5CONTECSI June 04 - 06, 2008 São Paulo, Brazil

5th International Conference on Information Systems and Technology Management
5º Congresso Internacional de Gestão da Tecnologia e Sistema de Informação

De 04 a 06 de Junho de 2008 - São Paulo - Brasil

PS-1066

MONITORING OF THE CONTINGENCY PLAN IN INFORMATION TECHNOLOGY

Vanessa Borges de Matos (FAE Business School) – vanessam@boticario.com.br
Carlos Eduardo de Almeida Machado (FAE Business School) –cmachado@montana.ind.br
Milton Pinheiro Fernandes (FAE Business School) – mpinheirofernandes@yahoo.com.br
Denis Alcides Rezende (Pontifícia Universidade Católica do Paraná,
FAE Business School, Paraná, Brasil) – denis.rezende@pucpr.br

The organizations have realized the importance of the strategic role of Information Technology (IT). The monitoring for Contingency Plan (PC) is a fundamental tool of organizations management. The objective is to present a model of indicators for the development of a cockpit directing the IT area to monitor a PC aligned to the organization's strategic planning. The methodology of the research focused on the analysis of literature and documentary tracking frameworks in IT, presenting a model to identify the major services and indicators, aimed at obtaining grants to identify the different practices of tracking the PC in the organization. The conclusion reiterates that the plan by itself does not ensure the continuity of business and relevant one continuous monitoring. All this, to ensure its availability and effectiveness if occurs any necessity for the survival for organizations in the current scenario.

Keywords: Information Technology; Plan Continence; Information Management; Monitoring Services; Indicators.

Agradecimento: CNPq.

MONITORAMENTO DO PLANO DE CONTINGÊNCIA EM TECNOLOGIA DA INFORMAÇÃO

Resumo:
As organizações têm percebido a importância do papel da Tecnologia da Informação (TI) mais estratégico. O monitoramento do Plano de Contingência (PC) é uma ferramenta fundamental de gestão das organizações. O objetivo é apresentar um modelo de indicadores para a elaboração de um *cockpit* direcionando a área da TI para monitorar um PC alinhado ao planejamento estratégico da organização. A metodologia da pesquisa enfatizou a análise documental e bibliográfica de *frameworks* de monitoramento em TI, apresentando um modelo que identificasse os principais serviços e indicadores, visando a obtenção de subsídios que permitissem identificar as diferentes práticas de monitoramento do PC na organização. A conclusão reitera que o referido plano não garante por si só a continuidade dos negócios, sendo relevante um monitoramento contínuo, para garantir sua disponibilidade e efetividade diante de uma eventual necessidade para a sobrevivência das organizações no cenário atual.

Palavras-chave:
Tecnologia da Informação; Plano de Continência; Gestão da informação; Monitoramento de Serviços. Indicadores.

1. INTRODUÇÃO

Muitas organizações adotam o monitoramento apenas verbalmente, embora um número crescente delas tenha instituído programas formais. Entretanto, a maioria pensa nisso como uma maneira de acelerar as pessoas menos experientes ou de lhes ensinar comportamentos de liderança. Se visto como uma forma de transferência de conhecimento, o conceito de monitoração torna-se mais fluído. Os especialistas trocam perspectivas com os trabalhadores mais novos, cada um fornecendo ao outro uma porta para um mundo diferente.

A delimitação do tema está embasada na apresentação do problema decorrente da Tecnologia da Informação (TI), que atualmente é difícil imaginar uma organização sem o uso de recursos computacionais, sem equipamentos de informática, telefonia, transferência de dados, sistema de informação, como alguém conseguir imaginar como seria a vida sem energia elétrica? Não há dúvidas que a eletricidade é essencial para a sociedade, assim como a tecnologia é para a maior parte das atividades de uma organização. Com essa dependência da TI, estar sempre disponível quando precisar, os sistemas e infra-estruturas tecnológicas devem ser concebidos e operados de modo a reduzir interrupções causadas por falhas momentâneas de equipamentos de geração ou transmissão. Por conseqüência, torna-se crucial a organização, planejar e monitorar planos de contingências com indicadores que evitem perdas de produtividade e a até acarrete falha num atendimento ao cliente.

Finalizam-se possíveis soluções para justificar o uso de monitoramento de planos de contingência em TI.

A problematização inicia-se em como a inexistência de um Plano de Contingência pode levar empresas a situações críticas de sobrevivência, quando necessário enfrentar situações de emergência. A velocidade da resposta com que consegue reagir frente a estas situações pode fazer a diferença no impacto que terão sobre os negócios. Alguns momentos históricos são explicados por Ferreira (2005) como a bolha dos projetos de Internet e seu conseqüente estouro, com muitas iniciativas minadas por problemas na concepção, principalmente de investimentos. Outro exemplo foi o *bug* do milênio, sob a problemática dos dígitos nos sistemas, mal avaliada em alguns casos. E mais recentemente, os escândalos financeiros que desaguaram na Lei *Sarbanes-Oxley*, contaminando os departamentos de TI.

O valor financeiro decorrente dos problemas nos serviços de TI preocupa qualquer investidor, outros exemplos apresentados por Magalhães e Pinheiros (2007) como se uma operação de corretagem tiver uma interrupção de 1 hora pode haver um prejuízo de US$ 7.840.000. E foi o que acontece com a *eBay* em junho de 1999, devido à falha no sistema, que ficou indisponível por 22 horas, teve um prejuízo entre US$ 3 e 5 milhões em receitas e um declínio na bolsa de 26% nas suas ações.

No ano de 2001 a ABNT homologa a norma NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação, que tem os seguintes objetivos: estabelecer referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança da informação; promover a confiança nas transações comerciais entre as organizações; manter a segurança dos recursos de processamento da informação por prestadores de serviços, controlando o seu acesso; proteger adequadamente os ativos da informação, inventariando-os e alocando uma equipe responsável para cada um; reduzir os riscos de erros humanos, roubo, fraude ou uso indevido das instalações; assegurar que os usuários estejam cientes das ameaças, treinando-os nos procedimentos de segurança e no uso correto das instalações de processamento da informação; prevenir acesso não autorizado às informações e instalações da empresa; minimizar o risco de falhas nos sistemas. Proteger a integridade do software e da informação; estabelecer procedimentos de rotina para execução de cópias de segurança e para a disponibilização dos recursos de reserva; garantir a proteção da infra-estrutura de suporte, principalmente do gerenciamento da rede; prevenir a perda, modificação ou mal uso de informações trocadas entre organizações; e proteger a confidencialidade, autenticidade ou integridade das informações, garantindo que a segurança seja parte integrante dos sistemas de informação.

A norma especifica 127 controles que podem compor o escopo do Sistema de Segurança, tratando aspectos como Política de Segurança, Plano de Contingência, Plano de Continuidade de Negócios, Organização da Segurança, Segurança Física e Ambiental, Controle de Acesso, Legislação, etc. (MACEDO, 2003).

As interrupções nos serviços de TI sempre afetam os negócios, provocando impactos muitas vezes irreversíveis, onde informação não é mais base para o negócio e sim o próprio negócio. Segundo o *Disaster Recovery*

Institute (DRI) de cada cinco organizações que sofrem interrupções nas suas operações por uma semana, duas fecham as portas em menos de três anos. As necessidades das organizações mudam e o plano deve acompanhar essas mudanças sob o risco de se não o fizer, tornar-se ineficaz em garantir a sobrevivência da organização (MAGALHÃES; PINHEIRO, 2007).

Diante do problema enfatizado, formaliza-se as seguintes questões-problema: será que existem padrões de planejamento de planos de contingência?. Faz parte do planejamento de Tecnologia da Informação (TI)? As organizações devem avaliar e atualizar esses planos?

O objetivo desse artigo é apresentar indicadores que direcionem a área de tecnologia da informação a monitorar o plano de contingência operacional.

Justifica-se esse trabalho com base em princípios de responsabilidade e sustentabilidade que as organizações devem gerir seus recursos para honrar compromissos assumidos com mercado, parceiros e colaboradores. E no contexto dos negócios, a competitividade é um divisor de águas no mundo globalizado. E a TI inserida em grande parte dos processos organizacionais, faz-se necessária uma abordagem que maximize a efetividade do valor criado pela TI, tendo um real aumento de produtividade. O Plano de Contingência é um documento que define um conjunto de mecanismos e políticas para evitar que uma situação de emergência seja tratada de maneira incorreta e leve a organização a uma irreversibilidade na continuidade de seus negócios (MAGALHÃES; PINHEIRO, 2007).

O Plano de Contingência deve assegurar que os sistemas de informação e os processos de negócios que sejam vitais para a empresa estejam resguardados. Fazem parte do Plano: a preservação patrimonial da organização e a manutenção dos níveis de serviços acordados com os Clientes. Em casos de sinistros, deve: auxiliar na detecção de causas e origens no menor tempo possível, antecipar problemas, relacionar quais pessoas devem ser capacitadas ou em condições de ser contatadas (MACEDO, 2003).

A ação de *hackers* e *crackers* pode colocar em risco a imagem da empresa, principalmente se for uma instituição financeira, onde a questão segurança faz parte do próprio negócio da organização. A IDC, empresa de pesquisas calcula que no Brasil o investimento com segurança já ultrapassa a marca de US$ 1 bilhão e o setor bancário é responsável por metade dessa cifra, o que representa 10% de todo o orçamento de TI (CORRÊA, 2007).

O *COBIT* 4.0 (2005) apresenta o processo de administração de riscos, não só financeiro, mas na proteção de ativos de TI e recuperação de falhas, e órgãos reguladores estão preocupados com os riscos de tecnologia e segurança de informação. Exemplifica que no *BIS* suporta a visão porque a maior parte dos artigos estudados na indústria financeira foi causada por colapso no controle interno e descuido e TI.

2. FUNDAMENTAÇÃO TEÓRICA

Tem por objetivo definir e apresentar a base conceitual fundamentando os pontos essenciais para o trabalho realizado.

