados, de acordo com Fernandes e Abreu (2008), por meio de pesquisas realizadas pela experiente empresa de consultoria em ITIL denominada *Pink Elephant* publicadas em 2006 (PINK ELEPHANT, 2012), a adoção do ITIL possibilitou a empresas e organizações reduções acima de 40% na indisponibilidade de sistemas.

Fernandes e Abreu (2008) salientam que o ITIL também pode trazer resultados positivos qualitativos como: otimização dos recursos de TI; melhoria da satisfação dos usuários da TI; redução dos custos referentes a incidentes e

problemas por pró-ativamente evitar a ocorrência de problemas conhecidos e aumento da disponibilidade de sistemas e aplicações, entre outros benefícios.

Esse guia de melhores práticas para o gerenciamento de TI tem sido adotado por milhares de empresas e organizações ao redor do mundo, podendo-se citar exemplos de grandes corporações como: Bank of America, Boieng, Citi, Disney, IBM, HP, Microsoft, Pfzier, Sony, Toyota e Wallmart que já adotaram o ITIL (OGC, 2010).

CAPÍTULO IV – O ESTADO DA ARTE EM ALTA DISPONIBILIDADE PARA SISTEMAS CRÍTICOS AO NEGÓCIO

Este capítulo descreve o estado de arte em termos de sistemas críticos de alta disponibilidade com base na revisão da literatura sobre as atuais tecnologias de alta disponibilidade para sistemas computacionais, governança de TI e em como os guias de melhores práticas de Governança e Gestão de TI podem contribuir para que os sistemas críticos ao negócio alcancem essa alta disponibilidade e se mantenham operacionais, gerando o mínimo de interrupções toleráveis ao negócio de empresas e organizações.

4.1. *Data Center*

Quanto ao *data center,* o estado da arte aponta para um *data center* com certificação *Tier IV* segundo a norma ANSI/TIA-942, visando ser totalmente tolerante a falhas de energia entre outras características importantes descritas na norma. Contudo, esse nível de certificação não é viável no país (COMPUTERWORLD, 2012b). Essa situação ocorre em virtude da norma exigir que o *data center* seja alimentado por no mínimo dois circuitos elétricos distintos oriundos de diferentes subestações e concessionárias de energia (TIA, 2005). E de acordo com a distribuição de energia no Brasil, criada a partir de monopólios estatais posteriormente privatizados, não existem localidades com essa capacidade, tendo cada região ou Estado, uma única concessionária de distribuição de energia.

Portanto, o estado da arte para *data centers* no Brasil são os certificados com a norma ANSI/TIA-942 *Tier III* com nível de disponibilidade de 99,982% que, segundo materia publicada pela ComputerWorld em 2010, o primeiro *data center* que recebeu esse nível de certificação no país, teve um investimento de US$50 milhões (COMPUTERWORLD, 2012c). Outro *data center* com certificação *Tier III* recentemente inaugurado em 2012 contou com investimentos ainda maiores próximos de US$100 milhões (EMBRATEL, 2012; COMPUTERWORLD,2012d).

Devido aos altos investimentos na infraestrutura de *data centers*, empresas e organizações podem avaliar alternativas, como a contratação de serviços de hospedagem ou *hosting* de seus equipamentos da infraestrutura de TI, ou seja, servidores, *storages* e equipamentos da rede instalando os mesmos em *data centers* de empresas especializadas na prestação deste tipo de serviço de TI.

O melhor cenário visando a mínima interrupção possível nos sistemas críticos quando da ocorrência de um desastre natural ou provocado pelo homem, como descrito na literatura técnica como recuperação de desastres ou *Disaster Recovery* (MARCUS; STERN, 2003; SCHMIDT, 2006), sugere não um *data center* mas dois tendo a replicação dos dados via dois *storages* e replicação dos sistemas. Desta forma, é outro ponto que reforça avaliar os investimentos envolvidos na construção de dois *data centers* certificados ou um *data center* próprio e outro terceirizado através da contratação de serviços de *hosting*.

Sumarizando sobre *data centers*, o estado da arte considera dois *data centers* com certificação *Tier III,* seguindo a norma ANSI/TIA-942, para fins de alcançar os dois níveis superiores de alta disponibilidade em termos de replicação de dados e sistemas e um plano de *disaster recovery*.

4.2. Equipamentos *(hardware)*

Com relação aos equipamentos (servidores, *storages* e dispositivos da rede), é importante considerar o RAS, ou seja, confiabilidade, disponibilidade e facilidade de manutenção como características básicas (SCHMIDT, 2006) na definição do estado da arte.

Especificamente para servidores, considerando o padrão da indústria (CACIATO, 2012; FUJITSU, 2012) que se adequam apropriadamente no contexto de Brasil, é fundamental para alta disponibilidade que tais equipamentos possuam fontes de alimentação e ventiladores redundantes e *hot-swappable,* além de módulos de memória com correção de erro (ECC), dualidade de interfaces de rede (NIC), dualidade de controladoras de acesso ao *storage* (HBA), concluindo

com uma controladora de discos com dois discos internos protegendo o sistema operacional com nível de RAID 1 para falhas de discos (WEYGANT, 2001; MARCUS e STERN, 2003; SCHIMDT, 2006).

A otimização de espaço físico e consumo de energia nos *data centers* também é um fator relevante na escolha dos servidores. Portanto, a tecnologia em lâmina ou *blade* deve ser considerada. A tecnologia *blade* através da alta densidade dos componentes concentra servidores, dispositivos de rede e até *storages* em um único gabinete internamente interconectado, eliminando cabeamento. Também compartilham componentes redundantes básicos como entradas de energia, fontes de alimentação e ventiladores adicionando um módulo de gerenciamento contendo ferramentas próprias que facilitam o gerenciamento e monitoração (GOLDWORM; SKAMAROCK, 2007).

A virtualização de servidores cria uma camada de abstração lógica e permite que vários servidores virtuais ou instâncias de sistemas operacionais estejam em execução em um servidor físico. Também é uma tecnologia a ser considerada visando a consolidação de servidores físicos maximizando do uso dos recursos em termos de processamento e memória (GOLDWORM; SKAMAROCK, 2007; CACIATO, 2012).

Com relação aos dispositivos de redes LAN, WAN e SAN (*switches* e roteadores), também necessitam ter componentes básicos (fontes de alimentação e ventiladores) redundantes e *hot-swappable,* bem como serem duplicados, deixando de caracterizar como pontos únicos de falha (SPOFs) (WEYGANT, 2001; SCHIMDT,2006). O cabeamento e os *links* externos também requerem ser dualizados permitindo a redundância de acesso entre os servidores e os dispositivos de rede LAN e WAN bem como com os *storages* na SAN e o mundo externo.

Ainda sobre equipamentos, o melhor cenário requer dispositivos de armazemento, ou seja, *storages* com as redundâncias nos componentes básicos (fontes de alimentação e ventiladores) e facilidade de manutenção, como os demais equipamentos da infraestrutura, além de tecnologia RAID, protegendo os dados de falhas de discos visando a proteção, integridade e disponibilidade dos

dados armazenados. Também são requeridas controladoras redundantes com memórias *cache* com ECC e características de *failover* que, em caso de falha, migrem automaticamente o acesso aos dados através da ou das controladoras remanecescentes sem causar interrupções de acesso aos dados pelos sistemas. A funcionalidade de *call home* também é desejada permitindo a conexão direta com o suporte do fabricante, apontando eventos de pré-falha ou falha dos componentes internos (SCHIMDT, 2006; TROPPENS *et al.*, 2009).

4.3. Sistemas Operacionais e Aplicações em *cluster*

Considerando que os servidores foram configurados com redundância de placas de rede (NICs) e controladoras de acesso ao *storage* (HBAs), exige-se que no sistema operacional desses servidores sejam instalados *drivers* e pacotes de software normalmente disponibilizados pelos próprios fabricantes dessas placas, para permitir as funcionalidades de *failover* e balanceamento de carga (*load balancing*), que possibilita que os sistemas e aplicações permaneçam com acesso a rede LAN e aos dados no *storage* sem gerar interrupções mesmo que uma NIC ou HBA falhe.

Conforme mencionado por Marcus e Stern (2003), falhas de *hardware* em servidores, principalmente quando intermitentes, podem levar várias horas para serem reparadas, ou a aplicação de uma correção de sistema operacional (*patch*) pode requerer a reinicialização programada do servidor. Portanto, em um ambiente computacional de alta disponibilidade, os sistemas necessitam dispor de uma camada adicional de *software* chamada *cluster,* estando protegidos a falhas de *hardware* que possam gerar a parada completa de um servidor (ZHU et al., 2009) e que possibilitem também manutenções programadas nos sistemas sem a necessidade de parada das aplicações, pois as mesmas podem ser migradas manualmente de um servidor para o outro dentro do *cluster* de forma rápida e transparente aos usuários.

4.4. Replicação de Dados entre *Storages* e *Disaster Recovery*

Em complemento a disponibilidade e integridade dos dados armazenados em um único *storage,* mesmo contendo seus principais componentes redundantes, e adotando a tecnologia RAID para proteção dos dados em casos de falhas de discos, o próprio *storage* permanece sendo um ponto único de falha. A replicação dos dados requer a mesma informação em dois locais, que pode ser uma simples cópia de segurança (*backup*) em fita magnética ou a replicação de forma *online,* onde dois *storages* em localidades diferentes mantém o espelhamento das informações, requerendo uma camada adicional de *software* para efetuar essa replicação de dados (SCHMIDT, 2006).

Considerando o estado da arte em alta disponibilidade, ou seja, o nível mais alto a ser alçando (WEYGANT, 2001; MARCUS; STERN, 2003; SCHIMDT, 2006) protegendo o ambiente de TI de desastres naturais, falhas humanas, falhas complexas de *hardware, software* ou na própria infraestrutura interna no *data center* principal, recomenda-se a adoção da replicação dos dados e inclusive dos sistemas mais críticos chamado ambiente em *Disaster Recovery*.

Um ambiente preparado para recuperação de desastres requer um planejamento detalhado e alinhado entre o alto nível executivo, as áreas de negócio e a área de TI definindo quais são os sistemas críticos essenciais à continuidade dos negócios requerendo treinamento da equipe e testes de validação pra garantir a efetividade do plano (SCHMIDT, 2006; HILES, 2007).

A Figura 12 exemplifica a topologia de um ambiente computacional configurado em *disaster recovery* (Nível de Alta Disponibilidade 5 segundo Zhu *et al.* (2009)) permitindo ilustrar o que foi mencionado neste trabalho até este ponto quanto as redundâncias de componentes deste a entrada de alimentação com dois *Nobreaks* ou UPS, servidores duplicados e configurados em *cluster,* permitindo o *failover* entre si em caso de falha de um dos servidores por completo e configurados em *metro cluster* permitindo a migração das aplicações e serviços entre *data centers*. Todos os componentes das redes LAN, WAN e SAN e conexões também duplicados e configurados em redundância bem como a

unidade de fita para realização das cópias de segurança (*backup*) possibilitando a restauração dos dados em ambos *data centers*.

Quanto a disponibilidade e integridade dos dados, a Figura 12 demonstra dois *storages,* entendendo-se ambos com tecnologia RAID com níveis de proteção contra falhas de discos e replicando os dados simultaneamente e de forma síncrona entre os *data centers,* tendo as duas instâncias, o espelhamento dos mesmos dados e informações.

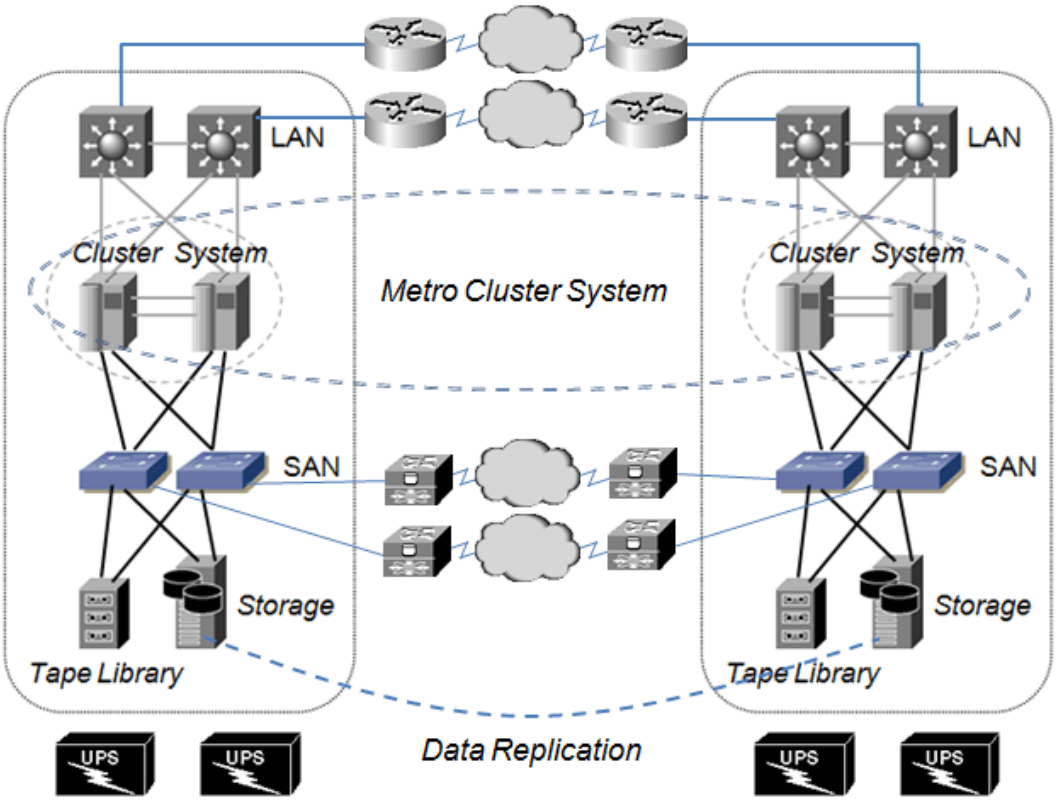

Figura 12. Ambiente de Alta Disponibilidade *(Disaster Recovery)* adaptado de Marcus e Stern (2003)

Salienta-se que conforme mencionado anteriormente neste estudo, o importante é alinhar a área de TI com as estratégias de negócio da empresa ou organização, sendo desta forma definidos: o grau de dependência do negócio em relação à Tecnologia da Informação, os níveis de riscos aceitos e o investimento na área de TI buscando a continuidade dos negócios, respeitando as capacidades de investimentos conforme o porte e saúde financeira da empresa.

Desta forma, é importante apresentar novamente a relação entre valores investidos com o nível de disponibilidade a ser desejado, ou seja, quanto maior a disponibilidade a ser alcançada maiores também serão os investimentos na infraestrutura de TI, como demonstra o gráfico disposto na Figura 13.

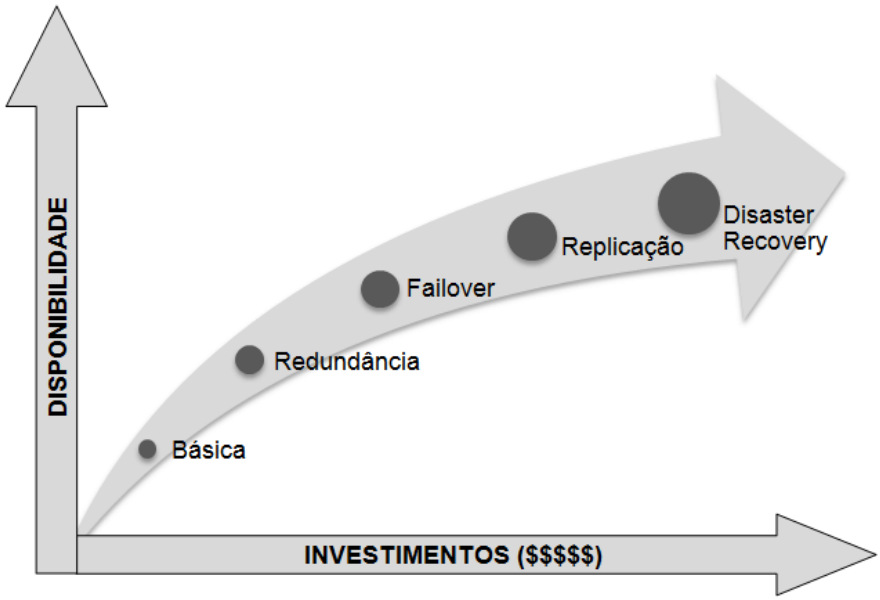

Figura 13. Escala de Alta Disponibilidade em relação aos investimentos necessários adaptado de Marcus e Stern (2003)

4.5. Ferramentas de Monitoração e Gerenciamento do Ambiente de TI

Segundo Stalling (1998), os cinco pilares que compõem a gerência de redes são: gerenciamento de falhas, gerenciamento de desempenho, gerenciamento da configuração, gerenciamento da segurança e gerenciamento da contabilidade este último permite cobrar pelo serviços conforme a utilização. Essa abordagem também pode ser aplicada a todos os componentes da infraestrutura de TI, principalmente em relação a falhas, desempenho e configuração.

Em um ambiente computacional de alta disponibilidade, o monitoramento é fator preponderante, sendo necessário definir quais componentes serão monitorados e que ações serão tomadas em caso de falha identificada pela ferramenta de monitoração (MARCUS; STERN, 2003).

Segundo o IDC (IDC, 2011a), com o avanço da virtualização em várias camadas da infraestrutura de TI, a utilização de ferramentas de gerenciamento e diagnóstico oferecem um maior controle do ambiente, reduzindo as falhas nos sistemas.

Para Schmidt (2006), a monitoração não só dos componentes, mas também a nível de aplicações, traz benefícios para manter a alta disponibilidade dos sistemas críticos ao negócio.

Portanto, para fins de estado da arte, é extremamente recomendado que sejam adotadas ferramentas de monitoração e gerenciamento disponíveis no mercado capazes de identificar e reportar falhas, bem como monitorar o desempenho e a utilização dos recursos, auxiliando tanto a rápida identificação e solução de problemas como também no gerenciamento de capacidade do ambiente. Desta forma, sendo capazes de contribuir para endereçar mais rapidamente as falhas do ambiente e planejar as demandas futuras, evitando paradas não programadas por estouro de espaço disponível em disco ou completa utilização de recursos de memória ou processamento.

4.6. Treinamento e Capacitação da Equipe da Área de TI

Ross, Weill e Robertson (2008), por meio de um estudo realizado com centenas de empresas, apontaram dez princípios de liderança, onde destaca-se o investimento nas pessoas, ou seja, desenvolver as capacidades das pessoas com treinamentos bem como a utilização do aprendizado após as implementações de projetos como fonte de conhecimento. Segundo eles, pesquisa publicada pelo instituto Gartner Group em 2005 apontava que apenas 2% do orçamento de TI é investido em treinamento e desenvolvimento dos funcionários e, quando crises financeiras aparecem, o corte em viagens e treinamentos são os primeiros a ocorrer.

Os autores (WEYGANT, 2001; MARCUS; STERN, 2003; SCHMIDT, 2006) reforçam a necessidade de manter a equipe técnica responsável pela

administração, operação e suporte dos sistemas críticos treinada e atualizada com as novas tecnologias, bem como motivada para desempenhar suas funções.

Portanto, como parte do estado da arte objetivando reduzir falhas humanas e principalmente ter uma equipe preparada com as habilidades técnicas necessárias para prontamente agir e solucionar problemas, é importante mantê-la treinada e atualizada nas tecnologias em uso na organização. Também considera-se importante ter o conhecimento das melhores práticas de governança e gerenciamento de TI tendo o entendimento de seu papel e a importância TI para a continuidade dos negócios.

Tanto os guias de melhores práticas de governança e gerenciamento de TI como os fornecedores da tecnologia, desenvolveram um plano de desenvolvimento e capacitação dessas habilidades por meio de treinamentos e provas de certificação, possibilitando uma forma de avaliar e qualificar os profissionais.

Desta forma, a certificação através de uma avaliação objetiva de seus conhecimentos profissionais, é capaz de identificar tanto as habilidades e competências já adquiridas pelo profissional como também aquelas que ainda precisa buscar para desempenhar sua função (SABOIA *et al.*, 2009).

4.7. Serviços de Suporte Missão Crítica com Fornecedores

Conforme estabelecido pelo Código de Defesa do Consumidor através da Lei Federal nº8.078 de 1990 (BRASIL, 2012), todos os serviços e produtos duráveis tem um prazo de garantia de 90 dias (artigo 26) que deve ser honrado pelo fornecedor. No artigo 50 da mesma lei, refere-se à garantia estendida do produto ou serviço que deve prover o mesmo nível de serviço e qualidade da garantia legal de 90 dias.

Normalmente para produtos duráveis, os fabricantes e fornecedores no Brasil dão um ano de garantia, sendo noventa dias da garantia legal e mais nove meses de garantia estendida. Os clientes podem adquirir, se disponível pelo fabricante ou fornecedor do produto, pacotes de serviços chamados garantia

estendida (PROCON-SP, 2012) aumentando o prazo de garantia do produto contra defeitos de fabricação.

Entretanto, apenas a garantia legal ou garantia estendida do produto, nos mesmos moldes da garantia legal onde não está definido um prazo para que o reparo completo do produto ou equipamento seja concluído, não é suficiente para atender as necessidades de um ambiente computacional de alta disponibilidade.

