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-1064

MEASURATION OF THE IMPACT IN THE BUSINESS CAUSED BY THE INFORMATION TECHNOLOGY INFRASTRUCTURE UNAVAILABLE: STUDY IN A COSMETIC AND PERFUMERY COMPANY

Cesar Luiz Panisson (FAE Business School) – cesar@boticario.com.br
Denis Alcides Rezende (Pontifícia Universidade Católica do Paraná, FAE Business School, Paraná, Brasil) – denis.rezende@pucpr.br

The Information Technology (IT) is in the current days intimately aligned to the organizations business processes. The IT intelligent association solutions with business strategies comes every day being used most to generate competitive differential in the globalized market. How to measure the impact in the business caused by the IT infrastructure unavailable is the objective. The exploratory research used the interviews technique, analysis of made available documentations and personal observations. As result was obtained the mensuration for the impact in the business that the IT infrastructure unavailable prejudice of the Cosmetics and Perfumery Company. The tangible impact can arrive to R$ 23.000.000,00 when considered an IT infrastructure unavailable in 30 day in the more aggressive scenery. The main intangible impacts considered to for being of the measure difficult, they are related to credibility or confidence loss in the image of the company or mark and clients' dissatisfaction.

Keywords: Information Technology; Impact in the Business; IT Infrastructure Unavailable; Business Impact Analysis; Business Continuity.

Agradecimento: CNPq

MENSURAÇÃO DO IMPACTO QUE A INDISPONIBILIDADE DA INFRA-ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO CAUSA NO NEGÓCIO: ESTUDO DE UMA EMPRESA DE PERFUMARIA, HIGIENE E COSMÉTICOS

Resumo:
A Tecnologia da Informação (TI) está nos dias atuais intimamente vinculada aos processos de negócios das organizações. A associação inteligente de soluções de TI com estratégias de negócios vem a cada dia sendo mais utilizada para gerar diferencial competitivo no mercado globalizado. Como mensurar o impacto no negócio causado pela indisponibilidade da infra-estrutura de TI é o objetivo deste estudo. A pesquisa exploratória utilizou a técnica de entrevistas, análise de documentações disponibilizadas e observações pessoais. Como resultado obteve-se a mensuração do impacto no negócio que a indisponibilidade da Infra-estrutura de TI causa em uma empresa do setor de cosméticos e perfumaria localizada em São José dos Pinhais. O impacto tangível pode chegar a R$ 23.000.000,00 quando considerado uma indisponibilidade de 30 dias no cenário mais agressivo. Os principais impactos considerados intangíveis por serem de difícil mensuração, estão relacionados à perda de credibilidade ou confiança na imagem da empresa ou marca e insatisfação de clientes.

Palavras-chave:
Tecnologia da Informação; Impacto no Negócio; Indisponibilidade da Infra-estrutura Tecnológica; Business Impact Analysis (Análise de Impacto no Negócio); Continuidade de Negócios.

1. INTRODUÇÃO

A informatização dos processos de negócios é nos dias atuais condição essencial para garantir a sobrevivência da maioria das organizações. A necessidade de manter a competitividade no mercado globalizado, implica em disponibilizar produtos e/ou serviços para consumidores cada vez mais exigentes, que primam por qualidade e baixo custo, bem como, em atender as expectativas dos acionistas, sociedade, funcionários, governo e fornecedores de forma a garantir um ecossistema saudável para toda a cadeia de valor e assim garantir a sustentabilidade e longevidade da empresa.

Possuir um Sistema Integrado de Gestão baseado em tecnologia da informação já é a realidade da maioria das empresas de médio a grande porte. Implementar processos informatizados para Integrar a cadeia de suprimentos e otimizar os resultados do negócio em toda a cadeia é o desafio atual da maioria das organizações. Fica claro neste contexto que a disponibilidade da infra-estrutura de tecnologia da informação é essencial para garantir a continuidade do negócio da empresa.

Em uma organização moderna as informações essenciais para o negócio estão somente disponíveis por intermédio dos sistemas de informação. Nenhuma empresa pode cogitar em ficar dias, horas e até minutos com um sistema informatizado fora do ar, pois isto pode causar danos irreparáveis à organização. Os desastres naturais, intenções dolosas, e acidentes catastróficos ou de menor

proporção podem interromper a disponibilidade de informações e causar um impacto negativo nos principais processos empresariais. Se a empresa não estiver preparada para se recuperar de tais desastres em um tempo aceitável para o negócio, grandes prejuízos ou em casos extremos a falência podem ser a resultante de não ter-se estabelecido planejamento e investimento prévio na implementação de um processo de gestão de continuidade de negócios.

As organizações vêm experimentando um aumento das taxas de incidentes nas áreas de segurança, disponibilidade, performance e conformidade, com impactos significantes em seus retornos financeiros, reputação, produtividade e custos. De acordo com o Computer Security Institute e o FBI, os custos por incidentes relacionados a acessos não autorizados a informações situaram-se em torno de U$85.000,00 em média, no ano de 2006 e os custos de paradas de sistemas alcançaram dezenas de milhares de dólares por hora (SYMANTEC-1, 2007).

As companhias temem mais o colapso de seus sistemas de Tecnologia da Informação (TI), que o terrorismo, os desastres naturais, riscos financeiros e as limitações legislativas. No entanto, de acordo com relatório elaborado pela Unidade de Inteligência da publicação The Economist, intitulado Coming to grips with IT risk ou “Assimilando os riscos da Tecnologia da Informação”, com base em uma pesquisa realizada junto a 145 altos executivos de empresas ao redor do mundo, a maioria destas empresas não administra eficientemente os riscos associados a TI (SAP, 2007).

À medida em que os negócios e até mesmo seus clientes vêem crescer dia após dia sua dependência em relação à internet e aos sistemas de TI, os riscos de infra-estrutura tornam-se mais visíveis e significantes. Violações ou falhas em sistemas de informação causam sérias crises de negócio - danos à reputação causados por roubo de identidade, vazamento de informações confidenciais em função de falhas de sistemas e o surgimento de restrições regulatórias em função da procura por conformidade. Recentes manchetes em publicações de áreas diversas destacaram com grande ênfase numerosos problemas relacionados aos riscos tecnológicos: roubos de mídias de backup, processos litigiosos resultantes da produção e/ou preservação imprópria de registros eletrônicos, roubo de identidade e quebras de propriedades intelectuais. Hoje é facilmente perceptível entender porque os quadros executivos das corporações mundiais buscam incansavelmente respostas para a pergunta: Como mitigar dramaticamente os riscos e melhorar o retorno sobre os investimentos em sistemas de informação (SYMANTEC-2, 2007).

Que impacto a indisponibilidade da Infra-estrutura de Tecnologia da Informação causa no negócio de uma empresa de perfumaria, higiene e cosméticos localizada em São José dos Pinhais-PR?, é a questão que se pretende responder no decorrer deste estudo.

Para tanto, o objetivo desse artigo é mensurar o impacto que a indisponibilidade da Infra-estrutura de Tecnologia da Informação causa no negócio de uma empresa de perfumaria, higiene e cosméticos localizada em São José dos Pinhais-PR.

Segundo o COBIT (2005), para muitas empresas, a informação e a tecnologia que a sustenta representa seu mais valioso, mas frequentemente menos compreendido, bem. As empresas bem sucedidas reconhecem os benefícios da tecnologia da informação e usam-na para direcionar valor aos seus

stakeholders. Estas empresas também entendem e gerenciam riscos associados, tais como o incremento de normas reguladoras e dependência crítica de muitos processos de negócios em TI.

A necessidade para a garantia sobre o valor da TI, administração de riscos relacionados da TI e o aumento de requisitos para o controle sobre as informações são agora entendidos como elementos chave da governança da empresa. Valor, risco e controle constituem o núcleo da governança de TI. Governança de TI é a responsabilidade dos executivos e do conselho de diretores, e consiste da liderança, estruturas e processos organizacionais que asseguram que a TI da empresa sustenta e estende as estratégias e objetivos da organização (COBIT, 2005).

Na visão da área de Continuidade de Negócios da IBM, clientes, funcionários, fornecedores e parceiros de negócios têm a expectativa de estarem aptos a acessar suas informações a qualquer hora do dia, em qualquer lugar do mundo. Se você tem operações contínuas de negócios, então as pessoas podem obter o que necessitam de seu negócio — o que ajuda a reafirmar seu sucesso e sua vantagem competitiva. Os negócios também precisam ser cada vez mais sensíveis às questões de privacidade e segurança de dados do cliente, de forma que os recursos vitais de informação não sejam comprometidos. Uma vez que você se depara com as exigências regulatórias e com as demandas inerentes de participar da economia global, começa a compreender alguns dos desafios enfrentados pelos gerentes de TI (IBM, 2007).