2.1. Tecnologia da informação e sistemas de informação

A Tecnologia da Informação (TI) é conceituada como o conjunto dos recursos tecnológicos e computacionais para guarda de dados, geração e uso da informação e de conhecimentos (REZENDE, 2000). O conceito de tecnologia se refere a um conjunto de conhecimentos científicos, empíricos e intuitivos (BARRETO, 2005).

Stair (1996) define sistema de informação (SI) como um conjunto de elementos ou componentes inter-relacionados que capturam (entrada), transforma e armazena (processo), distribuem (saída) os dados e informações e fornecem um mecanismo de adequação ou modificações nas atividades de entrada ou processamento. Laudon e Laudon (1999) definem sistema de informação como sendo um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações para dar suporte à tomada de decisão e ao controle da organização.

Rodrigues (2006) apresenta a importância da TI e das telecomunicações nos sistemas de informação. A evolução dos sistemas de informação mostra um novo caminho para a indústria da tecnologia de informação e de telecomunicações. Vários fatos e tendências têm contribuído para mudanças bastante significativas e dinâmicas como a globalização, função e propósitos múltiplos das organizações, minimização de custos, convergência de redes, entre outros.

Segundo Rodrigues (2006), as tecnologias da informação e da telecomunicação possuem representatividade nos sistemas de informação, contribuindo para sua evolução e o sucesso nas organizações. O uso destas tecnologias encontra-se em uma constante evolução e conseqüente influência sobre a estrutura organizacional e a maneira como tais recursos são utilizados pela organização.

A adequação e a forma de gerenciamento dos recursos tecnológicos exercem influência direta na produtividade dos usuários, expandindo as oportunidades, além de permitir uma maior flexibilidade nos negócios da organização (RODRIGUES, 2006).

Segundo Rezende (2002), a TI e seus recursos atuais evoluíram muito nesses últimos 45 anos, possibilitando a formação das pessoas e repercutindo na gestão dos negócios. A evolução integrada de recursos tecnológicos, pessoas e gestão contribuíram para o crescimento de organizações inteligentes, com visão macro de processos decisórios operacionais, gerenciais e estratégicos vinculados diretamente aos resultados da empresa.

Rezende (2002) destaca que na década de 1960, as organizações direcionavam os recursos tecnológicos para o processamento centralizado de dados em grandes centros de processamento (*mainframes*) e para os sistemas de controles operacionais, tais como faturamento, estoque, folha de pagamento, finanças e contabilidade. O processamento era realizado de forma mecanizada em grandes grupos ou lotes (*batch*). A finalidade do Processamento de Dados visava a redução de custos e diminuição da mão-de-obra. As funções de

informática não eram representativas e os poucos recursos eram centralizados na área de Processamento de Dados. Com a evolução tecnológica, as empresas começaram a perceber a importância da informação na gestão de seus negócios. As organizações passam a enxergar a informática por outro prisma e adotam esta nova ferramenta como parte integrante dos seus sistemas, substituindo o tradicional processamento de dados.

Nos dias de hoje, a "informática" denomina-se "tecnologia da informação", compreendendo a gestão de dados e controle de acesso às informações. Essa gestão requer um completo plano de contingência e um plano de segurança de dados e informações (REZENDE, 2002).

Para Natale (2007), a TI por meio dos seus sistemas, bases de dados, servidores, tráfego via rede, mídias, Internet, e-mails e outros tantos exemplos, dá suporte integral à organização. Imagine uma empresa que tem seu negócio suportado por TI, ficar algumas horas, dias ou semanas sem poder utilizar algum recurso tecnológico. Os diretores das empresas têm que se perguntar: É possível medir o impacto negativo deste tempo sem o uso da tecnologia para a empresa? Pode-se mensurar quanto cada processo de negócio pode ficar inoperante sem afetar de forma crítica a sobrevivência da empresa? Caso algum incidente de TI ocorra, pode-se recuperar?

Muitas empresas não conseguem mapear estes impactos ou responder a todos os questionamentos, mas podem imaginar todos os transtornos que teriam em suas atividades, caso algum recurso de TI ficasse inoperante por determinado período, interrompendo suas atividades. Cabe a cada empresa julgar o que é importante para o seu negócio. Para garantir que problemas, acidentes ou incidentes tecnológicos não acarretem em prejuízos ou danos irreversíveis, a empresa deve investir em um plano de contingência, que nada mais é que uma estratégia para retornar a um estado anterior a algum problema (NATALE, 2007).

2.2. Indicadores e tecnologia da informação

Ragland (1995) usa o termo indicador para referir-se à métrica que fornece informações úteis sobre o estado do processo e o termo métrica como uma medida da extensão ou do grau a que um produto possui e exibe uma qualidade, uma propriedade, ou um atributo. Os indicadores permitem acompanhar o andamento de um processo identificando riscos em potencial e problemas antes de se tornarem críticos além de controlar a qualidade de um processo bem como a produtividade e auxílio na tomada de decisões. Os Indicadores permitem que uma empresa possa obter informações importantes para a eficiência do processo, no entanto deve-se tomar cuidado quando se tratar de medições estratégicas, uma vez que uma escolha inadequada poderá levar a resultados errôneos. Esses indicadores podem ser classificados conforme: Indicadores operacionais, Indicadores estratégicos, Indicadores de ocorrências (*lagging indicators*) e Indicadores de tendências (*leading indicators*).

Kaplan e Norton (2001) consideram como medidas genéricas de resultados as medidas essenciais de resultados que refletem as metas comuns de muitas estratégias. Essas medidas genéricas de resultado tendem a ser indicadores de ocorrência enquanto que os indicadores de tendências, *leading indicators*, mostram um "estado futuro", permitindo interferências a fim de evitar que os

resultados desejáveis sofram prejuízos. Sendo fundamental que ambos estejam equilibrados, evitando erros futuros.

Takashina e Flores (1996) afirmam que indicadores são essenciais ao planejamento e controle dos processos das organizações, possibilitando o estabelecimento de metas e o seu desdobramento porque os resultados são fundamentais para a análise crítica dos desempenhos, para a tomada de decisões e para o novo ciclo de planejamento. A proposta destes autores é a de que os indicadores devem estar sempre associados às áreas de negócio cujos desempenhos causem maior impacto no sucesso da organização e permitam avaliação no período, em relação às metas e a outros referenciais. Com este procedimento estarão subsidiando a tomada de decisões, apontando níveis, tendências e comparações, conforme segue: níveis - patamar em que os resultados se situam no período; tendência - variação do nível dos resultados em períodos consecutivos; comparação: feita em relação a indicadores compatíveis de outros produtos, outras unidades de negócio ou outras organizações, visando parâmetros de referência para os resultados obtidos. Eles complementam que nos valores dos indicadores é possível, segundo os autores, estabelecer a taxa de melhoria obtida, sua amplitude e importância, lembrando que a geração dos mesmos deve ser criteriosa, de forma a assegurar a disponibilidade dos dados e resultados dos mais relevantes no menor tempo possível e ao menor custo. Acrescentaram, por outro lado, que os indicadores estão intimamente ligados ao conceito de qualidade centrada no cliente, podendo ser gerados a partir das necessidades e expectativas dos clientes, traduzidas pelas características de qualidade do produto ou serviço, sejam eles tangíveis ou não.

A obtenção das informações pode ser uma dificuldade a ser transposta para efetivação de um sistema de indicadores de desempenho. Como afirmam Takashina e Flores (1996), há necessidade de disponibilidade das informações. O sistema deve ser construído de forma a permitir à Administração, no nível de sua gestão estratégica, tomar decisões que exerçam no tempo a função de resolver problemas, readequar procedimentos, perceber problemas e, em último caso, redefinir o processo, seja de planejamento ou do seu controle.

2.3. Plano de contingência

Plano de contingência é documentação que define, passo a passo, ações que devem ser implementadas para determinado processo – ou mesmo a empresa como um todo – volte a operar em menos tempo possível, após a ocorrência de um incidente de segurança que tenha comprometido, total ou parcialmente, sua condição de operação (FAUSTINI, 2007).

O Plano de Contingência deve documentar as capacidades e requisitos técnicos que suportarão as operações de contingência. Sendo essencial à definição de regras definidas, desde as responsabilidades, equipes e procedimentos relacionados com a recuperação do ambiente informatizado após a ocorrência de um desastre (MARINHO, 2003). O plano de contingência deve ser constituído por uma série de ações determinadas relacionadas com o sistema que quer recuperar em caso de falha. A sua complexidade e profundidade deve ser proporcional a complexidade dos sistemas, sem desperdícios ou excesso de informação (MARINHO, 2006).

Caruso e Steffen (1999) complementam que plano de contingência de TI pode ser definido como uma série de documentos que tem como finalidade a recuperação de, uma ou várias, operações tecnológicas interrompidas por algum incidente ou acidente, e que afeta de forma crítica o negócio da empresa.

O plano de contingência envolve mais do que o planejamento para a recuperação da empresa após um desastre. Ele também ajuda a manter funções críticas de uma organização e como se comportar caso algum recurso de TI fique inoperante. Existem muitos modelos e padrões para a criação de planos de contingência, pelas práticas de segurança da informação. Mas cada empresa pode criar o seu plano de contingência de acordo com suas necessidades e suas restrições. Para poder nortear as empresas na criação de um plano de contingência de TI, pode ser levado em consideração alguns fatores e trabalhar em cima deles para adequar a cada empresa (MARINHO, 2003).

