IX SEGeT 2012
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
Tema: Gestão, Inovação e Tecnologia para a Sustentabilidade

AVALIAÇÃO DA APLICAÇÃO DOS RECURSOS EM TECNOLOGIA DA INFORMAÇÃO PARA MANTER A DISPONIBILIDADE DOS SISTEMAS CRÍTICOS DE NEGÓCIO

Mauricio Becker
mauricio.b@puccampinas.edu.br
PUC Campinas

Marciano Penaforte da Cruz
marciano.pc@puccampinas.edu.br
PUC Campinas

Vitor Chaves de Oliveira
vitor.co@puccampinas.edu.br
PUC Campinas

David Bianchini
davidb@puc-campinas.edu.br
PUC Campinas

Resumo: No atual contexto onde empresas e organizações dependem cada vez mais de suas infraestruturas de tecnologia da informação, tais sistemas e aplicações críticos às organizações necessitam estar disponíveis e operacionais aos usuários e clientes vinte e quatro horas por dia ao longo dos trezentos e sessenta e cinco dias do ano. Portanto, além de requerer equipamentos (hardware), aplicações (software) e ambientes (data centers) de alta qualidade e confiabilidade também necessitam mão de obra treinada e capacitada bem como processos de gestão estruturados e serviços de suporte diferenciados com os fornecedores dessa infraestrutura capazes de pró-ativamente evitarem paradas não programadas e prontamente responderem a incidentes minimizando a indisponibilidade desses sistemas e aplicações críticas a continuidade dos negócios. Este artigo apresenta o resultado de um estudo baseado em uma pesquisa quantitativa com gestores de TI em um dos três Estados do nordeste brasileiro de maior relevância econômica realizada em 2012 visando avaliar os atuais investimentos em recursos de TI, mensurar os impactos e identificar as principais causas das paradas não programadas apontando as oportunidades de melhoria no que tange infraestrutura, pessoas, processos e serviços para garantir a continuidade e disponibilidade dos recursos de TI à organização possibilitando a estudantes, engenheiros

de software e profissionais em geral da área de Tecnologia da Informação e Comunicação atualizarem seus conhecimentos sobre um tema relevante e alinhado com o ambiente globalizado em que vivemos.

Palavras Chave: Gestão de TI - Alta Disponibilidade - Sistemas Críticos - Infraestrutura de TI - Causa das Paradas

1. INTRODUÇÃO

No mundo globalizado em que empresas e organizações se inserem exige que estas apresentem uma incessante busca pela continuidade de seus negócios. Esta continuidade depende, em quase sua totalidade, da disponibilidade de acesso aos sistemas e aplicações que suportam o negócio e estão em operação na infraestrutura de tecnologia da informação. Torna-se cada vez mais evidente aos dirigentes das empresas, e também aos investidores, que não há mais espaço para paradas não programadas ou mesmo perdas de desempenho, ainda que momentâneas, nestes sistemas críticos ao negócio.

Manter a dinâmica destas organizações neste mercado altamente competitivo, sem comprometer sua presença em momento algum, exige considerar aspectos fundamentais, como: a) infraestrutura, que contempla os equipamentos, ou *hardware*, as aplicações e sistemas operacionais, ou *software,* e ambiente onde estes equipamentos estão instalados e operacionais, ou *data centers*; b) capacitação das pessoas que operam e suportam essa infraestrutura; c) nível de serviços de suporte e assitência técnica com os fornecedores que provêem essa infraestrutura de TI e, por fim; d) processos de governança de TI para gerir as pessoas e a infraestrutura. Esta última, seguindo guias de melhores práticas aplicados mundialmente como ITIL - *Information Technology Infrastructure Library* (APMG & CABINET OFFICE, 2012) ou COBIT - *Control Objectives for information and related Technology* (ITGM, 2007).

É importante salientar aqui a existência de um processo de aprendizado contínuo, que identifique a causa das paradas não programadas (*unplanned downtimes)* em sistemas e aplicações. Um processo que seja responsável por apontar oportunidades de melhorias e direcionar investimentos em TI, tornando-se com isto importante apoio aos gestores nos momentos de tomada de decisão, quando visam à continuidade dos negócios.

Dentro deste quadro é que institutos de pesquisa focados no mercado de TI, como o Gartner nos EUA, realizam pesquisas de campo visando prover subsídios para os gestores de TI, para que as diversas empresas e organizações em que estes atuam possam efetuar um correto direcionamento de seus investimentos assegurando a continuidade de suas operações e disponibilidade de seus sistemas e aplicações críticos.

Segundo pesquisa de abrangência mundial realizada pelo Gartner em 1998 (WEYGANT, 2001), apontou-se que as causas das paradas não programadas eram em 20% relacionadas a falhas da tecnologia, ou infraestrutura de TI, o que incluía também falhas de *hardware* nos equipamentos, sistema operacional ou de ambiente incluindo desastres naturais. Evidenciava-se ainda nesta pesquisa que 40% estavam em falhas de aplicação (*software*) e, por fim, que os outros 40% estavam relacionados a erros operacionais (falha humana). Estas informações podem ser obervadas na Figura 1.