Segundo a revista Info-Corporate (INFO-1, 2007) mais de 40% das companhias não têm um plano de recuperação de desastre. Essa é a conclusão do estudo Veritas Disaster Recovery Research 2004, junto a 1259 profissionais de TI em todo o mundo e capitaneado pela consultoria inglesa Dynamic Markets. A pesquisa indica que 38% das empresas possuem um plano integrado de continuidade de negócios, mas 92% dos entrevistados (incluindo os que possuem um planejamento) dizem que enfrentariam sérios problemas caso houvesse interrupção de sua infra-estrutura. Segundo a Dynamic, um dado preocupante é que, em relação à mesma pesquisa realizada entre 2002 e 2003, o número de empresas que precisaram usar seus planos de contingência subiu 18%, mas a proporção de companhias com plano de disaster recovery não aumentou.

Apenas 3% dos entrevistados acreditam que em caso de interrupção da infra-estrutura seus negócios não sofreriam impacto. O levantamento constatou que o tempo médio que as empresas levariam para restabelecer seus negócios no caso de um desastre supera 72 horas, resultando em redução de produtividade (62%); diminuição dos lucros (40%); e danos na relação com o cliente (38%) (INFO-1, 2007).

"Se diversos ativos suportam os processos de negócios de uma corporação, a questão é saber o que deve ser protegido: os ativos ou os processos?", afirma Paulo Beck, da HP. Como as ameaças causam falhas e interrupções em ativos que suportam processos, isso significa que quanto mais disponível e protegido o ambiente de infra-estrutura da empresa, maior é a garantia da continuidade nos negócios e menor a chance de uma ameaça causar a parada operacional dos processos corporativos. Por isso, Paulo Beck diz que um PCN deve suportar quatro pilares: os ativos, que pedem um plano de recuperação de desastres quando ocorrem falhas ou interrupções na operação; os processos de negócios (o plano de contingência deve evitar a indisponibilidade

dos ativos); as pessoas, que precisam estar sempre prontas para um plano de ação emergencial; e as ameaças, que sugerem um plano de gestão de crises, focado nos diferentes cenários de ameaças ao ambiente de negócios (TERZIAN, 2006).

Por causa da necessidade de contratação de pessoal qualificado, locais alternativos de processamento, equipamentos redundantes e armazenamento externo de dados, o PCN é geralmente caro, o que muitas vezes torna difícil sua aprovação pelo board ou pelo CEO. Para alcançar um valor plausível de investimento, e convencer o conselho de que é melhor gastar com um PCN do que perder muito no futuro, especialistas recomendam a realização de uma Análise de Risco, para identificar ameaças e vulnerabilidades nos ativos, e uma Análise de Impacto Empresarial, mais conhecida por Business Impact Analysis (BIA) (TERZIAN, 2006).

É regra: qualquer incidente pode causar algum impacto negativo na empresa, mesmo em se tratando de uma interrupção de curta duração. Segundo o Disaster Recovery Institute (DRI), duas em cada cinco empresas que sofrem interrupção por uma semana fecham as portas em menos de três anos. Por isso, Fábio de Franco, líder de consultoria em TI da IBM Global Service, sugere uma análise de risco bem minuciosa. "Ela deve tirar uma fotografia geral, de forma a identificar os riscos em um todo para depois ir para o detalhe, aos riscos mais críticos", afirma de Franco (TERZIAN, 2006).

Já no caso do Business Impact Analysis, Beck diz que a missão é identificar os riscos em potencial, estimar os efeitos (tangíveis e intangíveis) de um desastre na organização e determinar as exigências para uma estratégia de recuperação. "Regras e critérios com ênfase em estimativas de rendas perdidas e produtividade deixarão uma impressão mais duradoura na administração do que uma análise subjetiva", diz Beck. Ou seja, o board da companhia se convencerá mais facilmente se for dito que um vendedor perdeu 100 mil reais porque ele não conseguiu obter cotações de preços quando o computador central estava fora do ar (TERZIAN, 2006).

Desenvolver um plano de análise de impacto com a ajuda dos gestores de negócios e questionar quanto tempo determinado processo agüentaria sem TI e quais são os aplicativos mais críticos é um bom começo. Antônio Gesteira, gerente-executivo da PricewaterhouseCoopers, diz que é preciso ouvir cada um dos donos dos processos críticos de diferentes áreas e tirar deles quais seriam os impactos decorrentes de falhas nesses processos e em seus ativos, o ponto de vista a partir de um incidente simples, médio e gigantesco. "Isso tem de ser feito com todos os processos de negócios, sem exceção", diz Fábio de Franco, da IBM (TERZIAN, 2006).

Quase 60% das empresas americanas ainda não têm planos de disaster recovery para manter a TI no ar em caso de acidentes, afirma uma pesquisa da Info-Tech Research (INFO-2, 2007), divulgada ontem, seis anos após o atentado terrorista ao World Trade Center, em Nova York. A empresa de pesquisas avalia que as organizações ainda não absorveram as lições do episódio, como ficou comprovado em incidentes posteriores, como o furacão Katrina, em 2005, ou o apagão que ocorreu em julho deste ano em diversas cidades dos Estados Unidos. Segundo a Info-Tech, as empresas ainda estão mal aparelhadas em termos de software e hardware para recuperação de desastres e ainda relutam em investir em sites de redundância e equipamentos extras de armazenamento (storage).

De 1,1 mil empresas entrevistadas na pesquisa, apenas 475, 42% do total, implementaram planos de recuperação de desastres. Desse grupo, 25% das companhias já precisaram acionar os planos. Outra parcela de 30% das empresas declara estar preparando programas de recovery, o que a Info-Tech considera positivo, mas ainda insuficiente (INFO-2, 2007). O estudo faz recomendações para empresas que planejam investir em recuperação de desastre: avaliar as aplicações sob a ótica do risco de impacto nos negócios a fim de determinar prioridades para a organização; avalie o que é necessário em termos de pessoas, processos e tecnologia para garantir uma recuperação rápida e ao mesmo tempo eficiente em termos de custos em caso de desastres; nas terceirizações de infra-estrutura de TI, transfira o risco e não a responsabilidade. Não pressuponha que a iniciativa de outsourcing garante um plano completo de recuperação; após a implementação do plano de recuperação, faça testes e auditorias regularmente para assegurar que não há falhas.

As empresas estão cada vez mais dependentes dos sistemas de tecnologia de informação para suportar seus processos de negócio. Embora cientes desta situação, os acionistas e executivos de negócios, quando da decisão entre investir em soluções de contingência para a infra-estrutura de Tecnologia da Informação ou investir em processos de negócio que proporcionam lucratividade assegurada, geralmente optam pela segunda opção. Obter recursos para investimentos em ambientes de contingência de Tecnologia da Informação (TI) exige uma abordagem que relacione o impacto negativo nos resultados da empresa com a indisponibilidade de TI.

A finalidade deste estudo é propiciar ferramentas para que os executivos de tecnologia de informação possam justificar a implementação de uma solução de contingência, que suporte os processos de negócio na ocorrência de desastre ou evento que indisponibilize o ambiente principal de infra-estrutura tecnológica.

Analisar-se-a portanto, um item isolado do Plano de Continuidade de Negócios cujo objetivo é bem mais amplo e visa garantir a continuidade dos processos de negócio na ocorrência de desastre que afete pessoas, ativos e processos da organização.

2. REFERENCIAL TEÓRICO

A análise da literatura publicada sobre o assunto em questão representa uma importante etapa desta pesquisa. Optou-se por publicações recentes de autores com vivência prática na área de gestão de continuidade de negócio e gerenciamento de riscos. Priorizou-se também fontes reconhecidas e utilizadas no meio empresarial, de forma a subsidiar a pesquisa com informações atualizadas e que representem a realidade de como a Análise de Impacto no Negócio vem sendo conduzida nas organizações nos dias atuais.

A revisão da literatura está estruturada em seções que abordam de forma estruturada os temas: Tecnologia da Informação, Processo de Negócio e Tecnologia e as metodologias existentes para relacionar ambos. Dentro de cada seção, são abordados diversos tópicos considerados importantes para a constituição do arcabouço teórico.

2.1. Tecnologia da informação

Pode-se conceituar a tecnologia da informação como recursos computacionais para a geração e uso da informação. Está fundamentada nos seguintes componentes: *hardware* e seus dispositivos e periféricos; software e seus recursos; sistemas de telecomunicação; e gestão de dados e informação (REZENDE, 2002).

Os sistemas de telecomunicações são recursos que interligam o hardware e o software. A gestão de dados e informações com seus respectivos recursos, parte integrante da Tecnologia da Informação, também são subsistemas especiais do Sistema de Informação global das empresas. A gestão de dados e informações compreende as atividades de guarda e recuperação de dados, níveis e controle de acesso das informações (REZENDE, 2003).

Todos esses componentes interagem entre si e necessitam do componente fundamental que é o recurso humano, *peopleware* ou *humanware.* Embora conceitualmente este componente não faça parte de TI propiamente dita, sem ele essa tecnologia não teria funcionalidade e utilidade (REZENDE; ABREU, 2006).