De acordo com o NIST (2006) pode-se dividir a criação do plano de contingência em seis itens: identificar a missão ou função crítica do negócio: identificar os objetivos do negócio e priorizar o que deve ser contingenciado, de acordo com restrições e particularidades da empresa. É fundamental para o sucesso do plano de contingência identificar estes objetivos com clareza; identificar os recursos de TI que suportam o negócio: é necessário listar todos os recursos de TI utilizados pela empresa, e em seguida verificar se este recurso é utilizado em tempo integral ou apenas em alguns momentos. Além disso, é preciso analisar os impactos no negócio, caso cada um dos recursos sejam interrompidos; antecipar e monitorar possíveis riscos ou desastres: embora seja impossível pensar de todos os problemas, nesta etapa é necessário identificar os prováveis incidentes, e desenvolver um cenário com as falhas e suas respectivas contingências. Deve-se ter como base todos os recursos levantados no item anterior; criar uma estratégia para o plano de contingência: a estratégia para o plano de contingência pode ser dividida em três partes – emergência, recuperação e restabelecimento. Onde, na fase da emergência serão tomadas ações iniciais para proteger vidas (se for o caso) e evitar maiores danos. Na fase de recuperação a contingência entra para garantir que os sistemas críticos continuem operando. E na fase de restabelecimento indicará as medidas para que as operações retornem ao estado anterior; implementar o plano de contingência: nesta etapa, é necessário implementar as estratégias para proteção das funções críticas. Por exemplo, estabelecer procedimentos para *backup* dos arquivos e aplicações, ou de redundância de discos. Nesta etapa também é necessário fazer toda a documentação do plano de contingência, além de treinar as pessoas envolvidas; testar e revisar constantemente o plano de contingência: um plano de contingência deve ser testado periodicamente para garantir que todas as contingências estão funcionando perfeitamente. Por meio de testes, erros podem ser identificados e melhores práticas implementadas.

3. METODOLOGIA DA PESQUISA

O presente trabalho surgiu da motivação de apresentar um modelo de indicadores para monitorar um plano de contingência em TI, sendo eles feitos por meio de ferramentas, metodologias ou intuitivamente. Uma das preocupações básica dos pesquisadores relacionada com as questões metodológicas de suas pesquisas é a explicação sobre as características específicas dos procedimentos

adequados, para a realização da pesquisa proposta. Assim sendo, nesta, pretende-se utilizar mais que um procedimento de pesquisa e técnica de coleta de dados. Segundo Demo (2000, p. 22), pode-se distinguir, pelo menos, quatro gêneros de pesquisa, mas tendo em conta que nenhum tipo de pesquisa é auto-suficiente, pois "na prática, mescla-se todos acentuando mais este ou aquele tipo de pesquisa". Para a metodologia desta pesquisa referencia-se como modelo a classificação de Gil (1994), com base em seus objetivos, caracterizando-se como, pesquisas exploratórias e pesquisas descritivas.

Com a motivação proposta, definido o objetivo de estudo – gerar forma de compreender como ocorre o processo de monitoramento do plano de contingência de TI nas organizações. A elaboração deste modelo concentra o foco metodológico desse estudo, definindo seu objetivo primordial e permite traçar diretrizes de sua condução, tornando-se o ponto básico da metodologia utilizada.

Para desenvolver a resposta a tal questão, adotou-se a estratégia de, inicialmente, conduzir a pesquisa bibliográfica da área, com a intenção de apresentar corretas inserções, trazendo à comunidade a análise dos resultados com base conceitual. Durante esse processo, foi possível avaliar que o tipo de pesquisa exploratória seria o mais indicado para a pesquisa, em virtude de existirem lacunas de compreensão com relação à modelagem, questionamentos e ferramental de pesquisas para a área. Utilizando-se também de outras técnicas e métodos complementares que pudessem contribuir nos resultados.

Lakatos e Marconi (1985, p. 165) consideram que “o levantamento de dados, primeiro passo de qualquer pesquisa científica, é feito de duas maneiras: pesquisa documental (ou de fontes primárias) e pesquisa bibliográfica (ou de fontes secundárias)”. A pesquisa foi de natureza teórico-reflexiva e exploratória. O levantamento de dados foi feito por meio de análise documental/bibliográfica de frameworks de monitoramento em TI, elementos internos e externos que devem ser monitorados em TI e serviços e indicadores, com o intuito de obter subsídios que nos permitissem identificar as diferentes práticas de monitoramento.

Assim, após delimitar, teoricamente, os elementos e os indicadores, foram possíveis determinar os pontos a serem avaliados nos diferentes serviços de TI e fundamentar as bases da proposta de monitoramento. Para a avaliação de resultados foram considerados 3 aspectos (protocolo de pesquisa):

a) *frameworks* de gestão de TI - refere-se a ferramentas e técnicas das melhores práticas que dão suporte à gestão dos processos da TI;
b) elementos internos e externos - recursos, processos e infra-estrutura que interagem na governança de TI;
c) serviços e indicadores de TI - serviços são todos os produtos gerados pelos processos geridos pela TI e indicadores são índices que permitem monitorar e avaliar por meio de *framework*, o grau de eficácia dos serviços prestados aos seus elementos internos e externos.

Tendo como base as seguintes referências: *ITFlex*, *ITIL*, ABNT NBR ISO/IEC 27001:2006 e *COBIT*

4. MONITORAMENTO DE INDICADORES

Com base nos itens propostos na metodologia, pretende-se no desenvolvimento da pesquisa descrever os pilares para a construção de melhores práticas de monitoramento referenciadas nas ferramentas citadas e finaliza-se com um exemplo de uso dos *frameworks*.

4.1. Frameworks de gestão de TI

Apresentam-se ferramentas que dão suporte à gestão de TI.

4.1.1. ITFlex

A metodologia *ITFlex* tem como objetivo prover a área de TI com um alto grau de flexibilidade na prestação de serviços, de modo a manter o alinhamento estratégico no plano operacional. Tem como origem uma derivação da 3IM (*InterProm's Incremental Implementation Methodology*) e culmina com a proposta de uma "Fábrica de Serviços de TI". Esta "Fábrica" pressupõe que, sendo necessário maximizar a produção, entrega e suporte dos serviços de TI, quanto maior o volume de produção, menor o custo do produto. Desta forma, e utilizando-se dos mesmos conceitos de uma fábrica tradicional, a TI disponibilizaria serviços de forma continuada como em uma linha de produção. A metodologia *ITFlex* propõe estruturar a TI em quatro áreas básicas:

Serviços de TI - Os Clientes dos serviços de TI estão mais interessados nos resultados fornecidos do que na maneira como eles foram concebidos. Assim, a conformação dos processos de TI que suportam o fornecimento de serviços devem estar apoiados na funcionalidade, nos níveis de serviços (SLA's) e nos custos acordados.

Processos de TI - O conjunto de processos de entrega de serviços e suporte de TI deve assegurar que o Cliente receberá exatamente o que foi proposto em termos de TI e deverá suportar os seus processos de negócio. O *framework* utilizado é baseado nas melhores práticas constantes da *ITIL* e deve permitir que o Cliente interaja com os serviços oferecidos pela TI.

Organização dos Recursos de TI – A divisão das tarefas e responsabilidades entre as equipes da TI objetiva fornecer os serviços demandados pelas áreas de negócio e, para garantir competitividade e ser rápida e flexível para fazer frente às constantes mudanças e exigências do mercado, a TI tem que aprimorar programas de capacitação e mecanismos de alerta para o alcance desse objetivo. A flexibilidade proposta deve capacitar a área de TI a se adaptar rapidamente às constates alterações do mercado.

Tecnologia de TI – Provê o gerenciamento da infra-estrutura de TI utilizando-se das ferramentas de gerenciamento de sistemas disponibilizadas pelos próprios fornecedores de cada área. Esta opção baseia-se no fato de que o gerenciamento dos serviços é suportado por ferramentas específicas, mas devem interagir com as ferramentas de gerenciamento de sistemas.

A Fábrica de Serviços de TI deve, da mesma maneira que opera uma fábrica tradicional, ter uma arquitetura orientada a processos de forma a contribuir positivamente na agregação de valor para o negócio. Essa arquitetura permite que a TI identifique os processos que possam vir a ser reutilizados em outros serviços e quanto mais processos internos de serviços possam ser reutilizados, menores serão os prazos e o custo de desenvolvimento de novos serviços de TI.

4.1.2. ITIL (Information Technology Infrastructure Library)

No final da década de 80 a CCTA (Agência Central de Comunicação e Telecom), atual OGC (Escritório de Comércio do Governo), do governo Britânico, formou a *ITIL* com o propósito de padronizar as propostas de serviços dos diversos fornecedores dos órgãos oficiais. Essa metodologia facilitaria a comparação entre as diferentes propostas uma vez que garantia um mínimo de padronização de atendimento nos processos, terminologia, desempenho, qualidade e custo. Na década de 90 a *ITIL* passou a ser adotada pelas empresas privadas da Europa, primeiro porque foi elaborada como um padrão aberto, passível de ser adaptada às necessidades específicas de cada organização, segundo, porque seu grande foco na qualidade viabilizou um relacionamento direto com a ISO-9000 e ao EFQM (Fundação Européia para o Gerenciamento da Qualidade). Atualmente a *ITIL* é utilizada mundialmente como referência nas melhores práticas para gerenciar serviços de TI. A *ITIL* possui uma um conjunto de melhores práticas para identificar e alinhar os processos de TI às necessidades da organização, contribuindo dessa forma para melhorar a qualidade da entrega dos serviços de TI e contribuir assim com a geração de valor para a organização. A *ITIL* provê a valorização dos relacionamentos da TI com seus clientes assegurando entregas que atendam as suas expectativas e necessidades. A maturidade do processo de gerenciamento de TI pode ser medida entre o nível “Caótico” e o nível “Valor”.

É necessário identificar como e onde os processos e suas atividades são executados pelas diversas áreas da TI para adicionar medidas de qualidade ao resultado e obter efetividade para a organização. A interatividade entre os processos descritos na ITIL contempla quatro abordagens: organização; área de TI; suporte ao serviço; e entrega do serviço (MAGALHAES; PINHEIRO, 2007).

Descreve-se a seguir os processos da *ITIL* apresentados no diagrama acima.

Gerenciamento de Configuração – O controle dos meios de produção é essencial para se garantir que os produtos e serviços entregues ao Cliente possam gerar valor para a organização. O processo de Gerenciamento de Configuração é responsável pela criação e manutenção da base de dados dos itens de configuração, sejam eles físicos ou lógicos. Um item de configuração é qualquer componente que faz parte ou está relacionado com a infra-estrutura de TI.

Gerenciamento de Incidente – É o processo, apoiado na estrutura da Central de Serviços, responsável pelo restabelecimento dos serviços no menor tempo possível. A Central de Serviços é a área de contato da TI com o usuário, sendo assim é onde o Cliente percebe qualquer anomalia na entrega do serviço. Há dois tipos de Central de Serviços: a primeira só registra a ocorrência e a repassa para a equipe responsável pela solução do problema, a segunda resolve os problemas de nível um no momento em que o Cliente está comunicando a ocorrência e somente repassa problemas de nível dois.