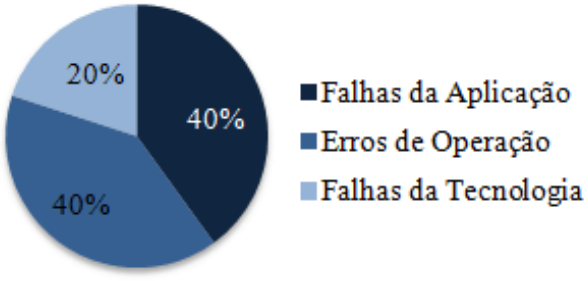

Figura 1: Causa das Paradas Não Programadas em Sistemas. Fonte: Gartner 1998

Complementando esta pesquisa do Gartner, Scott (1999) avaliou que tanto falhas da aplicação como erros de operação podiam ser considerados como falhas de pessoas e processos, o que vinha totalizar 80% dos incidentes, enquanto apenas 20% ficariam relacionados a tecnologia, ou seja, aos equipamentos (*hardware*), aos sistemas operacionais e a questões de ambiente (temperatura/fornecimento de energia) ou desastres naturais.

A questão de entender as causas da não disponibilidade dos serviços é de tal forma importante para empresas, organizações e profissionais da área, que instigou a realização deste trabalho. A pesquisa aqui apresentada teve por objetivo identificar o quanto os gestores de TI conhecem sobre as causas das paradas não programadas em seus sistemas críticos e se estão efetivamente investindo os recursos no foco correto visando mantê-los operacionais e disponíveis.

Compreende-se neste trabalho o conceito de investimento em tecnologias atuais de alta disponibilidade segundo apresentado por Marcus & Stern (2003) e que se depreende a existência de redundância de componentes de *hardware*; a presença de sistemas em *cluster* que permitem a continuidade das operações mesmo que ocorra a falha de um dos servidores, havendo com isto a mudança das aplicações para os servidores remanescentes (GOPALAKRISHNAN, 2007); ambientes ou *data centers* replicados; a melhoria das pessoas com a capacitação da equipe por meio de treinamentos técnicos, e também a gestão de TI acrescido da contratação de serviços de suporte e assistência técnica, em que se preveem acordos de níveis de serviço ou SLA's – *Service Level Agreements* (LEWIS, 1999) que contenplem tempos de solução pré-estabelecidos para problemas e atividades pró-ativas bem como na adoção de uma governança de TI baseada nas melhores práticas de guias como ITIL ou COBIT.

2. SISTEMAS CRÍTICOS DE NEGÓCIOS E AMBIENTES COMPUTACIONAIS DE ALTA DISPONIBILIDADE

Com este avanço da tecnologia da informação em praticamente todas as áreas de negócio, a dependência aos sistemas também tornou-se cada vez maior. Desta forma, surgiu o conceito de sistemas críticos, ou seja, sistemas onde as principais características são: confiabilidade, disponibilidade, proteção e segurança (SOMERVILLE, 2007). A falha destes sistemas críticos de negócios pode causar sérios impactos financeiros às organizações desde atrasos nas operações e manufatura, perdas irrecuperáveis de receita até prejuízos intangíveis à própria marca e imagem perante os clientes. Portanto, um sistema de tarifação de chamadas telefônicas para uma empresa de telecomunicações ou um sistema de vendas de passagens pela internet para uma determinada empresa aérea são considerados exemplos de sistemas críticos de negócios que não podem sofrer interrupções não planejadas.

Estas interrupções não planejadas chamadas na literatura como *unplanned downtimes* ou paradas não programadas representam a situação onde um cliente ou usuário não consegue executar sua tarefa por indisponibilidade ou perda de desempenho do sistema (MARCUS & STERN, 2003).

No intuito de evitar estas paradas não programadas e minimizar as paradas programadas para manutenções agendadas em sistemas críticos, foi definido um segundo conceito chamado ambientes computacionais de alta disponibilidade (WEYGANT, 2001). Trata-se de um conjunto de tecnologias de redundância e segurança aplicados aos componentes do sistema desde o ambiente ou *data center* onde os equipamentos encontram-se instalados com controle de acesso, *Nobreaks* ou UPS – *uninterruptable power supplies* para evitar desligamento abrupto por falhas de energia a servidores, dispositivos de rede e armazenamento de dados com componentes de *hardware* redundantes que mantém-se operacionais mesmo após apresentar algum tipo de falha, redundância de equipamentos,

redundância de conexões de rede até sistemas em *cluster* que mantém-se operacionais mesmo com a falha completa de um servidor ou componente da rede de dados sempre visando eliminar os pontos únicos de falha ou *SPOFs - Single Point of Failures*. Um componente do *hardware* ou *software* que não possua um segundo componente como espera ou redundante e cuja falha acarreta na indisponibilidade de todo o sistema é considerado um *SPOF* (WEYGANT, 2001).

Desta forma, os servidores, dispositivos de rede e demais equipamentos de um sistema crítico devem dispor de componentes básicos como fontes de alimentação e ventiladores redundantes que permitam a falha de um destes componentes sem que haja interrupção da operação do equipamento pois em caso de não haver tais componentes redundantes, a falha de uma fonte de alimentação representa uma parada não programada imediata do equipamento. Também é importante que estes equipamentos tenham a própria monitoração interna via *firmware* e provenham informações de falhas ou pré-falhas bem como de alterações de temperatura interna ou alimentação elétrica para alguma ferramenta de monitoração externa possibilitando a identificação e correção de falhas ou pré-falhas preventivamente.

Em termos de módulos de memórias, é recomendado a utilização de componentes com a tecnologia *ECC – Error Correction Code* que permite a autocorreção de erros mais simples, normalmente erros de um único bit, reduzindo as paradas não programadas por falha de memória.

Outro ponto de vulnerabilidade dos equipamentos é o código interno também conhecido como *firmware*. Embora também seja um ponto único de falha, a principal ação a ser adotada no intuito de evitar problemas é manter a versão de *firmware* sempre atualizada de acordo com o fabricante garantindo que as correções e melhorias conhecidas mais recentes estejam aplicadas.