A metodologia COBIT criada pelo ISACA – Information Systems Audit and Control estabelece quatro domínios para refletir o modelo de processos de Tecnologia da Informação: **planejamento e organização:** define as questões estratégicas ligadas ao uso da TI em uma organização, trata de vários processos, entre eles, a definição da estratégia de TI, arquitetura da informação, direcionamento tecnológico, investimento, riscos, gerência de projetos e da qualidade (COBIT, 2005); **aquisição e implementação:** define as questões de implementação da TI conforme as diretivas estratégicas e de projeto pré-definidos no Plano Estratégico de Informática da empresa, também conhecido como PDI (Plano Diretor de Informática). Possui uma série de processos como, por exemplo, identificação de soluções automatizadas a serem aplicadas ou reutilizadas na corporação, aquisição e manutenção de sistemas e de infra-estrutura, desenvolvimento e mapeamento de procedimentos nos sistemas, instalação e gerência de mudanças (COBIT, 2005); **entrega e suporte:** define as questões operacionais ligadas ao uso da TI para atendimento aos serviços para os clientes, manutenção e garantias ligadas a estes serviços. O momento destes domínios é após a ativação de um serviço e sua entrega ao cliente, que pode operar ou utilizar os serviços da empresa para operação terceirizada. Os processos relativos a este domínio tratam da definição dos níveis de serviço (SLA); gerência de fornecedores integrados às atividades; garantias de desempenho, continuidade e segurança de sistemas; treinamento de usuários; alocação de custos de serviços; gerência de configuração; gerência de dados, problemas e incidentes (COBIT, 2005); **monitoração:** define as questões de auditoria e acompanhamento dos serviços de TI, sob o ponto de vista de validação da eficiência dos processos e evolução dos mesmos em termos de desempenho e automação. Os processos deste domínio tratam basicamente da supervisão das atividades dos outros processos; adequações realizadas na empresa para garantia de procedimentos operacionais; coleta e análise de dados operacionais e estratégicos para auditoria e para controle da organização (COBIT, 2005);

Segundo o IT Governance Institute (2007), os recursos de Tecnologia de Informação (TI) podem ser definidos como segue: as aplicações são os sistemas automatizados de usuário e procedimentos manuais que processam a informação; a informação é o dado em todas as suas formas entrada, processamento e saída por sistemas de informação, em qualquer que seja a forma usada pelo negócio; a infra-estrutura é a tecnologia e as instalações (hardware, sistemas operacionais, sistemas de gerenciamento de banco de dados, rede, multimídia, etc., e o ambiente que os aloja e sustenta) que habilitam o processamento das aplicações; as pessoas e o pessoal necessário para planejar, organizar, adquirir, implementar, entregar, suportar, monitorar e avaliar os sistemas de informações e serviços. Eles podem ser internos, *outsourced* ou contratados de acordo com a necessidade.

Os sistemas de informação são o conjunto de partes (quaisquer) que geram informações, ou, também, o conjunto de *software*, *hardware*, recursos humanos e respectivos procedimentos que antecedem e sucedem o *software*. Tem como maior objetivo o apoio nos processos de tomada de decisões na empresa, e seu foco esta direcionado ao principal negócio empresarial. Genericamente, os sistemas de informação podem ser classificados em operacional, gerencial e estratégico (REZENDE, 2003).

2.2. Continuidade do negócio

Segundo o Board Briefing on IT Governance publicado pelo IT Governance Institute (2003), cada vez mais, a alta administração está descobrindo o impacto significativo que a tecnologia da informação pode ter no sucesso da empresa. A administração espera por uma alta compreensão da maneira como a TI funciona e a probabilidade de ser a alavanca de sucesso para a vantagem competitiva. Em particular a alta administração necessita saber se sua gerência de TI: provavelmente atingirá seus objetivos?; é resistente o bastante para aprender e adaptar-se?; é discreta administrando os riscos de frente?; reconhece apropriadamente as oportunidades e age sobre elas?.

As empresas bem sucedidas compreendem os riscos e exploram os benefícios de TI, e procuram meios para tratar de (IT GOVERNANCE INSTITUTE, 2003): alinhar a estratégia de TI com a estratégia de negócio; difundir em cascata objetivos e estratégias de TI na empresa; providenciar estruturas organizacionais que facilitem a implementação de metas e objetivos; criar relacionamentos construtivos e comunicações efetivas entre o negócio, a TI e parceiros externos; insistir que uma estrutura de controle de TI seja adotada e executada; medir desempenho de TI.

Mcclain (2006), vice-presidente da Sun Microsystems para o Marketing de Software diz que o motivo que determina a importância das empresas disporem de um plano de continuidade do negócio, é simplesmente porque isso distingue um bom negócio. Segundo MccLain, os clientes esperam que as empresas estejam disponíveis em qualquer momento, 24 horas x 7 dias. Por este motivo, um tempo de funcionamento operacional constante é uma das características de maior procura nos negócios dos nossos dias. A capacidade de manter uma empresa em operação apesar de grandes e pequenas interrupções é simplesmente uma questão de atender aos clientes e mercados, e ao mesmo tempo permanecer competitiva. As empresas que dispõem de planos de recuperação de desastres/continuidade de negócios são aquelas que estão

certamente preocupadas em manter em funcionamento o seu negócio em longo prazo. As empresas que não dispõem de um plano destes estão a jogar com a sua sorte, sendo que quem assume os riscos desse jogo são os seus acionistas e os seus clientes.

Segundo D'Addario (2006), consultor sênior em gestão de segurança da informação, é fundamental o entendimento pelas empresas da diferença existente entre contingência de TI e continuidade de negócio. Contingência de TI é identificar os serviços críticos de TI e promover recursos iguais para que estejam disponíveis na falta do principal, mas, não mapeia os processos de negócio. Continuidade de negócio está além do TI e entende o negócio da corporação, seus riscos, define papéis e responsabilidades por impactos decorrentes, planeja vários cenários de eventuais indisponibilidades e promove: planos de recuperação de desastres para TI (principais serviços e equipamentos críticos); seleciona estratégias de continuidade para pessoas, processos (incluindo fornecedores e parceiros) e TI; Planos de contingência para processos de negócios (como continuar sem o TI, por exemplo); Planos de gerenciamento de crises (que nomeia um comitê para tomada de decisões durante a crise). Já para Dourado Júnior (2006), diretor de operações e serviços da SERASA, a gestão de riscos é fundamental para se estabelecer um plano de continuidade de negócios. É um componente importante no modelo de governança. O primeiro passo é classificar cada risco: natural, tecnológico, cultural, social, comercial. O segundo é entender em que grau a empresa está madura para fazer a gestão de riscos. Gestão de riscos é um processo que nunca termina, e então o desafio é manter este processo sempre ativo, ou não é possível estar sempre um passo à frente. As empresas não gostam de destinar uma parcela do orçamento de TI à gestão de riscos, mas gestão de riscos é como apólice de seguro: é importante fazer seguro e renovar a apólice todo ano.

Porém, Castro (2006), gerente de segurança operacional da Caixa Econômica Federal, esclarece que para mitigar riscos, é interessante fazer um plano eficiente de continuidade dos negócios. É importante saber o quanto se vai perder, o quanto se está disposto a perder em determinado processo, e então decidir até quanto se deve investir em tecnologia para sustentar aquele processo em caso de sinistro. "Na Caixa, nós temos tratado disso como um programa contínuo, e os gastos começam a cair porque não gastamos vela boa com defunto ruim. Por que vou gastar X milhões com um processo, se ele pode ficar fora do ar por um ou dois dias sem me trazer prejuízos de X milhões".

Os argumentos que um executivo poderá utilizar para justificar o custo do investimento realizado no plano de recuperação de desastres deverá ser focalizado no dispêndio que teria de ser realizado no caso de uma interrupção do negócio, nomeadamente em termos de perdas de receitas, de perdas de clientes, da destruição da vantagem competitiva, da publicidade negativa, etc., que lhe estariam subjacentes. Para poderem determinar o custo deste investimento, as empresas devem primeiro, realizar uma análise exaustiva de impactos no negócio, que lhes permita determinar o quanto deve ser investido em plano de continuidade de negócios. Esta análise deverá incluir os custos da recuperação do negócio, incluindo serviços não de TI e processos de negócios que surgiriam com ou sem o plano de continuidade (MCCLAIN, 2006).

Sendo tomada uma decisão de investimento, o foco pode ir para o planejamento da continuidade dos aplicativos de software e de TI. Os critérios que deverão ser observados serão se a aplicação de software para ser tolerante a desastres é primordial para uma tarefa, para um negócio ou para uma missão. Por exemplo, a minha aplicação de correio eletrônico pode ser primordial para a realização de uma tarefa e importante para mim pessoalmente, mas se apenas o meu correio eletrônico deixar de funcionar, nada de mal sucederia à empresa no seu todo. Contudo, se a aplicação de correio eletrônico de uma empresa inteira deixar de funcionar, uma percentagem muito maior da empresa deixará de poder trabalhar e este fato aproximar-se-á muito mais de algo primordial para o negócio. Mas se estivermos a falar de uma empresa como a AOL e se for a aplicação de correio eletrônico externa desta empresa que deixar de funcionar, então, este fato tomará proporções desastrosas, visto falarmos de um fornecedor de serviços que tem a maior parte dos seus negócios nesta área, com ramificações gigantescas. Para a AOL, os aplicativos de e-mail são de missão crítica (MCCLAIN, 2006).