Com base neste contexto, ou seja, na necessidade de empresas e organizações buscarem por melhores níveis de serviço e qualidade em se tratando de TI e do impacto ao negócio quando problemas acontecem, os fabricantes ou fornecedores da tecnologia (*hardware* e *software*) disponibilizam níveis diferenciados de serviços desde a extensão do período de atendimento, passando 9x5 para 24x7, ou seja, do atendimento horário comercial cinco dias por semana entre 08:00hs e 17:00hs para o atendimento ininterrupto 24 horas por dia de 2ªfeira à domingo inclusive feriados, a estabelecer prazos de solução no SLA normalmente para problemas de *hardware* dos equipamentos até níveis denominados pelo mercado como Missão Crítica.

Marcus e Stern (2003) e Schmidt (2006) recomendam avaliar a disponibilidade e localidade das peças de reposição, reduzindo os tempos de espera para deslocamento e, consequentemente, diminuindo o tempo médio de reparo (MTTR) dos equipamentos. Especificamente o local onde foi realizada este estudo, ou seja, o Estado do Ceará, devido as distâncias e tempos de voo de São Paulo e Rio de Janeiro entre 03:00hs e 03:30hs (TAM, 2012 e AZUL, 2012) onde encontram-se os escritórios centrais dos fornecedores, torna-se importante avaliar a obtenção de níveis diferenciados de serviços e assistência técnica com os fornecedores prevendo tempos para resolução dos incidentes e disponibilidade local de peças de reposição.

Os serviços de Missão Crítica oferecidos pelos grandes fabricantes como IBM, HP, Oracle entre outros (IBM, 2012; HP, 2012; ORACLE, 2012; SYMANTEC, 2006) buscam ir além do reparo reativo, ou seja, apenas esperar quebrar para então consertar (*break & fix*). Tais serviços oferecem normalmente

ferramentas próprias adicionais de monitoração e notificação de falhas e pré-falhas automatizadas, estabelecendo uma conexão direta entre os equipamentos e a área de suporte e assistência técnica chamado na literatura de *call home*.

Os serviços de Missão Crítica proveem ações pró-ativas como a revisão do ambiente em termos de matrizes de suportabilidade e interoperabilidade entre os diversos equipamentos, sistemas operacionais e aplicações da infraestrutura, recomendando, de forma períodica estabelecida em contrato, atualizações de *drivers, firmwares* e correções *(patches)*. Assim, permitem manter o ambiente sempre atualizado de acordo com as versões mais recentes de correções e melhorias disponibilizadas pelas engenharias de produto dos fabricantes, evitando preventivamente a ocorrência de problemas já conhecidos e consequentemente riscos de paradas não programadas.

Tais serviços diferenciados também contam com uma equipe dedicada com um gerente para a conta (cliente) e especialistas técnicos que estabelecem uma relação melhor e mais próxima entre o fornecedor e empresa cliente (IBM, 2012; HP, 2012; ORACLE, 2012), auxiliando na documentação da infraestrutura, mantendo o controle e histórico de atendimentos técnicos, registro de problemas, controle de atualizações entre outras atividades que contribuem para a redução de paradas não programadas, bem como na resolução de problemas de forma mais rápida, pois etapas como: atualizações mínimas, histórico de problemas e conhecimento mais aprofundado do ambiente já são de conhecimento comum entre as equipes de operação de TI da empresa ou organização cliente e a equipe de suporte do fornecedor ou fabricante.

Pesquisa realizada pelo IDC em 2010, com algumas empresas que adotaram os serviços de Missão Crítica de um dos grandes fornecedores mundias de soluções de TI (IDC, 2010b), apontou a eficácia de tais serviços contribuindo para o aumento da disponibilidade dos sistemas críticos. Pois, segundo os dados dessa pesquisa, apresentaram 76% de redução do tempo das paradas não programadas aos usuários internos, diminuição de 20% dos incidentes de indisponibilidade mensais e redução de 26% do MTTR (tempo médio para reparo).

Em suma, considerando os benefícios dos serviços de Missão Crítica em termos de pró-atividade e garantia em contrato de cumprimento de SLAs com tempo de resolução para problemas de *hardware*, os mesmos são considerados dentro do estado da arte para sistemas críticos ao negócio.

4.8. Cópia de Segurança *(backup)* e Proteção de Acesso

Em complemento à disponibilidade dos dados armazenados em uso por aplicações e sistemas nos *storages*, é necessário garantir a cópia de segurança dos mesmos descrita na literatura como *backup*. Marcus e Stern (2003) salientam que *storages* com redundância de dados por RAID não substituem a necessidade de manter uma política de *backup* dos dados. Isso porque o RAID, ou espelhamento dos dados em discos distintos, não protege as informações por uma deleção de arquivos indevida ou uma corrupção gerada inadvertidamente por uma nova versão da aplicação.

Desta forma, automatizar as rotinas de *backup* através de ferramentas de mercado, como IBM Tivoli TMS, Veritas NetBackup, Computer Associates ARCserve ou HP Data Protector, reduzem a interação humana e consequentemente o risco de falhas operacionais no processo. Possibilitam também melhor integração com sistemas operacionais multiplataforma, bancos de dados e outras aplicações de mercado, bem como melhoram o gerenciamento das mídias e utilização dos recursos, permitem a centralização do gerenciamento e automação de processos de *disaster recovery* (MARCUS; STERN, 2003).

Logicamente, o estado da arte também recomenda a segurança e proteção dos sistemas e dados de empresas e organizações por meio de um conjunto de *hardwares* e *softwares* de proteção contra ataques externos, como *firewalls*, além de *software* de antivírus (WEYGANT, 2001; MARCUS; STERN, 2003) e uma política interna de segurança da informação seguindo as recomendações de melhores práticas dispostas nos guias COBIT e ITIL.

4.9. Documentação de Processos, Matriz de Responsabilidades e Escalação

Elaborar a documentação detalhada da configuração do ambiente após sua implementação, como também mantê-la atualizada, é fundamental para o controle de mudanças e apoio às equipes de suporte no rápido entendimento do cenário e diagnóstico de problemas.

Os autores Weygant (2001), Marcus e Stern (2003), Schmidt (2006) reforçam a importância da documentação do ambiente, não apenas da configuração instalada em termos de equipamentos, sistemas operacionais e topologias de redes LAN, WAN e SAN, mas também em ter os procedimentos documentados a serem adotados em caso de falhas. Em ambientes configurados em *disaster recovery*, é fundamental ter documentado o *disaster recovery plan* ou DRP para que o processo de migração entre os *data centers* seja conhecido e seguido pela equipe de TI, ocorrendo de forma adequada (HILES, 2007).

Considerando a importância da documentação do ambiente, não só os guias de melhores práticas de governança e gerenciamento de TI, como ITIL e COBIT, recomendam o gerenciamento de configuração e gerenciamento de mudanças que tratam desse tema, mas também os guias de melhores práticas de gerenciamento de projetos em geral como PMBOK (PMI, 2012) e PRINCE2 (APMG, 2012b), reforçam tal importância.

Além da documentação técnica do ambiente envolvendo suas configurações e procedimentos, também é fundamental que a equipe própria de operação e suporte de TI entenda a matriz de responsabilidades, sabendo quem deve ser acionado com a devida prioridade, conforme a gravidade e impacto da situação (WEYGANT, 2001; MARCUS; STERN, 2003).

Desta forma, a equipe de operação deve conhecer o processo de escalonamento ou escalação internamente na organização, informando rapidamente os níveis gerenciais da área de TI quando um problema mais sério ocorre, bem como ter os telefones de acesso ao suporte dos fabricantes dos equipamentos, sistemas operacionais e aplicações. Conforme salientam Marcus e Stern (2003), também é importante que o gestor de TI tenha os contatos da

gerência de suporte dos fabricantes, em caso de necessidade de escalação, buscando colocar a prioridade e criticidade adequada quando necessário.

4.10. Adoção de Guias de Melhores Práticas de Governança e Gerenciamento de TI

Os guias de melhores práticas de Governança e Gerenciamento de TI como o COBIT e ITIL estudados no Capítulo III deste trabalho proveem as formas e recomendações de como buscar um melhor alinhamento estratégico entre a empresa ou organização e a área de TI. Favorecem, desta forma, uma aproximação das áreas de negócio com a área de Tecnologia da Informação bem como no sentido inverso, ou seja, a área de TI compreendendo seu papel fundamental para a organização.

De acordo com Fernandes e Abreu (2008), o *framework* COBIT, da forma como está estruturado, possibilita um melhor entendimento dos processos de TI, tornando-se um ótimo referencial para avaliar os processos em uso, seu grau de maturidade e que melhorias devem ser adotadas em benefício da organização.

Sob a ótica da disponibilidade dos sistemas críticos, o COBIT contempla processos de TI desde a gerência dos investimentos em TI e recursos humanos passando pela definição da infraestrutura e SLAs, gerenciamento de terceiros (suporte com os fornecedores incluso nesse processo), do desempenho e capacidade e da própria continuidade dos serviços de TI.

O ITIL, com a adoção do ciclo de melhoria contínua dos serviços de TI, também demonstra contribuir para a continuidade e disponibilidade dos serviços, tendo inclusive medições e avaliações de serviços com essa mesma nomenclatura e finalidade.

Resumindo, o ITIL complementa a visão de Governança de TI disposta no COBIT sendo a adoção de ambos em conjunto por empresas e organizações o estado da arte para fins da gestão de processos e serviços de TI, visando a alta disponibilidade de sistemas críticos ao negócio.

CAPÍTULO V – METODOLOGIA

Neste capítulo, estão descritos os métodos e técnicas de pesquisa utilizados para alcançar os objetivos deste estudo. Embora a pesquisa científica requeira iniciativa, criatividade e originalidade do pesquisador, também necessita da aplicação de procedimentos disciplinados através de um roteiro a ser seguido, ou seja, de um método (RUDIO, 2010).

Portanto, segundo Rudio (2010), o método pode ser definido como:

> O método é o caminho a ser percorrido, demarcado, do começo ao fim, por fases ou etapas. E como a pesquisa tem por objetivo um problema a ser resolvido, o método serve de guia para o estudo sistemático do enunciado, compreensão e busca da solução do referido problema.
>
> (RUDIO, 2010, p.17)

De acordo com Rudio (2010), as fases do método de pesquisa científica podem ser sintetizados em: 1.definir o problema a ser estudado, 2.elaborar as hipóteses para solucionar esse problema, 3.coletar os dados para análise e comprovação das hipóteses e 4.analisar e interpretar os dados coletados apresentando os resultados obtidos.

Desta forma, este trabalho foi estruturado seguindo as fases de pesquisa conforme segue:

a) Delimitação do problema a ser estudado, ou seja, se os gestores de TI tem conhecimento sobre as causas das paradas não programadas em sistemas críticos ao negócio e de como os investimentos realizados na área da Tecnologia da Informação contribuem para evitar que tais problemas aconteçam;

b) Revisão da literatura relacionada ao tema explorando as atuais tecnologias voltadas a ambientes computacionais de alta disponibilidade e guias de melhores práticas de Governança e Gerenciamento de TI focando nos processos relacionados à disponibilidade e continuidade dos serviços de TI;

c) Elaboração das hipóteses para solucionar o problema definindo o "estado da arte", ou seja, o melhor cenário para manter disponíveis e operacionais os sistemas críticos ao negócio evitando ou minimizando paradas não programadas com base na revisão da literatura;

d) Escolha do tipo de pesquisa como método a ser aplicado para a coleta de dados próprios e contemporâneos sobre o problema em estudo no contexto local;

e) Análise estatística descritiva dos dados obtidos com a pesquisa *survey* correlacionando com o "estado da arte" consolidando os resultados e conclusões do estudo.

A revisão da literatura busca identificar o que já foi escrito sobre o tema, aspectos já abordados e quais oportunidades ou lacunas ainda existem sobre o assunto na literatura. Permite uma melhor delimitação do problema a ser estudado bem como possibilita determinar o "estado da arte" sobre o assunto (MORESI, 2003).

5.1 Caracterização da Pesquisa

Pesquisa pode ser definida de várias formas, Moresi (2003) buscou sintezar como:

> Pesquisa é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos.
> (MORESI, 2003, p.8).

Ainda segundo Moresi (2003), as pesquisas podem ser classificadas conforme sua natureza, abordagem, fins e meios de investigação. O autor também reforça que não são mutuamente exclusivas, ou seja, uma pesquisa pode adotar mais de uma metodologia simultaneamente.

Portanto, quanto a natureza, as pesquisas são classificadas como: básica, que busca obter conhecimentos novos sobre determinado tema universal sem preocupar-se com a aplicação prática; ou aplicada, que tem por objetivo

adquirir conhecimento sobre como solucionar um determinado problema envolvendo questões localizadas (MORESI, 2003).

Referente à abordagem, uma pesquisa pode ser classificada como qualitativa ou quantitativa. De acordo com Oliveira (2007), a pesquisa qualitativa busca explorar em profundidade o significado e características de um determinado tema normalmente através de entrevistas ou questões abertas, estimulando os entrevistados a pensarem livremente sobre o assunto abrindo espaço para a interpretação.

Já a pesquisa com abordagem quantitativa permite apurar opiniões e atitudes conscientes dos entrevistados através de instrumentos estruturados, normalmente questionários, traduzindo tais as informações obtidas em números a serem classificados e analisados. Necessita-se aplicar técnicas estatísticas como porcentagem, média, desvio padrão e coeficiente de correlação entre outras e seus resultados são menos passíveis de erros de interpretação (MARCONI; LAKATOS, 1999; MORESI, 2003; OLIVEIRA, 2007).

Quanto aos fins ou propósitos, as pesquisas podem ser qualificadas como: investigação exploratória, investigação intervencionista, pesquisa metodológica, investigação explicativa e pesquisa descritiva (MORESI, 2003).

A investigação explicativa tem por objetivo buscar esclarecer quais fatores contribuem para a ocorrência de determinado fenômeno. Já a pesquisa descritiva busca identificar características de determinada população ou fenômeno, podendo ainda estabelecer quais os fatores que de alguma forma contribuem para ocorrência de determinado fenômeno (MORESI, 2003) enquadram-se mais ao objeto deste estudo.

Quantos aos meios de investigação, ou seja, a forma ou método como os dados são coletados, as pesquisas podem ser também divididas como: pesquisa de campo, levantamento ou pesquisa de opinião também descrita como *survey*, pesquisa de laboratório, experiemantal, *ex post facto*, participante, pesquisa-ação, estudo de caso, investigação documental, pesquisa bibliográfica e pesquisa telematizada ou via Internet (FREITAS, 2000; MORESI, 2003; OLIVEIRA 2007; RUDIO, 2010).

Assim, conforme as definições expostas, este estudo caracteriza-se como uma pesquisa aplicada com abordagem quantitativa e propósitos explicativos e descritivos utilizando a pesquisa bibliográfica, pesquisa telematizada e *survey* como métodos para obtenção dos dados.

5.2 A Escolha do *survey* como Método de Pesquisa para este Estudo

O método de pesquisa *survey* busca obter informações a respeito de características, ações ou opiniões de determinado grupo de pessoas que representam uma determinada população a ser atingida através de um instrumento de pesquisa normalmente um questionário (PINSONNEAULT; KRAEMER, 1993 *apud* FREITAS, 2000).

Na avaliação abrangente de 285 artigos sobre gestão operacional (*Operational Management - OM*) que utilizaram *surveys* como método de pesquisa e foram publicados entre 1980 e 2000 nos seis principais periódicos internacionais relacionados ao tema, sendo 40,5% destes artigos sobre Gestão da Tecnologia, os autores concluiram empiricamente que os *surveys* tem crescido nas últimas duas décadas e se firmado como uma metodologia legítima e muito bem aceita para estudar as principais questões e problemas de OM (RUNGTUSATHAM, *et al*., 2003).

O método de pesquisa *survey* tem como principal característica: obter dados quantitativos de uma determinada população por meio de um questionário como instrumento de pesquisa. Portanto, sua utilização é apropriada quando deseja-se compreender questões “de o que”, “como” e “porque” determinadas situações estão ocorrendo no presente ou em um passado recente, tendo o ambiente natural como a melhor forma de estudar o fenômeno de interesse da pesquisa (FINK, 1995 *apud* FREITAS, 2000).

Segundo Alderman e Salem (2010), os *surveys* podem ser administrados através de correspondência convencional (carta), contatos telefônicos ou correio eletrônico (*email*). O formato eletrônico reduz custos e agiliza a análise e interpretação dos dados, tendo a disposição *softwares* como o

SurveyMonkey, SurveyTracker, QuestionPro e SurveyShare como ferramentas de mercado para aplicação e administração da pesquisa.

Desta forma, adotou-se o método de pesquisa *survey* para opter dados primários para este estudo, buscando alcançar a população alvo tomando a facilidade de acesso à Internet como estratégia de ação. Optou-se pelo SurveyMonkey (SURVEYMONKEY, 2012) como forma de viabilizar o instrumento de pesquisa (questionário) aos pesquisados considerando-se o reconhecimento de ser o principal provedor mundial de soluções de questionários pela internet (IDGNOW, 2012) e a disponibilidade da ferramenta em Língua Portuguesa.

5.3 A Escolha da população, amostra e momento

A pesquisa circunscreveu-se a uma determinada geografia e a um público especialista específico de coordenadores e gerentes de TI como população. Pois, embora o *CIO – Chief Information Officer* ou diretor da área de TI em conjunto com a diretoria executiva da organização sejam os principais responsáveis pela definição dos investimentos anuais destinados à área de TI (WEILL; ROSS, 2004; RODRIGUES *et al.,*2009), os coordenadores e gerentes de TI exercem importante influência nessa tomada de decisão em virtude de seu conhecimento técnico especialista e experiência na gestão operacional da área de Tecnologia da Informação.

Quanto a delimitação da geografia, optou-se por um levantamento no Estado do Ceará, ou seja, fora do eixo Rio de Janeiro – São Paulo. Este Estado foi escolhido por ser uma das três maiores economias da região Nordeste (IBGE, 2011) e por sediar parte importante das maiores empresas da região (BANCO DO NORDESTE, 2009) bem como pela facilidade de acesso do pesquisador ao público a ser pesquisado (GROVES, 2012).

A região Nordeste tem demonstrado níveis de crescimento superiores às demais regiões do país, sendo responsável por 20% da criação de novos empregos formais no país em 2010. Portanto, as capitais do Nordeste tem atraído a abertura de escritórios e filiais de empresas que antes não voltavam seu foco

para a região, assim como diversos projetos estão em andamento nas áreas de refinaria, indústria química, indústria alimentícia, construção civil e instalações portuárias (CEPLAN, 2011 *apud* VOCÊ S/A, 2011).

A pesquisa adotou uma amostragem não probabilística intencional (FREITAS, 2000; RUDIO, 2010), ou seja, definindo como critério de escolha da amostra, um subgrupo da população de coordernadores e gerentes de TI que, baseado nas informações disponíveis, pode ser considerado representativo (MORESI, 2003) buscando obter um número mínimo de cinquenta questionários respondidos.

Desta forma, após a validação do instrumento de pesquisa a ser descrita na próxima seção deste estudo, o endereço internet contendo o questionário disposto no SurveyMonkey foi encaminhado por correio eletrônico a um grupo aproximado de cento e oitenta gestores de TI.

Para esta fase da pesquisa, tomou-se como base tanto a relação de gestores de TI disposta na página da ETICE - Empresa de Tecnologia da Informação do Governo do Estado do Ceará presente na internet (ETICE, 2011), quanto foram efetuados contatos com os associados do GGTIC-CE - Grupo de Gestores de Tecnologia da Informação e Comunicação do Ceará (GGTIC-CE, 2011) buscando alcançar de forma aleatória as áreas de educação, manufatura, saúde, serviços e varejo de empresas pequenas, médias, média-grandes e de grande porte, seguindo a classificação do BNDES (BNDES, 2011), bem como organizações do setor público neste Estado.

A pesquisa *survey* adotou um corte transversal buscando a coleta de dados em um único momento, permitindo descrever e analisar o estado das variáveis da pesquisa em um dado momento (FREITAS *et al.*, 2000). Portanto, o período delimitado em que o questionário esteve disponível para respostas via SurveyMonkey compreendeu-se entre 07 de dezembro de 2011 e 30 de março de 2012.

5.4 O Instrumento de Pesquisa

Este estudo, por adotar o método de pesquisa *survey*, utilizou como instrumento de coleta da dados um questionário elaborado eletronicamente via ferramenta SurveyMonkey.

Conforme Moresi (2003), o questionário deve conter um conjunto de perguntas pré-elaboradas ordenadas de forma sequencial e sistemática buscando obter dados relacionados ao tema principal da pesquisa. Os questionários necessitam ser preenchidos por escrito ou, neste caso, de forma eletrônica, sem a presença do pesquisador, tornando o processo uma interlocução planejada.

Embora existam diversas formas de abordar o mesmo tema, Freitas (2000) reforça algumas recomendações importantes para a elaboração do questionário: o respondente não deve se sentir constragido para responder as perguntas; as questões devem ser redigidas de forma clara e objetiva, possibilitando uma única interpretação; as questões devem estar adequadas com o nível de informação dos pesquisados.

Portanto, seguindo as orientações de Freitas (2000) e Moresi (2003), foi elaborado um questionário composto de vinte questões, sendo dezenove questões fechadas e de resposta obrigatória (permitindo uma única opção de resposta entre as disponíveis) e uma vigésima pergunta aberta e opcional, possibilitando ao respondente discorrer sobre o tema “qual seu principal desafio para manter operacionais e disponíveis os sistemas críticos de sua empresa”.

Ainda seguindo as recomendações de Moresi (2003), após elaborado o questionário, o mesmo foi encaminhado a cinco gestores de TI como forma de validação do instrumento de pesquisa antes de ser encaminhado ao público alvo.