Conforme os autores (MARCUS & STERN, 2003), as falhas de *hardware* mais frequentes estão relacionadas a discos rígidos ou *HD*s devido seus componentes eletromecânicos, as altas velocidades de rotação e a complexibilidade dos seus mecanismos. Com o objetivo de evitar a perda ou corrupção de dados, adota-se dispositivos de armazenamento de dados com tecnologia RAID (*Redundant Array of Independent Disks)* que possibilitam um grupo de discos operarem em conjunto como uma única unidade lógica utilizando algoritmos de paridade ou espelhamento que mantém a integridade dos dados mesmo que ocorra a falha de um destes discos rígidos que compõe este grupo. 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), RAID4 (disco de paridade), RAID5 (paridade distribuída), RAID6 (dupla paridade distribuída) e RAID10 (espelhamento distribuído através da combinação de RAID0 + RAID1) (TROPPENS *et* al, 2009).

Como complemento, esses ambientes de alta disponibilidade, além da tecnologia aplicada a infraestrutura de TI requerem ferramentas automatizadas de monitoração que reportem falhas ou pré-falhas de componentes ou redução de desempenho bem como serviços de suporte e assistência técnica que apliquem correções e melhorias conhecidas de forma pró-ativa, ou seja, preventivamente evitando que um problema conhecido aconteça reduzindo a possibilidade de paradas não programadas.

Associados a estas tecnologias e configurações de alta disponibilidade da infraestrutura de TI e serviços de monitoração e pró-atividade também conhecidos como serviços de Missão Crítica, agregam-se processos de governança de TI que definem e controlam desde o planejamento, documentação e implementação até o gerenciamento das operações, controle de mudanças, gerenciamento de disponibilidade, gerenciamento de

incidentes, identificação de causa raiz dos problemas, gerenciamento de níveis acordados de serviços, capacitação de pessoal e melhoria contínua através das lições aprendidas alinhando as ações de TI com as estratégias da organização baseados em guias de melhores práticas como ITIL ou COBIT.

3. METODOLOGIA DA PESQUISA

O trabalho buscou apreender esta realidade no mercado brasileiro mais especificamente para uma das três maiores economias do nordeste do Brasil que é o Estado do Ceará (IBGE, 2011). Por isto, realizou-se uma pesquisa de campo, de abordagem quantitativa, com base no tema Avaliação da Gestão dos Ambientes de TI neste Estado.

Este trabalho inicialmente foi enviado para um grupo de cinco gestores de TI com o objetivo de avaliação de conteúdo e efetividade da pesquisa em estudo. Só depois da validação do instrumento de pesquisa foi então encaminhado a um grupo de 160 gestores de TI. Para esta fase da pesquisa, tomou-se como base tanto a relação de gestores de TIC disposta na página da Etice - Empresa de Tecnologia da Informação do Governo do Estado do Ceará presente na internet (ETICE, 2011), quanto se efetuou contatos com os associados do GGTIC-CE - Grupo de Gestores de Tecnologia da Informação e Comunicação do Ceará (GGTIC-CE, 2011).

O intuito foi de alcançar de forma aleatória as áreas de educação, manufatura, saúde, serviços, setor público e varejo de empresas pequenas, médias e de grande porte neste Estado. Tomando a facilidade de acesso à Internet como estratégia de ação, construiu-se com a ferramenta *Survey Monkey* a forma de viabilizar a participação de todos os pesquisados, visto que esta ferramenta é reconhecida como principal provedor mundial de soluções de questionários pela internet (IDGNOW, 2012).

Desta forma, a pesquisa circuncreveu-se a uma determinada geografia e a um público especialista específico de coordenadores e gerentes de TI. É importante ressaltar que, embora se entenda que seja o diretor de TI ou CIO – *Chief Information Officer* o executivo que define em conjunto com a diretoria executiva os investimentos anuais destinados a área de TI entre outras atribuições (RODRIGUES *et* al., 2009), são os coordenadores e gerentes de TI como detentores do conhecimento técnico na área e experiência na operação e gestão dos sistemas, os principais influenciadores na tomada de decisão pelo nível executivo da empresa em relação as necessidades da área de tecnologia da informação.

A pesquisa de campo na versão final foi aplicada entre dezembro de 2011 e março de 2012. Em sua estrutura contou com 20 perguntas, sendo 19 questões objetivas com cinco opções de escolha a serem respondidas obrigatoriamente pelo pesquisado e uma questão descritiva opcional. As quatro primeiras perguntas tiveram por objetivo caracterizar o cargo que entrevistado ocupava (coordenador ou gerente de TI), sua experiência profissional em anos de atuação na área bem como o ramo e porte da empresa. Cinco questões 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 serviços de suporte e assitência técnica contratados. Outras quatro questões buscaram identificar a qualificação da equipe técnica e perfil de investimento em treinamento da área de TI e se adotam algum conjunto de boas práticas de governança de TI como ITIL ou COBIT e qual o nível de maturidade dessa governança.

O ponto principal da pesquisa abordou com quatro questões objetivas se houveram paradas não programadas em sistemas críticos nos últimos 12 meses, a quantidade e duração destes *unplanned downtimes*, a existência de impactos financeiros e operacionais, e ainda, se a

causa ou causas foram identificadas. 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.