Gerenciamento de Mudança – É o processo encarregado de garantir que todas as alterações necessárias no ambiente de TI sejam efetivadas conforme foi planejado e autorizado. O processo consiste em identificar os itens de configuração envolvidos, testes do procedimento de mudança e plano de recuperação do serviço em caso de imprevistos.

Gerenciamento de Liberação – Tem a responsabilidade de garantir a implementação segura de todas as alterações e inovações nos itens de configuração. A entrada em produção de qualquer alteração ou inovação é um ponto delicado na continuidade da prestação de serviços de TI por alterar a forma como a infra-estrutura está entregando seus requerimentos, este processo garante que a todas as alterações tenha sido previamente testadas e aprovadas e registra sua implementação.

Gerenciamento do Nível de Serviço – Toda entrega de serviços de TI tem que ser realizadas de acordo com os requerimentos acordados com o Cliente. Pela importância deste processo, que pode afetar a imagem da TI perante o Cliente, sua condução é de responsabilidade do próprio gerente da área de TI. Este processo é o responsável pela garantia da entrega de serviços e pode ser dividido nos seguintes sub-processos: revisão dos serviços disponibilizados; negociação com os clientes; revisão dos contratos de serviços com fornecedores externos; desenvolvimento e monitoração dos acordos de nível de serviço; implementação das políticas e dos processos de melhoria contínua; estabelecimento de prioridades; planejamento do crescimento dos serviços; definição do custo dos serviços em conjunto com o gerenciamento financeiro e da forma de ressarcimento destes custos.

Gerenciamento da Capacidade – É o processo que garante que toda entrega de serviços de TI ocorra no tempo certo, volume adequado e custo apropriado dos recursos de infra-estrutura de TI. Garante também que os recursos disponíveis de infra-estrutura de TI sejam utilizados com maior eficiência e para isso é necessária a identificação dos recursos disponíveis, os serviços que serão requeridos pelas áreas de negócio da organização, nível de contingência e custos envolvidos. O processo de Gerenciamento de Capacidade pode ser dividido nos seguintes sub-processos: monitoração do desempenho; monitoração da carga de trabalho/demanda; dimensionamento da aplicação; projeção de recursos; projeção da demanda; estabelecimento de modelos.

Gerenciamento da Disponibilidade – Visa o estabelecimento dos acordos de Níveis de Serviço com os Clientes da TI. Este acordo deve ser discutido com os Clientes a partir da disponibilidade da TI em atender a demanda de entrega de serviços contratados. Recomenda-se a utilização da técnica FTA (*Fault Tree Analysis*) que faz um mapeamento da disponibilidade média resultante do impacto de falhas.

Gerenciamento da Continuidade dos Serviços de TI – Responsável pela validação dos planos de contingência de TI, este processo garante que a aplicação do plano de contingência restabeleça a capacidade da TI em entregar serviços após a ocorrência de acidentes. O plano de contingência de TI deve estar alinhado ao Plano de Continuidade do Negócio que garante a normalização da organização no menor prazo e impacto possível para atender seus Clientes finais após a ocorrência de desastres.

4.1.3. ABNT NBR ISO/IEC 27001:2006

Esta norma foi criada para compor um modelo que estabeleça, implemente, opere, monitore, analise, mantenha e melhore um Sistema de Gestão de Segurança da Informação (SGSI). As necessidades, objetivos, requisitos de segurança e processos empregados devem determinar a especificação e a

implementação de um SGSI em uma organização e sua adoção é uma decisão estratégica. Toda atividade que utiliza recursos gerenciados para transformar entradas em saídas pode ser considerada processos e freqüentemente a saída de um processo é entrada do processo seguinte e seu gerenciamento e denominado abordagem de processo. Esta norma adota a abordagem de processo utilizando o modelo PDCA (*Plan-Do-Check-Act*).

Esta norma especifica os requisitos de segurança para a criação e manutenção de um SGSI que é projetado para assegurar que a seleção dos requisitos de segurança sejam identificados adequadamente para satisfazer a necessidade das partes envolvidas em proteger seus ativos de informação. A norma provê os seguintes tópicos para estabelecer e gerenciar um SGSI:

Estabelecer um SGSI – A organização deve definir o escopo e limites do SGSI de acordo com as características do negócio. Qualquer exclusão do escopo deve ser justificada. A definição da política do SGSI deve incluir a definição de objetivos e os princípios para ações relacionadas à segurança da informação; deve considerar todos os requisitos de negócio, legais e obrigações contratuais; estar alinhada ao plano estratégico da organização no que diz respeito à gestão de riscos; deve estabelecer critérios claros sobre quais riscos serão avaliados e monitorados e finalmente, deve ser aprovada pela direção da organização. A organização deve identificar uma metodologia para análise e avaliação de riscos que contemple os requisitos legais, regulamentares e de segurança da informação que atenda as necessidades da organização. A verificação dos riscos é composta da identificação dos ativos e seus proprietários, das ameaças possíveis a esses ativos, das vulnerabilidades existentes nestes ativos e dos impactos decorrentes da perda destes ativos. É necessário avaliar o impacto que a organização sofreria como conseqüência da perda de cada um destes ativos e a avaliação da probabilidade de ocorrência dos riscos estimando seus níveis de aceitação utilizando critérios pré-estabelecidos. As ações possíveis são: aplicar controles adequados; aceitar os riscos que satisfaçam as políticas da organização e seus critérios de aceitabilidade; mitigação dos riscos e transferência dos riscos a seguradoras e fornecedores. Controles devem ser implementados para identificação, avaliação e tratamento de riscos.

Implementar e operar o SGSI – A organização deve elaborar um plano de tratamento de riscos que identifique as ações apropriadas a cada ocorrência, os recursos e responsabilidades envolvidos. A implementação do plano deve alcançar os objetivos de controle identificados e incluir as medidas utilizadas para avaliar a eficácia desses controles. Este tópico da norma prevê a implementação de programas de conscientização e treinamento, gerenciamento das operações do SGSI e o gerenciamento dos recursos para o SGSI.

Monitorar e analisar criticamente o SGSI – A organização deve monitorar e analisar o SGSI para identificar erros nas entregas de procedimentos, tentativas de violação e incidentes de segurança da informação. Utilizando-se de indicadores, deve detectar e prevenir incidentes de segurança e avaliar se as ações tomadas foram eficazes. A organização deve divulgar as partes envolvidas os resultados de auditorias de segurança da informação, medições de eficiência e sugestões de melhoria. A análise crítica dos riscos deve ser efetuada em intervalos regulares e programados para identificar a eficácia dos controles e os níveis de aceitação dos riscos, levando-se em conta mudanças relativas à

organização, tecnologias, objetivos e processos de negócio, ameaças identificadas e eventos externos. Todas as ações e eventos que possam impactar a eficácia ou o desempenho do SGSI devem ser registrados e divulgados às partes envolvidas.

Manter e melhorar o SGSI – Periodicamente planos de ações preventivas e corretivas devem ser executados e seus resultados registrados e comunicados a todas as partes envolvidas. Recomenda-se aplicar as experiências de segurança de informação, próprias e de outras organizações. As melhorias que forem identificadas devem ser implementadas de forma a atingir os objetivos pretendidos.

Requisitos de documentação – A documentação deve incluir: declarações documentadas da política e objetivos do SGSI; o escopo do SGSI; procedimentos e controles que apóiam o SGSI; uma descrição da metodologia de análise e avaliação de riscos; o relatório de análise e avaliação de riscos; o plano de tratamento de riscos; procedimentos documentados que assegurem o planejamento, operação e controle dos processos de segurança de informação e a descrição de como medir a eficácia dos controles; registros de controle; declaração de aplicabilidade.

Os documentos requeridos acima devem ser controlados e as ações de gestões devem ser estabelecidas por meio de um procedimento documentado que assegurem: aprovação, reprovação, atualização, disponibilização e identificação.

Compete à direção se comprometer com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI. Este compromisso se materializa pelo estabelecimento de políticas do SGSI; definição de planos e objetivos; atribuição de papéis e responsabilidades pela segurança de informação; a comunicação à organização da importância em atender os objetivos de segurança; o provimento de recursos suficientes para atender os objetivos de segurança do SGSI; a definição de critérios e níveis de aceitação de riscos; garantia de realização de auditorias internas e a condução de análises críticas do SGSI. A análise crítica do SGSI é base para a organização continuamente melhorar a efetividade pelo uso da política de segurança da informação, resultados de auditorias internas e análise de eventos monitorados. As ações para eliminar causas de não-conformidade com os requisitos são executadas pela organização para evitar a sua reincidência e seus procedimentos devem ser documentados de modo a: identificar não-conformidades; determinar as causas de não-conformidade; avaliar a necessidade de ações para assegurar que aquelas não-conformidades não ocorram novamente; determinar e implementar as ações corretivas necessárias; registrar os resultados das ações executadas.

4.1.4. COBIT (Control Objectives for Information and Related Technology)

Os principais elementos que compõe a governança corporativa incluem a necessidade de agregar valor aos serviços de TI, o gerenciamento de riscos e o aumento de requerimentos para controle da informação. O *COBIT* provê boas práticas por meio de modelos e processos gerenciáveis, garantindo que a TI suporte as estratégias e objetivos da organização. O modelo de controle do *COBIT* propõe: realizar a ligação entre os serviços de TI aos requerimentos de

negócio; organizar as atividades de TI em um modelo previamente acordado; identificar os recursos de TI a serem gerenciados; e definir os objetivos de controle a serem considerados.

O COBT define sete critérios de informação como requerimento de negócio que necessitam estar em conformidade com critérios de controle:

Efetividade – Consiste na disponibilização da informação no tempo certo, com consistência e de maneira apropriada para ser relevante ao processo de negócio.

Eficiência – Trata do uso otimizado dos recursos para disponibilizar as informações de forma mais produtiva e econômica.