Foram escolhidos cinco gestores de TI para validação do questionário, considerando 10% da amostra esperada de cinquenta questionários na pesquisa definitiva. Destes cinco, três estavam na região a ser aplicada a pesquisa e outros dois se localizavam em regiões distintas no Sul e Centro-oeste.

Optou-se por profissionais com no mínimo 5 anos de experiência na área de TI, sendo dois mestrandos do curso de Engenharia Elétrica na PUC-

Campinas, um professor especialista titular das faculdades UNICE e FATENE em Fortaleza/CE, desempenhando funções de gestão na área de TI, e outros dois profissionais também gestores de TI. Portanto, ao todo foram três gerentes e dois coordenadores da área de TI em empresas privadas e do setor público em ramos de atividade e portes variados assemelhando-se ao perfil do público alvo.

Os questionários para validação da pesquisa foram respondidos entre 02 e 08 de novembro de 2011, não registrando nenhuma oportunidade de melhoria expressiva em seu conteúdo e formato, permitindo seguir com a pesquisa e encaminhamento para o público alvo.

Em relação às vinte questões do questionário, as quatro primeiras visam caracterizar o cargo que ocupa o entrevistado (coordenador ou gerente de TI), sua experiência profissional em anos de atuação na área de TI bem como o ramo de atividade e porte da empresa ou organização. A classificação quanto ao porte da empresa, seguiu a definição do BNDES (BNDES, 2011) com base no faturamento bruto anual focando em empresas de pequeno, médio, médio-grande e grande porte.

Quanto as 15 questões seguintes, todas fechadas com cinco opções de escolha em gradação de opinião, ou seja, possibilitando medir extremos das variáveis da pesquisa (MORESI, 2003) a serem respondidas obrigatoriamente pelo respondente.

Destas 15 questões, as cinco primeiras buscaram caracterizar o atual ambiente de TI da empresa ou organização quanto as suas características de redundância de *hardware* dos equipamentos, sistemas e ambiente bem como as ferramentas de gerenciamento e monitoração em uso e os níveis de serviços de suporte e assitência técnica contratados com os fornecedores.

Outras quatro questões buscaram identificar o perfil de investimento em treinamento e certificação da área de TI e se é adotado algum guia de melhores boas práticas de governança e gerenciamento de TI, como ITIL ou COBIT, e qual o nível de maturidade dessa governança, em termos de tempo de implementada e utilização de métricas de SLA e SLM (*Service Level Management*), para medir e controlar a eficácia e qualidade dos serviços de TI.

O ponto principal da pesquisa abordou com quatro questões objetivas se houve paradas não programadas em sistemas críticos nos últimos 12 meses e se a causa foi identificada, apontando cinco alternativas de resposta entre infraestrutura, aplicação, falha humana, falha de processo ou não identificada. A quantidade e duração dessas indisponibilidades, a existência de impactos financeiros e operacionais, também foram coletadas permitindo a gradação das respostas. Optou-se pelo período de 12 meses por considerar que as empresas normalmente definem SLAs para a disponibilidade dos sistemas críticos bem como orçamentos para investimentos incluindo na área de TI de forma anual.

Ao final, foram feitas duas perguntas específicas buscando identificar o perfil de investimento na área de TI da empresa ou organização para o próximo ano e uma última questão descritiva tendo a resposta opcional em texto livre sobre os principais desafios dos gestores de TI para manter os sistemas críticos disponíveis e operacionais.

5.5 Guia para análise dos resultados

Com base nas respostas obtidas através dos questionários, inicialmente são levantados as quatro primeiras respostas buscando identificar o perfil dos respondentes e das empresas e organizações aos quais fazem parte.

Dando sequência na análise estatística descritiva dos dados, busca-se obter a porcentagem de empresas que reportaram paradas não programadas em seus sistemas críticos ao negócio nos últimos dozes meses e qual a relação percentual com as empresas que não reportaram indisponibilidades nesse período.

O próximo passo é a análise se os gestores conhecem as causas das paradas não programadas, avaliando, entre as respostas que apontaram paradas, qual foi o percentual de respostas entre as opções de falha da infraestrutura, aplicação, pessoas, processos ou causa não identificada considerado o pior cenário. Demonstra-se que não houve aprofundamento de identificação de causa

raiz e consequentemente não houve aprendizado, podendo a situação voltar a ocorrer.

Ainda analisando os dados quanto aos gestores que apontaram paradas não programadas, são apontadas as quantidades de paradas não programadas registradas no último ano, o tempo de indisponibilidade e o impacto aos negócios como solicitado aos respondentes com base nas opções disponíveis para escolha. O questionário está disponível na íntegra no Apêndice C.

Buscando identificar potenciais diferenças em termos de investimentos em infraestrutura, capacitação das pessoas, nível de suporte técnico com os fornecedores e adoção de melhores práticas de governança e gerenciamento de TI entre as empresas que reportaram paradas com as empresas que não tiveram incidentes, ambas amostras são comparadas.

Seguindo uma sequência lógica visando comparar amostras distribuídas de forma semelhante quanto a ramo de atividade e principalmente quanto a porte das empresas e organizações, primeiramente os dois grupos são avaliados em relação a estas características e, havendo uma semelhança entre as duas amostras, as mesmas serão comparadas conforme descrito no parágrafo acima.

Detalhando como será feita essa comparação, considerou-se a lógica convencional com o conceito de dualidade, ou seja, que uma determinada variável é verdadeira ou falsa utilizando-se da álgebra booleana (GUNTZEL; NASCIMENTO, 2001) integrada a própria ferramenta SurveyMonkey através da adoção de filtros entre as questões e suas respostas focando nas respostas D e E (melhor cenário) seguindo a escala de gradação adotada.

A Figura 14 apresenta a página de análise dos dados do *survey* e o menu de opções tendo a alternativa de criação de filtros utilizados na análise dos dados diretamente pela ferramenta SurveyMonkey. Já a Figura 15 demonstra como configurar filtros na ferramenta por meio da lógica booleana com as portas "E" *(AND)*, "OU" *(OR)* e "NÃO" *(NOT)* (GUNTZEL;NASCIMENTO, 2001).

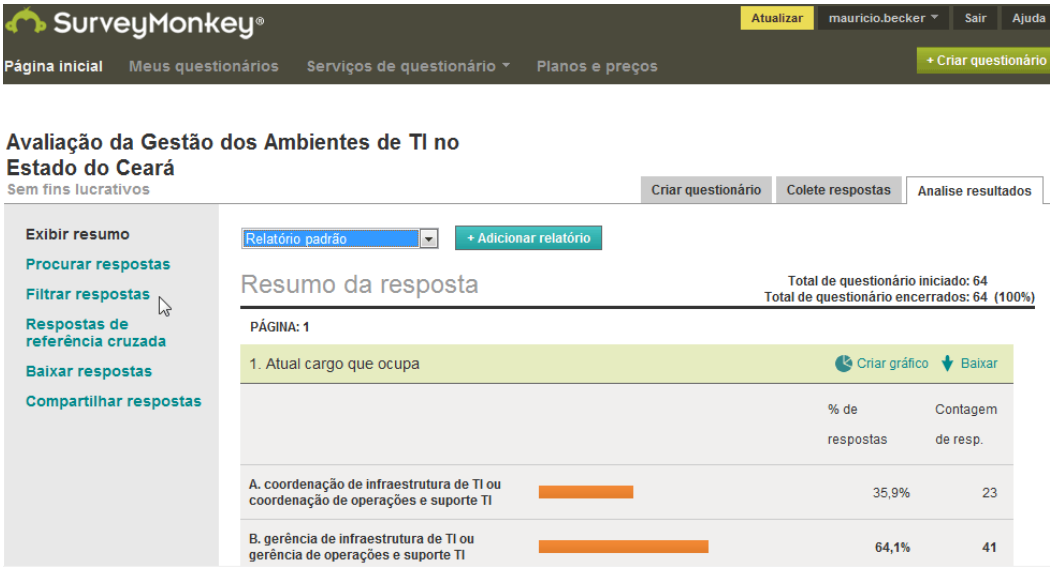

Figura 14. Página de análise de resultados da ferramenta SurveyMonkey

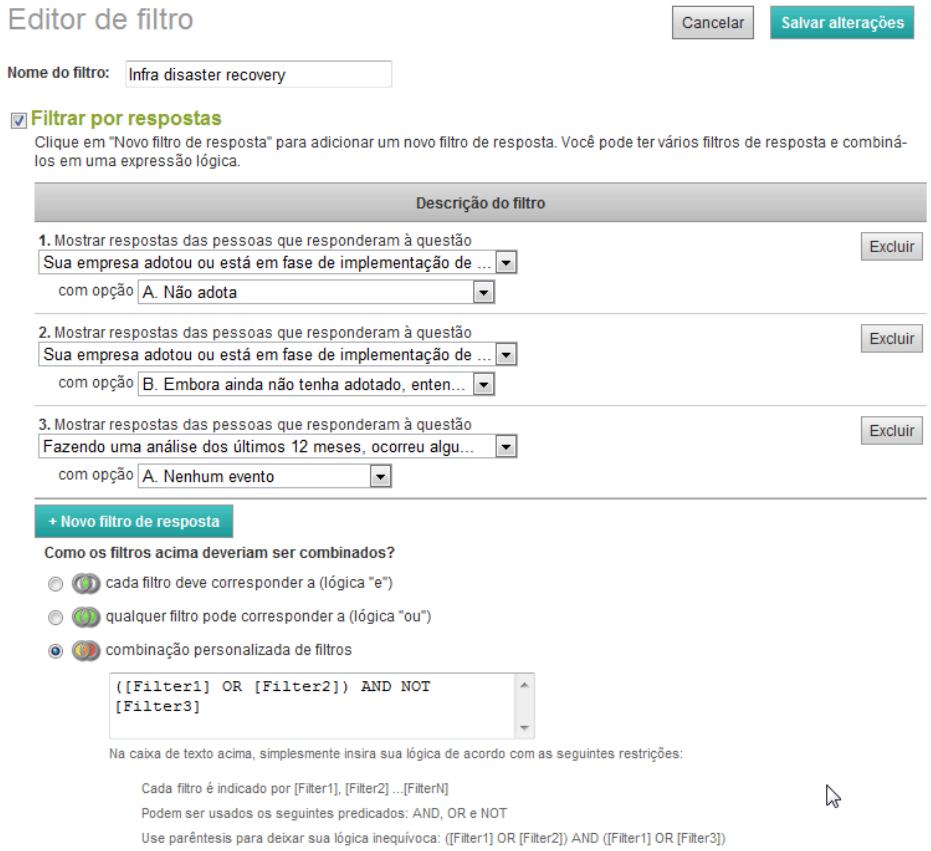

Figura 15. Criação de Filtros para análise de resultados via ferramenta SurveyMonkey

Portanto, será realizada a comparação entre os dois grupos, os que reportaram paradas não programadas e os que não as reportaram da seguinte forma:

Questões 5, 6 e 7, referente às características de redundância de *hardware* e proteção dos dados (RAID) dos equipamentos, adoção de configuração em *cluster* permitindo por *software* o *failover* entre sistemas e implementação de replicação de storages e sistemas em dois *data centers (disaster recovery).* Na comparação destas questões especificamente adotou-se apenas o estado da arte, ou seja, entre respostas "E" afirmando que todos os sistemas críticos tem tais características descartando as respostas "A", "B", "C" e D".

As comparações entre as questões 8, 9, 10 e 12 perguntando sobre a implementação e características das ferramentas de monitoração, contratação de níveis de serviços de suporte com os fornecedores, investimento em treinamento da equipe de TI e adoção de melhores práticas de Governança e Gerenciamento de TI, foram mantidas a análise considerando as respostas "D" e "E" como melhor cenário seguindo a escala de gradação das características em cada uma das quatro questões.

Em complemento a está análise estatística descritiva comparando apenas as respostas das questões 5, 6, 7, 8, 9, 10 e 12 entre as empresas que reportaram e as que não reportaram paradas não programadas, também foi realizada uma comparação completa de todas as outras 12 questões objetivas tomando como varíaveis fixas e testando uma de cada vez, os quatro P's relacionados a produtos (infraestrutura), pessoas (capacitação e treinamento), parceiros (serviços de suporte com fornecedores) e processos (melhores práticas de Governança e Gerenciamento de TI) e as respostas obtidas entre as opções "D" e "E" como melhor cenário.

Buscando tornar mais justa essa análise, visto que na amostra geral haverá empresas de pequeno, médio, médio-grande e grande porte, ou seja, com níveis e capacidade de investimentos em TI de certa forma limitados comparando pequenas e grandes empresas, para fins da variável fixa produto (infraestrutura),

adotou-se apenas as questões 5 e 6 referente a redundâncias de *hardware* e proteção dos dados com tecnologia RAID e a capacidade de *failover* via *software* de *cluster* respondidas no melhor cenário com opções “D” e “E” selecionadas.

Referente ao quadrante P de parceiros, ou seja, avaliando os níveis de serviços de suporte e assistência técnica contratados com os fornecedores além da garantia padrão dos equipamentos com suporte 9x5 até serviços de Missão Crítica, a varíavel fixa definida foram as respostas selecionadas com opções “D” e “E” quanto a questão de número 9 que aponta contratos prevendo SLA de tempo de resolução para problemas de *hardware* nos equipamentos até serviços de pró-atividade e Missão Crítica.

Quanto ao P referenciando pessoas, a varíavel fixa adotada foram as respostas selecionadas com opções “D” e “E” quanto a questão de número 10 onde há investimentos anuais pré-estabelecidos para treinamentos formais em sala de aula para os principais membros ou a todos colaboradores da área de TI.

Sobre adoção de guias melhores práticas de Governança e Gerenciamento de TI referente ao quarto P, a questão número 12 que trata de ter ou não adotado e em que fase está a implantação, a varíavel fixa foi definida como respostas a esta pergunta nas opções “D” e “E” onde os respondentes afirmam que a implementação das melhores práticas de TI já estão adotadas há no mínimo dois anos ou em fase final de implementação.

O objetivo principal desta comparação isolando os investimentos nos quatro quadrantes, é avaliar os resultados obtidos em termos de ocorrência de paradas não programadas, tempo de indisponibilidade, impacto de negócios bem como a visão de futuro com base nas respostas das questões 18 e 19 que tratam dos investimentos em TI para o próximo ano (próximos 12 meses).

Por final, serão transpostas as repostas da última questão aberta e de cunho opcional apresentando as opiniões dos gestores de TI pesquisados em texto livre sobre seu principal desafio para manter disponíveis e operacionais os sistemas críticos ao negócio.

CAPÍTULO VI – RESULTADOS OBTIDOS

A pesquisa *survey* obteve sessenta e quatro questionários respondidos durante o período de coleta de dados, compreendido entre 07 de dezembro de 2011 e 30 de março de 2012, ou seja, superando a amostragem mínima pré-estabelecida de cinquenta participantes.

6.1 Caracterização dos pesquisados quanto a função, experiência, ramo de atuação e porte da empresa ou organização em que atuam

As respostas das duas primeiras questões caracterizaram a amostra quanto ao cargo ocupado e tempo de experiência na área de TI conforme apresentado nas Tabelas 2 e 3. Os resultados demonstraram que a população pesquisada tem grande experiência na área da Tecnologia da Informação, sendo constituída por 79,7%, ou seja, quase 80% de profissionais com mais de 10 anos na área e 39,1% acima dos 20 anos.

Tabela 2. Função ocupada pelos entrevistados

1. Atual cargo que ocupa	**Porcentagem**	**Quantidade de respostas**
A. coordenação de infraestrutura de TI ou coordenação de operações e suporte TI	35,9%	23
B. gerência de infraestrutura de TI ou gerência de operações e suporte TI	64,1%	41
	TOTAL	**64**

Tabela 3. Experiência na área de TI

2. Tempo de Experiência na área de TI	**Porcentagem**	**Quantidade de respostas**
A.1 a 3 anos	4,7%	3
B. 3 a 5 anos	3,1%	2
C. 5 a 10 anos	12,5%	8
D. 10 a 20 anos	40,6%	26
E. acima de 20 anos	39,1%	25
	TOTAL	**64**

As duas perguntas seguintes buscaram caracterizar genericamente as empresas e organizações quanto ao ramo de atuação e tamanho em termos de faturamento anual. Utilizou-se da divisão definida pelo BNDES (BNDES, 2012) para fins de porte das empresas e organizações pesquisadas.

A Tabela 4 demonstra uma maior concentração de respostas de empresas e organizações nos ramos do setor público (31,3%), serviços (26,6%) e manufatura (10,9%) entre os pesquisados.

Tabela 4. Ramo de atividade das empresa e organizações pesquisadas

3. Ramo de atividade da empresa em que trabalha	**Porcentagem**	**Quantidade de respostas**
A. educação	6,3%	4
B. financeiro	1,6%	1
C. manufatura	**10,9%**	7
D. saúde	6,3%	4
E. serviços	**26,6%**	17
F. setor público	**31,3%**	20
G. varejo	4,7%	3
H. Construção Civil	6,3%	4
I. Outros	6,3%	4
	TOTAL	**64**

Quanto ao porte das organizações e empresas aos quais os entrevistados atuam, a Tabela 5 mostra que houve um volume menor de respostas em empresas de médio-grande porte com faturamento anual entre R$90 e R$300 milhões.

Tabela 5. Porte das empresas e organizações pesquisadas pelo faturamento anual

4. Porte da empresa em que trabalha em termos de faturamento anual	**Porcentagem**	**Quantidade de respostas**
A. Pequena Empresa (entre R$ 2,4 milhões e R$ 16 milhões)	26,6%	17
B. Média Empresa (entre R$ 16 milhões e R$ 90 milhões)	31,3%	20
C. Média-Grande Empresa (entre R$ 90 milhões e R$ 300 milhões)	14,1%	9
D. Grande Empresa (acima de R$ 300 milhões)	28,1%	18
	TOTAL	**64**

6.2 Ocorrência de paradas não programadas em sistemas críticos, suas principais causas e impactos gerados aos negócios

De acorco com as respostas obtidas dos gestores de TI que participaram desta pesquisa, apenas 25% das empresas e organizações não apresentaram indisponibilidades não programadas em seus sistemas críticos de negócio nos últimos doze meses. Sendo assim, a grande maioria, ou seja, 75% dos pesquisados, respondeu que tiveram indisponibilidade(s) de sistemas críticos e algum tipo de impacto em suas operações de negócios nesse mesmo período, como ilustra a Figura 16.

Figura 16. Gráfico de Empresas e Organizações que registraram ou não indisponibilidades em seus sistemas críticos nos últimos doze meses.

Quanto a conhecer a causa de tais paradas não programadas, os gestores de TI pesquisados reportaram que: em 66,7% dos casos a falha ocorreu na infraestrutura, ou seja, nos *data centers*, equipamentos *(hardware)* ou sistemas operacionais, seguido de 14,7% de falhas da aplicação, 8,3% de erro humano ou falha operacional, 8,3% em falha de processos e em apenas 2,1%, a causa não foi identicada, conforme apresentado na Figura 17.

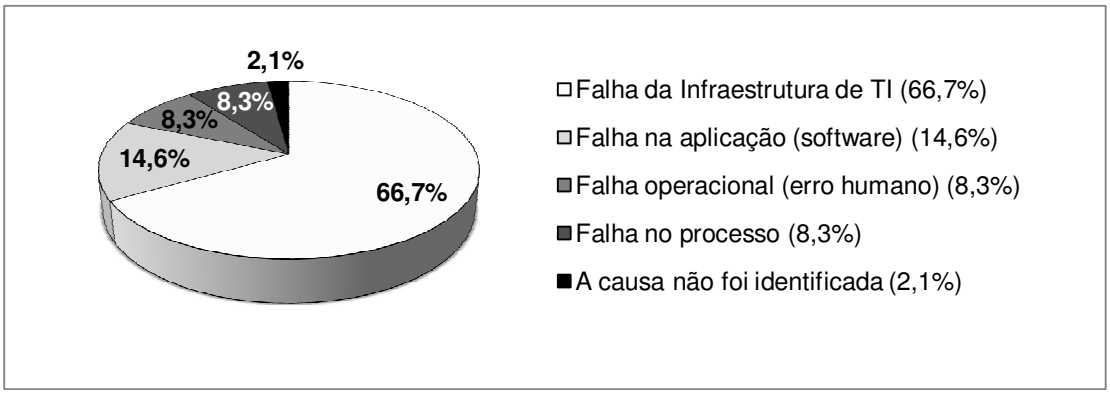

Figura 17. Causa das paradas não programadas em sistema críticos

Os resultados apresentados nesta pesquisa, em relação às causas das paradas não programadas demonstra uma tendência diferente ao estudo anterior apresentado pelo Gartner (WEYGANT, 2001). A pesquisa anterior, disposta na revisão da literatura, apontava apenas 20% das causas como relacionadas a falhas da tecnologia. Portanto, ao longo deste capítulo, haverá um aprofundamento das características destes sistemas computacionais localizados nesse Estado da região Nordeste, buscando identificar alguma informação relevante que possa justificar tal comportamento.

Referente ao impacto de negócios causado por essas paradas não programadas em sistemas críticos, segundo os gestores de TI responderam, 77,1% relataram que houve algum impacto nas operações de negócio sendo que em 12,5%, geraram perdas financeiras e inclusive impacto na imagem da empresa no mercado como ilustra o gráfico na Figura 18.