Segundo D'Addario (2006), devido às novas leis e regulamentações muitas empresas buscaram no COBIT® um referencial para poder auditar e para poder implementar controles para demonstrar uma boa gestão e principalmente atos de governança. A Garantia de sobrevida para uma companhia é um ato maduro e ético para as corporações no mundo todo, sejam estatais ou privadas e a Continuidade de Negócios está promovendo isto ao mercado de uma forma simples, mas, com uma pitada de processos e segurança acentuada para que as empresas promovam a gestão e definitivamente alinhem, ordenem, agreguem e conectem as decisões Estratégias da Corporação ao TI e ao Mercado. Para conectar Gestão de Riscos (PO.9), Gestão de TI (ITIL), Gestão de Segurança da Informação (BS 7799-2:2002 e ISO 27001) e o Negócio da corporação é necessário somente uma coisa para termos uma Governança mais efetiva: Continuidade de Negócios.

O maior desafio dos gestores ainda é fazer com que a TI desempenhe seu relevante papel estratégico nas organizações, agregando valores a seus produtos e/ou serviços e auxiliando na promoção das inteligências competitiva e empresarial, à medida que seus recursos computacionais possibilitem a geração de cenários decisórios produzidos com as informações oportunas e com os conhecimentos personalizados. Mas esse papel deve ser desempenhado com uma positiva análise de viabilidade e riscos, em que os custos investidos sejam compensados pelos benefícios auferidos (REZENDE, 2002).

2.3. Impacto no negócio – relação entre TI e continuidade do negócio

A Análise de Impacto no Negócio (Business Impact Analysis – BIA) é uma técnica que pode ser utilizada para identificar os principais processos de negócios da corporação e os impactos decorrentes de paradas nos mesmos. Marinho (2006), formado pelo *Disaster Recovery Institute*, escreveu sobre o tema, destacando que no ambiente de Continuidade de Negócios, uma das mais importantes atividades realizadas em qualquer trabalho é o "Business Impact Analysis" (Análise de Impacto nos Negócios) ou, simplesmente, BIA. Uma visão estratégica de continuidade deve dar prioridade aos processos de negócios mais importantes da empresa (críticos), para só então partir para o planejamento dos procedimentos de contingência e a definição mínima dos componentes que devam ser replicados. Entretanto, nesse momento, a empresa encontra uma

grande dificuldade: como mensurar dentre os seus mais importantes processos a sua ordem de retomada? Quem teria o conhecimento de cada um deles para definir quem merece e de quanto seria um investimento para Continuidade? E, o mais importante: como evidenciar esta decisão? Para solucionar este dilema, definiu-se uma Análise de Impacto nos Negócios. Todo empresário e executivo conhece a definição de "custo" e o seu reflexo, na estrutura da Empresa. Uma "BIA" dá um passo além desta definição, indicando o valor de custo de parada para cada Processo analisado. O Custo de parada é a avaliação, caso a caso, do respectivo valor agregado que o Processo adiciona ao fluxo de Processos, no Principal Negócio da Empresa. De uma forma mais simples: torna-se fácil avaliar a importância dos Processos de Negócios empresariais, frente aos Impactos causados (multas, dano à imagem da empresa, suspensão de serviço ao cliente, etc.) em situações de paralisação de atividades. Difícil é saber em qual ordem vamos restaurar cada um dos processos afetados. A "BIA" nos indica este caminho, mensurando o VALOR da parada do processo, em função da perda que o negócio da empresa sofre. Desta forma, fica fácil para quem planeja, avaliar o custo de investimento na Continuidade da Empresa (MARINHO, 2006, p.1).

O propósito do BIA é auxiliar a organização a identificar quais unidades de negócios, operações e/ou processos são essenciais para a sobrevivência do negócio. O BIA facilitará a identificação do prazo em que unidades essenciais de negócios e/ou processos devem retornar a sua operação integral após uma situação de desastre. O objetivo é relacionar a habilidade de entregar produtos ou suportar serviços de missão crítica com o impacto gerado no negócio quando sujeito a cenários de desastre. O BIA também facilitará a identificação de recursos requeridos para retornar as operações do negócio a um nível de sobrevivência (MARINHO, 2006).

Segundo a Northrop Grumman Organization (2006), o processo de Análise de Riscos quando planejado para Recuperação de Desastres, fornece a base para planejar todo o esforço necessário na Recuperação de Desastres. Esta análise envolve identificar as ameaças mais prováveis de ocorrer para uma organização e minimizar a exposição a elas. Analisando as possibilidades, o negócio tem uma idéia melhor do que é importante para recuperação de desastres. A organização como um todo também ganha uma melhor compreensão do mecanismo de desastre, resultando em um plano mais útil.

As principais atividades envolvidas na estratégia do BIA são (NORTHROP, 2006): definir critério para determinar o que é crítico; identificar processos vitais para ao negócio; identificar sistemas e informações que são vitais para o suporte do negócio; determinar o impacto do custo nos negócios; identificar interdependências; definir a janela de recuperação.

Os quatro objetivos principais do BIA são (NORTHROP, 2006): identificar os ativos e funções que são necessárias para reiniciar o negócio da organização após um desastre, e priorizar eles de acordo com a sensibilidade ao tempo e criticidade; identificar as ameaças mais prováveis para os ativos e funções da organização; desenvolver estratégias para eliminar riscos que são passíveis de eliminação e minimizar o impacto dos riscos que não podem ser eliminados; desenvolver estratégia para proteger e recuperar as funções críticas do negócio que podem ser perdidas após o evento do desastre.

O BIA consiste de duas operações básicas: Coleta de dados e análise de dados. Recomenda-se na coleta de dados a inclusão da lista de computadores e equipamentos de telecomunicações e o inventário completo das aplicações e sistemas informatizados (NORTHROP, 2006).

Tipicamente, os dados são coletados dos funcionários que utilizam e gerenciam os sistemas no dia a dia. Um questionário pode ser enviado para cada usuário de um sistema ou aplicação específica (e para aqueles responsáveis por manter estas aplicações) para identificar seu uso em um dia de trabalho normal. O recomendável no entanto é realizar um diálogo com os usuários e preencher as respostas dos questionários à medida que o diálogo vai ocorrendo. Um questionário bem elaborado incluirá questões a respeito de como o usuário lida com situações em que o sistema ou aplicativo permaneça indisponível por 1 hora, 24 horas, 48 horas, 72 horas e assim por diante. Se não forem identificadas estratégias para enfrentar estas situações, provavelmente o sistema em função é crítico (NORTHROP, 2006).

O BIA é o processo de análise de todas as funções do negócio e o efeito que um determinado tipo de desastre poderá ter sobre elas. Determinando o tipo ou o escopo da dificuldade que um evento potencial identificado na análise de riscos causaria na empresa no caso de sua ocorrência. O BIA deve quantificar, se possível, o impacto da perda sob o ponto de vista financeiro e do tempo de interrupção do negócio.Outra questão que a maioria das companhias esperam responder é quais sistemas e aplicações devem ser recuperadas e em que tempo (DRJ, 2007).

Por último, o BIA ajudará a companhia determinar em quanto tempo as aplicações devem estar disponíveis após o desastre e a posição dos dados em relação ao tempo. Se o BIA obtiver sucesso na entrega destes resultados, então ele será uma valiosa ferramenta (DRJ, 2007).

De acordo com o Disaster Recovery Journal (2007), os seguintes pontos devem ser considerados na execução do BIA para evitar problemas nos resultados:

Uma vez que a entrevista está completa, o questionário é retornado ao executivo para revisão. Enquanto a maioria dos executivos defendem que seus processos de negócios são extremamente vitais para a organização e devem ser recuperados em um curto espaço de tempo, na maioria dos casos, eles não são capazes de quantificar os impactos financeiros no caso da indisponibilidade dos mesmos (DRJ, 2007).

Assegurar que a quantificação do impacto financeiro foi obtida de fontes confiáveis para evitar questionamentos relativos a acuracidade dos dados quando da apresentação do resultado do BIA à direção da empresa. Os profissionais que conduzem as entrevistas devem conhecer conceitos de análise financeira, de forma a conduzir o executivo na correta interpretação do objetivo do BIA, a fim de obter informações precisas sobre os impactos financeiros (DRJ, 2007).

A habilidade de enfrentar interrupções de sistemas é chamada tolerância. Em termos práticos, tolerância pode ser expressa em termos financeiros. Ele representa a perda em receitas para a companhia devido à indisponibilidade de sistemas durante um período específico de tempo. Se existe uma tolerância muito baixa dentro da companhia no caso da perda de um equipamento ou interrupção de uma função que ele provê, esta baixa tolerância é expressa como um alto valor de perda financeira. Por outro lado, se a companhia pode tolerar por um grande

período de interrupção, esta alta tolerância é expressa como um baixo valor de perda financeira (NORTHROP, 2006).