Confidencialidade – Trata da proteção à informação contra acessos não autorizados.

Integridade – Garante o conteúdo da informação no que diz respeito à acurácia e completeza.

Disponibilidade – Consiste na disponibilização da informação no momento em que é requerida pelos processos de negócio e na garantia dos recursos e capacidades necessários.

Conformidade – Garante conformidade às regulamentações externas e internas, sejam legais ou contratuais.

Confiabilidade – Trata de prover informações apropriadas para a gerência exercer suas responsabilidades de governança e confidência.

O *COBIT* é orientado a processo e provê: um modelo de processos de referência, uma linguagem padronizada de modo que seja entendida e tenha visibilidade a todas as áreas envolvidas, e modelo para monitorar o desempenho da TI. O modelo de Processos de Negócios de TI provido pelo *COBIT* é dividido em quatro domínios: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoração e Avaliação:

PO – Planejamento e Organização – Dispõe sobre o planejamento pelo qual a TI pode contribuir para atender os objetivos de negócio.

PO1 – Definir Plano Estratégico de TI – Objetiva alinhar as atividades de TI aos requisitos de negócio da organização, por meio de Planos Operacionais para as metas de curto prazo e Planos Estratégicos para as metas de médio e longo prazo. As atividades recomendadas são: Alinhar as metas de TI às metas de negócio; identificação das dependências críticas e o desempenho atual; Elaborar um Plano Estratégico de TI; Elaborar Planos Táticos de TI e analisar e gerenciar os portfólios de programas, projetos e serviços.

PO2 – Definir arquitetura de informação – Objetiva otimizar a organização dos sistemas de informação e garantir que sejam utilizados de forma adequada, por meio de um modelo de informações de negócio. As atividades recomendadas são: Criar e manter o modelo corporativo de informação; Cria e manter dicionários corporativos de dados; Estabelecer e manter um esquema de classificação de dados; Prover procedimentos e ferramentas para classificar os sistemas de informação, identificando-os aos respectivos proprietários e utilizar o modelo proposto para planejar sistemas otimizados de negócio.

PO3 – Determinar direção tecnológica – Objetiva criar e manter um plano de infra-estrutura tecnológica de modo a extrair vantagens dos recursos tecnológicos emergentes para a estratégia de negócio. As atividades recomendadas são: Criar e manter um Plano de Infra-estrutura de Tecnologia;

Criar e manter padrões de tecnologia; Publicar padrões de tecnologia; Monitorar a evolução da tecnologia e Definir o uso estratégico das novas tecnologias.

PO4 – Definir processos, organização e relacionamentos de TI – Objetiva definir papéis e responsabilidades a toda a estrutura organizacional de TI e os relacionamentos com as áreas envolvidas. As atividades recomendadas são: Estabelecer a estrutura organizacional de TI; Desenvolver um modelo de processo de TI; Identificar os proprietários dos processos; Identificar os proprietários dos sistemas; Identificar os proprietários das informações e Estabelecer e implementar a definição de papéis e responsabilidades incluindo supervisões e segregação de funções.

PO5 – Gerenciar investimentos de TI – Objetiva definir e acompanhar um Plano Orçamentário que garanta recursos financeiros para a gestão da TI. As atividades recomendadas são: Manter o portifólio de programas, projetos e serviços; Estabelecer e manter o processo orçamentário de TI e Identificar, comunicar e monitorar os investimentos de TI, seus custos e o valor para os negócios.

PO6 – Comunicar metas e direcionamentos gerenciais – Objetiva desenvolver um modelo de comunicação da missão, metas e políticas de TI de modo a suportar o alcance dos objetivos da TI e de maneira que garanta a compreensão dos riscos do negócio pelas áreas envolvidas. As atividades recomendadas são: Estabelecer e manter um modelo e um ambiente de controle; Desenvolver e manter políticas de TI e Comunicar o modelo de controle, objetivos e direção de TI.

PO7 – Gerenciar recursos humanos de TI – Objetiva prover e manter uma equipe motivada, competente e com perfil adequado às necessidades de cada responsabilidade das áreas de TI. As atividades recomendadas são: Identificar as habilidades, descrição de cargos, faixas salariais e referenciais de avaliação de desempenho do pessoal de TI; Executar políticas e procedimentos de recursos humanos relevantes para a TI.

PO8 – Gerenciar qualidade – Objetiva atender os padrões de qualidade definidos no planejamento do sistema de gerência da qualidade. As atividades recomendadas são: Definir, estabelecer e manter um Sistema de Gerenciamento da Qualidade; Elaborar e comunicar padrões de qualidade para as áreas envolvidas; e medir, monitorar e revisar a conformidade com os padrões definidos no Plano da Qualidade.

PO9 – Avaliar e gerenciar riscos de TI – Objetiva identificar, avaliar e mitigar riscos, e analisar e avaliar os impactos decorrentes de riscos de TI. As atividades recomendadas são: Determinar o alinhamento do gerenciamento de riscos; entender os objetivos estratégicos e de processos de negócios relevantes; Identificar os objetivos de TI e estabelecer o contexto de risco; Identificar os eventos associados com os objetivos; Avaliar os riscos associados aos eventos; Avaliar e selecionar as respostas aos riscos; Priorizar e planejar atividades de controle; Aprovar e garantir recursos financeiros para os planos de ação para mitigar os riscos e Manter e monitorar os planos de ação para mitigar os riscos.

PO10 – Gerenciar projetos – Objetiva identificar e priorizar o *portifólio* de projetos que estejam alinhados ao plano operacional pela adoção de técnicas de gerenciamento de projetos. As atividades recomendadas são: Definir um modelo de gerenciamento de protifólio para os investimentos de TI; Estabelecer e manter

um modelo de gerenciamento, medição e monitoramento de projetos; Elaborar plano de gerenciamento da comunicação e gerenciamento de riscos; Garantir a participação e o comprometimento das áreas envolvidas no projeto; Definir e implementar métodos de avaliação e revisão de projetos.

AI – Aquisição e Implementação – Dispõe sobre a identificação das necessidades a serem desenvolvidas ou adquiridas e sua integração ao processo de negócio, além de garantir que as alterações continuem a atender os objetivos de negócio.

AI1 – Identificar solução de TI – Pela definição das necessidades e avaliação das alternativas de solução de mercado, objetiva garantir uma solução efetiva e eficiente que atenda os requisitos de negócio. As atividades recomendadas são: Definir os requerimentos funcionais e técnicos do negócio; Estabelecer processos que garantam a integridade e validade dos requerimentos; Identificar, documentar e analisar os riscos envolvidos; Conduzir estudo de viabilidade e avaliação de impacto sobre a solução proposta; avaliar os benefícios operacionais e de negócios da solução proposta; Desenvolver um processo de aprovação.

AI2 – Prover e manter aplicativo de software – Objetiva prover funções automatizadas que suportem o processo de negócio, por meio desenvolvimento de softwares em conformidade com os padrões definidos. As atividades recomendadas são: Traduzir os requerimentos de negócio em especificações de desenvolvimento; Preparar o projeto detalhado e os requerimentos técnicos do software; Especificar os controles da aplicação; Customizar e implementar as funcionalidades desenvolvidas; Desenvolver um plano para a manutenção futura da aplicação.

AI3 – Prover e manter infra-estrutura tecnológica – Objetiva elaborar um plano de evolução do parque de infra-estrutura de modo a suportar as aplicações de negócio com aquisições e implementações de hardware, software e administração dos ambientes. As atividades recomendadas são: Definir os procedimentos e processos de aquisição; Discutir os requerimentos da infra-estrutura com os fornecedores selecionados; Definir o plano de manutenção da infra-estrutura e configurar os seus componentes.

AI4 – Habilitar operação e uso – Objetiva elaborar manuais de procedimentos operacionais e de treinamento para garantir a utilização correta das aplicações e soluções tecnológicas. As atividades recomendadas são: Desenvolver uma estratégia de operacionalização dos procedimentos; Desenvolver metodologias de treinamento; Desenvolver documentação de procedimentos para os usuários das áreas envolvidas; Desenvolver documentação técnica para das suporte às equipes de operação e de suporte; Desenvolver e promover treinamentos e avaliar seus resultados.

AI5 – Adquirir e contratar recursos de TI – Objetiva elaborar procedimentos de seleção e contratação de fornecedores de recursos de TI, incluindo pessoal, hardware, software e serviços, e definição cláusulas contratuais que garantam recebimentos no prazo e custo acordados. As atividades recomendadas são: Desenvolver políticas e procedimentos de contratação de TI, alinhadas com as políticas da organização; desenvolver processo de Homologação de fornecedores; Desenvolver contratos que garantam os interesses da organização e Contratar em conformidade com o estabelecido.

AI6 – Gerenciar mudanças – Objetiva elaborar um sistema de gerenciamento da mudança que garanta o funcionamento pleno da área de TI nas situações de implementações de inovações tecnológicas e manutenção da infra-estrutura existente. As atividades recomendadas são: Desenvolver e implementar um procedimento para registrar, avaliar riscos e priorizar as requisições de mudança; Avaliar o impacto e priorizar as mudanças baseado nas necessidades do negócio; Garantir que todo processo de mudança seja previamente aprovado; Autorizar as mudanças e disseminar informações pertinentes às áreas envolvidas.

AI7 – Instalar e aprovar soluções e mudanças – Objetiva a verificação e confirmação de que a solução adotada está conforme o previsto. As atividades recomendadas são: Elaborar e revisar os planos de implantação; Definir uma metodologia de teste operacional e Recomendar a entrada em ambiente de produção os novos procedimentos que estão conforme os critérios de aceitação.

DS – Entrega e Suporte – Dispõe sobre a garantia das entregas e gerenciamento dos serviços de suporte ao cliente.

DS1 – Definir e manter níveis de serviço – Pela identificação das necessidades do cliente e disponibilidades da TI, estabelece-se acordos de níveis de serviço que formalizem os critérios de prazo e qualidade do serviço entregue. As atividades recomendadas são: criar um modelo para a definição dos serviços de TI; Elaborar, revisar e manter um catálogo de serviços de TI; Definir acordos de nível de serviço (SLA); Definir acordos de nível operacional (OLA) para suportar os acordos de nível de serviço; Monitorar, reportar e revisar os acordos de nível de serviço e suas cláusulas contratuais; Elaborar um plano de melhoria contínua dos serviços de TI.