Com base nos resultados desta pesquisa, foi efetuada uma análise estatística descritiva visando identificar as principais causas das paradas não programadas nos sistemas críticos bem como compreender se os gestores de TI estão efetivamente investindo recursos nas áreas necessárias que garantam continuidade das empresas, ou seja, investimentos em termos de infraestrutura, pessoas, serviços e processos. O escopo do trabalho buscou desvelar os esforços para evitar novas paradas mantendo os ambientes de TI, disponíveis e operacionais, contribuindo assim para a continuidade dos negócios das empresas e organizações.

4. RESULTADOS DA PESQUISA DE CAMPO COM GESTORES DE TI

A pesquisa contou com sessenta e quatro questionários respondidos ao todo durante o período em que esteve disponível para respostas. Destes, 33% foram respondidos por coordenadores de suporte ou infraestrutura e 67% por gerentes de infraestrutura de TI ou gerentes de operações e suporte de TI. A população pesquisada mostrou-se de grande experiência na área de atuação, sendo constituída por profissionais cuja distribuição era dada por 19,0% entre 5 e 10 anos de experiência, 28,6% entre 10 e 20 anos e 47,6% acima de 20 anos. Assim evidenciou-se que acima de 95% dos entrevistados tinham 5 ou mais anos de experiência na área de tecnologia da informação.

Segundo as respostas destes gestores de TI pesquisados, apenas 25% das empresas e organizações não apresentaram paradas não programadas em seus sistemas críticos ao longo dos últimos doze meses. Desta forma, compreende-se que a grande maioria sofreu indisponibilidade de sistemas críticos e algum impacto, mesmo que mínimo, em suas operações de negócios conforme ilustra o gráfico da Figura 2.

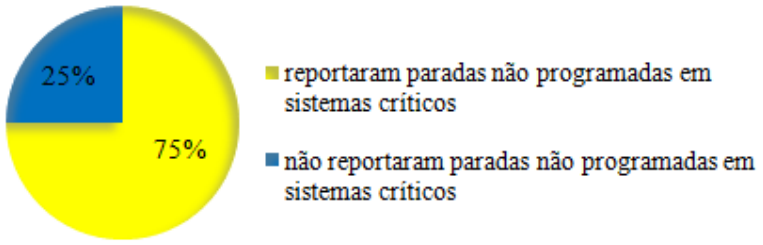

Figura 2: Gráfico de Empresas e Organizações que apresentaram ou não paradas não programadas em seus sistemas críticos nos últimos doze meses.

Comparando as empresas e organizações que reportaram paradas não programadas com as que não sofreram indisponibilidades não previstas em seus sistemas críticos, pode-se observar que quanto ao porte das empresas em termos de faturamente anual seguindo a distribuição definida pelo BNDES (2012), ambas as amostras apresentam uma distribuição semelhante entre o perfil das empresas pesquisadas validando a comparação entre essas duas situações (com paradas não programadas e sem paradas não programadas nos sistemas críticos nos últrimos doze meses) conforme demonstra a Tabela 1.

Tabela 1: Comparação de porte das empresas entre as que apresentaram e as que não apresentaram paradas não programadas em seus sistemas críticos.

Porte da empresa 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%

Salienta-se que as informações obtidas dos gestores de TI que em suas respostas reportaram paradas não programadas em sistemas críticos ao longo dos últimos 12 meses, vieram apresentar uma tendência diferente ao estudo anteriormente realizado pelo Gartner (SCOTT, 2001). Este estudo anterior apontou que apenas 20% das paradas não programadas seriam relacionadas a falhas da tecnologia ou infraestrutura de TI, composta por equipamentos *(hardware)*, sistema operacional e ambiente *(data center).* Já a pesquisa recente realizada entre os gestores de TI no Ceará questionando sobre o mesmo tema reportou que em 66,7% dos casos a falha ocorreu na infraestrutura, seguido de 14,7% de falhas da aplicação, 8,3% falha operacional ou erro humano, 8,3% em falha de processos e apenas 2,1% a causa não foi identicada como ilustra a Figura 3.

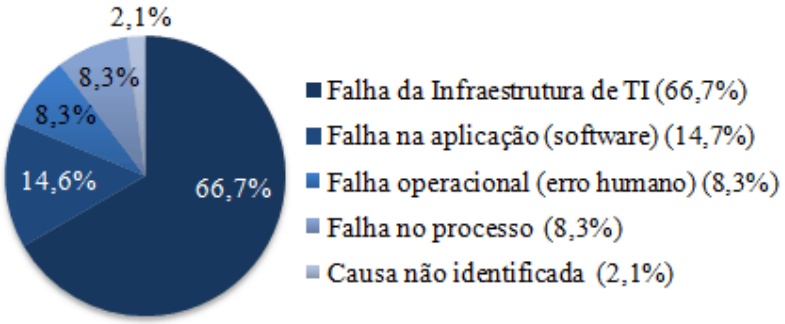

Figura 3: Causa das paradas não programadas em sistema críticos

Com o objetivo de aprofundar a análise buscando identificar um motivo ou motivos para um índice tão relevante de paradas não programadas em sistemas críticos relacionadas a falhas na infraestrutura de TI, foi realizada uma comparação entre as empresas e organizações que não reportaram paradas com aquelas outras que reportaram paradas, com base nas respostas relacionadas à infraestrutura, no que tange a redundâncias de *hardware* nos servidores, sistemas configurados em *cluster* e redundâncias de *data centers* onde claramente apontaram diferenças substanciais que podem justificar tal resultado.