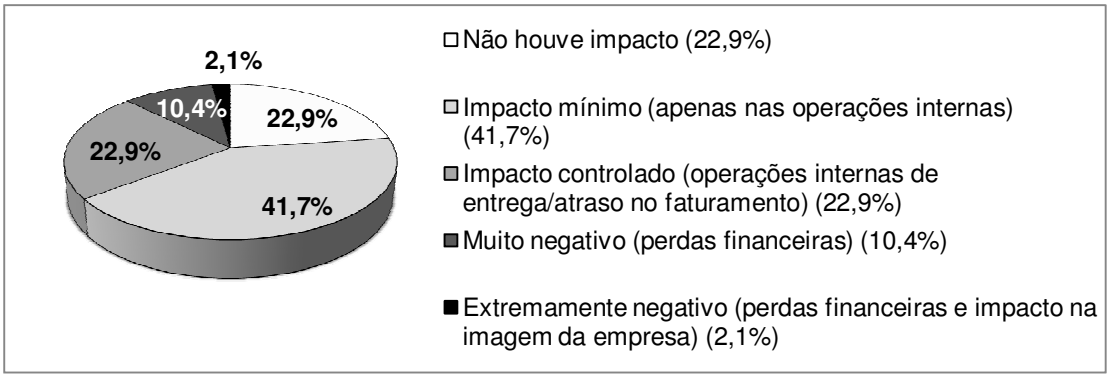

Figura 18. Impacto de negócios gerado pelas paradas não programadas

6.3 Quantidade de *downtimes* reportados e tempo de indisponibilidade

Conforme a quantidade de incidentes ao longo de um determinado período, no caso estudado, os últimos doze meses, pode passar à organização uma percepção negativa de instabilidade do ambiente de TI. O tempo total desses incidentes que geram paradas não programadas em sistemas críticos também é de extrema importância devido aos impactos associados com a continuidade dos negócios que normalmente tendem a ser maiores e acumulativos à medida que a parada não planejada se prolonga.

Desta forma, os gestores de TI foram questionados quanto a quantidade de paradas não programadas nos últimos doze meses, bem como quanto ao tempo total de indisponibilidade, considerando a soma de todos os eventos caso tenha ocorrido mais de um no período pesquisado.

A Tabela 6 apresenta o tempo de indisponibilidade reportado pelos pesquisados demonstrando que quase 48% dos incidentes são restabelecidos em até duas horas e a grande maioria, ou seja, próximo de 90% são resolvidos em até seis horas. Porém, houve o registro de 8,3% dos casos endereçados em até 12 horas e 2,1% gerando uma situação crítica de até 48 horas indisponível. Nenhum caso entre 12 e 24 horas de parada não programada foi reportado.

Tabela 6. Tempo de indisponibilidade dos sistemas críticos

Tempo de indisponibilidade dos sistemas e aplicações críticos ao negócio	**Respostas (%)**
até 02 horas	**47,9%**
entre 02 e 06 horas	**41,7%**
entre 06 e 12 horas	**8,3%**
entre 12 e 24 horas	0,0%
entre 24 e 48 horas	**2,1%**

O gráfico disposto na Figura 19 apresenta a quantidade de incidentes reportados pelas empresas que informaram a ocorrência de paradas não programadas nos últimos doze meses. Registros entre 2 e 4 eventos que representaram 18,8% das respostas ou acima de 4 eventos por ano (6,3% das respostas obtidas) podem ser considerados preocupantes, pois podem também impactar na credibilidade da equipe de TI frente a organização.

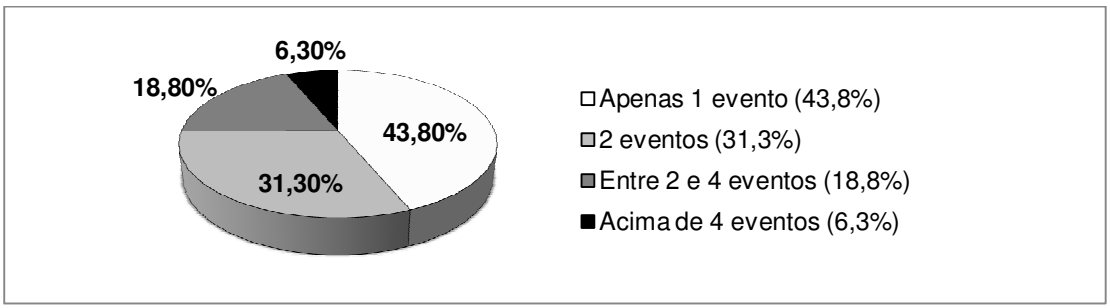

Figura 19. Quantidade de paradas não programadas registradas

6.4 Comparação entre empresas e organizações que reportaram e as que não reportaram paradas não programadas em sistemas críticos ao negócio

Com o objetivo de identificar possíveis características com relação a infraestrutura de TI implementada, ferramentas de monitoração, contratação de serviços de suporte com os fornecedores, investimentos em capacitação da equipe e adoção de guias de melhores práticas de governança e gerenciamento de TI, foi realizada uma comparação entre as empresas que reportaram paradas não programadas em seus sistemas críticos ao negócio com as empresas e organizações que não reportaram tais incidentes.

Inicialmente ambas as amostras foram comparadas quanto a distribuição por ramo de negócios e porte da organização em termos de faturamento anual, para fins de tornar válidos os resultados apresentados.

As Tabelas 7 e 8 desmontram que tanto as empresas que reportaram paradas quanto as que não reportaram indisponibilidades em seus sistemas críticos ao negócio tem uma distribuição semelhante, tanto em relação ao ramo de atividade, como em relação ao porte em termos de faturamento anual, permitindo considerar válida tal comparação e consequentemente os resultados obtidos.

Tabela 7. Comparação de ramo de atividade das empresas e organizações entre as que reportaram e as que não reportaram paradas não programadas

Porte da empresa ou organização em termos de faturamento anual	**Com registro paradas não programadas**	**Sem registro paradas não programadas**
Pequena Empresa (acima de R$2,4milhões e inferior a R$16milhões)	25,0%	31,3%
Média Empresa (acima de R$16milhões e inferior aR$90milhões)	33,3%	25,0%
Média - Grande Empresa (acima de R$90milhões e inferior aR$300milhões)	14,6%	12,5%
Grande Empresa (acima de R$300milhões)	27,1%	31,3%

Tabela 8. Comparação de ramo de atividade das empresas e organizações entre as que reportaram e as que não reportaram paradas não programadas

Ramo de atividade da empresa ou organização	Com registro paradas não programadas	Sem registro paradas não programadas
educação	8,3%	0,0%
financeiro	2,1%	0,0%
manufatura	**10,4%**	**12,5%**
saúde	6,3%	6,3%
serviços	**25,0%**	**31,3%**
setor público	**31,3%**	**31,3%**
varejo	4,2%	6,3%
construção civil	6,3%	6,3%
outros	6,3%	6,3%

6.4.1 Comparação quanto a infraestrutura implementada

Buscando aprofundar a análise estatística descritiva, com o objetivo de identificar potenciais motivos para um índice tão relevante de paradas não programadas em sistemas críticos relacionadas a falhas na infraestrutura de TI, comparou-se as empresas e organizações, entre as que não reportaram paradas com aquelas outras que reportaram paradas não programadas, quanto as respostas relacionadas à infraestrutura, no que tange a redundâncias de *hardware* nos servidores, sistemas configurados em *cluster* e redundâncias de *data centers*.

Com relação à redundância de componentes de *hardware* para proteção de falhas de componentes como ventiladores e fontes de alimentação bem como quanto a adoção da tecnologia RAID preservando a integridade dos dados quanto a falha de disco, ou seja, dentro Nível 2 de Disponibilidade descrito por Zhu *et al.* (2009), 62,5% dos pesquisados que não reportaram indisponibilidades relataram que todos os seus sistemas críticos dispõem de tais características de redundância de *hardware*. Contudo, apenas 35,2% dos gestores de TI que reportaram paradas não programadas responderam que todos

os sistemas críticos ao negócio tem estas características, ou seja, quase duas vezes menor como ilustra o gráfico disposto na Figura 20.

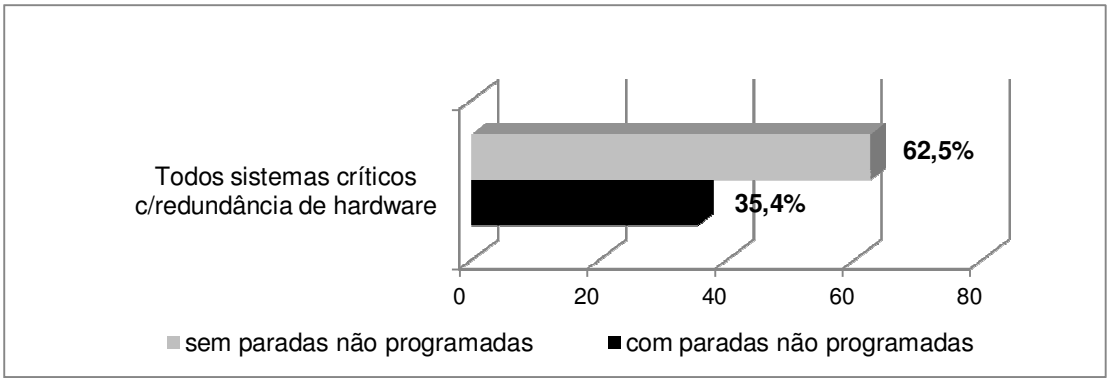

Figura 20. Comparação quanto as características de redundância de *hardware* entre as empresas que reportaram e as que não reportaram paradas não programadas

Diante deste cenário, quanto a esses sistemas que não dispõem de redundância de componentes de *hardware*, a simples falha de uma fonte de alimentação desligará o servidor e consequentemente causará uma parada não programada em um sistema crítico ao negócio dessa organização. Tratando-se de falha em disco, o impacto é ainda maior pois, sem a tecnologia RAID ou espelhamento de discos por *software*, a falha de um disco rígido, além de causar a indisponibilidade, ainda requer a restauração dos dados via cópia de segurança, tendendo a aumentar ainda mais o tempo de reparo e restabelecimento do sistema.

Quanto a configuração dos sistemas críticos em *cluster,* que permite a rápida migração da aplicação entre servidores via processo de *failover,* em caso de falha de um servidor por completo, mantendo a disponibilidade da aplicação em outro servidor remanescente que compõe o *cluster*, as respostas demonstraram uma discrepância ainda maior que o dobro. Apenas 12,5% dos gestores de TI das empresas e organizações que apresentaram paradas não programadas responderam que todos os sistemas críticos estão configurados em *cluster,* enquanto 31,3% dos gestores de TI que não reportaram paradas responderam que os sistemas críticos contém tal característica, como demonstra a Figura 21. Essa característica engloba o Nível 3 de Disponibilidade descrito por Zhu *et al.* (2009).

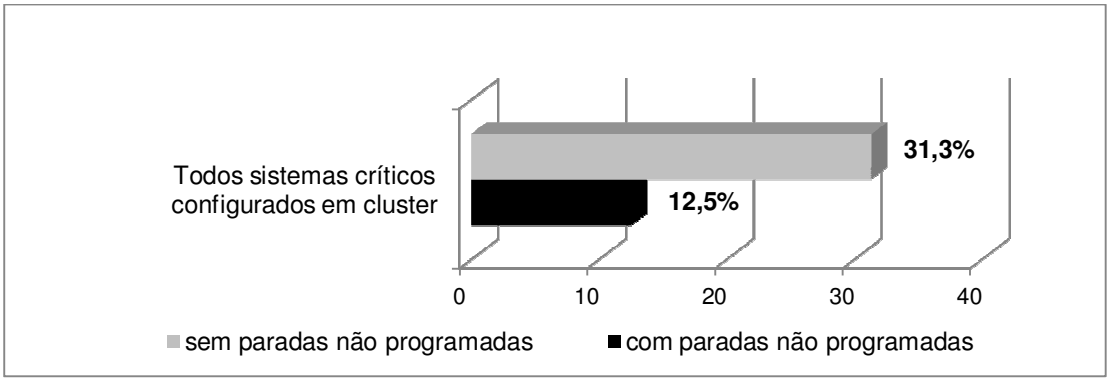

Figura 21. Comparação quanto as características de redundância de sistemas *(cluster)* entre as empresas que reportaram e as que não reportaram paradas não programadas

Referente à característica de *data centers* reduntantes, isto é, sistemas críticos replicados em dois ambientes físicos distintos, permitindo a funcionalidade de *disaster recovery* contidas no Nível 4 de Disponibilidade (replicação de dados) e Nível 5 (*disaster recovery*) segundo Zhu *et al.* (2009), 25% dos pesquisados que não reportaram paradas responderam que todos seus sistemas críticos estão replicados em dois *data centers.* Porém, somente 10% dos gestores de TI que responderam a pesquisa e relataram paradas não programadas informaram que todos os seus sistemas críticos tem essa característica, estando replicados em *data centers* distintos, como apresentado na Figura 22.

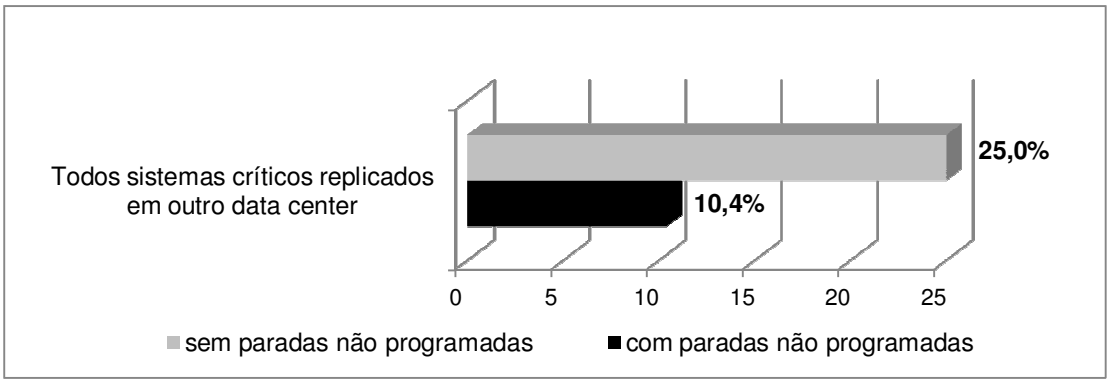

Figura 22. Comparação quanto as características de replicação de *data centers (disaster recovery)* entre as empresas que reportaram e as que não reportaram paradas não programadas

As diferenças substanciais nas características de infraestrutura de TI, principalmente no que tange a falta de redundâncias de *hardware* e configuração em *cluster* dos sistemas críticos nas empresas e organizações que reportaram

paradas não programadas, quando comparadas as empresas e organizações que apresentaram esses incidentes de indisponibilidade, podem claramente justificar a falha da infraestrutura de TI como principal causa das paradas não programadas.

6.4.2 Comparação quanto a adoção de ferramentas de monitoração

Dando sequência à comparação entre as respostas obtidas com os gestores que reportaram paradas não programadas e os que não reportaram esses eventos nas empresas e organizações aos quais fazem parte, buscou-se avaliar a amostra quanto à existência de ferramentas de gerenciamento e monitoração instaladas e configuradas em sua infraestrutura de TI, visando a monitoração dos dispositivos de rede, servidores, *storages*, sistemas e aplicações críticas, bem como alguma relação com o fato de haver ou não o registro de indisponibilidades críticas.

De acordo com as respostas dos gestores, ambas as categorias relataram que apenas entre 25,1% e 35,4% adotam ferramentas de gerenciamento de falhas e desempenho em toda a infraestrutura de TI como ilustrado na Figura 23. E uma porcentagem ainda menor das duas categorias, entre 6,3% e 14,6%, tem implementadas ferramentas avançadas de gerenciamento monitorando pró-ativamente a disponibilidade e desempenho das aplicações atreladas à continuidade do negócio.

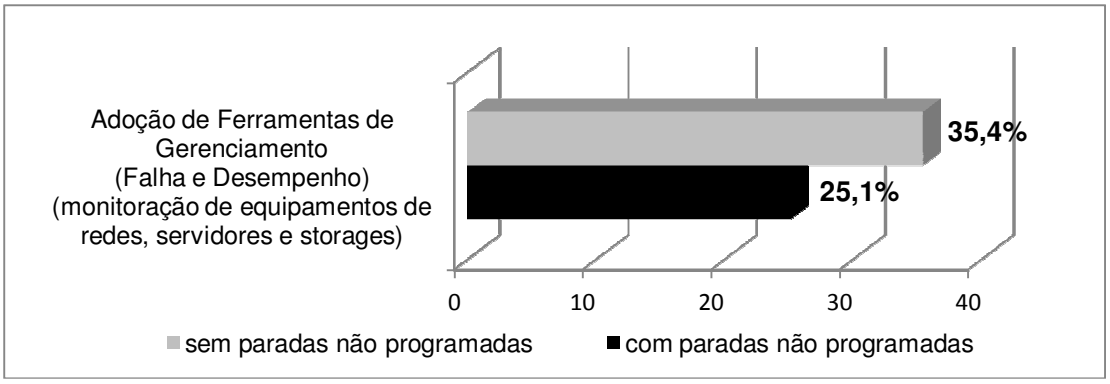

Figura 23. Comparação quanto a adoção de ferramentas de monitoração e gerenciamento entre as empresas que reportaram e as que não reportaram paradas não programadas

Assim, com base nos dados analisados, onde tanto as empresas e organizações que adotam ferramentas de gerenciamento e monitoração como as que não adotam tem relatos de paradas não programadas, percebe-se que apenas a adoção de tais ferramentas pode não ser suficiente para evitar que indisponibilidades não planejadas em sistemas críticos ao negócio ocorram.

Entretanto, a análise comparativa a ser apresentada na Tabela 10 da seção 6.5 deste capítulo, referente à relação entre a adoção de ferramentas de monitoração da infraestrutura de TI e a duração das paradas não programadas aponta que, embora tais ferramentas não evitem a indisponibilidade dos sistemas, contribuem significativamente como instrumento de apoio à equipe técnica no endereçamento de forma mais rápida do problema apresentado e restabelecimento do sistema, reduzindo o tempo total da parada não programada em sistemas críticos ao negócio. Portanto, mantendo-se como uma boa prática a ser avaliada e adotada pela gestão de TI de empresas e organizações.

6.4.3 Comparação quanto a contratação de serviços de suporte com os fornecedores da infraestrutura de TI

Novamente foram confrontadas as respostas dos gestores de TI entre os dois grupos, ou seja, os que reportaram indisponibilidades não planejadas nos sistemas críticos com aqueles que não o fizeram, buscando agora a relação entre os níveis de serviços de suporte e assistência técnica contratados com os fornecedores da solução de infraestrutura de TI e sua possível influência em evitar que problemas aconteçam.

Conforme as demais perguntas do questionário, existem cinco opções de resposta, sendo elas:

a) Apenas a garantia padrão dos equipamentos com atendimento 9x5 (horário comercial);

b) Adota contratos de suporte dos equipamentos prevendo o atendimento 24x7 incluindo finais de semana e feriados;

c) Além do suporte 24x7 para os equipamentos, mantém contrato de suporte com os fornecedores do sistema operacional e aplicações também em regime 24x7, ou seja, suporte de *hardware* e *software* 24x7;

d) Além do suporte de *software* 24x7 com os fornecedores do sistema operacional e aplicações, mantém um contrato de suporte 24x7 com os fornecedores dos equipamentos prevendo SLA com um prazo de solução do problema normalmente de 4, 6 ou 12 horas para o *hardware*;

e) Em complemento aos contratos de suporte 24x7 para *hardware* prevendo SLA com um prazo de solução e suporte de *software* 24x7, também contempla um serviço diferenciado de Missão Crítica com atualizações pró-ativas do ambiente, geração de relatórios de cumprimento de métricas e equipe dedicada para o atendimeto de suporte e gerenciamento da conta.

Essa última opção corresponde aos serviços chamados de Missão Crítica que além do atendimento reativo 24x7, também revisam periodicamente os equipamentos e sistemas e aplicam preventivamente atualizações de *firmwares* e *softwares* evitando a ocorrência de problemas já conhecidos pelos fabricantes e, consequentemente, contribuindo para a redução de falhas na infraestrutura e aplicações.

Os termos 9x5 e 24x7 definem quantas horas por dia o serviço está disponível, ou seja, 9x5 representa nove horas por dia (normalmente entre 08:00 horas da manhã e 17:00hs) e cinco dias por semana (de 2ªfeira a 6ªfeira) resumidamente, o horário comercial. Já 24x7 representa um serviço ininterrupto disponível 24 horas por dia ao longo dos sete dias da semana, ou seja, de 2ªfeira à domingo, incluindo feriados.

A avaliação se deu comparando as respostas às opções “D” e “E”, ou seja, os níveis de serviços que preveem em SLA tempos de solução a serem cumpridos bem como ações pró-ativas e de monitoração do ambiente entre os dois grupos de pesquisados que reportaram interrupções nos sistemas críticos e

que não as fizeram. A Figura 24 ilustra o resultado obtido, onde 43,8% das empresas que não reportaram paradas tem esses serviços diferenciados contratados com seus fornecedores e apenas 25% das empresas que apresentaram problemas os tem.