Segundo o Northrop (2006) em termos convencionais de processamento de dados, as aplicações podem ser classificadas usando o seguinte espectro de tolerâncias. **Crítica:** As funções não poderão ser executadas a menos que capacidades idênticas sejam encontradas para substituir as capacidades danificadas. Aplicações críticas não podem ser substituídas por métodos manuais sob nenhuma circunstância. A tolerância por interrupção é muito baixa e o custo da interrupção é muito alto. Assim, para os sistemas e aplicações críticas, a companhia necessita disponibilizar acesso a equipamentos similares aos originais, e em uma emergência, planejar a transferência dos sistemas aplicativos e dados associados para o hardware de contingência de forma a restabelecer o processamento. **Vital:** Estas funções não poder ser executadas por meios manuais ou podem ser executadas de forma manual por curtos períodos de tempo. Existe uma moderada tolerância à interrupções e a um custo baixo, desde que as funções sejam restauradas em até cinco dias. Nas aplicações classificadas com vitais, uma suspensão breve do processamento pode ser tolerada, mas é necessário um considerável esforço para restabelecer os dados para uma condição de usabilidade. **Sensitiva**: Estas funções podem ser executadas, com dificuldade mas a um custo aceitável, por meio de processos manuais por um extenso período de tempo. Contudo, aplicações sensitivas, requerem um considerável esforço para restaurar de sincronismo após restauradas. **Não Crítica**: Estas aplicações podem ser interrompidas por um longo período de tempo, a um custo baixo ou inexistente para a companhia, e requer pequeno ou nenhum esforço para sincronização após restaurada.

Em adição as perguntas para os usuários classificarem seus sistemas pela criticidade e identificarem as estratégias para enfrentar uma indisponibilidade, uma outra questão deveria ser feita durante a coleta inicial de dados: Quanto uma indisponibilidade de específica duração custaria para a empresa? Os usuários departamentais são geralmente capazes de calcular estes custos. Eles podem utilizar as informações existentes para demonstrar a performance do departamento, adaptando-as para mostrar o custo da indisponibilidade de determinada função (NORTHROP, 2006).

A Análise de Impacto no Negócio (BIA) tem sido considerada a ferramenta favorita no desenvolvimento da análise de viabilidade para um programa de Recuperação de Desastres. Por muitos anos ela tem sido a abordagem padrão (com algumas pequenas variações) que as empresas utilizam para determinar o impacto que uma interrupção no negócio causa ao longo do tempo. O BIA é um mecanismo maravilhoso para obter informações sobre as prioridades dos processos de negócio e o impacto no negócio na ocorrência de um desastre. Isto é obtido pela determinação de qual processo de negócio teria o maior impacto financeiro (perda de receita, aumento das despesas, perda de market share, etc.) ou o maior impacto operacional (impossibilidade de tomada de decisão, falta de controle, etc.) no evento de um desastre (NORTHROP, 2006).

Segundo Walch (2006), em relação ao processo de coleta de dados utilizado no BIA, baseado em entrevistas individuais, que conduzem a perda de objetividade e consumo de tempo, sugere-se convidar um grupo de executivos (não mais de seis) e conduzir um encontro para Análise de Criticidade do Negócio, o qual não deve durar mais que 45 minutos, e tem por objetivos:

educação sobre análise de impacto, obtenção de informações do negócio e validar dados/aplicações de forma a identificar quais são os processos críticos do negócio. O processo consiste em solicitar o seguinte aos executivos: listar os processos de negócios de sua unidade de negócio; assinalar a prioridade do processo em: imediata, critica, importante, vital ou não prioritária; justificar a prioridade utilizando o impacto financeiro, operacional ou descritivo.

Este método elimina a preocupação dos executivos sobre as estimativas financeiras que estão fornecendo. Eles estão simplesmente provendo opiniões sobre a criticidade de seus processos de negócio, nada mais. Por outro lado, a equipe responsável pela condução do processo, está colhendo informações sobre quais aplicações suportam aqueles processos de negócio. Agendamento, esforço e acompanhamento é mais fácil com este tipo de abordagem colaborativa (WALCH, 2006).

O próximo passo neste processo é conversar com a equipe de Tecnologia da Informação, utilizando a mesma metodologia anterior, para informar o que foi comunicado pelas unidades de negócio e determinar o seguinte (WALCH, 2006): onde reside a aplicação – data center e servidor; em quanto tempo pode a aplicação ser realmente recuperada atualmente; baseado em informações históricas (quantos chamados de help-desk são recebidos) que prioridade eles colocariam para esta aplicação? Isto coincide com o que os executivos de negócio informaram?.

Em paralelo com as reuniões de trabalho, é importante informalmente identificar os riscos e ameaças as quais a localização do negócio estão sujeitos. Isto habilitará a medição dos riscos contra os impactos para determinar onde a companhia deve focar seu tempo, esforço e investimento. Não é este o real objetivo do BIA; Determinar onde e como a companhia deveria aplicar o dinheiro que orçou para continuidade de negócio? (WALCH, 2006).

Após completar todas as reuniões de trabalho, sugere-se a criação de duas planilhas eletrônicas. A primeira descreve cada processo de negócio – sua prioridade, justificativa, contato primário e aplicações associadas. A segunda planilha deve conter uma lista de aplicações com os respectivos contatos, localização, espaço de armazenamento de dados, e tempo realista de recuperação. Estes dois documentos combinados podem ser utilizados de forma contínua em conjunto com o programa de continuidade de negócio (WALCH, 2006).

Apesar de existir muitas outras distinções entre o BIA e a Análise de Criticidade, as principais razões por que esta última é mais eficaz inclui (WALCH, 2006): as reuniões de Análise de Criticidade são colaborativas e auto-validadas e educam os executivos no processo; a paralisia da análise desaparece, porque se foca na justificativa da prioridade e não na coleta de impactos detalhados; as planilhas de que priorizam os objetivos dos processos de negócio e recuperação das aplicações são utilizadas em longo prazo como parte de ao longo de todo o programa de continuidade; as informações baseadas em considerações/opiniões pessoais e informais sobre os impactos diminui as potenciais críticas dos executivos de finanças.

Esta abordagem é construída sob uma premissa muito simples. Quando você coloca um grupo de executivos juntos em uma sala, eles podem dizer que processos geram mais receitas, quais são altamente dependentes de tecnologia e identificar quem gritará mais alto quando a tecnologia não estiver disponível. A

Análise de Criticidade ajuda a determinar os objetivos de continuidade de negócio de forma mais rápida e eficaz que o BIA e previne que as iniciativas de cair em um grande buraco negro (WALCH, 2006).

3. METODOLOGIA DA PESQUISA

Foi utilizada a pesquisa exploratória, que segundo Gil (1994) tem como principal finalidade desenvolver, esclarecer e modificar conceitos e idéias, com vistas na formulação de problemas mais precisos. Quanto aos meios foi realizado levantamento bibliográfico e documental em livros, revistas, sites e periódicos. Na seqüência, realizou-se um estudo de caso, que constitui segundo Vergara (1990), um "estudo circunscrito a uma ou poucas unidades, entendidas como uma pessoa, uma família, um produto, uma empresa, um órgão público, uma comunidade ou mesmo um país. Tem caráter de profundidade e detalhamento. Pode ou não ser realizado no campo". Para Yin (2001), "um estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos". O estudo de caso teve por objetivo mensurar o impacto no negócio causado pela indisponibilidade da Infra-estrutura de Tecnologia de Informação, utilizando-se as ferramentas e metodologias identificadas na pesquisa exploratória.

Com relação aos sujeitos da pesquisa ou unidade de observação, as Informações foram obtidas junto aos acionistas, executivos da área de negócio, executivos da área de tecnologia da informação e os fornecedores estratégicos da área de TI. O estudo foi realizado em uma empresa de perfumaria, higiene e cosméticos localizada na cidade de São José dos Pinhais – PR no período de Julho a Setembro de 2007. Quanto à coleta de dados, foram realizadas entrevistas e análise de documentação disponível.

Para o tratamento dos dados coletados foi utilizada a análise de conteúdo proposta por Minayo (1998), que evidencia que existem basicamente duas funções na aplicação da técnica de análise de conteúdo. A primeira diz respeito à *verificação de hipóteses ou questões*, onde pode-se encontrar respostas para as questões formuladas e também confirmar ou não as afirmações estabelecidas antes do trabalho de investigação (hipóteses). A segunda, diz respeito à *descoberta do que está por trás dos conteúdos manifestos*, indo além das aparências do que está sendo comunicado.