A Figura 4 demonstra que quando perguntados sobre as características de redundância no *hardware* dos equipamentos, apenas 35,2% responderam que todos os sistemas críticos das empresas, que apresentaram paradas não programadas, dispunham de tais características contra 62,5% das empresas que não tiveram indisponibilidades não planejadas, ou seja, quase duas vezes menor. Cabe observar aqui que isto significa que uma simples falha de fonte de alimentação do servidor, pode causar uma parada indesejada em um sistema crítico à empresa.

Na questão de configuração dos sistemas críticos em uma solução de *cluster,* que permite a rápida migração da aplicação entre servidores em caso de falha de um servidor por completo mantendo a disponibilidade da aplicação para os usuários no servidor remanescente que compõe o *cluster*, as respostas demonstraram uma discrepância ainda maior que o dobro. Neste ponto, apenas 12,5% dos gestores de TI das empresas que apresentaram paradas não programadas responderam que todos os sistemas críticos estão configurados em *cluster* quando 31,3% dos gestores de TI que não reportaram paradas responderam que todos os sistemas críticos estão configurados em *cluster*.

A diferença considerável também ocorre na pergunta sobre *data centers* reduntantes, isto é, sistemas críticos replicados em dois ambientes físicos distintos, 25% dos entrevistados que não reportaram paradas responderam que todos seus sistemas críticos estão replicados em dois *data centers*, já somente 10% dos entrevistados que relataram paradas não programadas informaram que seus sistemas críticos tem esta característica estando replicados em *data centers* distintos.

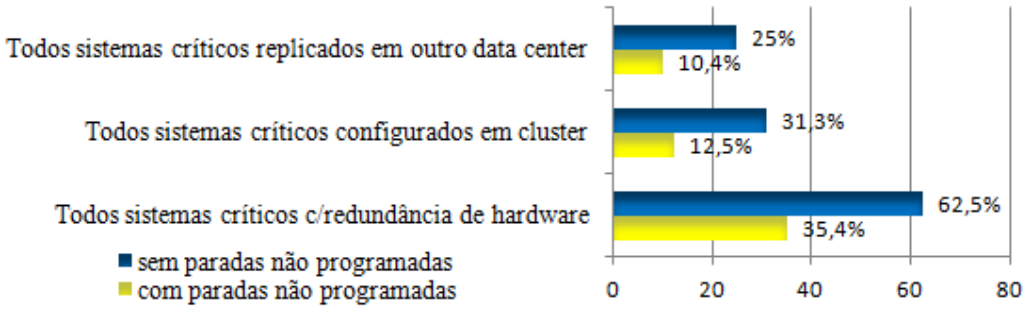

Figura 4: Quadro comparativo entre as características da infraestrutura de TI de empresas e organizações que apresentaram paradas não programadas com as que não apresetaram tais incidentes.

Complementando a análise sobre estes três pontos relacionados a infraestrutura, isto é, redundância de componentes de *hardware* nos equipamentos, configuração em *cluster* dos servidores e replicação de *data centers*, com base na comparação da adoção dos mesmos com a duração das paradas não programadas, pode-se perceber através das respostas dos gestores de TI entrevistados que, com a implementação destas três técnicas ou tecnologias, menor foi o tempo reportado de indisponibilidade dos sistemas. Desta forma, a infraestrutura de TI contendo estas três características quando não evita paradas indesejadas, reduz consideravelmente o tempo de recuperação dos sistemas críticos minimizando o impacto às operações e ao próprio negócio das empresas e organizações.

As Figuras 5, 6 e 7 demonstram esta alta porcentagem de restabelecimento de incidentes que geraram indisponibilidades não programadas em até duas horas considerando as respostas dos gestores que apontaram conter tais características de redundância de *hardware*, sistemas em *cluster* e *data centers* replicados nos sistemas críticos.

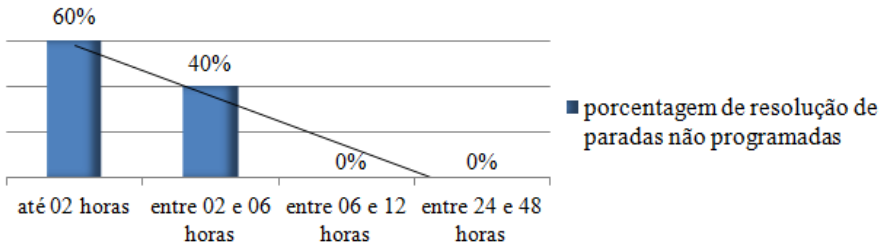

Figura 5: Tempo para resolução das paradas não programadas em sistemas críticos replicados em entre *data centers* salientando que não houve resposta apontando paradas não programadas entre 12 e 24 horas sendo esta opção excluída deste e próximos gráficos.

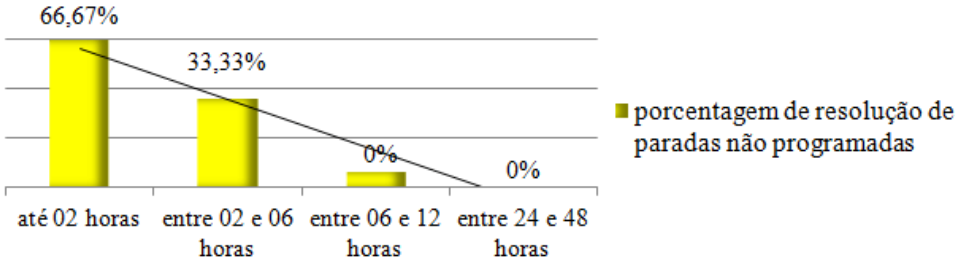

Figura 6: Tempo para resolução das paradas não programadas em sistemas críticos configurados em *cluster*.