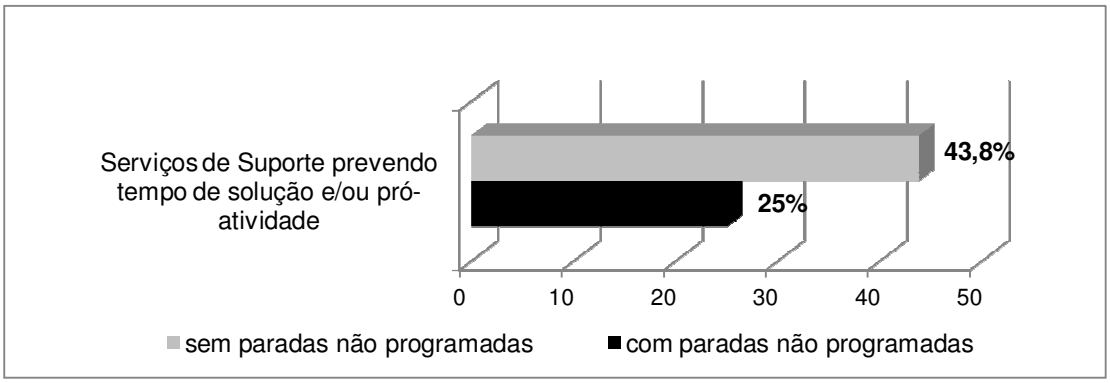

Figura 24. Comparação quanto aos serviços de suporte contratados entre as empresas que reportaram e as que não reportaram paradas não programadas

Como complemento, a eficácia da contratação de serviços de suporte e assistência técnica contemplando SLA para solução dos problemas, bem como serviços pró-ativos, também será demonstrada na seção 6.5 Tabela 10 deste capítulo quando poderá ser observado que em 100% dos casos reportados na pesquisa onde ocorreram indisponibilidades e a empresa ou organização possuia um contrato diferenciado com o fornecedor, esses incidentes foram solucionados em até 06 horas mais precisamente 42% dos eventos em até duas horas e 58% entre 02 e 06 horas, conforme apresentado na Figura 25.

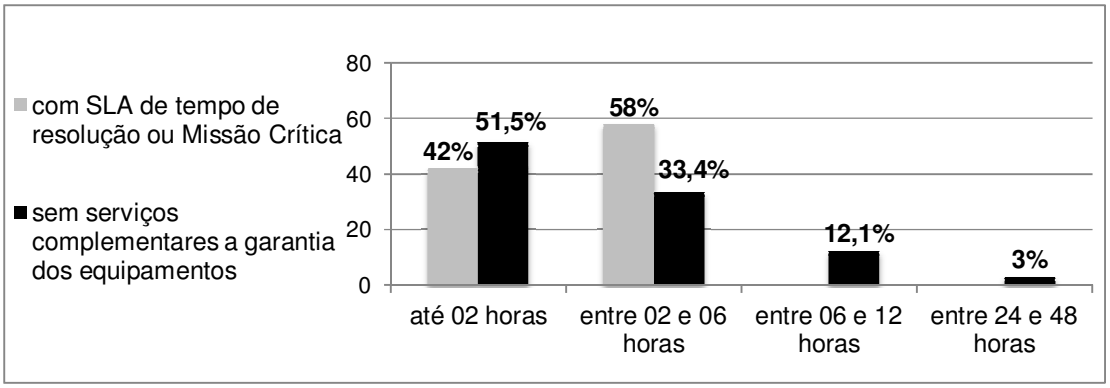

Figura 25. Comparação quanto aos serviços de suporte contratados entre as empresas que reportaram e as que não reportaram paradas não programadas

6.4.4 Comparação quanto os investimentos em treinamento e capacitação da equipe de TI

Referente aos investimentos em treinamento e capacitação da equipe da área de TI, os gestores tiveram as seguintes opções de resposta quando perguntados:

a) Não há investimento direto em treinamento deixando a cargo de cada profissional o seu próprio desenvolvimento;

b) Minimiza o investimento em treinamento incentivando a participação em treinamentos remotos (ensino a distância) e fora do horário de trabalho;

c) Há investimento em treinamentos remotos (ensino a distância) para toda a equipe e definição de pontos focais para participarem de treinamentos em sala dos próprios fornecedores da tecnologia e posteriormente compartilha o conhecimento com os demais colegas internamente na empresa

d) Há investimentos anuais pré-estabelecidos em treinamentos possibilitando a participação dos principais membros da equipe em treinamentos formais em sala e ensino a distância a todos;

e) Além de investimentos anuais pré-estabelecidos em treinamento também há uma política mínima de horas de treinamento anuais para cada membro da equipe possibilitando treinamentos formais em sala mesmo que incluam despesas de viagem e hospedagem.

Utilizando a mesma aborgadem, ou seja, comparando o resultado das respostas nas opções “D” e “E” (onde há maior investimento em treinamento da equipe) 43,8% dos gestores de TI de empresas e organizações que reportaram paradas não programadas informaram que investem consideravelmente na capacitação da equipe selecionando as opções “D” e “E” para esta pergunta. Já 35,5% dos pesquisados que reportaram paradas não programadas em seus

sistemas críticos ao negócio selecionaram essas mesmas opções de resposta. O gráfico disposto na Figura 26 ilustra o resultado dessa comparação.

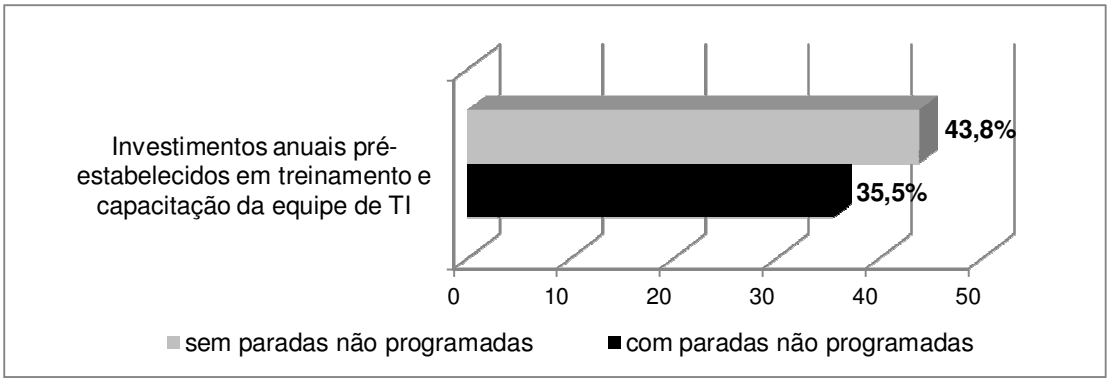

Figura 26. Comparação quanto aos investimentos em treinamento da equipe de TI entre as empresas que reportaram e as que não reportaram paradas não programadas

Embora a diferença não tenha sido substancial demonstrando que permanecem ocorrendo paradas não programadas mesmo em empresas que possuem investimentos anuais pré-estabelecidos em treinamento da equipe na área de TI, a avaliação quanto ao tempo de indisponibilidade, demonstra que equipes onde existem investimentos em treinamento e capacitação detém as habilidades necessárias para restabelecer os ambientes em menor tempo. A Figura 27 ilustra essa situação, demonstrando que empresas e organizações que investem em treinamento tem a capacidade de restabelecer os incidentes de paradas não programadas em 65% dos casos em até duas horas enquanto apenas 30% desses incidentes são restabelecidos no mesmo prazo em empresas que não investem em treinamento.

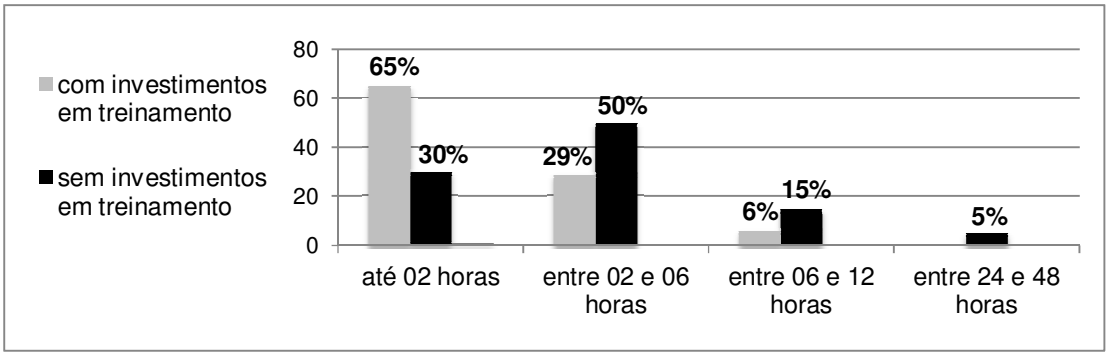

Figura 27. Comparação quanto ao investimento em treinamentoe a capacidade de restabelecer os sistemas críticos após a ocorrência de uma indisponibilidade

6.4.5 Comparação quanto a adoção de guias de melhores práticas de Governança e Gerenciamento de TI

Seguindo a análise comparativa entre os grupos de gestores que reportaram paradas não programadas nos sistemas críticos ao negócio e os que não reportaram, avaliou-se também quanto a adoção de guias de melhores práticas de Governança e Gerenciamento de TI como COBIT e ITIL na gestão de processos e serviços.

De acordo com as respostas de ambos grupos com relação à adoção de melhores práticas de Governança e Gerenciamento de TI, apenas 14,6% dos entrevistados que reportaram indisponibilidades nos últimos doze meses demonstraram um maior grau de maturidade estando em fase final de implementação do ITIL ou COBIT ou implementado há mais de dois anos, enquanto que 31,3% das empresas que não reportaram tais incidentes nos sistemas críticos tem o mesmo nível de maturidade em melhores práticas de TI conforme apresenta a Figura 28.

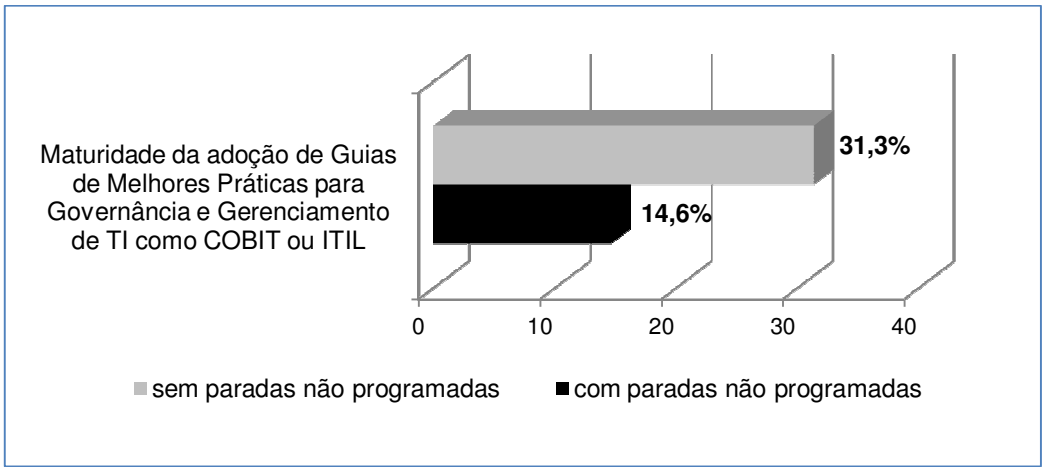

Figura 28. Comparação quanto a adoção e maturidade de Guias de Melhores Práticas de TI entre as empresas que reportaram e não reportaram *unplanned downtimes*

Considerando o posicionamento de apenas terem ou não terem adotado melhores práticas de Governança e Gerenciamento de TI, ou seja, sem considerar o grau de maturidade dos processos de controle e serviços de TI sendo providos, a diferença aponta que: enquanto 56,3% das empresas e organizações que não reportaram paradas não programadas já adotoram o ITIL,

COBIT ou *framework* semelhante para melhorar seus processos e serviços, a mesma proporção, ou seja, 56,3% das empresas que reportaram incidentes nos sistemas críticos ainda não os adotaram.

Desta forma, apenas adotar tais guias de melhores práticas não é fator preponderante para não haver mais incidentes. Contudo, a maturidade dos processos e serviços obtidas ao longo da melhoria contínua e aprendizado dispostos no ciclo de vida do serviço do ITIL (OGC, 2010) tendem a apresentar melhores resultados após efetivamente terem sido implementados.

6.5 Comparação entre foco de investimento em cada um dos P's (produtos, parceiros, pessoas e processos) na área de TI e resultados com relação a paradas não programadas e tempo de indisponibilidade

Como complemento à comparação entre as empresas e organizações que reportaram paradas não programadas com as que não a fizeram, foi efetuada uma comparação em termos de foco de investimento na área de TI, considerando como variáveis fixas os quatro P's descritos no guia de melhores práticas do gerenciamento de TI ITIL, ou seja: em produtos que englobam a infraestrutura composta de *data centers*, equipamentos sistemas operacionais e ferramentas de monitoração; em parceiros quanto a contratação de níveis de serviço de suporte e assistência técnica diferenciados além da garantia padrão dos produtos com os fornecedores; em pessoas no que tange treinamento e investimento em preparação e certificação dos profissionais da área de TI; e em processos relacionando à adoção de guias de melhores práticas de TI.

O objetivo foi correlacionar o foco de investimentos com os demais quadrantes dos quatro P's e, principalmente, os resultados obtidos quanto a evitar paradas não programadas, quantidade de incidentes reportados, tempo de indisponibilidade, impactos gerados nos negócios e identificação de causa destes eventos críticos.

A Tabela 9 apresenta a comparação entre os focos de investimentos na área de TI correlacionando-os entre os quatro P's. Foram considerados o

melhor cenário, ou seja, respostas das questões selecionando as opções “D” e “E” para cada P sendo que no foco produto, consideraram-se apenas os investimentos em redundância de *hardware* e sistemas em cluster (*failover*) permitindo uma melhor comparação entre empresas pequenas, médias, média-grandes e grandes devido sua possível capacidade de investimentos em TI. Utilizou-se da álgebra boolena criando filtros para as questões 5 e 6 (produto) e depois isoladamente, para as questões 9 (parceiros), 10 (pessoas) e 12 (processos) com uma porta OR entre as respostas com as opções “D” e “E” para obter os dados de cada um dos P’s de forma isolada.

Tabela 9. Comparação entre os Focos de Investimentos na Área de TI

Foco	**Produto**	**Parceiros**	**Pessoas**	**Processo**
Quantidade de Respostas	26	19	24	12
Questão 5. Redundância de *Hardware* (Produto)				
D. Grande parte dos sistemas críticos	34,60%	36,80%	45,80%	58,30%
E. Todos os sistemas críticos	65,40%	57,90%	41,70%	41,70%
Total: D + E	**100,00%**	**94,70%**	**87,50%**	**100,00%**
Questão 6. *Failover* (*software* de *cluster*) (Produto)				
D. Grande parte dos sistemas críticos	57,70%	36,80%	33,30%	33,30%
E. Todos os sistemas críticos	42,30%	31,60%	20,80%	41,70%
Total: D + E	**100,00%**	**68,40%**	**54,10%**	**75,00%**
Questão 7. Replicação/*Disaster Recovery*				
D. Grande parte dos sistemas críticos	23,10%	21,10%	16,70%	25,00%
E. Todos os sistemas críticos	26,90%	26,30%	20,80%	33,30%
Total: D + E	**50,00%**	**47,40%**	**37,50%**	**58,30%**
Questão 8. Ferramentas de Monitoração				
D. Gerenciamento Falhas e Desempenho de todos equipamentos críticos	38,50%	42,10%	33,30%	50,00%
E.Avançada gerenciando disponibilidade e desempenho das aplicações	23,10%	26,30%	12,50%	25,00%
Total: D + E	**61,60%**	**68,40%**	**45,80%**	**75,00%**

Tabela 9. Comparação entre os Focos de Investimentos na Área de TI (continuação)

Foco	Produto	Parceiros	Pessoas	Processo
Questão 9. Serviços e Suporte (Parceiros)				
D. 24x7 SW e 24x7 HW c/ SLA de solução	30,80%	68,40%	33,30%	41,70%
E. Missão Crítica (pró-atividade)	19,20%	31,60%	25%	50,00%
Total: D + E	**50,00%**	**100,00%**	**58,30%**	**91,70%**
Questão 10. Investimentos anuais pré-estabelecidos em treinamento (Pessoas)				
D. Principais membros da equipe	38,50%	52,60%	83,30%	58,30%
E. Para toda a área	11,50%	21,10%	16,70%	25,00%
Total: D + E	**50,00%**	**73,70%**	**100,00%**	**83,30%**
Questão 11. Incentivo a obtenção de certificações (Pessoas)				
D. Contém profissionais certificados e incentiva cobrindo as despesas	**26,90%**	31,60%	33,30%	33,30%
E. Muitos profissionais certificados e exige a certificação cobrindo despesas	**11,50%**	15,80%	12,50%	33,30%
Total: D + E	**38,40%**	**47,40%**	**45,80%**	**66,60%**
Questão 12. Adoção de melhores práticas de TI (Processos)				
D. Fase final de implementação	26,90%	42,10%	29,20%	66,70%
E. Implementado há mais 2 anos	7,70%	15,80%	12,50%	33,30%
Total: D + E	**34,60%**	**57,90%**	**41,70%**	**100%**
Questão 13. Maturidade dos Processos (adoção de SLA e SLM) (Processos)				
D. SLAs definidos com clientes da TI	15,40%	31,60%	29,80%	50,00%
E. SLM para medir e controlar os SLAs	23,10%	26,30%	20,80%	41,70%
Total: D + E	**38,50%**	**57,90%**	**50,60%**	**91,70%**

Com a análise comparativa desses dados estatísticos, pode-se perceber que quando o foco está em produto, ou seja, investimentos na infraestrutura, há um foco consideravelmente menor nos demais investimentos em pessoas, parceiros e processos quando comparados com os demais focos da área de TI.

Quando o foco está em parceiros ou pessoas, ou seja, contratação de serviços de suporte diferenciados e capacitação e treinamento da equipe da área de Tecnologia da Informação, os investimentos são melhores balanceados entre os outros quadrantes.

Entretanto, quando os investimentos estão focados em processos, ou seja, na adoção de guias de melhores práticas de Governança e Gerenciamento de TI como COBIT, ITIL ou semelhantes, a distribuição dos investimentos nos quatro quadrantes, além de tornar-se mais equilibrada, é maior em todos os quatro P's, inclusive na melhora da própria infraestrutura (quadrante produto) com mais sistemas críticos em *cluster* e replicados e configurados em *disaster recovery,* bem como a implementação de ferramentas de gerenciamento e monitoração da infraestrutura.

A análise comparativa também aponta que os serviços de suporte estão mais adequados com o nível de criticidade e impacto que sistemas críticos ao negócio requerem, ou seja, com SLAs prevendo prazos de solução pré-estabelecidos e a maior porcentagem de serviços de Missão Crítica contratados quando o foco está em investir em melhores práticas de TI.

O mesmo ocorre no maior investimento em capacitação e treinamento da equipe de TI, ou seja, nas pessoas demonstrando também foco na qualificação e certificação dos colaboradores quando o foco está em melhores práticas de TI.

Após a análise comparativa correlacionando os investimentos nos quatro quadrantes, produtos, parceiros, pessoas e processos, buscou-se avaliar os resultados obtidos em cada foco de atenção das empresas e organizações pesquisadas em relação a ocorrência de paradas não programadas, tempo de indisponibilidade e impactos as operações e negócios, conforme descreve a Tabela 10.

Tabela 10. Resultados obtidos com a comparação entre os Focos de Investimentos na Área de TI

Foco	**Produto**	**Parceiros**	**Pessoas**	**Processo**
Quantidade de Respostas	26	19	24	12
Questão 14. Registro de Paradas não programadas nos últimos 12 meses	**76,90%**	**63,20%**	**70,80%**	**58,30%**
Questão 14a. Quantidade de paradas não programadas				
B. Apenas um evento	45%	41,70%	41,20%	17%
C. 2 eventos	35%	25%	35,30%	50,00%
D. Entre 2 e 4 eventos	15%	33,30%	23,50%	33%
E. Acima de 4 eventos	5%	0%	0%	0,00%

Tabela 10. Resultados obtidos com a comparação entre os Focos de Investimentos na Área de TI (continuação)

Foco	Produto	Parceiros	Pessoas	Processo
Questão 15. Tempo de indisponibilidade				
A. até 2 horas	55%	41,70%	64,70%	28,60%
B. entre 2 e 6 horas	40%	58,30%	29,40%	71,40%
C. entre 6 e 12 horas	5%	0%	5,90%	0%
D. entre 12 e 24 horas	0%	0%	0%	0%
E. entre 24 e 48 horas	0%	0%	0%	0%
Questão 16. Impacto nos negócios				
A. não houve impacto	20%	8,30%	5,90%	0%
B. impacto mínimo	45%	33,30%	41,20%	14,30%
C. Impacto controlado (atrasos)	25%	50%	41,20%	85,70%
D. Muito negativo (perdas)	10%	0%	11,80%	0%
E. Extremo (perdas e impacto imagem)	0%	8,30%	0%	0%
Questão 17. Causa das Paradas				
A. Não identificada	5%	8,30%	5,90%	0%
B. Infraestrutura	60%	66,70%	52,90%	57,10%
C. Aplicação	5%	0%	17,60%	14,30%
D. Erro Humano	15%	8,30%	11,80%	0%
E. Processo	15%	16,70%	11,80%	28,60%

Os resultados comprovam os benefícios das adoção de guias de melhores práticas de Governança e Gerenciamento de TI, reduzindo em 22,3% o registro de paradas não programadas considerando que a amostra total registrou 75% destes incidentes e a amostra com a adoção de melhores práticas em fase final de implantação ou já implementados há mais de dois anos registrou apenas 58,3%.

Outros três pontos importantes identificados foram: 100% dos incidentes foram endereçados entre duas e seis horas sem que houvesse impactos muito negativos ou extremos ao negócio, bem como todos os incidentes tiveram sua causa identificada como responderam os participantes do *survey*.

Este terceiro ponto reintera o benefício atribuído aos guias de melhores práticas de TI quanto à melhoria contínua dos processos de serviço de TI e lições aprendidas tendo como importante entrada, através do gerenciamento de problemas, em apontar as causas dos incidentes visando evitar reocorrências.

