UBIRAJARA FERREIRA DE AGUIAR JUNIOR

PLANO DE RECUPERAÇÃO DE DESASTRES: UMA PESQUISA-AÇÃO EM EMPRESA DO SETOR ENERGÉTICO

Trabalho de Graduação apresentado ao Conselho de Curso de Graduação em Engenharia Mecânica da Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Mecânica.

Orientador: Prof. Dr. Valério A. P. Salomon

Guaratinguetá
2012

Aguiar Junior, Ubirajara Ferreira de
A282p Plano de recuperação de desastres: uma pesquisa-ação em empresa do setor energético / Ubirajara Ferreira de Aguiar Junior – Guaratinguetá : [s.n], 2012.
42 f : il.
Bibliografia: f. 41-42

Trabalho de Graduação em Engenharia Mecânica – Universidade Estadual Paulista, Faculdade de Engenharia de Guaratinguetá, 2012.
Orientador: Prof. Dr. Valério A. P. Salomon

1. Tecnologia da informação I. Título

CDU 658

unesp UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
CAMPUS DE GUARATINGUETÁ

PLANO DE RECUPERAÇÃO DE DESASTRES: UMA PESQUISA-AÇÃO EM EMPRESA DO SETOR ENERGÉTICO

UBIRAJARA FERREIRA DE AGUIAR JUNIOR

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO REQUISITO PARA OBTENÇÃO DO DIPLOMA DE
"GRADUADO EM ENGENHARIA MECÂNICA"

APROVADO EM SUA FORMA FINAL PELO CONSELHO DE CURSO DE GRUADUAÇÃO EM ENGENHARIA MECÂNICA

Prof. Dr. ANTÔNIO WAGNER FORTI
Coordenador

BANCA EXAMINADORA:

Prof. Dr. VALÉRIO A. P. SALOMON
Orientador/UNESP-FEG

Prof. Dr. JOSÉ ROBERTO D. LUCHE
UNESP-FEG

Eng. LUCAS MATOS RODRIGUES ALVES
Membro Externo

Dezembro de 2012

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me dado forças, oportunidades e permitido chegar até aqui. Agradeço pela minha saúde, vida, família e amigos,

ao meu orientador, *Prof. Dr. Valério A. P. Salomon* que me orientou, auxiliou e incentivou durante o desenvolvimento deste trabalho,

aos meus pais *Ubirajara* e *Sandra* que me deram todo o apoio que sempre precisei e sempre me incentivaram com meus estudos,

à minha tia *Solange* que sempre me ajudou e me incentivou durante meu período de graduação,

à minha família que sempre me apoiou e torceu por mim,

aos integrantes da *República Ama-Zonas*, lugar onde colecionei amizades e vivi momentos que sempre deixarão saudade.

AGUIAR JR, U. F. **Plano de Recuperação de Desastres:** uma pesquisa-ação em empresa do setor energético. 2012. 42 p. Trabalho de Graduação (Graduação em Engenharia Mecânica) – Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, Guaratinguetá, 2012.

RESUMO

Este trabalho tem o intuito de demonstrar como elaborar um Plano de Recuperação de Desastres. Para atingir tal objetivo, uma adaptação do método PDCA foi empregada. Este plano visa reestabelecer a retomada das operações da TI dentro do menor tempo possível após algum incidente que cause a parada dos serviços ou atividades. Além de servir como um seguro para o funcionamento contínuo das atividades da empresa, é fato que a sua não existência apresenta riscos de prejuízo financeiro e de imagem para a empresa. Para exemplificar a funcionalidade e validade, o método foi aplicado em um departamento de TI de uma empresa do setor energético. Concluiu-se que o plano foi bem elaborado atendendo aos propósitos descritos nos objetivos deste trabalho e validando o projeto desenvolvido até então, tendo 85% de sucesso no geral dos sistemas testados.

PALAVRAS-CHAVE: Plano de continuidade de negócios. Plano de recuperação de desastres. Contingência. Tecnologia da informação.