Ainda, seguindo as recomendações de Minayo (1998), a análise do conteúdo contemplou as seguintes fases: pré-análise, exploração do material, tratamento dos resultados obtidos e interpretação. A fase de pré-análise compreendeu a definição da unidade de registro, unidade de contexto, trechos significativos e categorias. Na fase de exploração foi aplicado o que foi definido na fase anterior. Na fase de tratamento dos resultados, além do tratamento quantitativo, foi realizada a análise qualitativa, onde tentou-se desvendar o conteúdo subjacente ao que estava sendo manifesto.

Para que análise dos dados da pesquisa fosse viabilizada, foi necessário elaborar critérios para interpretar os seus resultados por meio de um protocolo de análise (GIL, 1999). Nesse protocolo se estabeleceu uma relação entre os construtos e respectivas variáveis com os autores que fundamentaram as perguntas constantes nos questionários utilizados na pesquisa. A estratégia de análise e a forma de medição também estão descritas nesse protocolo que tem

como base o modelo proposto no BIA para identificar a relação existente entre a tecnológica da informação e o impacto que sua indisponibilidade causa no negócio da empresa em análise, conforme descrito no capítulo 4. O construto tecnologia da informação possui as variáveis: sistemas de TI; criticidade dos sistemas; e infra-estrutura de TI. O construto continuidade do negócio contém as variáveis: processos críticos do negócio; e riscos em TI. O construto impacto no negócio (relação entre tecnologia da informação e continuidade do negócio) possui a variável: impactos tangíveis e intangíveis.

Cada uma das variáveis possui seus respectivos autores que as fundamentam.

A técnica utilizada, no levantamento das informações no estudo de caso, foi de entrevistas em profundidade com os principais usuários chaves, solicitação de preenchimento de questionários e observação dos processos de negócio, de TI e recursos de informação. Assim, foram questionados aos usuários chaves da organização os elementos necessários para que se tenha o conhecimento e a importância do uso da Tecnologia da Informação na empresa, como suporte aos seus processos de negócio.

O levantamento dos dados e informações foi efetuado por meio de entrevistas feitas com gestores de processos de negócio e a área de Tecnologia da Informação.

As medidas de impactos organizacionais foram divididas em duas categorias principais: os impactos tangíveis, que podem ser expressos em termos financeiros (e por essa razão podem fornecer justificativa financeira para o investimento em medidas de continuidade do serviço), e impactos não quantificáveis, que apresentam maior dificuldade de serem traduzidos em valores monetários. Sendo **impactos tangíveis** (custo de oportunidade; redução ou perda de lucro; aumento do custo operacional). E **impactos não tangíveis** (recuperação da imagem da empresa; perda de share de mercado; perda de reputação e credibilidade; penalidades e multas devido a descumprimento da lei; perda de clientes).

Este estudo fundamentou-se também em documentos e informações resultantes de consultoria previamente realizada na área de Plano de Continuidade de Negócios.

4. ANÁLISE DO ESTUDO DE CASO

Garantir um único ambiente tecnológico na organização, contemplando requisitos de performance, segurança, atualização tecnológica e disponibilidade é hoje um desafio para a maioria dos executivos de tecnologia da informação, não só pela dificuldade de acompanhar a velocidade das mudanças inerentes a está área, mas também pela complexidade em relacionar investimentos em tecnologia com resultados do negócio. Justificar investimentos em um Plano de Continuidade dos Negócios (PCN) que pode ou não resultar na necessidade de implementação de um Plano de Contingência é uma tarefa ainda mais árdua.

Conduzir a Análise de Impacto no Negócio, ou simplesmente BIA em uma grande organização é difícil e requer muito tempo e dedicação. É necessário envolver todos os principais executivos e usuários-chave para que o resultado tenha credibilidade e seja aceito como base para estabelecer um plano efetivo de investimentos e ações na área de continuidade de negócio. O BIA identifica e avalia os impactos resultantes da interrupção e dos cenários de desastres que

podem afetar a organização, bem como as técnicas para quantificar e qualificar esses impactos. O BIA também define a criticidade dos processos de negócios, suas prioridades de recuperação e interdependências, para que os objetivos de recuperação sejam atendidos nos prazos necessários e estabelecidos.

No estudo de caso, foi realizada uma Análise de Impacto nos Negócios (BIA), que consistiu num exame detalhado das funções e da importância dos serviços informatizados que suportam os processos de negócio, na perspectiva de seus gestores e usuários chaves, para identificar os impactos da interrupção do seu funcionamento.

Os objetivos da análise de impacto consistiram na identificação dos sistemas de informação e classificação dos mesmos em ordem de importância, **na perspectiva do negócio.** Com esse conhecimento a direção da empresa, bem como a Liderança de TI, consegue fundamentar a tomada de decisão de investimento em recursos que evitem interrupções não desejadas da TI a uma melhor relação custo/benefício.

4.1. Análise da tecnologia da informação

As seguintes variáveis foram analisadas para o constructo **Tecnologia da Informação**: Sistemas de TI, Criticidade dos Sistemas e Infra-estrutura de TI.

Foram distintas as áreas e os cargo das pessoas que participaram das entrevistas do BIA e que possibilitaram o levantamento dos possíveis impactos decorrentes de uma indisponibilidade dos serviços de TI, no decorrer do tempo. Foram 23 pessoas entrevistadas. Além dessas pessoas, houve uma ativa participação da equipe de TI no levantamento, tabulação, análise e validação das informações obtidas junto aos entrevistados. Quando necessário dirimir alguma dúvida, em relação a um ponto qualquer, convocava-se reunião extraordinária com as áreas de negócios e equipe de TI para tratar do assunto em questão e chegar a uma conclusão final.

a. Sistemas de TI

Com base nas entrevistas realizadas e posterior alinhamento com a área de TI, identificou-se 67 sistemas de informação que suportam todos os processos de negócio da empresa.

b. Criticidade dos Sistemas

Da análise e consolidação das entrevistas, considerando-se somente os sistemas classificados com nível de criticidade alto e que não podem ser realizados de forma alternativa (sem o uso dos serviços de TI), evidenciando o tempo máximo de indisponibilidade que não implique em prejuízos tangíveis, chega-se ao Mapa Estratégico de Recuperação de Sistemas.

Este tempo também orientará quais sistemas devem ser contingenciados e a respectiva prioridade de retorno quando da recuperação de uma indisponibilidade. O tempo máximo de recuperação dos sistemas variou entre 8 e 360 horas.

c. Infra-estrutura de TI

Identificou-se por meio de levantamentos em campo e de reuniões com a equipe de TI toda a infra-estrutura tecnológica que suporta os processos de negócios da organização. A mesma pode ser organizada nos seguintes grupos:

data center em São José dos Pinhais; servidores de sistemas de negócios; servidores de infra-estrutura básica; soluções de armazenamento de dados e backup; infra-estrutura de telecomunicações; infra-estrutura de rede local; Infra-estrutura de segurança. Foram destacados 13 itens da infra-estrutura existente.

4.2. Análise da continuidade do negócio

As seguintes variáveis foram analisadas para o constructo **Continuidade do Negócio**: Processos de Negócio e Riscos em TI.

a. Processos de Negócio

A análise das entrevistas realizadas com os gestores da organização resultou na identificação de 114 subprocessos que viabilizam 51 processos e 12 macroprocessos de negócio relacionados com as funções organizacionais da empresas e seus subsistemas funcionais.

Identificou-se os sistemas que suportavam cada subprocesso, e principalmente, se o subprocesso poderia ser executado de forma alternativa (sem o uso dos sistemas). Está informação é de suma importância na análise do impacto no negócio causado pela indisponibilidade de TI.

O resultado da análise dos processos de negócio da organização tem uma forte dependência da Tecnologia da Informação. O menor percentual foi da gestão financeira (23%) e o maior percentual (100%) foi da gestão de portfólio e do planejamento estratégico de produtos e serviços.

b. Riscos em TI

A análise de Riscos identifica os prováveis riscos e conseqüências associadas às vulnerabilidades dos serviços de TI, e gera a base para estabelecimento de um programa de segurança com custo benefício apropriado. Esta análise é a base para a definição da estratégia de continuidade de negócios.

A avaliação dos riscos permite identificar as ameaças contra os ativos (tudo que representa valor para o negócio – tecnológicos e físicos), as vulnerabilidades e as suas probabilidades de ocorrência, e também, os seus impactos sobre a organização. Quanto maior o conhecimento sobre os riscos, mais fácil se torna tomar as decisões de como tratá-los.

Identificados os riscos, a estratégia de mitigação pode ocorrer das seguintes formas: aceitá-los, reduzi-los ou mesmo transferi-los. É por meio da análise de riscos que são obtidas as informações necessárias para a definição das opções que melhor se aplicam ao cenário, sempre levando em consideração os objetivos de negócio.

O objetivo desta análise é Identificar os principais riscos que podem provocar uma interrupção significativa nos processos de negócio críticos dependentes de TI. Foram levantados **113 itens** a serem analisados relativos a diversas categorias de vulnerabilidades provenientes das melhores práticas de análise de riscos do DRI e NIST, adicionando a eles, aqueles relacionados diretamente ao escopo da SOX, em um total de **29** objetivos e **110** controles e que também compõem esta análise.