A amostra também aponta que não houve registros de erro operacional ou falha humana nas empresas que investem na adoção de guias de melhores práticas de Governança e Gerenciamento de TI.

Quanto ao registro de falhas de processos como causa das paradas não programadas registradas, mesmo em empresas e organizações que relatam a adoção de guias de melhores práticas, embora não existem dados complementares para uma análise mais aprofundada, sugere-se que devido ao controle, monitoramento e medição aplicados pelo ITIL e COBIT, também é possível identificar falhas de processos com maior clareza diferentemente de empresas que não possuem tais processos adequadamente desenhados e em uso pela área de TI.

Este estudo não visou apenas a análise pontual dos dados no presente mas também buscou obter dados para estimar a visão de futuro das organizações e empresas pesquisadas com base nas respostas dos gestores de TI que participaram desta enquete.

Com uma pergunta quanto a porcentagem de investimentos na relação produtos e serviços tomando por base levantamento do IDC apontando que no Brasil em 2012 os investimentos em TI tendem a uma proporção 67% entre produtos (*hardware e software*) e 33% para serviços (IDC, 2011 *apud* SUCESU-MG, 2012), foram avaliados os investimentos planejados para os próximos 12 meses.

Uma segunda pergunta neste contexto também foi aplicada buscando mensurar como será distribuído esse investimento em serviços, ou seja, se mais voltado apenas para os serviços de suporte e assistência técnica ou se haverá uma maior parcela em investimentos em implantação de ferramentas de gerenciamento, treinamento e capacitação da equipe da área de Tecnologia da Informação e adoção de guias de melhores práticas de governança e gerenciamento de TI. A Tabela 11 demonstra os resultados.

Tabela 11. Investimentos nos próximos 12 meses na área de TI

Investimentos Futuros na área de TI (próximos 12 meses):				
Foco	**Produto**	**Parceiros**	**Pessoas**	**Processo**
Questão 18. Proporção de Investimentos entre Produtos e Serviços da área de TI				
D. 70%/30% produtos e serviços	30,80%	31,60%	45,80%	50,00%
E. 60%/40% produtos e serviços	42,30%	47,40%	37,50%	33,30%
D. 70%/30% produtos e serviços (total geral)	31,30%			
E. 60%/40% produtos e serviços (total geral)	35,90%			
Questão 19. Distribuição dos investimentos em Serviços da área de TI				
D. 50%/50% suporte e treinamento/melhores práticas de TI	19,20%	21,10%	25%	16,70%
E. 33%/66% suporte e treinamento/melhores práticas de TI	11,50%	10,50%	8,30%	8,30%
D. 50%/50% suporte e treinamento/melhores práticas de TI (total geral)	15,60%			
E. 33%/66% suporte e treinamento/melhores práticas de TI (total geral)	7,80%			
Questão 12. opção C – Adoção de Melhores Práticas de Governança e Gerenciamento de TI				
Embora não adote, entende ser importante adotar	90,00%	100%	85,70%	N/A
Considerando todas as respostas do *survey* que ainda não adotaram mas entendem ser importante adotar (total geral)	67,60%			

A Tabela 11 demonstra que segundo os gestores respondentes, cerca de um terço das empresas e organizações espera investir na proporção de 60% em produtos (*hardware e software*) e outros 40% em serviços enquanto outro terço dos pesquisados pretende investir em TI na proporção de 70% em produtos e 30% em serviços, ou seja, quase 70% dentro da média de investimentos em TI brasileira esperada com base nos números informados pelo IDC (SUCESU-MG, 2012).

Outro ponto significativo apontado na pesquisa, é que os gestores de TI de organizações que ainda não investiram em guias de melhores práticas de TI entendem a importância de tal direcionamento e as respostas à questão 19,

também disposta na Tabela 11, confirma que estima-se investimentos maiores em capacitação e treinamento bem como em adoção de guias de melhores práticas de Governança e Gerenciamento de TI nas organizações que ainda não o fizeram.

6.6 Resultados gerais do *survey* quanto a investimentos em produtos (infraestrutura), parceiros(serviços), pessoas e processos

Como complemento a visão de investimentos futuros obtida com a análise das questões 18 e 19, buscou-se analisar os resultados das respostas às questões 5, 6 e 7, referente à infraestrutura (produtos), questão 9, sobre os atuais níveis de serviço contratados com os fornecedores para suportar os sistemas críticos ao negócio (parceiros), questão 10 que aponta os atuais investimentos em capacitação e treinamento das pessoas da área de TI e questão 12 sobre a adoção de guias de melhores práticas de Governança e Gerenciamento de TI (processos) buscando um maior alinhamento estratégico entre os objetivos da organização e os objetivos da área de TI e consequentemente a melhora dos serviços prestados pela área de Tecnologia da Informação.

A Figura 29 apresenta os resultados quanto a atual configuração da infraestrutura de TI das empresas e organizações pesquisadas.

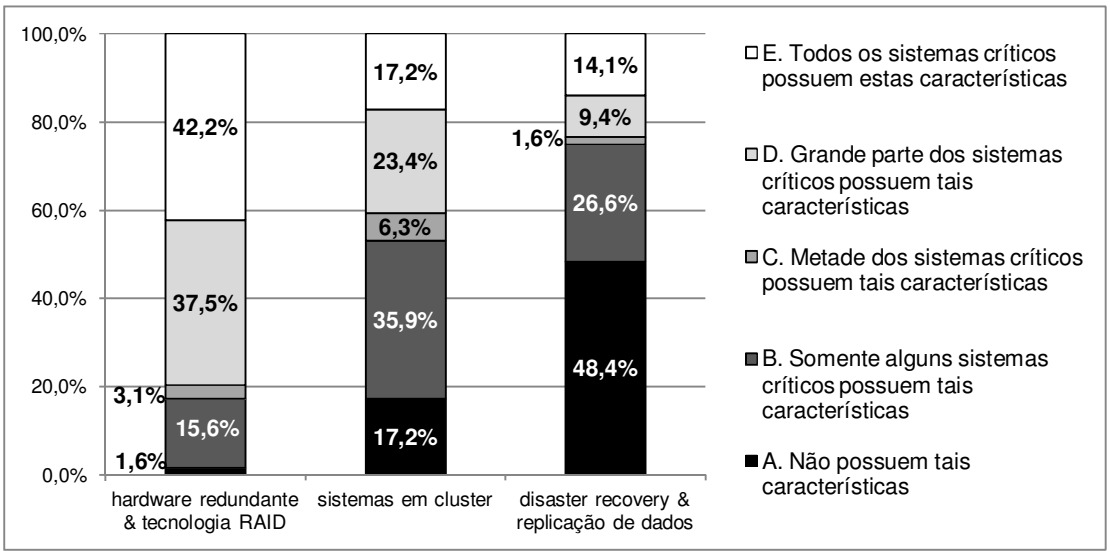

Figura 29. Investimentos em Infraestrutura de TI (Produtos)

Quanto as atuais características da infraestrutura de TI dos sistemas críticos ao negócio, a Figura 30 demonstra os resultados quanto a componentes de *hardware* redundantes representados no gráfico por HW, configuração em *cluster* descritos como *Cluster* no gráfico e *Disaster Recovery* ou replicação de *data centers* representados no gráfico como DR. Com base na análise da Figura 30, as empresas de grande porte demonstram um maior investimento em tecnologias para prover alta disponibilidade a estes sistemas críticos.

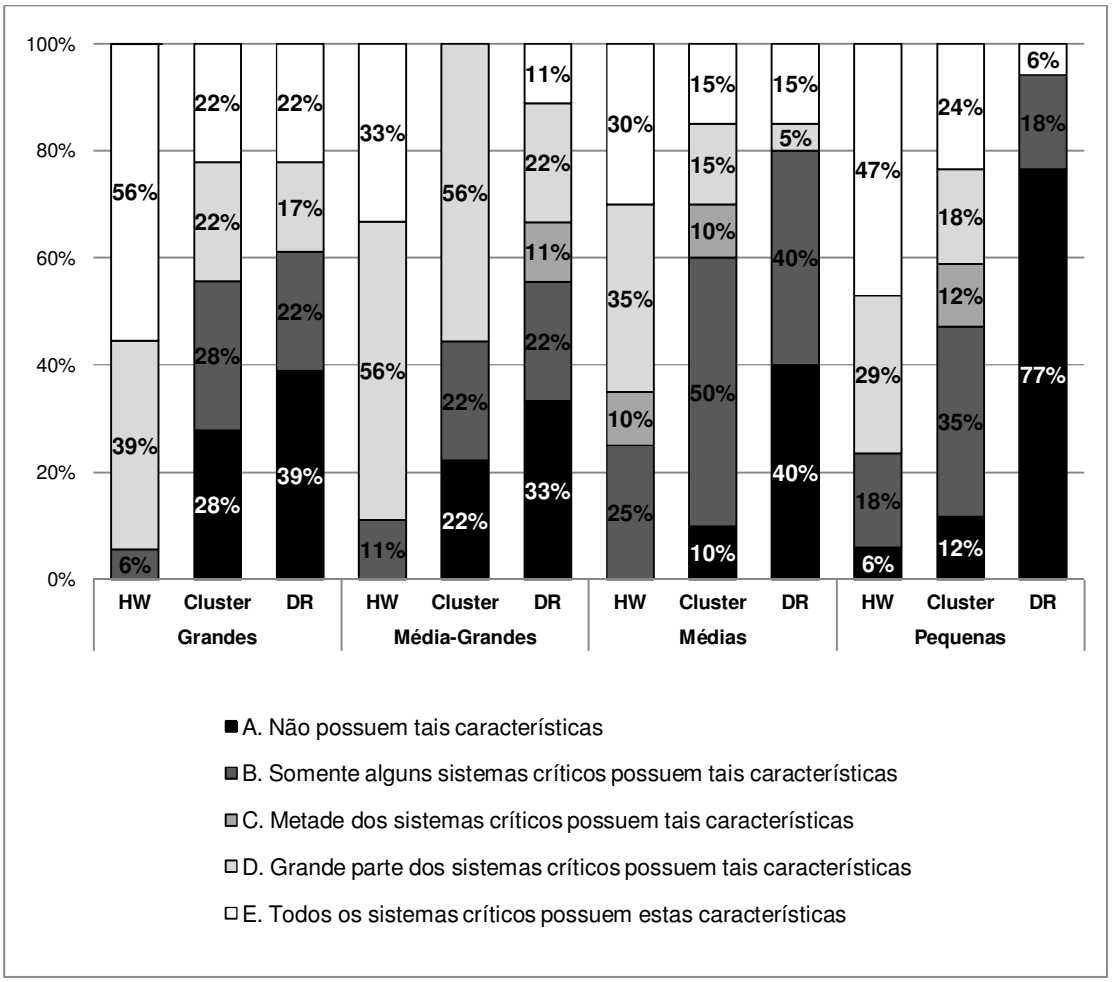

Figura 30. Investimentos em Infraestrutura de TI (Produtos) conforme porte da empresa ou organização pesquisada

Com relação ao nível de serviço contratado com os fabricantes, a Figura 30 ilustra graficamente que a grande maioria dos respondentes ao *survey* apontou que possuem apenas a garantia padrão dos equipamentos ou no máximo suporte 24x7 ao hardware dos equipamentos, sem garantias de prazos de solução dos problemas descrito em contrato, nem tão pouco o auxílio dos

fornecedores na adoção de suporte pró-atividade, visando evitar a ocorrência de problemas conhecidos.

A Figura 31 também demonstra que apenas 9,4% dos gestores de TI pesquisados apontaram que suas empresas e organizações tem serviços de suporte Missão Crítica contratados com os fornecedores da infraestrutura.

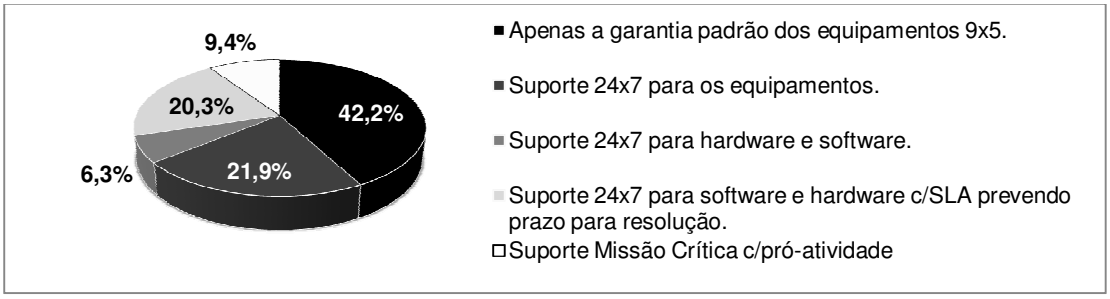

Figura 31. Investimentos em Serviços e Suporte com Fornecedores (Parceiros)

Com o objetivo de segmentar a análise, avaliando os investimentos em serviços de suporte e assistência técnica contratados com os fornecedores, a Figura 32 mostra que empresas pequenas optam por minimizar os investimentos na contratação de serviços complementares a garantia dos equipamentos, enquanto as empresas de maior porte, optam por tais serviços diferenciados incluindo serviços de Missão Crítica.

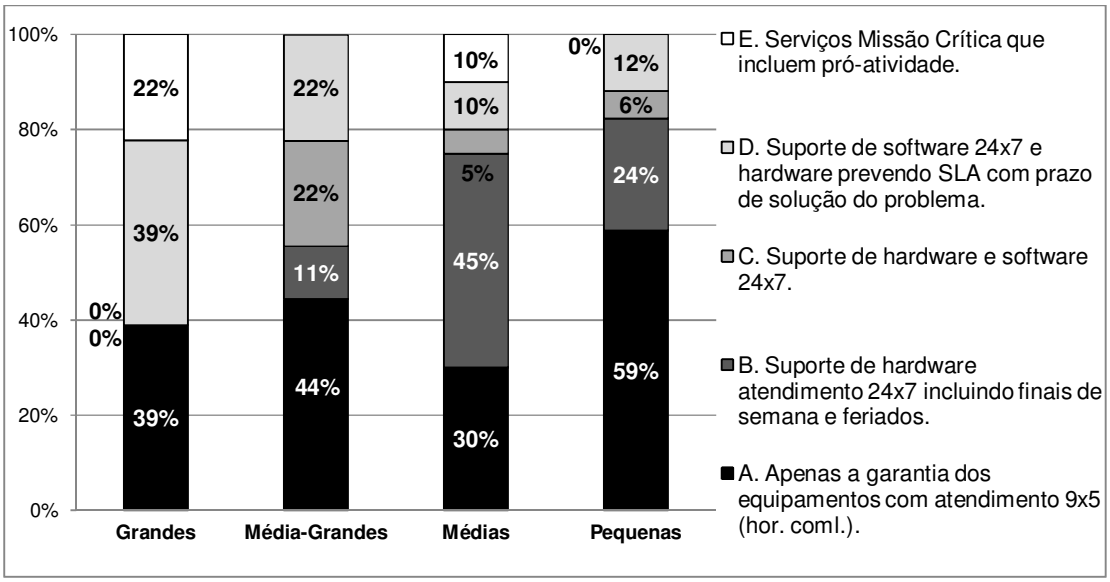

Figura 32. Investimentos em Serviços e Suporte com Fornecedores (Parceiros) conforme porte da empresa ou organização pesquisada

Quanto a investimentos em capacitação e treinamento das pessoas que compõe a área de TI, as respostas registradas na questão 10 demonstram que apenas 37,6% dos respondentes afirmaram que suas empresas e organizações tem investimentos anuais pré-estabelecidos visando a capacitação e atualização da equipe de TI e 17,2% reportaram que não há investimento algum por parte da organização na equipe de TI. Tais resultados estão demonstrados graficamente na Figura 33.

Figura 33. Investimentos em Capacitação e Treinamento (Pessoas)

A Figura 34 apresenta graficamente a divisão das empresas e organizações pesquisadas em termos porte pelo faturamento anual, apontando que investimentos em treinamento e capacitação da equipe de TI estão diretamente relacionados ao porte, ou seja, a amostra pesquisada demonstra que quanto maior a empresa, maior tem sido o investimento nas pessoas.

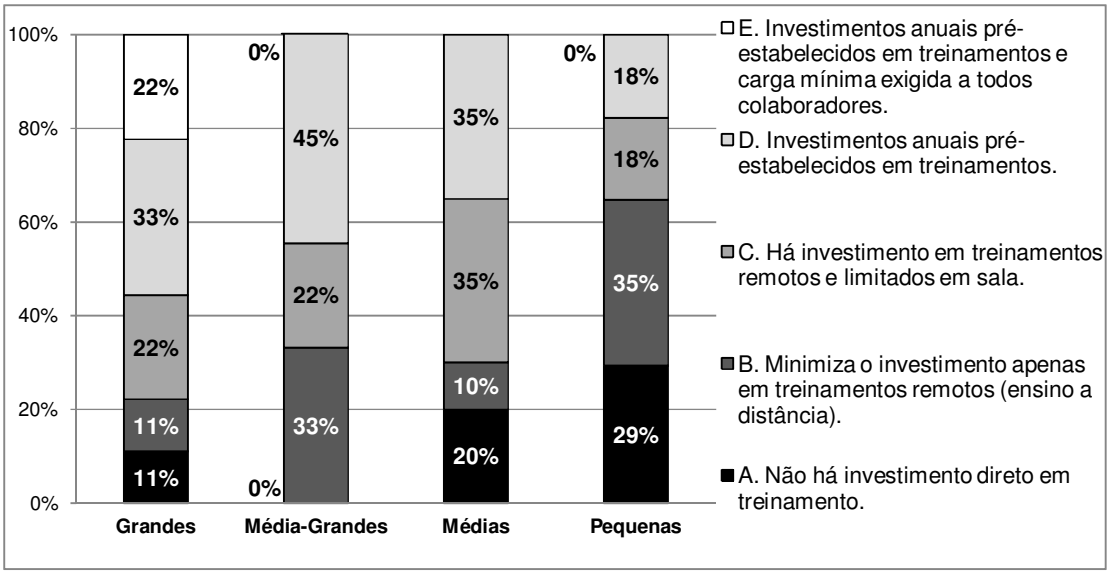

Figura 34. Investimentos em Capacitação e Treinamento (Pessoas) conforme porte da empresa ou organização pesquisada

Com relação à adoção de melhores práticas de Governança e Gerenciamento de TI, o resultado geral do *survey* com base nas respostas a questão 12 ilustrado na Figura 35, demonstra que apenas 6,3% já tem adotado tais práticas há mais de dois anos enquanto que 53,1%, ou seja, a maioria, afirmaram que ainda não adotaram tais práticas. Porém, as respostas também apresentam um entendimento que embora ainda não tenham adotado, 35,9% consideram importantes sua implementação podendo caracterizar-se uma tendência de mudança de posicionamento futura quanto a abordagem para a melhor gestão da área de TI.

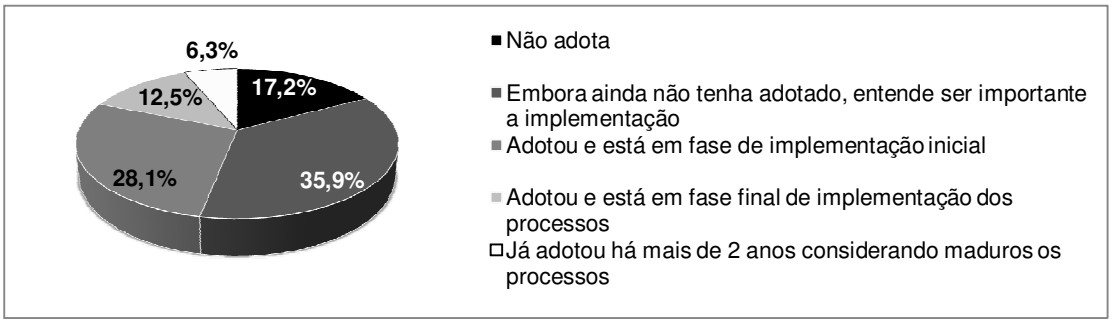

Figura 35. Investimentos na adoção de Melhores Práticas de Governança e Gerenciamento de TI (Processos)

A Figura 36 permite visualizar o resultado dos investimentos em melhorias de processos de TI de acordo com o porte das empresas e organizações em relação ao faturamento anual. Percebe-se que empresas grandes tem uma maior adoção a guias de melhores práticas de Governança e Gerenciamento de TI em comparação com empresas médias e pequenas.

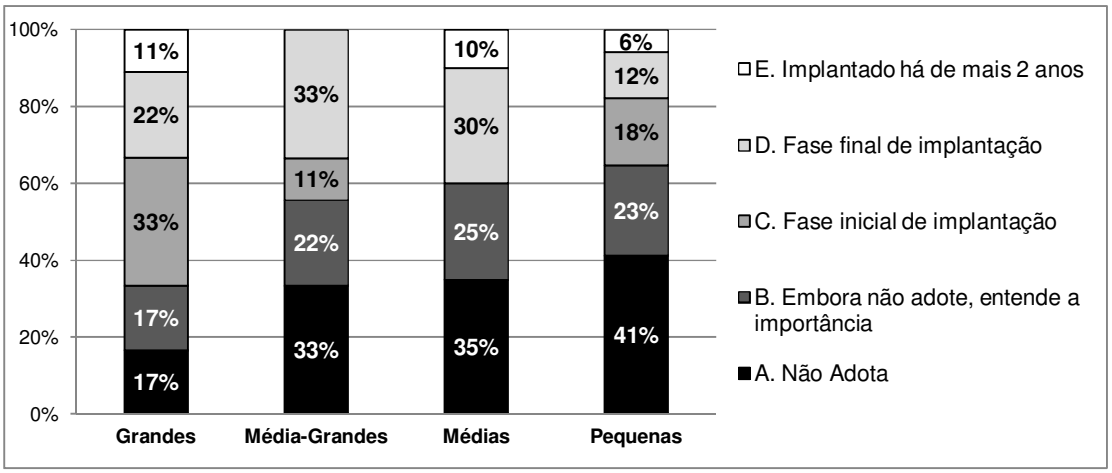

Figura 36. Investimentos na adoção de Melhores Práticas de Governança e Gerenciamento de TI (Processos) por porte das empresas e organizações

6.7 Respostas à questão 20 quanto ao principal desafio dos gestores de TI para manter os sistemas críticos disponíveis e operacionais

Esta última questão 20 de cunho opcional para resposta, buscou de forma textual livre obter dos pesquisados na própria visão deles qual é seu principal desafio como gestores da área de Tecnologia da Informação para manter operacional e disponíveis os sistemas críticos ao negócio.