AGUIAR JR, U. F. **Disaster Recovery Plan:** an action research in an energy company. 2012. 42 p. Final Paper. (Graduation in Mechanical Engineering) – Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, Guaratinguetá, 2012.

ABSTRACT

This work has the purpose of demonstrating how to build a Disaster Recovery Plan. In order to achieve such objective, an adaptation of the PDCA method was applied. This plan aims resuming the IT operations as fast as possible after some kind of incident which result the stop of the services or activities. Besides serving as insurance for the continued functioning of the company's activities, indeed your non-existence brings up risks of financial loss and threatens the company's image. As to illustrate the functionality and validity, the method was applied in an IT department of an energy company. It was concluded that the plan was well elaborated living up to the purposes described in the objective section of this work and validating the project developed so far, having a percentage of 85% of the overall success of the systems tested.

KEYWORDS: Business continuity plan. Disaster recovery plan. Contingency. Information technology.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BIA – Business Impact Analysis

DC – Data Center

MTD – Maximum Tolerable Downtime

PCN – Plano de Continuidade de Negócios

PRD – Plano de Recuperação de Desastres

RPO – Recovery Point Objective

RTO – Recovery Time Objective

TI – Tecnologia da Informação

UPS – Uninterruptible Power System

WRT – Work Recovery Time

SUMÁRIO

1 INTRODUÇÃO

1.1 Apresentação do Tema

Como conceito inicial, pode-se dizer que o plano de continuidade dos negócios identifica ameaças ou riscos aos negócios tanto interno quanto externo à organização, prevendo uma medida de contingência para cada caso se objetivando a retomada das operações normais do negócio dentro do menor tempo possível (SNEDAKER, 2007). Quando se trata de planos de contingência, temos dois planos que são comumente aplicados: o plano de continuidade de negócios (PCN) e o plano de recuperação de desastres (PRD). O PCN é o plano corporativo que leva em consideração a organização como um todo incluindo as pessoas após um incidente que resulte na parada dos negócios. O PRD é um segmento do PCN voltado para sistemas e tecnologias, ou seja, TI.

A elaboração de um PRD é um meio o qual traz uma estratégia de recuperação pronta a empresas num momento em que qualquer tipo de incidente gere uma interrupção dos negócios, sendo este incidente de caráter natural, proposital ou mesmo acidental. Agindo como diz a velha máxima “prevenir é melhor do que remediar” pode salvar empresas de prejuízos astronômicos em momentos de crise, até mesmo evitando uma possível falência.

Ao longo dos anos temos uma série de exemplos de desastres que impactaram de alguma forma centros corporativos. Em 1993, na ilha de Manhattan, as torres gêmeas do World Trade Center sofreram um ataque terrorista quando um caminhão cheio de explosivos colidiu com a base da torre norte com a intenção de fazê-la ceder e tombar atingindo a torre sul, matando assim milhares de pessoas. O atentado não obteve sucesso mas na ocasião, o prédio foi indisponibilizado. Como resultado desta interrupção de negócios, 150 das 350 empresas faliram (SNEDAKER, 2007). Oito anos depois, o mundo corporativo já estava mais conscientizado dos possíveis riscos causados por possíveis desastres. No famoso ataque terrorista de 11 de setembro de 2001 que levou as torres gêmeas abaixo, a maioria das empresas que possuíam suas sedes corporativas no World Trade Center voltaram com suas operações dentro de dias graças à preocupação de seus executivos em ter um PCN elaborado e ativo.

Vale comentar que este tipo de prática não inclui somente empresas internacionais, mas também as empresas nacionais estão cada vez mais preocupadas em possuir um plano de contingência. Como exemplo de casos nacionais, pode ser citado o incêndio que ocorreu no prédio da companhia de energia elétrica Eletrobras, em 26 de fevereiro de 2004, no Rio de

Janeiro. Este acidente acabou por afetar o prédio todo que continha o escritório administrativo da empresa e em reunião do comitê executivo, foi decidido que a empresa não voltaria ao prédio. Apesar das dificuldades, seu PCN foi colocado em prática e a empresa estava operando com operações parciais dentro de dias.