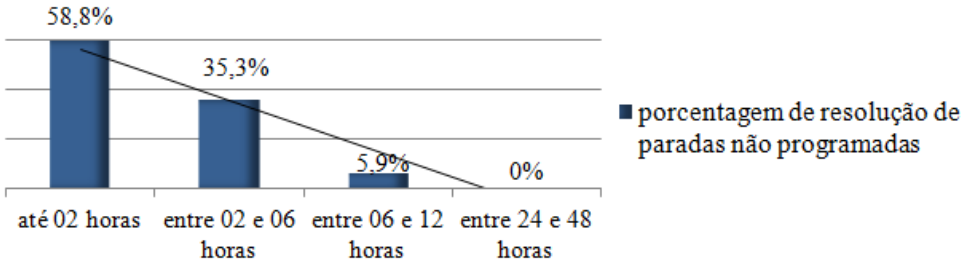

Figura 7: Tempo para resolução das paradas não programadas em sistemas críticos que contenham componentes de *hardware* reduntantes.

Quando perguntados sobre a existência de ferramentas de gerenciamento e monitoração pró-ativas instaladas e configuradas em seus ambientes de TI visando a monitoração de servidores, sistemas, aplicações críticas e infraestrutura de redes, ambos grupos de gestores, ou seja, tanto os que reportaram indisponibilidades como os que não reportaram tais eventos relataram que apenas entre 25,1% e 35,4% adotam ferramentas de gerenciamento de falhas e desempenho em toda a infraestrutura de TI. Portanto, diante deste cenário onde tanto as empresas que adotam ferramentas de gerenciamento como as que não adotam tem relatos de indisponibilidades não planejadas, percebe-se que apenas a adoção de tais ferramentas pode não ser suficiente para evitar paradas não programadas nos sistemas críticos. Salvo se pela falta da monitoração, a falha de um componente redundante não for identificada e corrigida pela equipe técnica antes que ocorra uma segunda falha no outro componente da redundância gerando a indisponibilidade de todo o sistema. Entretanto, a análise comparativa entre a duração das paradas não programadas e a relação com a adoção de ferramentas de monitoração da infraestrutura de TI aponta que, embora as ferramentas não evitem a indisponibilidade, contribuem significativamente como instrumento de apoio à equipe técnica para a resolução mais rápida da situação e restabelecimento do sistema reduzindo o tempo total da parada não programada. Portanto, uma boa prática a ser considerada e adotada pela gestão de TI.

Com o objetivo de avaliar os aspectos de níveis de serviço de suporte e assistência técnica contratados com os fornecedores da solução de infraestrutura de TI confrontou-se os resultados com base nas respostas dos gestores de TI que reportaram incidentes nos sistemas críticos com aqueles que não o fizeram. O resultado sugere às empresas e organizações que apresentaram paradas não programadas em ambientes críticos uma reavaliação no nível de serviço contratato com os fornecedores para prever Acordos de Nível de Serviço (SLAs) com um tempo de resolução pré-definido para os problemas de *hardware* apresentados e serviços complementares de pró-atividade. Estes últimos correspondem àqueles aplicados preventivamente em atualizações de *firmwares* e *softwares* evitando a ocorrência de problemas já conhecidos pelos fabricantes e contribuindo para a redução de falhas na infraestrutura e aplicações. A Figura 8 permite visualizar este quadro onde 43,8% das empresas que não reportaram paradas tem estes serviços diferenciados contratados com seus fornecedores e apenas 25% das empresas que apresentaram problemas os tem.

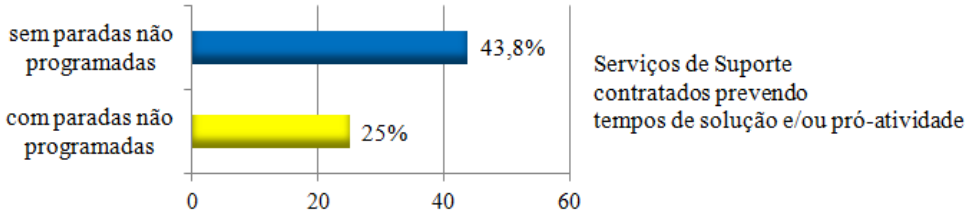

Figura 8: Comparação entre as empresas e organizações que apresentaram paradas não programadas com as que não apresentaram tais incidentes relacionando com a contratação de serviços de suporte prevendo SLAs.

A eficácia da contratação de serviços de suporte e assistência técnica que preveem um SLA de tempo em horas para solução do problema apresentado e em adicional contemplem serviços pró-ativos no intuito de minimizar indisponibilidades dos sistemas críticos também é demonstrada no tempo decorrido para restabelecimento do sistema que em 100% dos casos reportados na pesquisa, foram solucionados em até 06 horas sendo 42% em até duas horas e 58% entre 02 e 06 horas.

Seguindo a análise comparativa entre os grupos de gestores que reportaram indisponibilidades e os que não reportaram, avaliou-se também os investimentos em treinamento e capacitação do pessoal e a adoção de melhores práticas de governança de TI como ITIL e COBIT na gestão de processos e serviços.

Quanto a capacitação da equipe da área de TI, observou-se que nas empresas onde não foram reportadas paradas não programadas há um maior investimento em treinamentos possibilitando a participação dos principais membros da equipe em treinamentos formais em sala e ensino a distância a todos como ilustrado na Figura 9.