Vinte e cinco dos sessenta e quatro respondentes depositaram suas opiniões, ou seja, 39% do total de pesquisados compartilhou sua percepção quanto essa questão relevante.

O Quadro 5 buscou agrupar as respostas baseado-se na análise de conteúdo das mesmas onde foram subdivididos por quatro características: sugestões de melhorias ao *survey*, dificuldades operacionais da área de TI, capacitação das pessoas da área de TI e Governança de TI.

Quadro 5. Respostas a Questão do Desafio do Gestor de TI em manter os sistemas críticos operacionais e disponíveis

Agrupamento das respostas	**Respostas dos entrevistados quanto a pergunta: Considerando sua experiência na gestão de TI, segue um espaço em texto livre para compartilhar seu principal desafio para manter operacionais e disponíveis os sistemas críticos de sua empresa.**
Governança de TI	1- A implantação de ferramentas de gerenciamento de processos ainda é um desafio junto aos setores internos. 2- Conseguir deixar claro a função da TI, dentro da empresa. 3- Implantar processos de Gerenciamento de Continuidade de Negócios, Gerenciamento de Capacidade e Gerenciamento de Disponibilidade 4- Mostrar para a alta administração e demais gestores o valor gerado pela aplicação das boas práticas adotadas. 5- Fazer com que a alta direção entenda que os gastos com suporte e manutenção, são necessários para manter a continuidade do negócio. 6- O principal desafio é manter o monitoramento dos serviços, agir preventivamente nos problemas previsíveis, identificar de forma inequívoca e prontamente os problemas imprevisíveis e dar uma solução rápida para os mesmos. 7- O principal desafio para um Gestor de TI que trabalha com poucos recursos, tanto financeiro como de RH, é conseguir implantar as boas práticas de serviços de TI que estejam alinhados com o planejamento estratégico da instituição. Não é nada fácil, fazer isso com essas dificuldades, acrescido da falta de apoio da alta gestão em reconhecer a TI como área estratégica.

Quadro 5. Respostas a Questão do Desafio do Gestor de TI em manter os sistemas críticos operacionais e disponíveis (continuação)

Agrupamento das respostas	Respostas dos entrevistados quanto a pergunta: Considerando sua experiência na gestão de TI, segue um espaço em texto livre para compartilhar seu principal desafio para manter operacionais e disponíveis os sistemas críticos de sua empresa.
Capacitação das Pessoas da área de TI	1- Equipe capacitada e proativa. 2- O principal desafio em nossa região é a dificuldade em encontrar mão de obra qualificada. 3- O maior desafio é manter o pessoal técnico especializado fidelizado em nossa empresa. 4- Capacitação da equipe. 5- Em se tratando de empresas de porte e que possuem uma estrutura de governança corporativa estabelecida, o maior desafio é qualificar e manter profissionais. Esta qualificação deve contemplar tanto a capacitação técnica quanto em governança de TI. 6- Fazer os diretores/investidores entenderem a importância da T.I. para o sucesso do negócio e com isso a necessidade de investimentos não só no ambiente mas também nas pessoas.
Dificuldades Operacionais da área de TI	1- "Dar manutenção no avião em pleno vôo". 2- montagem do *site (datacenter)* secundário. 3- Virtualizar os sistemas operacionais, onde estão os sistemas críticos, exceto banco de dados. 4- Estamos em processo de transferência de *outsourcing* ainda com uma infraestrutura obsoleta. 5- Na empresa pública, nosso caso especifico, ainda existe a dificuldade para o cumprimento de metas, em virtude da impontualidade na liberação de recursos para execução de projetos aprovados.
Sugestões de melhoria para a pesquisa *(survey)*	1- Sugiro a inclusão de itens de *outsourcing* porque muitas das grandes empresas terceirizam sua TI. 2- Alguns ítens foram respondidos por falta de opcao. O survey (enquete) esta direcionando as respostas ao nao permitir respostas em branco ou N/A. 3- Questões 4, 18 e 19 precisam de opcoes de fuga. 4- Não tenho informação real das perguntas 18 e 19. 5- Obs: a resposta da pergunta 14 é que não houve evento, portanto a resposta das perguntas 15 e 17 deveria ser que “não ocorreu”, como não existe essa resposta marquei a primeira opção. Obrigado 6- Considerando que nossa empresa é um Órgão Público, os itens 4, 14,15,16, 17, 18 não se aplicam ou não temos investimento na área de TI.

A sugestões ao *survey* dispostas nas respostas a questão 20, foram adotadas no processo de análise, visto que durante a validação da pesquisa, os cinco avaliadores apontaram que houveram paradas não programadas e portanto, não foi observado que quando o respondente apontava que nenhum evento foi reportado (questão 14), as questões 15 quanto quantidade de paradas, questão

16 quanto a tempo de indisponibilidade e questão 17 referente à causa da parada, não haviam opções de fuga. Com a álgebra booleana disposta na ferramenta SurveyMonkey através da porta AND NOT, isolalaram-se as respostas a questão 14 que reportaram nenhum evento removendo adequadamente das questões 15, 16 e 17 considerando apenas repostas para estas questões quando efetivamente na questão 14 foi registrado eventos de paradas não programadas.

Nas respostas agrupadas como dificuldades operacionais da área de TI, estavam mais relacionadas as atividades do dia a dia e implementação de novos projetos como a instalação de um *data center* secundário demonstrando o investimento em replicação e *disaster recovery,* virtualização dos sistemas críticos, dificuldades do setor público em termos de cumprimentos de metas e *outsourcing* que trata da terceirização dos serviços prestados pela área de TI para empresas especializadas.

Sobre os desafios apontados pelos gestores de TI relacionados a treinamento e capacitação da equipe da área, foram compartilhadas seis opiniões neste contexto relatando as dificuldades de encontrar mão de obra qualificada na região, capacitar as pessoas e depois de capacitadas mantê-las na empresa, adicionando o fato da dificuldade de demonstrar ao nível executivo da organização a necessidade não apenas de investir na infraestrutura mas também na capacitação e treinamento das pessoas que a operam e suportam no dia a dia. Tais opiniões vem ao encontro dos resultados obtidos na análise das respostas obtidas nas questões 10 e 11, apontando realmente a necessidade das empresas e organizações terem uma melhor visão quanto aos investimentos em capacitação das pessoas da TI e seus benefícios para a continuidade dos sistemas críticos que suportam os negócios.

Com relação a Governança de TI, assunto onde mais foram agrupadas opiniões dos respondentes, totalizando sete entradas, pode-se observar a preocupação dos gestores da área no nível operacional em relação ao papel desempenhado pela TI, a visibilidade e reconhecimento da alta direção, ou seja, do nível executivo das empresas e organizações bem como o alinhamento ou a falta dele com as estratégias e objetivos da organização.

O resultado das opiniões apresentadas sobre Governança de TI alinham-se às respostas obtidas na questão 12, dispostas na Figura 35, sobre a pouca adoção à guias de melhores práticas de Governança e Gerenciamento de TI como COBIT, onde 53,1% reportaram que ainda não adotaram tais práticas e outros 28,1% estão em fase inicial de implementação, que envolve o esforço e entendimento de importância de todos os níveis da organização desde as áreas de negócios e TI com o apoio fundamental da alta gestão como patrocinadores ou *sponsors* para o sucesso de um projeto deste porte.

CAPÍTULO VII – CONCLUSÃO

Este estudo buscou, por meio da revisão da literatura especializada considerando os aspectos das atuais tecnologias voltadas a ambientes computacionais de alta disponibilidade e da Governança e Gerenciamento de TI, bem como na perspectiva dos dois guias de melhores práticas de gestão de TI mais adotados, apreender o estado da arte em termos de recomendações para manter os sistemas críticos ao negócio operacionais e disponíveis evitando paradas não programadas e impacto aos negócios de empresas e organizações.

Com o objetivo de complementar a contribuição deste estudo para o conhecimento da área de Tecnologia da Informação e continuidade dos sistemas críticos ao negócio, foram analisados dados primários e atualizados sobre o tema com a aplicação de uma pesquisa do tipo *survey* com abordagem quantitativa entre gestores de TI do Estado do Ceará como uma das três maiores economias da região Nordeste do Brasil.

Como resultados da análise estatística descritiva dos dados obtidos no *survey*, a primeira questão sobre os gestores de TI pesquisados conhecerem as causas das paradas não programadas em seus sistemas críticos ao negócio foi esclarecida. Os respondentes demonstraram ter o entendimento de tais causas pois em apenas 2,1% das respostas apresentadas, não foram capazes de apontar o motivo que causou a indisponibilidade.

Entretanto, a segunda questão deste estudo em relação como os investimentos estão sendo direcionados na área de TI nos quatro quadrantes (produtos, pessoas, processos e parceiros), recomenda importantes oportunidades de melhoria com base nas respostas alcançadas com o *survey* e comparação com o estado da arte visando a continuidade de operação dos sistemas críticos ao negócio.

Os sistemas críticos da forma como estão atualmente implementados, segundo respostas dos próprios gestores, carecem de investimentos na robustez dos equipamentos em termos de características de redundância de componentes de *hardware* e tecnologia RAID bem como de configuração em *cluster* para

aumento da disponibilidade e confiabilidade dos sistemas, até a avaliação de investimentos em replicação de sistemas em configuração de *disaster recovery* para sistemas críticos, que em caso de indisponibilidade, impactem diretamente o negócio principal da organização.

Porém, esta pesquisa demonstrou que apenas investimentos na infraestrutura não são capazes de sozinhos manter os ambientes estáveis e sem ocorrência de indisponibilidades. São também necessários investimentos em serviços de suporte preferencialmente Missão Crítica com os fornecedores, quadrante parceiros, que no caso especificamente do Ceará, devido à distância e à limitação de voos diários, reforça a avaliação por parte dos gestores de TI quanto a contratação de serviços diferenciados com SLAs que possibilitem o rápido acesso a peças de reposição reduzindo o tempo de reparo e indisponibilidade dos sistemas.

Quanto à capacitação das pessoas, compreende-se aqui não apenas vista como conhecimento técnico, que certamente auxiliará esses profissionais a adequar as infraestruturas de TI em conformidade com as atuais tecnologias de alta disponibilidade e ferramentas automatizadas de gerenciamento e monitoração mas também, fundamentalmente necessário o entendimento de quão importante a adoção de melhores práticas de Governança e Gerenciamento de TI que se encontram dispostas em guias como COBIT ou ITIL é para contribuir na continuidade dos serviços prestados pela área de Tecnologia da Informação.

Esse último quadrante estudado, ou seja, adoção de *frameworks* de melhores práticas de Governança e Gerenciamento de TI como COBIT ou ITIL apresentou os melhores resultados em termos de redução de paradas não programadas e menor impacto aos negócios e constância no tempo para resolução dos incidentes. Percebeu-se também que esses *frameworks* trazem à área de TI um melhor entendimento a respeito da distribuição dos investimentos nos quatro quadrantes, ou seja, na infraestrutura, na capacitação das pessoas, na contratação de serviços de suporte diferenciados com os fornecedores através da melhoria contínua dos processos de gerenciamento, operação, monitoração, medição e controle atendendo os anseios dos gestores de TI.

Embora os resultados alcançados por meio da metodologia adotada para esta pesquisa não possam ser generalizados, este esforço na padronização dos processos e serviços de TI com o gerenciamento da continuidade dos serviços, da disponibilidade, dos serviços de parceiros, de mudanças e configuração, bem como de incidentes e problemas, além de conceitualmente estabelecer um melhor alinhamento entre as áreas de négocio, os objetivos estratégicos e o papel da TI, permitem recomendar a adoção de melhores práticas de Governança e Gerenciamento de TI como principal foco dos gestores visando atender as demandas de negócio atuais e futuras de empresas e organizações com o mínimo de indisponibilidades não planejadas em seus sistemas críticos de negócio.

Como oportunidades de estudos futuros, sugere-se o aprofundamento dos resultados positivos da adoção do ITIL em termos de redução de indisponibilidades com estudos de caso avaliando as medições de indicadores chave de desempenho (KPIs – *key performance indicators*) em processos como o gerenciamento da disponibilidade demonstrando a efetividade da gestão dos serviços de TI com a adoção de guias de melhores práticas.

Também sugere-se a elaboração de uma ferramenta mesclando a lógica crisp e a lógica nebulosa (*fuzzy*) capaz de auxiliar os gestores de TI na definição de investimentos para reduzir a ocorrência de paradas não programadas em seus sistemas críticos ao negócio.

A terceirização da área de Tecnologia da Informação ou *outsourcing* e a computação em nuvem ou *cloud computing* são áreas também a serem estudadas em trabalhos futuros visando avaliar sua influência positiva ou negativa na busca das organizações por manter seus sistemas críticos ao negócio operacionais e disponíveis.

REFERÊNCIAS

ADDY, R. *Effective IT Service Management: To ITIL and Beyond!* EUA: Springer, 2007.

ALDERMAN, A.K. e SALEM,B. *Survey Research*. PRS Journal. p.1381-1389 vol.126 nº4. out.2010.

APMG. *What is ITIL?* Disponível em:<http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx>. Acesso em: 15 Mai.2012.

APMG. *Welcome to the Official PRINCE2 Website.* Disponível em:< http://www.prince-officialsite.com/>. Acesso em: 17 jun.2012.

ASSIS, C.B. *Governança e Gestão da Tecnologia da Informação: Diferenças na Aplicação em Empresas Brasileiras*. 2011.210p. Dissertação (Mestrado em Engenharia de Produção) - Departamento de Engenharia de Produção, Escola Politécnica da Universidade de São Paulo, São Paulo, 2011.

ATOS ORIGIN (UK). Keith Inight. *The management of Service Availability: Keeping services running without breaking the bank. (paper)* SA. 2401-1108. fev.2009.

AZUL. Azul Linhas Aéreas Brasileiras. Disponível em:<http://www.voeazul.com.br>. Acesso em: 12 out.2012.

BALANCED SCORECARD INSTITUTE. *BSC – Balanced Score Card*. Disponível em:<http://www.balancedscorecard.org/>. Acesso em: 5 ago.2012.

BANCO DO NORDESTE. *As Maiores Empresas do Nordeste em 2008.* Escritório de Estudos Econômicos do Nordeste – ETENE Ano 4 – Nº. 13, 2009.

BECKER, M. *et al. Avaliação da Aplicação dos Recursos em Tecnologia da Informação para Manter a Disponibilidade dos Sistemas Críticos de Negócio.* IX SEGeT – Simpósio de Excelência em Gestão e Tecnologia – AEDB. Resende, RJ, 2012. Disponível em:<http://www.aedb.br/seget/artigos2012.php>. Acesso em 31 out.2012.

BENDER, W.L. e JOSHI, A. *High Availability Technical Primer.* EUA: PPC, 2005. Disponível em:<http://www.ppc.com/documents/high-availability-tech-full.pdf> Acesso em: 8 ago.2011.

BNDES. *Porte de Empresa*: Classificação de porte de empresa adotada pelo BNDES. Disponível em: <http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Navegacao_Suplementar/Perfil/porte.html> Acesso em: 22 ago.2011.

BRASIL. Lei nº 8.078, de 11 de setembro 1990. Dispõe sobre o Código de Defesa do Consumidor. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 30 out.2011.

CACIATO, L. E. *Virtualização e Consolidação dos Servidores do Datacenter*, UNICAMP, Campinas, SP, 2010. Disponível em:<http://www.ccuec.unicamp.br/biti/download/Artigo_Virtualizacao_Datacenter.pdf>. Acesso em: 6 set.2012.

CAMPOS, V. F. *TQC*: Controle de Qualidade Total. Belo Horizonte: Fundação Christiano Ottoni, 1992.

CARTLIDGE, A. *et al. An Introductory Overview of ITIL v3: A high-level overview of the IT Infrastructure Library.* version 1.0. EUA: itSM, 2007.

COMPUTERWORLD. *Who do you blame when IT breaks?* Disponível em:<http://www.computerworld.com/s/article/9224650/Who_do_you_blame_when_IT_breaks_?taxonomyId=154epageNumber=1>. Acesso em: 6 set.2012.

_____. *Certificações Ampliam Competitividade de Data Centers*. Disponível em:<http://computerworld.uol.com.br/tecnologia/2011/04/27/certificacoes-ampliam-competitividade-de-data-centers/ 2011>. Acesso em: 2 out.2012.

_____. *Primeiro Data Center com Selo Tier III abre em Agosto*. Disponível em:<http://computerworld.uol.com.br/negocios/2010/07/08/primeiro-data-center-do-pais-com-selo-tier-iii-abre-em-agosto/2010>. Acesso em: 6 set.2012.

_____. *Embratel inaugura data center em SP e se lança na nuvem*. Disponível em:<http://computerworld.uol.com.br/negocios/2012/09/26/embratel-inaugura-data-center-em-sp-e-se-lanca-na-nuvem/ 2012>. Acesso em: 18 out.2012.

DOLEWSKI, R. *System & Disaster Recovery Planning*, EUA: MC Press, 2008.

EMBRATEL. *Embratel anuncia novo Data Center no Brasil.* Disponível em:< http://www.embratel.com.br/Embratel02/cda/portal/0,2997,PO_P_161_1677,00.html>. Acesso em: 12 out.2012.

EMERSON NETWORK POWER, *Liebert Data Center Assessment: Identify And Resolve The Vulnerabilities in Your Data Center. (white paper)* EUA: Emerson Network Power, 2008.

ESTADÃO. Pane na Telefonica derruba web e pára serviços pelo Estado. 03 jul.2008. Disponível em:<http://www.estadao.com.br/noticias/cidades,pane-na-telefonica-derruba-web-e-para-servicos-pelo-estado,200088,0.htm>. Acesso em: 12 dez.2011.

ETICE, *Relação de Gestores de TIC do Estado do Ceará*. Disponível em:<http://www.etice.ce.gov.br/categoria2/gestores> Acesso em: 09 dez.2011.

FERNANDES, A. A. e ABREU, V. F. *Implantando a Governança de TI: da Estratégia à Gestão de Processos e Serviços.* 2ªedição. Rio de Janeiro: Brasport, 2008.

FOLHAONLINE. *Falha em rede atinge conexão à internet no Estado de SP. 03 jun.2008.* Disponível em:< http://www1.folha.uol.com.br/folha/informatica/ult124u418802.shtml>. Acesso em: 12 dez.2011.

FOX, A. e PATTERSON, D. *When Does Fast Recovery Trump High Reliability?* 2nd Workshop on Evaluating and Architecting System Dependability. EUA. 2002.

FREITAS, H. *et al. O Método de Pesquisa Survey*. Revista de Administração. São Paulo v.35.nº3.p.105-112. jul/set. 2000.

FUJITSU. *Servidores Padrão da Indústria PRIMERGY.* Disponível em: <http://www.fujitsu.com/pt/products/computing/servers/primergy/>. Acesso em: 8 ago.2012.

GARTNER. Disponível em:<http://www.gartner.com/technology/why_gartner.jsp>. Acesso em: 16 ago. 2011.

GGTIC-CE, *Grupo de Gestores de Tecnologia da Informação e Comunicação do Estado do Ceará.* Disponível em:<http://www.ggtic-ce.org.br/institucional/associados.html> Acesso em: 12 nov.2011.

GOLDWORM, B. e SKAMAROCK, A. *Blade Servers and Virtualization: Transforming Enterprise Computing While Cutting Costs*. EUA:John Wiley & Sons, 2007.

GREMBERGEN, W. V. e HAES, S. *Implementing Information Technology Governance: Models, Practices and Cases.* EUA: IGI Global, 2008.

GROVES,R.M. *Three Eras of Survey Research*: Public Opinion Quartely. Oxford University Press. vol.75,nº5.p.861-871.2011.

GOPALAKRISHNAN, K. *Oracle Database 10G Real Application Clusters Handbook.* EUA: Oracle Press, 2007.

GUNTZEL, J.L. e NASCIMENTO, F.A. *Álgebra Booleana e Circuitos Lógicos*. UFSC, 2001. Disponível em: <http://www.inf.ufsc.br/~guntzel/isd/isd2.pdf>. Acesso: 2 abr.2012.

HILES, A. *The Definitive Handbook of Business Continuity Management*, 2nd Edition, EUA: John Wiley e Sons, 2007.

HP (EUA). *Blades for Business.* Disponível em:<http://h20384.www2.hp.com/serverstorage/us/en/servers/blades-for-business.html>. Acesso em: 12 out.2012.

IBGE. Contas Nacionais número: 35. Contas Regionais do Brasil 2005-2009. *(relatório técnico)* IBGE: Rio de Janeiro, 2011.

IBM (EUA). *Help protect critical data with an innovative business continuity solution from IBM. (white paper)* TIS10428-USEN-00. mar.2006.