DS2 – Gerenciar serviços de terceiros – Objetiva garantir que as responsabilidade de terceiros estejam aderentes à política da organização e os papéis estejam claramente definidos nos acordos existentes. As atividades recomendadas são: Identificar e categorizar os serviços de terceiros; Definir e documentar um processo de gerenciamento de terceiros; Estabelecer políticas de seleção e avaliação de fornecedores; Identificar, classificar, avaliar e mitigar riscos relacionados a recebimentos de fornecedores; Monitorar os recebimentos.

DS3 – Gerenciar desempenho e capacidade – Objetiva colecionar e analisar dados sobre desempenho e demanda de carga para garantir disponibilidade otimizada de recursos no atendimento das necessidades. As atividades recomendadas são: Estabelecer um processo de planejamento para revisões periódicas do desempenho e capacidade dos recursos de TI; Elaborar um processo de planejamento de contingência para prevenir indisponibilidade de recursos. Monitorar e reportar a disponibilidade, desempenho e capacidade dos recursos de TI.

DS4 – Garantir serviço contínuo – Objetiva garantir que os recursos de TI estejam disponíveis para cumprir os níveis de serviços acordados e que estejam alinhados com o plano global de disponibilidade da organização. As atividades recomendadas são: Desenvolver e testar regularmente um plano de continuidade de TI; Elaborar modelo de avaliação de riscos e análise de impacto no negócio; Planejar e disponibilizar treinamento sobre a continuidade de TI; Planejar e implementar ações de retomada dos serviços de TI e Estabelecer procedimentos para efetuar revisões no plano de continuidade pós-retomada.

DS5 – Garantir segurança dos sistemas – Objetiva garantir que informações e programas estejam seguros quanto a acessos não-autorizados, destruição, perda ou violação. As atividades recomendadas são: Definir e manter um plano de segurança de TI; Definir estabelecer e operar um processo de gerenciamento de identificação e autorização de acessos; Monitorar incidentes de segurança; Revisar e validar periodicamente os direitos e privilégios de acesso.

DS6 – Identificar e alocar custos – Objetiva a identificação, apropriação e alocação de custos aos serviços de TI. As atividades recomendadas são: Mapear os recursos de TI por processos de negócio; Identificar e mapear os custos de TI sobre base unitária; Estabelecer e manter um processo de contabilização de custos; Estabelecer e manter políticas e procedimentos de lançamento de custos aos serviços executados.

DS7 – Treinar usuários - Objetiva garantir que todas as áreas envolvidas estejam treinadas e aptas a utilizar efetivamente os recursos de TI disponibilizados e conscientes dos riscos e responsabilidades inerentes. As atividades recomendadas são: Identificar e caracterizar as necessidades de treinamento; Estabelecer programas de treinamento; Conduzir atividades de conscientização, educação e treinamento; Avaliar desempenho dos treinamentos; Identificar e avaliar métodos e ferramentas para execução de treinamento.

DS8 – Gerenciar atendimento e incidentes – Objetiva estabelecer uma função de atendimento que registre e organize os incidentes reportados por usuários bem como encaminhe a resolução do problema. As atividades recomendadas são: Elaborar procedimentos para classificação dos incidentes baseados em critérios de severidade e impacto para a organização; Atender, registrar, resolver, recuperar e encerrar incidentes; Manter os usuários informados sobre as ações pertinentes à recuperação do incidente reportado e Produzir relatórios gerenciais.

DS9 – Gerenciar configuração – Objetiva verificar e controlar os componentes de TI quanto a alterações e instalações não autorizadas. As atividades recomendadas são: Desenvolver procedimentos para planejamento e gerenciamento de configuração; Inventariar as configurações iniciais de todos os componentes para estabelecer uma base inicial de averiguação; Verificar e auditar periodicamente as informações de configuração em confronto com a base inicial para detecção de alterações não autorizadas; Atualizar a base de dados de configurações.

DS10 – Gerenciar problemas – Objetiva a criação de um sistema de gerenciamento que garanta que problemas reportados sejam identificados, classificados e resolvidos de forma a maximizar a disponibilidade dos serviços de TI. As atividades recomendadas são: Identificar e classificar problemas; Executar análise de causa e efeito; Resolver problemas; Acompanhar, gerar recomendações e manter registro dos problemas reportados.

DS11 – Gerenciar dados – Objetiva garantir que os dados armazenados atendam os requisitos de qualidade, disponibilidade e temporalidade, bem como estabelecer procedimentos para gerenciamento do armazenamento e segurança física dos dados. As atividades recomendadas são: Estabelecer procedimentos para atender os requerimentos de armazenamento e retenção de dados; Definir, implementar e manter procedimentos para gerenciamento das mídias de

armazenamento; Executar procedimentos de *backup* conforme definido; Definir, implementar e manter procedimentos para restauração de dados.

DS12 – Gerenciar ambiente físico – Objetiva disponibilizar ambiente físico apropriado e que proteja equipamentos de TI e pessoas contra perigos naturais e de acesso não autorizado. As atividades recomendadas são: Definir o nível de proteção física requerido; Selecionar o ambiente físico apropriado; Gerenciar o ambiente físico; Definir e implementar procedimentos de acesso e manutenção.

DS13 – Gerenciar operações – Objetiva garantir que as funções operacionais de TI sejam executadas de forma ordenada por meio de uma programação de atividades. As atividades recomendadas são: Elaborar e manter procedimentos de operação; Escalonar a carga de trabalho por prioridades e disponibilidades de recursos; Monitorar a infra-estrutura, processamento e resolução de problemas; Gerenciar as saídas físicas de informação; Solucionar problemas e implementar mudanças no processamento e na infra-estrutura; Estabelecer e implementar um processo que garanta os componentes contra interferência, perda e roubo; Programar e executar manutenções preventivas.

ME – Monitoração e Avaliação – Dispõe sobre o processo de avaliação da qualidade e conformidade aos requerimentos de controle.

ME1 – Monitorar e avaliar desempenho de TI – Objetiva garantir o atendimento dos objetivos de desempenho dos processos de TI, por meio de indicadores de desempenho e da ação sobre os desvios identificados. As atividades recomendadas são: Estabelecer a abordagem de monitoração; Identificar os indicadores mensuráveis e relevantes para os objetivos de negócio; Elaborar um painel de indicadores; Identificar, avaliar, monitorar e reportar o desempenho e ações de melhoria.

ME2 – Monitorar e avaliar controle interno – Objetiva garantir o atendimento dos objetivos de controle interno dos processos de TI. As atividades recomendadas são: Monitorar e controlar as atividades de controle interno de TI; Monitorar os processos de auto-avaliação; Monitorar o resultado de auditorias; Monitorar o processo de garantia sobre os controles operados por terceiros; Monitorar o processo para identificar as exceções de controle; Reportar às áreas envolvidas.

ME3 – Garantir conformidade regulatória – Objetiva estabelecer revisões no processo que garante conformidade com leis, regulamentos e requerimentos contratuais. As atividades recomendadas são: Definir e executar um processo de identificação dos requerimentos legais, regulatórios e contratuais; Avaliar e reportar a conformidade das atividades de TI com as políticas de TI e da organização; Prover recursos para o alinhamento das políticas e procedimentos de TI em resposta aos requerimentos de conformidade.

ME4 – Prover governança de TI – Objetiva estabelecer um modelo de governança que garanta que os investimentos em TI estão alinhados às estratégias e objetivos da organização. As atividades recomendadas são: Estabelecer visibilidades e transparência sobre as atividades de TI aos gestores da organização; Revisar, avaliar e comunicar o desempenho, estratégia e gestão de recursos e riscos de TI alinhando-os à estratégia de negócios; Obter periodicamente avaliação independente de desempenho e de conformidade; Garantir implementações recomendadas por avaliações independentes; Gerar relatórios sobre governança de TI.

4.2. Elementos internos e externos do ambiente organizacional

Apresenta-se os elementos que influenciam o ambiente organizacional que serão influenciados no monitoramento de um plano de contingência em TI.

Perrow (1981) na sua perspectiva sociológica afirma que as organizações influenciam o ambiente e são influenciadas por ele, podendo ser um recurso ou uma ameaça. E na perspectiva tecnológica elas são vistas como sistemas abertos, permitindo permutas com o meio externo (REZENDE; ABREU, 2000).

Tompson (1976) divide o ambiente denominado por ele de operacional em 4 setores em clientes, desde usuário aos distribuidores; fornecedores de material, mão-de-obra, equipamento; concorrentes de mercados e recursos; e grupo regulamentadores, desde o governo às associações e firmas. Ele ainda complementa a importância da interação da empresa com o ambiente para sua sobrevivência.

Já London e London (1999) fatia os ambientes em dois grandes grupos: o ambiente tarefa, que está mais próximo à organização, subdividido em fornecedores, leis, acionistas, clientes e concorrentes e o ambiente-geral, que compreende economia, política, mudanças internacionais e tecnologia e ciências. E complementam que para ela ser bem sucedida, deve-se monitorar e reagir aos acontecimentos nos ambos ambientes propostas.

Andrade e Rosseti (2004) apresentam uma proposta dos principais *stakeholders* e seus respectivos focos que interagem com as corporações no processo de governança corporativa. Dividindo em três grupos: público interno (acionistas, empregados e fundações de seguridade); público externo (credores, fornecedores, clientes e consumidores) e entorno das corporações (comunidades em que atuam, sociedade, governo e meio ambiente).

Ferreira (2005) apresenta os grupos de interesse divididos em: investidores(retorno do investimento e maximização do valor da empresa); empregados (empregos, salários e reconhecimento); consumidores (produtos confiáveis e seguros); fornecedores (regularidade e relações pautadas por rigorosa conformidade); comunidades locais (geração de empregos e contribuições para o desenvolvimento); governos (crescimento, geração de empregos, conformidade legal); organizações não governamentais (ambientalismo, direitos de minorias e provisões de interesse social).