Mais especificamente, analisando empresas pelo seu departamento de TI, qualquer tipo de interrupção que cause uma perda de dados representa um grande impacto financeiro para a empresa, não só pelos dados perdidos, mas também pela recuperação do funcionamento usual dos sistemas. Logo, faz-se necessário ter um plano de contingência para este departamento que executa funções tão cruciais no universo corporativo.

Um estudo realizado por empresas, que não tinham um PRD, que passaram por algum tipo de incidente e que gerou uma grande perda de dados apontou que 43% delas interromperam suas operações e nunca voltaram aos negócios, 51% fecharam dentro de dois anos e 6% sobreviveram à longo prazo (CUMMINGS et al., 2005).

Foi pensando nesta área, que a cada dia se torna mais relevante para empresas, que este trabalho foi desenvolvido. Será apresentada aqui uma pesquisa-ação sobre a elaboração do PRD de uma empresa e será discutido ao longo do mesmo as métricas adotadas pela mesma e os critérios de adoção do projeto.

1.2 Objetivos e Justificativas

Este trabalho tem como objetivo geral apresentar como elaborar um PRD e são discutidas algumas variáveis que podem afetar o seu sucesso.

O foco deste trabalho está na informática corporativa, logo a maior preocupação que vem à tona é o DC (*Data Center*) da empresa. O DC pode ser considerado o coração da empresa por ser a central do processamento de dados. Todas as transações, operações e funcionalidades que a TI provém para o ambiente corporativo estão inevitavelmente atreladas ao DC. É de suma importância que este ambiente tenha o máximo possível de disponibilidade para que a empresa não sofra impactos críticos aos seus negócios. Em outras palavras: se o DC para, a empresa para.

Como escopo inicial do projeto, foi definido que o PRD da TI da empresa, que é o alvo desta pesquisa-ação, tem como objetivo criar um plano que estruture de maneira sistêmica ações para que a empresa possa retomar o processamento normal de suas aplicações críticas, dentro de um espaço de tempo adequado aos requisitos dos negócios. Outro objetivo

totalmente relevante foi por sua não existência constituir um grande risco de continuidade de negócios da companhia e consequentemente riscos de prejuízo financeiro e de imagem.

1.3 Método e Estrutura de Trabalho

Esta pesquisa-ação, termo que pode ser aplicado a projetos em que os práticos buscam efetuar transformações em suas próprias práticas (BROWN; DOWLING, 2001), utilizou como método o PDCA (*Plan*, *Check*, *Do and Act*), que visa além de servir como controle para a elaboração de um projeto, garantir também sua melhoria contínua. O ciclo se reinicia, corrigindo-se falhas encontradas.

Figura 1 – Representação do Ciclo PDCA

De acordo com Moen e Norman (2011), as quatro etapas que fazem parte deste método são:

- *Plan* (Planejar): estabelecer a missão, visão, objetivos, processos, procedimentos e metodologias necessários para o atender os resultados;
- *Do* (Executar): realizar e executar as atividades;
- *Check* (Verificar): avaliar os resultados comparando-os com os objetivos e consolidando as informações coletadas;
- *Act* (Agir): identifica falhas e levanta possíveis melhorias quanto ao trabalho já realizado tornado possível o seu aprimoramento.

Utilizando este método, foi feita uma adaptação trazendo as métricas de trabalho para a realidade de um PRD. Seus passos também foram adaptados e assim originou-se o modelo da Figura 2.