Supondo que os eventos causadores de indisponibilidades dos serviços de TI atuem sobre o Datacenter de São Jose dos Pinhais no Estado do Paraná, pela análise dos 113 itens, e 29 objetivos do escopo da SOX (com respectivos

110 controles), foram encontradas **41 vulnerabilidades** passíveis de acontecerem.

Para cada uma das 41 vulnerabilidades estabeleceu-se qualitativamente a probabilidade (alta, média ou baixa) da vulnerabilidade ser explorada e a amplitude do impacto sobre TI (alto, médio ou baixo). Como resultado desta análise, identificou-se 10 vulnerabilidades que possuem alta probabilidade de ocorrer e alto impacto sobre a infra-estrutura de TI e conseqüentemente na indisponibilidade ou operacionalidade de processos de negócio.

As principais vulnerabilidades, detectadas sob a perspectiva de continuidade de negócios e da TI no datacenter são (Tabela 1): inexistência de um datacenter de contingência que prontamente restabeleça ou mantenha a operacionalidade do ambiente de TI de forma rápida e segura; catástrofe na infra-estrutura do datacenter, em função de sinistros, como por exemplo, incêndio total ou parcial, que provoquem indisponibilidades prolongadas de todo o ambiente de TI, ou parte dele, abrangendo infra-estruturas ou sistemas críticos; deficiências na infra-estrutura atual, que provoquem interrupções no ambiente, ou que coloquem em risco os seus ativos, como é o caso de deficiências detectadas na parte de suprimento de energia elétrica no datacenter, em função do histórico de paralisações.

Tabela 1 – Vulnerabilidades do datacenter

Vulnerabilidades	Ações sugeridas para mitigação do risco	Impacto	Probabilidade	Risco
Inexistência de um datacenter de contingência para pronto restabelecimento no caso de catástrofe na infra-estrutura do datacenter de São José dos Pinhais-PR, em função de sinistros com perdas parciais ou totais de seus ativos	Implantação de um datacenter de contingência	Alto	Baixa	Baixo
Deficiências na infra-estrutura atual, que provoquem interrupções no ambiente, ou que coloquem em risco os seus ativos	Melhorias e realização periódica de inspeções e testes na infra-estrutura	Alto	Media	Médio
Dependência de infra-estrutura ou serviços de TI,	Exigência de SLAs que eliminem os pontos únicos de falhas	Alto	Baixa	Baixo

A classificação do impacto como **alto** significa que a vulnerabilidade explorada tem capacidade de causar indisponibilidade sobre toda a infra-estrutura de TI.

4.3. Análise do impacto no negócio – relação entre tecnologia da informação e continuidade do negócio

Nessa etapa, tão importante quanto o envolvimento dos especialistas e gestores dos processos de negócio, é a organização e estruturação dos dados e informações obtidas. Para atender a esta organização e estruturação, foi utilizada a visão de valor, conforme modelo abaixo, para organização e apresentação dos impactos quantitativos e qualitativos no decorrer do tempo após a interrupção dos serviços informatizados.

a. Perdas tangíveis e intangíveis

Percebe-se pela análise dos resultados das entrevistas realizadas com gerentes e usuários chaves, uma dificuldade muito grande em quantificar financeiramente as **perdas tangíveis** em 1 hora, 2 horas, 4 horas, 24 horas, 48 horas, 7 dias e 15 dias de indisponibilidade dos serviços de TI.

As respostas obtidas nas entrevistas para 1 hora (menor impacto) e 15 dias (maior impacto) demonstram esta dificuldade. Foram identificados 49 itens com prejuízo de 1 hora de indisponibilidade de TI. E identificados 24 itens com prejuízo de 15 dias de indisponibilidade de TI.

Em relação aos **impactos intangíveis**, obteve-se 24 itens nas entrevistas realizadas, destacando-se: acumulo de trabalhos e controles; marca e imagem da empresa; dificuldades de planejamentos; descontentamento dos colaboradores; retrabalhos; qualidade das informações; tomada de decisões; dificuldade de identificar oportunidades de melhoria; inúmeras insatisfações; perda de histórico dos equipamentos; qualidade das informações da quantidade lógica e física dos estoques; e até prejuízos financeiros.

b. Impacto financeiros

Devido à dificuldade de valorizar o impacto em termos financeiros baseado nas respostas às entrevistas como tabulado acima, optou-se em estabelecer um método alternativo. Esse método é baseado nos dados financeiros fundamentadas em resultados obtidos no exercício de 2005 e 2006, bem como indicadores de cálculos informados pelos gestores dos processos de negócio e disponibilizados pela empresa (Tabela 2).

Tabela 2 – Parâmetros utilizados no cálculo do BIA

PARÂMETROS UTILIZADOS NO CÁLCULO DO BIA

	Ano 1	Ano 2
Ano:	2005	2006
Margem Bruta:	52,37%	50,21%
Margem Líquida:	16,90%	13,49%
Custo de Oportunidade (Anual):	15,64%	15,64%
Considerar Faturamento Médio nos	Não	Não
Horas Úteis Por Dia (entre 1h e 24hs):	10	12

Dados do Balanço da Empresa	2005	2006
Receita Operacional Bruta:	709.043.000	780.053.000
Receita Operacional Líquida:	549.975.000	610.944.000
Lucro Bruto	288.025.000	306.735.000
Lucro Operacional:	141.196.000	150.004.000
Lucro Líquido do Exercício:	92.945.000	82.415.000
Margem Bruta = Lucro Bruto / Receita Operacional Líquida		
Margem Líquida = Lucro Líquido / Receita Opearcional Líquida		

Ano: 2005		Ano: 2006	
Mês	Receita Operacional Líquida	Mês	Receita Operacional Líquida
jan-05	32.998.500	jan-06	36.656.640
fev-05	43.998.000	fev-06	48.875.520
mar-05	38.498.250	mar-06	42.766.080
abr-05	43.998.000	abr-06	48.875.520
mai-05	38.498.250	mai-06	42.766.080
jun-05	49.497.750	jun-06	54.984.960
jul-05	43.998.000	jul-06	48.875.520
ago-05	32.998.500	ago-06	36.656.640
set-05	49.497.750	set-06	54.984.960
out-05	54.997.500	out-06	61.094.400
nov-05	65.997.000	nov-06	73.313.280
dez-05	54.997.500	dez-06	61.094.400
TOTAL	549.975.000	TOTAL	610.944.000
Média	45.831.250	Média	50.912.000

A sazonalidade da receita operacional líquida foi alterada em relação ao real da empresa por tratar-se de informação interna e não divulgada no balanço da empresa. Esta alteração somente influenciará na análise real da distribuição do impacto ao longo do ano. Em termos de valores médios que é o normalmente utilizado na avaliação do BIA não haverá alteração do resultado final.

Os cálculos apresentados representam o potencial de perda financeira considerando a interrupção dos serviços informatizados hospedados no datacenter de São José dos Pinhais - PR.

Em conjunto com a área de finanças e controladoria ficou estabelecido as seguintes possíveis perdas financeiras no cálculo dos impactos tangíveis em função do tempo de indisponibilidade dos serviços de tecnologia da Informação.

Quanto ao Custo de Oportunidade: A indisponibilidade não chega a gerar perda de vendas. A duração da indisponibilidade apenas compromete os processos internos sem impacto visível para os clientes. Os processos podem ser recuperados com pequeno esforço e sem custos adicionais significativos durante este período (PerdaHora = ReceitaOperacionalLíquidaHora * MargemLíquida * TaxaCustoOportunidade(diária))

Quanto a Redução de Lucro: A indisponibilidade implica em acréscimo nos custos operacionais da empresa. A duração da indisponibilidade não compromete o atendimento aos clientes. É necessário aumento do esforço e ações para realizar o mesmo processo de negócio. Exemplo: Despesas com fretes especiais para atender os prazos de entrega, necessidade de horas extras, custos adicionais com infra-estrutura operacional, etc. (PerdaDia = ReceitaOperacionalLíquidaDiária * (MargemBruta - MargemLiquida)).

Quanto a Perda de Lucro: A indisponibilidade implica em perda de vendas. A duração da indisponibilidade compromete o atendimento aos clientes. Esforços adicionais não conseguem recuperar as vendas perdidas. Exemplo: Se a empresa não consegue atender pedidos colocados para suprir demandas em datas comemorativas, os mesmos serão cancelados pelos clientes, pois não

haverá a mesma demanda por esses produtos após o evento (PerdaDia = ReceitaOperacionalLíquidaDiária * MargemLiquida).

c. Elaboração de Cenários

A Análise de Impactos no Negócio é projetada com base em cenários de perdas. Dessa forma o tempo em que perdas tangíveis se realizam é diretamente proporcional ao instante em que ocorre uma indisponibilidade, podendo assim causar impactos diferentes, em instantes diferentes, para eventos de mesma duração.

Estabeleceu-se três cenários de análise com os respectivos tempos de indisponibilidade informados (Tabela 3).