O *COBIT* 4.0 (2005) que o controle de governança de TI visa servir a uma variedade de stakeholders internos e externos, de acordo com a sua necessidade: dentro da empresa preocupados em gerar valor dos investimentos de TI (fazem decisões de investimento; decidem sobre requisitos; usam serviços de TI); internos e externos que fornecem os serviços de TI (administram a organização e os processos de TI; desenvolvem capacidades; operam os serviços); internos e externos que têm responsabilidade de controle/risco (fazem segurança, privacidade e/ou responsabilidade de risco; executam funções de conformidade; exigindo ou fornecendo serviços de garantia).

O *COBIT* 4.0 (2005) apresenta um modelo emergente da empresa, argumentando que a nova economia e constantes mudanças requerem organizações adaptáveis rapidamente ao mercado, ou seja, as empresas bem sucedidas monitoram seu ambiente em uma base contínua, impulsionando a informação e o conhecimento que obtém de sua monitoração para adaptar e inovar. E a TI com seus serviços de coletar, construir e distribuir conhecimento

força o a alta administração de efetivamente direcionar e controlar a TI. Os elementos internos e externos são: aprender; inovar; perceber; e mudar (gerando conhecimento na organização).

4.3. Serviços e indicadores de TI

Pretende-se apresentar os principais indicadores que contribuirão para o monitoramento e aprimoramento dos serviços prestados pela área de TI.

4.3.1. Serviços de TI

Cada vez mais as organizações dependem dos serviços da Tecnologia da Informação (TI) para atingir seus objetivos estratégicos e às necessidades do negócio em que atuam.

Uma pesquisa realizada pelo *IT Governance Institute*, aponta que mais de 50% das organizações de diferentes segmentos, consideram a área de TI muito importante para execução da estratégia de negócio.

Para muitas organizações, TI deixou de ser apenas uma área de suporte, passando a atuar como um provedor de tecnologia, criando uma relação de parceria com as demais áreas da organização, alinhada com a governança corporativa.

Algumas áreas de TI estão deixando o modelo tradicional, baseado na disponibilização de recursos e caminhando para se tornarem orientadas a serviços. O novo modelo exige uma maior interação entre as áreas de negócios e TI. O primeiro passo da área de TI é definir o seu catálogo de serviços e outros elementos necessários para garantir a entrega e o suporte dos serviços focados nas necessidades dos seus clientes e alinhados à estratégia de negócio da organização.

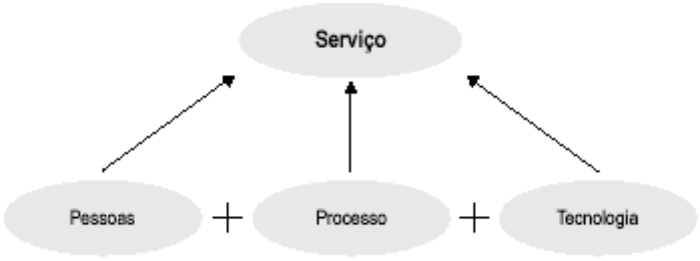
Existem várias definições de serviço, a seguir, apresentam-se cinco definições de diferentes autores, buscando uma definição pertinente á área de TI: “atividades, benefícios ou satisfações que são colocados à venda ou proporcionados em conexão com a venda de bens” (*American Marketing Association*, 1960); “quaisquer atividades colocadas à venda que proporcionem benefícios e satisfações valiosas; atividades que o cliente prefira ou não possa realizar por si próprio” (Bessom, 1973); “uma atividade colocada à venda que gera benefícios e satisfações, sem levar a uma mudança física na forma de um bem” (Stanton, 1974); “qualquer atividade ou benefício que uma parte possa oferecer a uma outra, que seja essencialmente intangível e que não resulte propriedade de alguma coisa. Sua produção pode ou não estar ligada a um produto físico” (Kotler, 1988); “serviço ao cliente significa todos os aspectos, atitudes e informações que ampliem a capacidade do cliente de compreender o valor potencial de um bem ou serviço essencial” (UTTAL; DAVIDOW, 1991).

Uma possível definição de serviço de TI é: conjunto de recursos, TI e não-TI, mantidos por um provedor de TI, visando satisfazer uma ou mais necessidades de um cliente (áreas de negócio), suportando os seus os objetivos estratégicos e sendo percebido pelo cliente como um todo coerente.

O serviço de TI é composto pela integração entre pessoas, processos e tecnologias, visando o alcance de objetivos de custo e desempenho estabelecidos pelos acordos de nível de serviço entre a área de TI e as demais áreas de negócio da organização.

A Figura a seguir ilustra a composição de um serviço de TI.

FIGURA 1: COMPOSIÇÃO DE UM SERVIÇO DE TI



FONTE: MAGALHAES; PINHEIRO, 2007.

Para Rezende (2003) a TI está fundamentada nos seguintes componentes: hardware e seus dispositivos periféricos; softwares e seus recursos; sistemas de telecomunicações e gestão de dados e informações. Todos esses componentes interagem e necessitam de um componente essencial, que é o recurso humano, *peopleware* ou *humanware*. Conceitualmente esse componente não faça parte da TI, mas sem ele esta tecnologia não teria funcionalidade e utilidade.

No Gerenciamento de Serviços de TI, o valor de um serviço pode ser medido por quatro parâmetros: alinhamento estratégico com o negócio – Grau em que o serviço de TI está alinhado com as atuais e as futuras necessidades do negócio; custo – Valor monetário desembolsado pela disponibilização do serviço de TI e em cada interação; qualidade – Nível de atendimento do serviço de TI em relação aos Acordos de Nível de Serviço (*Service Level Agreement* – SLA) e Acordos de Nível Operacional (*Operational Level Agreement* – OLA), estabelecidos externa e internamente à área de TI, respectivamente; independência em relação ao tempo – Capacidade da área de TI em reagir a demandas de suporte e em atender às mudanças planejadas em relação ao serviço de TI disponibilizado.

A qualidade de um serviço pode ser medida pela satisfação do cliente em relação ao serviço previsto/entregue. Existem cinco fatores que influenciam na avaliação de um serviço: serviço esperado: é o que o cliente espera receber em troca do valor pago; serviço adequado: é o que atende as necessidades do cliente; serviço desejado: é o que o cliente deseja receber a mais do que ele expressou necessitar; serviço previsto: é o que o cliente recebe pelo que foi acordado com o fornecedor; serviço percebido: é como o cliente percebe o serviço prestado, considerando suas expectativas em relação ao que entender ser o serviço adequado e o serviço desejado.

Na prestação de serviços de TI, o grande desafio é conseguir equilibrar as necessidades dos clientes e usuários com a capacidade disponível e os custos definidos pelas áreas de negócio da organização.

O nível de satisfação do cliente é diretamente proporcional à diferença entre o desempenho percebido e o desempenho previsto. Na maioria dos casos, as necessidades são mais fáceis de satisfazer do que as expectativas geradas pelo cliente.

As chaves para alcançar a satisfação do cliente são: serviços e produtos superiores; equipe de venda e entrega de serviços e produtos altamente capacitados; processos de suporte rápidos, baratos e eficazes.

Para atingir um elevado nível de satisfação dos clientes, os serviços de TI devem estar fundamentados nos seguintes requisitos: especificação: saber de antemão o que irá receber; conformidade: a solução deve atender à especificação; consistência: a cada intervenção o comportamento deve ser idêntico; mais valor pelo seu dinheiro: o preço pago deve ser justo pelo produto ou serviço recebido.

4.3.2. Indicadores de Desempenho

O Gerenciamento de Serviços de TI necessita de controles que permitam o monitoramento e avaliação de sua eficiência, eficácia, efetividade e economicidade. Esses pontos de controle são conhecidos como Indicadores-Chave de Desempenho (*Key Performance Indicator* – KPI).

4.4. Quadro exemplo

O objetivo desse item é demonstrar a aplicação dos *frameworks*, relacionado aos elementos e serviços prestados pela área de TI.

O exemplo de tipos de indicadores de gestão estratégica apresentada pelo COBIT, em que a área de TI alinha seus objetivos a área de negócio com suas perspectivas utilizadas pelo *Balanced Scored Card* (BSC): financeira (otimizar a utilização dos recursos; e controlar riscos do negócio); interna (conformidade com leis externas e regulamentos); conhecimento e crescimento (obter informações confiáveis e úteis para a tomada de decisão estratégica). Cada uma dessas perspectivas possui seus respectivos indicadores.

A Tabela 1 é a demonstração da aplicação dos resultados dos indicadores, intitulado de ***Cockpit***, permitindo ao gestor, visualizar o desempenho dos serviços prestados. Auxiliando na tomada de decisão, como realocação de recursos e substituição de equipamentos.

TABELA 1: EXEMPLO DE *COCKPIT*

Painel Central de Indicadores de TI

Processo de Negócio - CSC - Serviços Compartilhados

ID Grupo	Grupos de Serviços	Matriz de Riscos - Impacto x Probabilidade	Disponibilidade Atual - %	AST - Horas Paralizações / mês	Disponibilidade Desejada - %	AST - Desejado Paralização / mês	Estratégia
GS10	ERP		98,73%	14			Com a implementação de balanceamento dos serviços entre os sites primário e secundário será possível um incremento na capacidade de garantir os serviços continuados bem como melhorar a utilização dos recursos disponíveis.
GS20	Correio Eletrônico		99,41%	9			
GS30	Silos		99,08%	12			
GS40	Acesso Internet		98,45%	16			
GS50	Informações Gerenciais		98,98%	12			
GS60	Office Automation		98,72%	14			
GS70	Desenvolvimento e homologação de sistemas		98,11%	19			
GS80	Telefonia						
GS90	Impressão						
GS100	Estações de Trabalho						
		TOTAL %	91,7717	TOTAL %	0		

5. CONCLUSÃO

Uma parcela significativa dos serviços prestados pela TI dependem de fornecedores contratados, o que coloca a TI em uma situação delicada de tomador e prestador de serviços, assumindo para si a responsabilidade de adotar práticas formais que garantam um fluxo contínuo de disponibilidade. Este trabalho apresenta ferramentas que permitem monitorar a disponibilidade dos serviços prestados pela TI, garantindo que o plano de contingência adotado tenha sua validade e eficiência testada formalmente. Garantir a usabilidade do plano de contingência é como ter uma contingência do próprio plano, certificando, desta maneira, a adoção das melhores práticas de governança para a área de TI.