Figura 2 – Ciclo de vida do PCN/PRD

A primeira etapa denominada de análise de riscos define quais ameaças entrarão para o escopo do plano. A análise de impacto nos negócios ou, do inglês, *Business Impact Analysis* (BIA), define se baseando na análise de riscos quanto tempo a empresa pode ficar sem dada função ou sistema. Feito os estudos de BIA, escolhe-se uma estratégia para o seu PCN/PRD de acordo com a sua necessidade e seus recursos definidos. Em seguida, com o esqueleto de seu plano pronto, desenvolve-se o modelo do plano e é feita sua execução. O teste serve como base para se validar todo o trabalho desenvolvido até então e a manutenção do plano reinicia o ciclo de forma que o plano esteja sempre atualizado.

2 EMBASAMENTO TEÓRICO

2.1 Sobre a Tecnologia da Informação

Para Ramos (2007), a área de TI é o principal pilar de desenvolvimento das empresas e necessita cada vez mais um fortalecimento sendo o organismo complexo que a representa. A TI varia na sua atuação dentro da organização desde uma atividade de suporte administrativo até uma posição estratégica (HENDERSON & VENKATRAMAN, 1993). Tal posicionamento vem ganhando espaço ao longo dos anos não só pela rápida e dinâmica evolução que os meios de sistemas de informação vêm apresentando gerando ganhos para a TI em si, mas também pelos ganhos adjuntos das organizações como um todo.

Além de se posicionar possuindo este papel estratégico, a organização enxerga a TI como uma prestadora de serviços (WEILL; ROSS, 2005). Tal ponto de vista é reforçado pelo *grid* estratégico de McFarlan (1984) apresentado na Figura 3. Neste grid, a TI é apresentada com quatro possibilidades de definição estratégica dentro da empresa correlacionando os impactos presente e futuro dos sistemas para a continuidade da empresa:

- Suporte: tem pequena influência nas estratégias gerais da empresa;
- Fábrica: considera que as atuais aplicações de TI são atualmente de suma importância para a empresa, mas que futuramente não serão decisivas do ponto de vista estratégico;
- Transição: a TI passa a ser vista futuramente como uma área de fundamental importância futuramente;
- Estratégico: a TI tem uma enorme importância dentro da organização tanto atualmente quanto futuramente considerando que suas decisões manterão uma posição estratégica.

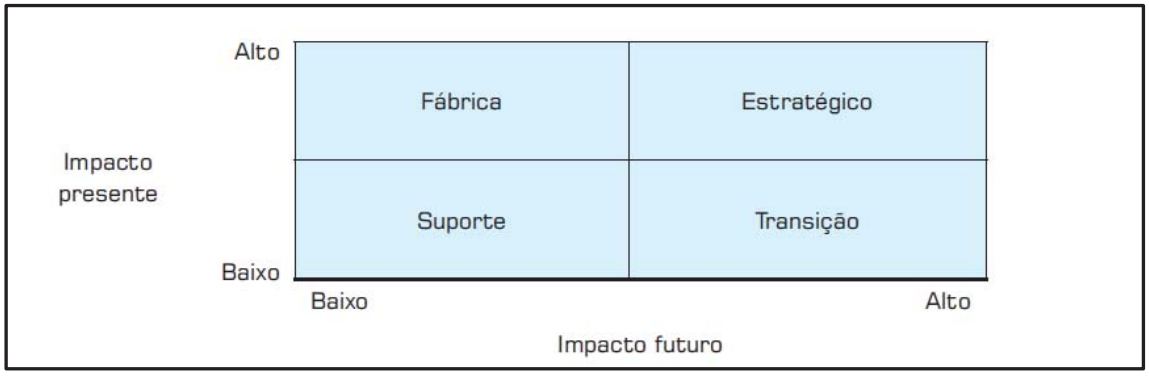


Figura 3 – Grid Estratégico (Adaptado de McFarlan, 1984)

Aproveitando esta matriz proposta, podemos classificar a TI da empresa descrita neste trabalho como um caráter estratégico tendo tanto um forte impacto no presente por desenvolver um PRD quanto no futuro por já estar preparada para eventualidades que exijam a ativação do plano.