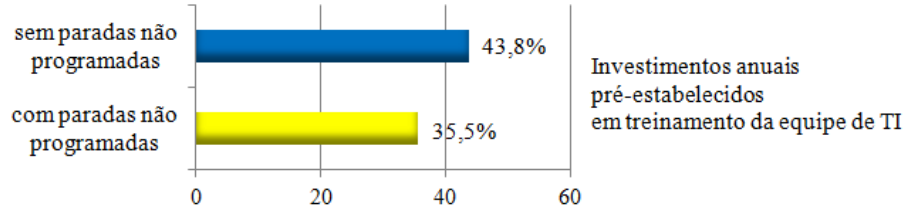

Figura 9: Comparação entre as empresas e organizações que apresentaram paradas não programadas com as que não apresentaram tais incidentes relacionando com os investimentos anuais pré-estabelecidos em treinamento.

Não obstante a diferença observada com relação aos investimentos em treinamento entre empresas que registraram paradas e as que não registraram tais eventos, pode-se constatar, através da comparação com o tempo de restabelecimento dos sistemas críticos após uma parada não programada, que uma equipe melhor treinada tem a habilidade resolver a situação em um menor espaço de tempo reduzindo o impacto aos negócios das empresas e organizações conforme demonstra a Figura 10 onde empresas que investem regularmente em treinamento recuperam a maior parte dos incidentes de indisponibilidade em até duas horas.

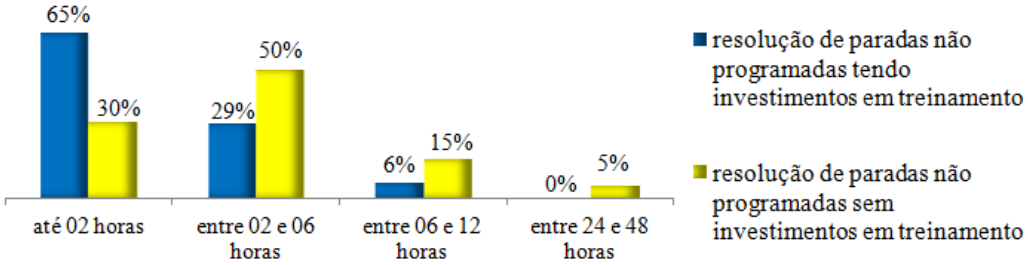

Figura 10: Quadro comparativo entre as empresas e organizações que possuem investimentos anuais em

treinamento da equipe e as que não fazem investimentos nessa área em relação ao tempo de recuperação dos incidentes de indisponibilidade de sistemas críticos

Com relação a adoção de melhores práticas de governança de TI como ITIL e COBIT, 56,3% das empresas que reportaram paradas não programadas nos últimos doze meses ainda não adotaram tais práticas enquanto o mesmo número, ou seja, 56,3% das empresas que não registraram indisponibilidades já aplicam um conjunto de melhores práticas de governança de TI. Quanto a maturidade da aplicação de melhores práticas de gestão, controle e processos, a diferença ainda é maior onde 31,3% das empresas capazes de manter seus sistemas críticos sem indisponibilidades tem as melhores práticas ou em fase final de implementação ou implementadas há mais de dois anos enquanto apenas 14,6% das empresas que permanecem sofrendo paradas inesperadas em seus sistemas críticos tem o mesmo nível de maturação dos processos de controle e gestão seguindo melhores práticas de governância de TI.

Analisando os casos de paradas não programadas onde o gestor apontou como causa falha no processo ou erro humano, 75% destes eventos ocorreram em empresas ou organizações que ainda não adotaram uma governança de TI baseada em um guia de melhores práticas como o ITIL de acordo com o apresentado na Figura 11.

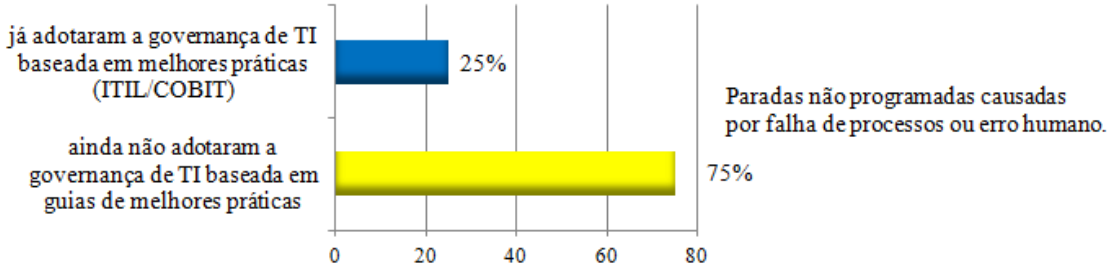

Figura 11: Análise das paradas não programadas causadas por falha de processo ou erro humano em comparação com a adoção de melhores práticas de governança de TI pelas empresas

Desta forma, levando em consideração as respostas relatadas com os resultados obtidos na análise desses dados bem como que o ITIL, na versão atual v3 é baseado em cinco livros (KNELLER, 2010): Estratégias de Serviços, Transição de Serviços, Operação de Serviços, Melhoria Contínua de Serviços e Modelo de Serviços sendo que neste último contém o processo de gerenciamento da disponibilidade responsável por garantir que a infraestrutura, processos, ferramentas e responsabilidades das pessoas estejam adequados para atender as demandas pelos serviços de TI havendo ainda um subprocesso de monitoramento e registro dos níveis de disponibilidade dos sistemas, permite concluir-se quão benéfico é para a continuidade das operações de TI aplicar o ITIL nas empresas.