IDC. International Data Corporation. Disponível em:<http://www.idc.com/>. Acesso em: 16 ago.2011.

IDC (EUA). Richard L. Villars e Bill North. *Business Continuity: More than Just Waiting for Disaster*. *(white paper)* #3829. set.2003.

_____. Jean S. Bozman. *Oracle's MAA Portfolio: Deploying High-Availability Solutions Across the Enterprise*. *(white paper)* #223019. jun.2010.

_____. Matt Healey e Randy Perry. *HP Mission Critical Services: ROI Benefit Analysis. (white paper)* #224529. ago.2010.

_____. Matt Healey Robert Brothers. *Support for Virtualized Environments: HP's Critical Advantage*. *(white paper)* #226743. fev.2011.

_____. Robert Brothers. *The Business Value of Post-Warranty Contracts. (white paper)* #228064. nov.2011.

_____. Robert Brothers. *Leveraging the Always On Support Experience for IT Transformation*. *(white paper)* #233646. mar. 2012.

IDGNOW. *Líder em pesquisas via web, SurveyMonkey chega ao Brasil.* Disponível em: <http://idgnow.uol.com.br/mercado/2012/04/13/lider-em-pesquisas-via-web-surveymonkey-chega-ao-brasil/#&panel2-1>. Acesso em 15 mai.2012.

INTERNETNEWS.COM, *Comair Back in Air After Computer Outage, 27 dez.2004.* Disponível em:<http://www.internetnews.com/bus-news/article.php/3451981>. Acesso em: 02 jul.2012.

ISACA. *COBIT 4.1: Framework for IT Governance and Control.* Disponível em:<http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>. Acesso em: 18 jun.2012.

_____. *Val IT Framework for Business Technology Management*. Disponível em:< http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx>. Acesso em: 09 set. 2012.

ITGI, *COBIT 4.1 em Português: Modelo, Objetivos de Controle, Diretrizes de Gerenciamento e Modelos de Maturidade.* EUA: IT Governance Institute, 2007.

KNELLER, M. *Executive Briefing: The Benefits of ITIL*, Reunido Unido: OGC, 2010.

MARCONI, M., LAKATOS, E. M. *Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados,* 4ª edição. São Paulo: Atlas, 1999.

MARCUS, E. e STERN, H. *Blueprints for High Availability*: Second Edition, EUA: John Wiley e Sons, 2003.

MASUR, R. *Governança Avançada de TI*. Rio de Janeiro: Brasport, 2009.

MICHAELIS (BRA). Moderno Dicionário da Língua Portuguesa. Disponível em:< http://michaelis.uol.com.br/>. Acesso em 10 set.2012.

MORESI, E. *Metodologia da Pesquisa,* Universidade Católica de Brasília, Brasília, 2003. Disponível em:<http://www.inf.ufes.br/~falbo/files/MetodologiaPesquisa-Moresi2003.pdf>. Acesso em: 4 out. 2011.

NETAPP (EUA). Subra Mohan. *A Comprehensive Approach to Application Availability.* (*white paper*) WP-7002-1006, out.2006.

OLIVEIRA, M. M. *Como Fazer uma pesquisa Qualitativa*, Petrópolis: Vozes, 2007.

OPEN GROUP. *TOGAF version 9.1*. Disponível em:<http://www.opengroup.org/ standards>. Acesso em: 28 set.2012.

ORACLE. *Oracle Business Critical Assistance Delivered by Oracle Advanced Customer Support Services: Mission Critical Support. (data sheet)* 2009.

PATTERSON, D. A. *A Simple Way to Estimate the Cost of Downtime*. Sixteenth LISA - Systems Administration Conference. Philadelphia, EUA. USENIX Association. p.185-188. Nov.2002.

PERTET, S. e NARASIMHAN, P. *Causes of Failure in Web Applications*: CMU-PDL-05-109. Paper 48. dez.2005. *(technical report)* Parallel Data Laboratory. Carnegie Mellon University EUA. Disponível em: <http://repository.cmu.edu/pdl/48>. Acesso: 2 mai.2011.

PMI. Project Management Institute. Disponível em:<http://www.pmi.org>. Acesso em: 28 set.2012.

PROCON-SP. *Garantia Estendida. Você sabe o que realmente é?* Disponível em: <http://www.procon.sp.gov.br/pdf/ACS_orienta_garantia_estendida.pdf>. Acesso em: 30 out.2011.

RODRIGUES, C. A. P. Estudo da Adoção das Melhores Práticas em TI – ITIL e Integração com Metodologia de Gestão e Avaliação de Desempenho BSC. 2006. 170 f. Dissertação (Mestrado) – Universidade Federal Fluminense, Niterói, 2006.

RODRIGUES, L. C., MACCARI, E. A. e SIMÕES, S. A. *O Desenho da Gestão da Tecnologia da Informação nas 100 Maiores Empresas na Visão dos Executivos de TI*, Revista de Gestão da Tecnologia e Sistemas de Informação Vol. 6, No. 3, p. 483-506, USP, São Paulo, 2009.

ROSS, J. W., WEILL, P. e PETER, R. *Arquitetura de TI como estratégia empresarial*, São Paulo: M.Books, 2008.

RUDIO, F. V. *Introdução ao Projeto de Pesquisa Científica*, Rio de Janeiro: Vozes, 2001.

RUNGTUSATHAM, *et al. Survey research in operations management: historical analyses*, Journal of Operations Management 21 p.475-488, 2003. Elsevier Science B.V.

SABOIA *et al. Projeto PIB (Perspectivas do Investimento no Brasil): Tendências da Qualificação da Força de Trabalho.* Rio de Janeiro: UFRJ e UNICAMP, 2009.

SCHMIDT, K. *High Availability and Disaster Recovery:* Concepts, Design, Implementation, EUA: Springer, 2006.

SCOTT, D., *Tactical Guidelines*: TG-07-4033 Research Note 16 March 1999, EUA: Gartner, 1999.

SNIA. *SNIA Dictionary:* Storage and Networking Industry Associates, Disponível em: <http://www.snia.org/education/dictionary/> Acesso em: 12 ago.2012.

STALLING, W. *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*, 3rd edition, EUA: Addison Wesley, 1998.

STEINBERG, H *et al. A dimensão Humana da Governança Corporativa*: pessoas criaram as melhores e as piores práticas, 4ª edição, São Paulo: Gente, 2003.

SYMANTEC. *Symantec Enterprise Support Services Handbook for Business Critical Services: Revision 1.3. Dec. 2006.* Disponível em:<http://www.symantec. com>. Acesso em: 10 out.2012.

SUCESU-MG. *TIC do Brasil deverá crescer acima de 10% em 2012*. Disponível em: <http://www.sucesumg.org.br/index.php?option=com_content&view=article&id =519:tic-do-brasil-devera-crescer-acima-de-10-em-2012&catid=45:ultimas-noticias &Itemid=1>. Acesso em: 10 out.2012.

SOMERVILLE, I. *Engenharia de Software*: 8ª edição. São Paulo: Pearson Addison-Wesley, 2007.

SURVEYMONKEY. Disponível em:<http://www.surveymonkey.com.br>. Acesso em: 02 jul.2011.

TAM. TAM Linhas Aéreas. Disponível em:<http://www.tam.com.br>. Acesso em: 10 out.2012.

THE NEW YORK TIMES. *Crash Shuts Down Ebay for Much of the Day.* Disponível em: <http://www.nytimes.com/1999/06/12/business/crash-shuts-down-ebay-for-much-of-the-day.html> Acesso em: 22 jul.2011.

TIA, *ANSI/TIA-942-2005: Telecommunications Infrastructure Standard for Data Centers,* EUA: TIA, 2005.

TROPPENS, U. *et al. Storage Networks Explained:* Basics and Application of Fibre Channel SAN, NAS, iSCSI, InfiniBand and FCoE: 2ª Edição, EUA: John Wiley & Sons, 2009.

UPTIME INSTITUTE. *Data Center Site Infrastructure Tier Standard: Operational Sustainability,* EUA: Uptime Institute Professional Services, 2010.

VOCÊ S/A. *Bônus e ônus do crescimento: Região Nordeste*. Disponível em:<http://vocesa.abril.com.br/desenvolva-sua-carreira/materia/bonus-onus-crescimento-regiao-nordeste-624961.shtml>. Acesso em: 02 abr.2011.

WEILL, P. e ROSS, J. W.,*Governança de Tecnologia da Informação*, São Paulo: M.Books, 2004.

WEYGANT, P. *Clusters for High Availability:* A Primer of HP-UX Solutions, first edition, EUA: Prentice Hall PTR, 1996.

_____. *Clusters for High Availability: 2nd Edition*, EUA: Prentice Hall PTR, 2001.

ZHU,W. *et al. IBM High Availability Solution for IBM FileNet P8 Systems*. EUA: IBM Redbooks, 2009.

APÊNDICE A – Encaminhamento da Pesquisa *Survey* Prévia

Prezado(a),

Como profissional da área de TI e mestrando do Programa de Pós-Graduação em Engenharia Elétrica da Pontifícia Universidade Católica de Campinas (PUC-Campinas/SP) na área de concentração em Gestão de Redes e Serviços, peço sua gentileza de participar da avaliação prévia desta pesquisa que posteriormente será encaminhada a campo e servirá de base para minha dissertação de Mestrado visando a avaliação dos ambientes de TI no Estado do Ceará quanto a sua disponibilidade, capacitação de pessoal, processos e serviços associados.

Reforço que tal pesquisa objetiva um trabalho científico sem vínculos a qualquer empresa pública ou privada bem como todas as informações compartilhadas serão sigilosas sem identificação do pesquisado ou empresa ao qual trabalha.

Portanto, peço sua atenção para que tal pesquisa seja preenchida até o dia 18 de novembro de 2011.

Desde já meus sinceros agradecimentos,

Atenciosamente,

Mauricio Becker

APÊNDICE B – Encaminhamento da Pesquisa *Survey* Definitiva

Avaliação da Gestão dos Ambientes de TI no Estado do Ceará

Prezado(a),

Como profissional da área de TI e mestrando do Programa de Pós-Graduação em Engenharia Elétrica da Pontifícia Universidade Católica de Campinas (PUC-Campinas/SP) na área de concentração em Gestão de Redes e Serviços, peço sua gentileza de participar desta pesquisa *survey* que servirá de base para minha dissertação de Mestrado visando a avaliação dos ambientes de TI no Estado do Ceará quanto a sua disponibilidade, capacitação de pessoal, processos e serviços associados.

Reforço que tal pesquisa objetiva um trabalho científico sem vínculos a qualquer empresa pública ou privada bem como todas as informações compartilhadas serão sigilosas sem identificação do pesquisado ou empresa ao qual trabalha.

Portanto, peço sua atenção para que esta pesquisa seja preenchida até o dia 30 de março de 2012.
https://www.surveymonkey.com/s/MWH77HS

Desde já meus sinceros agradecimentos,
Atenciosamente,
Mauricio Becker

APÊNDICE C – Pesquisa *Survey* Definitiva

Informações do Colaborador e Empresa em que trabalha

1. Atual cargo que ocupa
A. coordenação de infraestrutura de TI ou coordenação de operações e suporte TI
B. gerência de infraestrutura de TI ou gerência de operações e suporte TI

2. Tempo de Experiência na área de TI
A.1 a 3 anos
B. 3 a 5 anos
C. 5 a 10 anos
D. 10 a 20 anos
E. acima de 20 anos

3. Ramo de atividade da empresa em que trabalha
A. educação
B. financeiro
C. manufatura
D. saúde
E. serviços
F. setor público
G. varejo
I. outros

4. Porte da empresa em que trabalha em termos de faturamento anual
A. Pequena Empresa (entre R$ 2,4 milhões e R$ 16 milhões)
B. Média Empresa (entre R$ 16 milhões e R$ 90 milhões)
C. Média-Grande Empresa (entre R$ 90 milhões e R$ 300 milhões)
D. Grande Empresa (acima de R$ 300 milhões)

Pesquisa *Survey*

5. Os sistemas críticos de sua empresa possuem algum nível de tolerância a falhas de *hardware*, ou seja, redundância de componentes tipo fontes de alimentação, ventiladores bem como controladoras de discos rígidos com tecnologia RAID que toleram pelo menos uma única falha mantendo-se operacionais?
A. Não possuem tais características
B. Somente alguns sistemas críticos possuem tais características
C. Metade dos sistemas críticos possuem tais características
D. Grande parte dos sistemas críticos possuem tais características
E. Todos os sistemas críticos possuem tolerância a falhas de *hardware*

6. Os sistemas críticos de sua empresa estão configurados em *cluster* permitindo a rápida migração das aplicações de um servidor para outro minimizando o impacto das falhas de *hardware* ou *software*?
A. Nenhum sistema crítico está configurado em *cluster*
B. Somente alguns sistemas críticos estão
C. Metade dos sistemas críticos estão configurados em *cluster*
D. Grande parte dos sistemas críticos estão configurados em *cluster*
E. Todos os sistemas críticos estão configurados em *cluster*

7. Os sistemas críticos estão replicados em um segundo ambiente de contingência permitindo a rápida recuperação dos sistemas em casos de desastre *(disaster recovery)*?
A. Nenhum sistema crítico está replicado em outro *data center*
B. Somente alguns sistemas críticos estão
C. Metade dos sistemas críticos estão replicados em outro *data center*
D. Grande parte dos sistemas críticos estão replicados em outro *data center*
E. Todos os sistemas críticos estão replicados em outro *data center*

8. Existem ferramentas de gerenciamento e monitoração pró-ativa instaladas e configuradas em seu ambiente de TI (monitoração de servidores, sistemas, aplicações críticas e infraestrutura de redes)?
A. Não são utilizadas ferramentas de monitoração e gerenciamento do ambiente
B. Apenas a monitoração e gerência de falhas da infraestrutura de redes
C. Além da gerência de falhas, também é gerenciado o desempenho da infraestrutura de redes.
D. O gerenciamento de falhas e desempenho (utilização dos recursos) monitora não somente a infraestrutura de redes mas também os servidores e storages, ou sejam todos os equipamentos críticos da infraestrutura de TI.
E. Estão implementadas ferramentas avançadas de gerenciamento monitorando pró-ativamente a disponibilidade e desempenho das aplicações atreladas a continuidade do negócio.

9. Sua empresa adota a contratação de serviços de suporte diferenciados com SLAs pré-definidos com os fornecedores de sua infraestrutura de TI?
A. Apenas a garantia padrão dos equipamentos com atendimento 9x5 (horário comercial).
B. Adota contratos de suporte dos equipamentos prevendo o atendimento 24x7 incluindo finais de semana e feriados.
C. Além do suporte 24x7 para os equipamentos, mantém contrato de suporte com os fornecedores do sistema operacional e aplicações também em regime 24x7, ou seja, suporte de *hardware* e *software* 24x7.
D. Além do suporte de software 24x7 com os fornecedores do sistema operacional e aplicações, mantém um contrato de suporte 24x7 com os fornecedores dos equipamentos prevendo SLA com um prazo de solução do problema normalmente de 4, 6 ou 12 horas para o *hardware*.
E. Em complemento aos contratos de suporte 24x7 para *hardware* prevendo SLA com um prazo de solução e suporte de *software* 24x7, também contempla um serviço diferenciado de Missão Crítica com atualizações pró-ativas do ambiente, geração de relatórios de cumprimento de métricas e equipe dedicada para o atendimeto de suporte e gerenciamento da conta.

10. Quanto a capacitação técnica de sua equipe responsável pela administração, operação e suporte da infraestrutura de TI, sua empresa:
A. Não há investimento direto em treinamento deixando a cargo de cada profissional o seu próprio desenvolvimento.
B. Minimiza o investimento em treinamento incentivando a participação em treinamentos remotos (ensino a distância) e fora do horário de trabalho.
C. Há investimento em treinamentos remotos (ensino a distância) para toda a equipe e definição de pontos focais para participarem de treinamentos em sala dos próprios fornecedores da tecnologia e posteriormente compartilha o conhecimento com os demais colegas internamente na empresa.
D. Há investimentos anuais pré-estabelecidos em treinamentos possibilitando a participação dos principais membros da equipe em treinamentos formais em sala e ensino a distância a todos.

E. Além de investimentos anuais pré-estabelecidos em treinamento também há uma política mínima de horas de treinamento anuais para cada membro da equipe possibilitando treinamentos formais em sala mesmo que incluam despesas de viagem e hospedagem.

11. Sua empresa incentiva a obtenção de certificações providas pelos fornecedores da tecnologia e amplamente reconhecidas no mercado como forma de avaliar a capacitação profissional e técnica de sua equipe de TI?
A. Não incentiva essa prática e não contém profissionais certificados em seu quadro de colaboradores.
B. Embora não incentive a obtenção de certificações, contém alguns profissionais certificados em seu quadro de colaboradores.
C. Incentiva a obtenção de certificações e contém profissionais certificados na equipe porém não há reembolso das despesas com o custos das provas.
D. Incentiva e apoia financeiramente a obtenção de certificações com reembolso parcial das despesas contendo uma parte importante de profissionais certificados em sua equipe.
E. Exige a certificação de sua equipe nas tecnologias utilizadas na empresa bem como em fundamentos de governança de TI (ITIL/COBIT) custeando integralmente as despesas relacionadas tendo em sua equipe muitos profissionais certificados nas tecnologias e em governança de TI.

12. Sua empresa adotou ou está em fase de implementação de processos de governança de TI baseado em um conjunto de melhores práticas como ITIL ou COBIT?
A. Não adota
B. Embora ainda não tenha adotado, entende ser importante a implementação de processos padronizados
C. Adotou e está em fase de implementação inicial
D. Adotou e está em fase final de implementação dos processos
E. Já adotou há mais de 2 anos considerando maduros os processos de governança de TI

13. Quais as formas adotadas para medir os resultados obtidos com a implementação de processos de governança de TI em sua empresa?
Nota: O *SLM (Service Level Management)* visa alinhar e medir os *SLAs* (*Service Level Agreement*) dos serviços providos pela área de TI de acordo com os processos de negócio da empresa.
A. Não adotou tais processos
B. Os processos de governança de TI ainda estão em fase de implementação inicial
C. Existem métricas pré-estabelecidas mas ainda sem SLAs definidos com os clientes da área de TI
D. As métricas estão estabelecidas com base em SLAs definidos com os clientes da área de TI
E. Utiliza SLM para medir e controlar os SLAs estabelecidos provendo relatórios regulares para apresenteção dos resultados

14. Fazendo uma análise dos últimos 12 meses, ocorreu alguma parada não programada em algum sistema crítico de seu ambiente de TI que afetou os negócios da empresa?
A. Nenhum evento
B. Apenas 1 evento
C. 2 eventos
D. Entre 2 e 4 eventos
E. Acima de 4 eventos

15. Por quantas horas o sistema ou aplicação crítica permaneceu inoperante?
Nota: Em caso de mais de evento respondido na questão anterior, favor considerar o tempo total de parada somando todos os eventos.
A. até 02 horas
B. entre 02 e 06 horas
C. entre 06 e 12 horas
D. entre 12 e 24 horas
E. entre 24 e 48 horas

16. Houve impacto financeiro negativo para o negócio da empresa durante este(s) evento(s)?
A. Não houve impacto
B. Impacto mínimo (apenas nas operações internas)
C. Impacto controlado (operações internas de entrega/atraso no faturamento)
D. Muito negativo (perdas financeiras)
E. Extremamente negativo (perdas financeiras e impacto na imagem da empresa)

17. Qual foi a causa da principal parada não programada?
A. A causa não foi identificada
B. Falha da Infraestrutura de TI (falha de *hardware* nos equipamentos ou Sistema Operacional ou ambiente)
C. Falha na aplicação (falha de *software*, banco de dados, ERP, CRM, etc)
D. Falha operacional (erro humano)
E. Falha no processo (exemplos: gerenciamento de mudança ou controle de acesso ao data center)

18. Qual a proporção de investimentos em TI de sua empresa para o próximo ano?
Nota: Favor responder de forma aproximada com a resposta disponível que mais se assemelha a realidade de sua empresa considerando que serviços inclui os serviços de suporte complementares a garantia dos equipamentos, implementação de ferramentas de gerenciamento/monitoração, treinamento e adoção/revisão de processos de governança de TI tipo ITIL/COBIT.
A. 100% em infraestrutura de TI (*hardware, software e data center*)
B. 90% em infraestrutura de TI e 10% em serviços
C. 80% em infraestrutura de TI e 20% em serviços
D. 70% em infraestrutura de TI e 30% em serviços
E. 60% em infraestrutura de TI e 40% em serviços

19. Com relação a pergunta anterior, considerando apenas a porcentagem em serviços do total de investimento em TI da sua empresa para o próximo ano, como estarão divididos?
A. Não haverá investimento em serviços além da garantia padrão já inclusa nos equipamentos.
B. Integralmente em serviços de suporte complementares a garantia dos equipamentos.
C. Maior parte em serviços de suporte e algum investimento na implementação de ferramentas de gerenciamento e treinamento.
D. Metade em serviços de suporte e a outra metade em ferramentas de gerenciamento, treinamento e adoção/revisão de processos de governança de TI tipo ITIL/COBIT.
E. Um terço em serviços de suporte e os outros dois terços em ferramentas de gerenciamento, treinamento e adoção/revisão de processos de governança de TI tipo ITIL/COBIT.

20. Considerando sua experiência na gestão de TI, segue um espaço em texto livre para compartilhar seu principal desafio para manter operacionais e disponíveis os sistemas críticos de sua empresa. (opcional)

Agradeço sua atenção e tempo dedicado ao preenchimento desta pesquisa de campo.