Segundo Laurindo (2001), a TI evoluiu como função dentro da organização de suporte administrativo para um contexto estratégico, sendo que ela não só sustenta as atuais operações do negócio, mas também permite novas estratégias para a empresa. Mas apesar desta posição proeminente dentro da empresa, ainda existe dificuldade principalmente para as diretorias das empresas em se enxergar o real retorno do investimento realizado na TI. Para Henderson e Venkatraman (1993), esta dificuldade em se obter retornos consideráveis vindo de projetos oriundos da TI está na falta de alinhamento entre a TI e o negócio em si. Este processo de alinhamento entre os objetivos da própria empresa e seu departamento de TI deve ocorrer de forma lenta, gradual e contínua, buscando-se sempre aumentar o nível de maturidade obtido. É de conhecimento, ainda, que existe dificuldade em se avaliar o retorno dos investimentos que seus projetos trazem (MORAES; LAURINDO, 2003). Balarine (2002) indica que os investimentos aplicados à área de TI não devem ser feitos partindo de impulsos ou modismos, estes investimentos devem receber um tratamento adequado com realização de análises de custo-benefício e análise das possíveis consequências perante as decisões tomadas quanto à evolução da empresa a longo prazo.

Mais importante do que ter uma análise de investimentos, é saber empregar e gerenciar projetos que possam trazer os resultados esperados. As implantações e gerenciamentos de projetos em TI têm sido bastante complexos, o que tem refletido em operações mal sucedidas desperdiçando o investimento realizado (McAFEE, 2004; JEFFERY; LELIVELD, 2004). Serve ainda de embasamento para esta ideia o levantamento realizado por Maizlish e Handler (2005), que alega que 72% dos projetos de TI falham, ou seja, atrasam, superam o orçamento, não atendem os objetivos ou não são concluídos; os que são concluídos com sucesso, representando a fatia de 28%, também apresentam inconformidades sendo que destes, 45% ultrapassam o orçamento e 68% levam mais tempo que o planejado.

Quando o projeto da qual estamos avaliando se trata de um plano de continuidade de negócios, este deve ser muito bem estudado no que se tange à obtenção dos resultados esperados, ou seja, uma estratégia sólida de mitigação de risco, principalmente para TI. Estatísticas apontam que das empresas que sofreram uma grande perda de dados, sem possuir um plano de continuidade de negócios ou recuperação de desastres em prontidão, 43% interromperam os negócios e nunca retornaram, 51% retornaram mas fecharam as portas em

até dois anos e apenas 6% sobreviveram a longo termo (CUMMINGS et al., 2005). Outro estudo realizado pela Gartner, Inc., citado por Snedaker (2007), exaltou que 40% das empresas que sofreram algum tipo de desastre sem ter um plano de recuperação fecharam as portas em até cinco anos. Existe ainda uma análise feita pela *Contingency Planning and Management Magazine*, também citada por Snedaker (2007), concluiu que 40% das empresas que interrompem seus negócios por três dias, vão à falência em até 36 meses.

Logo, avaliando todos estes dados apresentados, pode surgir a questão: até que ponto vale-se a pena investir num plano de continuidade de negócios? Snedaker (2007) cita que tudo varia com tamanho da sua empresa e os recursos que ela dispõe. Não faria sentido uma empresa gastar 1 milhão de reais investindo em um plano de recuperação de desastres ou um plano mais robusto de continuidade de negócios para mitigar seus riscos quando sua receita anual gira em torno dos 1,25 milhões de reais. Por outro lado, pode fazer sentido a uma empresa que possua receita anual de 50 milhões de reais fazer tal investimento. Obviamente o custo gerado por uma eventual interrupção nos negócios deve ser correlacionado com o investimento empregado no seu plano de continuidade de negócios. A Figura 4 apresenta uma visão que explicita graficamente esta diferença.