Com relação à questão-problema “será que existem padrões de planejamento de plano de contingência?”, verificou-se na bibliografia a inexistência de padronização, o que é coerente, uma vez que o Plano de Contingência deve refletir o alinhamento da TI ao Planejamento Estratégico da organização, tornando-o único para cada situação. Verificou-se ainda, que as ferramentas que suportam as melhores práticas de governança recomendam a escolha dos itens componentes do Plano de Contingência deve refletir cada processo crítico para a organização e também espelhar suas estratégias que são amparadas por processos de TI. Caracterizando, dessa forma, a dependência crítica dos processos de TI para a organização.

A questão-problema “faz parte do planejamento de TI?” é respondida positivamente em todos os *frameworks* pesquisados, por meio de recomendações para as melhores práticas. É de responsabilidade da TI garantir a disponibilidade de acesso a informações e serviços prestados, no menor tempo possível após ocorrências de desastres ou situações de emergência.

A composição do Plano de Contingência é de alto valor para o negócio da organização e por esse motivo não deve ser descuidado a ponto de testar sua validade no momento da necessidade. Essa constatação, presente em todos os *frameworks* pesquisados, responde afirmativamente a questão-problema “As organizações devem avaliar e atualizar esses planos?”.

Por entender que o Plano de Contingência não garante por si só a continuidade dos negócios da organização e sendo necessário que a TI antecipe ações que permitam garantir a integridade e disponibilidade operacional do Plano de Contingência, este trabalho teve como objetivo secundário identificar as metodologias disponíveis para compor um plano de monitoramento. Concluiu-se que as recomendações descritas pelo COBIT no domínio Monitoração e Avaliação, pela ITIL no processo Gerenciamento da Continuidade dos Serviços de TI e pela norma ABNT NBR ISO/IEC 27001:2006 por meio do modelo PDCA atendem plenamente este objetivo.

A adoção do modelo proposto de *framework* caracteriza os elementos internos e externos envolvidos em situações de crise organizacional atingindo deste modo o objetivo secundário de caracterizar estes elementos.

Para atingir os objetivos secundários de correlacionar o *framework* ao processo de monitoramento e estabelecer um modelo de referência, foi proposto o modelo exemplificado na tabela 6, de acordo com recomendação do COBIT. Este *framework* relaciona todos os elementos de risco constante no Plano de Contingência e os associa a indicadores de disponibilidade e estratégias a serem adotadas.

Finalmente, para atingir o objetivo de apresentar indicadores que direcionem a área de TI, compôs-se este trabalho que culmina com a apresentação de um modelo de *cockpit* funcional por meio de indicadores, baseado nas melhores práticas de governança de TI. Estes indicadores devem recomendar ações de verificação, validação e comunicação às áreas envolvidas, de todos os elementos críticos que compõe o Plano de Contingência, buscando a certificação, desse modo, da real disponibilidade dos serviços de TI.

Todas as ferramentas de governança pesquisadas recomendam a adoção de Planos de Contingência, mas deixam a critério da organização a elaboração do *framework* que satisfaça suas necessidades de alinhamento estratégico, no quesito disponibilidade dos serviços de TI. Entende-se que assim é necessário, uma vez que o grau de importância dos processos e os próprios processos são particularizados para cada organização e a adoção de um modelo padrão não teria a flexibilidade necessária para contemplar toda a variedade de situações de risco aos quais os processos estariam sujeitos. Da mesma forma, o *Cockpit* proposto não tem seus indicadores padronizados. Trata-se de uma recomendação para que se adotem indicadores adequados a cada organização, que reflitam o status de confiabilidade de cada processo amparado no Plano de Contingência.

No que diz respeito as contribuições desse trabalho, destacam-se as comparações dos *frameworks* proposto com outros trabalhos e o fato de terem sido feitas com a intenção de mostrar que o modelo exemplo é outra alternativa viável a ser utilizada na criação de indicadores e monitoramento dos resultados.

Com relação as limitações, o objetivo inicial do projeto era a aplicação de um questionário aos gestores de TI nas organizações, no intuito de obter como resultado, quais e como eles utilizam os indicadores.

Outros trabalhos futuros podem ser elaborados a partir desse, no sentido de melhorar o modelo proposto. Estas melhorias vão desde o aperfeiçoamento de aplicação do uso até a simulação.

REFERÊNCIAS

BARRETO, Aldo. **Tecnologia da Informação em C&T**. Disponível em: <http://listas.ibict.br/pipermail/bib_virtual/2005-March/001041.html>. Acesso em: 29 maio 2007.

COBIT - CobiT mapping: mapping of PMBOK with CobiT 4.0. Rolling Meadows, 2006 (2006).

____. CobiT® 4.1, Rolling Meadows, 2007 (2007).

____. **CobiT mapping**: mapping of ITIL with CobiT 4.0. Rolling Meadows,

2007 (2007).

OGC-**ITIL®** – Service Strategy. The Stationery Office (2007a).

____. **ITIL®** – Service Design. The Stationery Office (2007b).

____. **ITIL®** – Service Transition. The Stationery Office (2007c).

____. **ITIL®** – Service Operation. The Stationery Office (2007d).

____. **ITIL®** – Continual Service Improvement. The Stationery Office

(2007e).

CORRÊA, Lucia Helena. Segurança: Uma questão de comportamento. **Revista Informática Hoje**, São Paulo, ano 23, p. 48-49, Jul. 2007.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. 2. ed. São Paulo: Editora SENAC, 1999.

DEMO, Pedro. **Pesquisa e construção do conhecimento**: metodologia científica no caminho de Habermas. Rio de Janeiro: Tempo Brasileiro, 1994. _____. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2000.

DRI. **The Institute for Continuity Management.** Disponível em: < http://www.drii.org/DRII/> Acesso em: 12 jun. 2007.

FAUSTINI, Rodrigo. **Plano de Contingência**: Planejamento. Disponível em: <http://www.faustiniconsulting.com/>. Acessa em: 12 maio 2007.

FERREIRA, Cláudio. **Gestão de TI com gosto de Governança.** TI Inside, jun. 2005.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 3. ed. São Paulo: Atlas, 1994.

ISO/IEC 20000-1:2005. **Information Technology** – Service Management – Part 1: Specification (2005).

___. ISO/IEC 20000-2:2005**. Information Technology** – Service

Management – Part 1: Code of practice (2005).

KAPLAN, Robert S., NORTON, David P. **Organização orientada para a estratégia**. Rio de Janeiro: Campus, 2001.

LAKATOS, Eva Maria; MARCONI, Maria de Andrade. **Fundamentos de metodologia científica.** São Paulo: Atlas, 1985. 238 p.

LAUDON, Kenneth C., LAUDON, Jane P. **Gerenciamento de Sistemas de Informação.** 3. ed. Rio de Janeiro: Livros Técnicos e Científicos, 2001.

MACEDO, Paloma de Oliveira. **Plano de Contingência do setor de Tecnologia da Informação para empresa de Telecomunicações**. Canoas, 2003. 86 p. Monografia (Bacharelado em Ciência da Computação) - Universidade Luterana do Brasil.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de Serviços de TI na Prática.** São Paulo: Novatec, 2007.

MARINHO, Fernando. **Como proteger e manter seus negócios.** Rio de Janeiro: Campus, 2003.

_____. PCN. **Imprensa WEB**, São Paulo, 15/06/2001. Entrevista concedida a Fernanda do Couto. Disponível em: Acesso em: 13 out. 2006.

NATALE, Carlos Henrique Cotta. **A importância da criação de um plano de contingência de TI para as pequenas e médias empresas**. Boletim Gestão e Tecnologia da Informação, n. 43, Jun. 07. Disponível em: <http://www.google.com.br/search?source=ig&hl=pt-BR&q=import%C3%A2ncia+de+TI+no+monitoramento+plano+de+conting%C3%AAncia&btnG=Pesquisa+Google&meta=lr%3Dlang_pt>. Acesso em 22 set. 2007.

NIST - NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-12: An Introduction to Computer Security**. US Washington DC, 2002. Disponível em < http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf >Acesso em: 15 jul. 2007.

PERROW, Charles B. **Análise organizacional**: um enfoque sociológico. São Paulo: Atlas, 1981.

RAGLAND, Bryce. Measure or indicator: what's the difference?. **Crosstalk**, v. 8, n. 3, Software Technology Support Center, Mar. 1995.

REZENDE, Denis Alcides. Evolução da Tecnologia da Informação nos últimos 45 anos. **Revista Fae Business**, dez. 2002, n. 4, p. 42-46.

_____. **Planejamento de Sistemas de Informação e Informática**: Guia Prático para planejar a tecnologia da informação integrada ao planejamento estratégico das organizações. São Paulo: Atlas, 2003.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da informação**: aplicada a sistemas de informação empresariais. São Paulo: Atlas, 2000.

RODRIGUES, Rivelino. **A Importância da Tecnologia da Informação e das Telecomunicações nos Sistemas de Informação**. Disponível em: http://guia.mercadolivre.com.br/importncia-tecnologia-informaco-e-telecomunicacoes-sistemas-7788-VGP> Acesso em: 29 maio 2007.

SILVA, Edna Lúcia da; MENEZES, Estela Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. Florianópolis: Laboratório de Ensino à distância da UFSC, 2001.

STAIR, Ralph M. **Princípios de Sistemas de Informação**: Uma Abordagem Gerencial. 2. ed. Rio de Janeiro: Livros Técnicos e Científicos, 1998.

TAKASHINA, Newton Tadashi; FLORES, Mario Cesar X. **Indicadores da qualidade e do desempenho**: como estabelecer metas e medir resultados. Rio de Janeiro: Qualitymark, 1996.

THOMPSON, James D. **Dinâmica organizacional**: fundamentos sociológicos da teoria administrativa. São Paulo: McGraw Hill, 1976.