Tabela 3 – Relação de cenários para cálculo do impacto no negócio

Tipo de Perda	Cenários					
	Provável		Conservador		Agressivo	
	do dia	até o dia	do dia	até o dia	do dia	até o dia
Custo de Oportunidade	1	1	5	5	Não	Não
Redução de Lucro	2	5	6	10	6	10
Perda de Lucro	6	30	11	30	4	30

Os meses de maiores e menores prejuízos não se alteraram em função do cenário quando considerada uma indisponibilidade de 30 dias. A variação do impacto financeiro (prejuízo) do cenário conservador para o agressivo é de 8,70% se considerarmos a ocorrência da indisponibilidade iniciando no dia 1 de Novembro de 2006 com 30 dias de duração. Esta variação passa para 21,4% se considerado uma indisponibilidade de 10 dias iniciando na mesma data.

d. Análise de Caso – Situação mais crítica

O período mais crítico para a empresa em termos de realização do faturamento é o mês de Novembro. No caso da ocorrência de evento que indisponibilize a infra-estrutura de TI no dia 1 de Novembro de 2006.

Nas primeiras 24 horas não existe impacto financeiro caso ocorra o cenário conservador. O prejuízo é de R$ 2.860,00 no cenário provável e atinge o valor expressivo de R$2.600.000,00 na ocorrência do cenário agressívo.

Quanto a evolução do prejuízo ao longo dos 30 primeiros dias de indisponibilidade, observa-se que após o décimo dia de indisponibilidade, o prejuízo dos três cenários se aproximam e a diferença entre eles permanece praticamente constante ao longo do tempo.

4. CONCLUSÃO

A Análise de Impacto no Negócio (BIA) ajudou a identificar os processos críticos de negócio que requerem o maior nível de proteção e a infra-estrutura tecnológica necessária para suportá-los. Forneceu recomendações de possíveis estratégias de recuperações e alternativas de investimento de forma a minimizar riscos;

Também demonstrou que é preferível investir entre R$ 6.000.000 a R$ 12.000.000, valores estes que correspondem às perdas no décimo e vigésimo dia após a indisponibilização dos serviços de TI no período de 15 de Outubro e 15 de Novembro de 2006, de forma pró-ativa nas estratégias de recuperação do que submeter o negócio à riscos tangíveis e intangíveis de maior impacto.

Em tecnologia de informação a idéia de algum sinistro interromper o negócio, mesmo que por um dia, é assustador. Paradas não programadas custam dinheiro, e existem processos de negócio que devem permanecer disponíveis a despeito da ocorrência de um desastre natural ou causado pelo homem. No entanto, tentar assegurar um processo de contingência para cada recurso de infra-estrutura tecnológica pode tornar-se inviável devido ao alto custo envolvido, pois a solução implicaria em duplicar e manter toda a infra-estrutura tecnológica em outro datacenter.

O desafio dos gerentes de TI é a priorização: conhecer quais processos de negócio devem ser restabelecidos primeiro após a ocorrência de um desastre pode representar a diferença entre a sobrevivência ou extinção do negócio.

No que diz respeito ao objetivo proposto, foi atingido e demonstrado por meio das análises quantitativas e qualitativas realizadas.

Quanto às contribuições dessa pesquisa, para a empresa, este estudo de caso propiciou as seguintes contribuições: disponibilizou modelo em planilha *excel* para a manutenção anual da Análise de Impacto no Negócio (BIA) nos próximos anos; forneceu informações consistentes para justificar o investimento em soluções de contingência e continuidade do negócio; propiciou a disseminação da cultura de gestão de riscos e gestão de continuidade de negócio para o grupo executivo; favoreceu a implementação de um comitê destinado a Gestão da Continuidade do Negócio (GCN); sugeriu novo modelo de levantamento de dados para o próximo ciclo do BIA. Para a academia este estudo pode agregar valor, pois demonstra que nem sempre se obtém os resultados esperados quando da aplicação de uma técnica de levantamento das informações e análise tal qual estabelecida na metodolgia de pesquisa. As expectativas de resultados previamente definidos na estratégia de análise associadas a um determinado construto/variável nem sempre são passíveis de realização tal qual efetivamente planejado se as premissas adotadas não se verificarem durante a aplicação prática.

As limitações da pesquisa estão relacionadas ao estudo único em uma empresa que não pode ser generalizado para outras. A metodologia utilizada para quantificar o prejuízo decorrente da indisponibilidade de TI deve ser ajustada para cada organização, pois varia em função do modelo de negócio e do grau de dependência que os processos de negócio tem das soluções de tecnologia da informação.

Outros trabalhos ainda podem complementar esse para aprofundar e aprimorar mais o tema deste estudo, tais como: repetir este estudo para os próximos anos na mesma organização para avaliar os resultados na linha do

tempo; realizar pesquisa similar em outras organizações com modelos de negócio e graus de dependência de TI variados; estabelecer um modelo matemático, que permita calcular o impacto no negócio devido à indisponibilidade de TI de forma assertiva e rápida em função de variáveis de fácil obtenção.

REFERÊNCIAS

CASTRO, Jacob Batista de. Gerente de segurança operacional da Caixa Econômica Federal. **Revista Informática Hoje:** mesa redonda – gestão de riscos é a palavra chave, p.21, Ago. 2006.

COBIT 4.0. IT Governance Institute, 2005.

D'ADDARIO, Jeferson. **Continuidade de negócio e governança corporativa**. Disponível em: <http://www.daryus.com.br/noticias.asp?act=1&id=65> Acesso em: 17 Set. 2006.

DOURADO JÚNIOR, Dorival. Diretor de operações e serviços da Serasa. **Revista Informática Hoje:** mesa redonda – gestão de riscos é a palavra chave, p.20, Ago. 2006.

DRJ - **Disaster Recovery Journal**. Disponível em: <http://www.drj.com> Acesso em 2 Out. 2007.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 4. ed. São Paulo: Atlas, 1995.

IBM. **Continuidade de negócios:** aprimorando a competitividade através da proteção de informações e da redução de riscos de negócios. Disponível em: <http://www.ibm.com/br/products/storage/solutions/business_continuity/index.phtml> Acesso em: 2 Out. 2007.

INFO-1. **Empresas não estão preparadas para disaster recovery**. Web Site da Info-Corporate. Disponível em: <http://info.abril.com.br/corporate/noticias/conteudo_49004.shtml> Acesso em: 25 Out. 2007.

INFO-2. **Investimento em disaster recovery é baixo**. Web Site da Info-Corporate publicado em 12/09/2007. Disponível em: <http://info.abril.com.br/corporate/noticias/noticia_250992.shtml> Acesso em: 25 Out. 2007.

IT GOVERNANCE INSTITUTE. **Board briefing on IT governance**. 2.ed., 2003.

MARINHO, Fernando. **Você precisa de uma BIA?** Disponível em: <http://www.fernandomarinho.com.br/html/business_impact.htm> Acesso em: 29 Set. 2006.

MCCLAIN, Mark. **Um plano de continuidade de negócio:** a sua ferramenta imprescindível para 2005. Disponível em: <http://www.sun.com/emrkt/boardroom/newsletter/portugal/0105leadingvision.html> Acesso em: 14 Set. 2006.

MINAYO, Maria Cecilia de Souza. **Pesquisa social:** teoria, método e criatividade. 9. ed. Petropolis:Vozes,1998.

NORTHROP, Grumman Organization. **The risk and impact on business**.

Disponível em: <http://recovery-disaster.info/disaster_recovery/disaster-recovery-business.htm> Acesso em: 15 Out. 2006.

REZENDE, D. A.; ABREU, A. F. **Tecnologia da informação aplicada a sistemas de informação empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. 4.ed. São Paulo: Atlas, 2006.

REZENDE, Denis Alcides. **Tecnologia da informação integrada à inteligência empresarial:** alinhamento estratégico e análise da prática nas organizações. São Paulo: Atlas, 2002.

REZENDE, Denis Alcides. **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.

SAP. **Assimilando os riscos da Tecnologia da Informação**. Disponível em: <http://www.sap.com/brazil/press/releases/press.epx?pressid=8042> Acesso em: 3 Dez. 2007.

SYMANTEC-1. **Gerenciamento de Riscos de TI - Evolução em 5 passos.** Disponível em: <http://www.virtue.com.br/blog/?p=28> Acesso em: 3 Dez. 2007.

SYMANTEC-2. **Gestão de Riscos - Conceitos e definições.** Disponível em: <http://www.virtue.com.br/blog/?p=28> Acesso em: 3 Dez. 2007.

TERZIAN, Françoise. Dossiê Business Continuity: saudável paranóia. **Revista Info Corporate**, p.50, Fev. 2006.

VERGARA, S. C. Tipos de pesquisa em administração. **Cadernos EBAP**, Rio de Janeiro: FGV, n. 52, Jun. 1990.

WALCH, Damian. **Business impact analysis**. Disponível em: <http://www.drj.com/articles/win04/1701-16.html> Acesso em 9 Nov. 2006.

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