Sobre as respostas apresentadas à pergunta final descritiva e opcional referente ao principal desafio do gestor de TI para manter disponíveis e operacionais os sistemas críticos para sua empresa ou organização, 36% dos entrevistados expuseram suas opiniões. Dentre os desafios do gestor de TI mais apontados pelos participantes da pesquisa que responderam esta pergunta opcional estão a questão de capacitação de pessoal, entre elas, foram significativas as afirmações: "*O principal desafio em nossa região é a dificuldade em encontrar mão de obra qualificada.*", "*equipe capacitada e pró-ativa.*", "*o maior desafio é qualificar e manter profissionais. Esta qualificação deve contemplar tanto a capacitação técnica quanto em governança de TI.*" e as questões relacionadas a adoção de boas práticas de governança de TI, podem ser vistos como exemplos as afirmações: "*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.*", "*Implantar processos de Gerenciamento de Continuidade de Negócios,*

Gerenciamento de Capacidade e Gerenciamento de Disponibilidade" e "*A implantação de ferramentas de gerenciamento de processos ainda é um desafio junto aos setores internos.*".

Portanto, tais dificuldades expressas pelos gestores de TI que colaboraram com a pesquisa, evidenciam, de forma inequívoca, a importância do treinamento e capacitação das equipes, bem como a aplicação de melhores práticas de governança de TI.

5. CONCLUSÕES

A análise dos dados obtidos com esta pesquisa de campo aplicada a gestores de TI do Estado do Ceará apresenta tendência diferente ao observado na pesquisa realizada pelo Gartner, ainda no início da década passada (SCOTT, 2001), no que se refere à causa das paradas não programadas em sistemas críticos apontando uma maior incidência de falhas da tecnologia ou infraestrutura de TI em relação a falhas de aplicação e erros de operação.

A pesquisa descrita neste trabalho teve por objetivos identificar o quanto os gestores de TI conhecem sobre as causas das paradas não programadas em seus sistemas críticos e nesse quesito, com base nas respostas apresentadas, os entrevistados demonstraram ter o entendimento das causas pois em apenas 2,1% das respostas, não foram capazes de identificar o motivo que causou a indisponibilidade. Entretanto, sobre o investimento de recursos em TI no foco correto visando manter os sistemas críticos operacionais e disponíveis, segundo objetivo deste estudo, as informações apontam para importantes oportunidades de melhoria pois os sistemas críticos da forma como estão atualmente implementados ainda carecem de investimentos na robustez do *hardware* em termos de características de redundância a falhas de componentes bem como de configuração de *sotfware* em *cluster* para aumento da disponibilidade até a avaliação de investimentos em replicação de *data centers* para sistemas críticos que impactem o negócio principal da organização. Considerando as possíveis perdas financeiras associadas as paradas não programadas e a redução do custo da tecnologia em equipamentos e *softwares* ao longo dos últimos anos, torna-se viável esta reavaliação de posicionamento por parte dos gestores de TI quanto os futuros investimentos na infraestrutura, serviços, pessoas e processos.

Compreende-se aqui capacitação das pessoas não apenas vista em conhecimento técnico, que certamente auxiliará estes profissionais a adequar as infraestruturas de TI em conformidade com as atuais tecnologias de redundância de *hardware* (utilização de sistemas em *cluster,* virtualização, equipamentos de armazenamento de dados com tecnologia RAID) e ambiente (*data center*), mas também, fundamentalmente importante o entendimento do quanto é necessária a adoção de melhores práticas de governança de TI que se encontram dispostas em guias como ITIL ou COBIT.

Este esforço estará visando a padronização de processos de gerência de disponibilidade dos sistemas, incidentes, problemas, mudanças e documentação e auxiliará muito na definição da infraestrutura de TI necessária para atender as demandas bem como na contratação de serviços de suporte prevendo SLAs de tempo de solução e pró-atividade junto a fornecedores que contemplem ações de monitoramento e pró-atividade minimizando problemas e paradas não programadas nos sistemas críticos e mantendo disponíveis e operacionais tais sistemas e aplicações indispensáveis para a continuidade dos negócios de empresas e organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

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

BNDES, Brasil 2012, 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 12 Jan 2012.

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.

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.

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

IBGE, Contas Regionais do Brasil 2005-2009, IBGE, Rio de Janeiro, 2011. Disponível em:< http://www.ibge.gov.br/home/estatistica/economia/contasregionais/2009/contasregionais2009.pdf> Acesso em 19 Nov 2011.

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.

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

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

LEWIS, Lundy, *Service Level Management for Enterprise Networks*, ed. Artech House, EUA, 1999.

MARCUS, Evan & STERN, Hal, *Blueprints for High Availability: Designing Resilient Distributed Systems*, 2ª edição, ed. John Wiley & Sons, EUA, 2003.

RODRIGUES, Leonel C., MACCARI, Emerson A., SIMÕES, Sergio 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, 2009, p.483-506

SCOTT, D., *NSM: Often the Weakest Link in Business Availability, AV-13-9472 Research 03 July 2001*, Gartner, EUA, 2001.

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

SOMERVILLE, Ian, Engenharia de Software, 8ª edição, Ed. Pearson Addison-Wesley, São Paulo, 2007.

TROPPENS, Ulf, ERKENS, Rainer, MUELLER-FRIEDT, Wolfgang, WOLAFKA, Rainer & HAUSTEIN, Nils, *Storage Networks Explained: Basics and Application of Fibre Channel SAN, NAS, iSCSI, InfiniBand and FCoE*, 2ª Edição, Ed. John Wiley & Sons, EUA, 2009.

WEYGANT, Peter, *Clusters for High Availability: A Primer of HP Solutions*, 2ª edição, Ed. Prentice Hall, EUA, 2001.