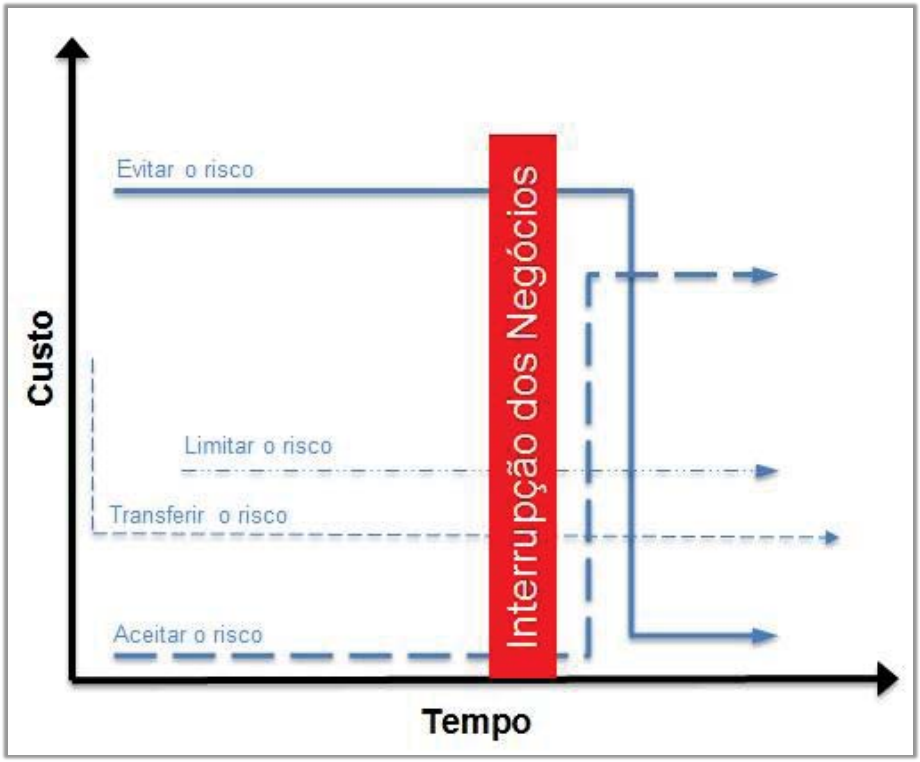


Figura 4 – Gráfico de riscos Custo x Tempo (SNEDAKER, 2007)

Dos conceitos expostos na Figura 4, temos: evitar o risco, aceitar o risco, limitar o risco e transferir o risco. Pode-se tratar os dois primeiros como opostos. Com um exemplo simples: supõe-se que uma seguradora de veículos queira evitar riscos e seu cliente estaciona seu carro embaixo de uma árvore. Existe o risco do tronco da mesma cair sobre o carro do cliente, gerando custo à seguradora. Para evitar este risco, a seguradora pode optar por cortar o tronco da árvore, evitando um custo futuro em caso de acidente. À curto prazo, esta é a estratégia mais cara.

Em contrapartida, tem-se a opção de aceitar o risco. Utilizando o exemplo anterior, a seguradora tem a noção de que pode cair um galho no carro do seu segurado, mas a probabilidade é bem pequena de ocorrer, logo ela pode aceitar o risco e esperar o mesmo acontecer arcando com as consequências financeiras. À longo prazo, esta é a estratégia mais cara.

Limitar o risco e transferir o risco são estratégias que apresentam custos intermediários. Quando a intenção está em se limitar o risco, empregam-se soluções que minimizam o impacto de determinada situação. Como exemplo, pode-se citar *backups* diários que são feitos numa empresa pela TI. Estes *backups* não evitam que o DC pare num eventual desastre, mas mitiga os esforços de recuperação que venham a ser empregados. As fitas de *backup* são armazenadas num local externo à empresa ou armazenadas por uma empresa terceirizada.

Transferir o risco é uma prática comum e consiste em transferir o prejuízo de um eventual desastre para uma empresa terceirizada. Usando o exemplo anterior da seguradora, supõe-se que o cliente queira transferir o risco de ter o seu carro danificado a um terceiro, neste caso, a seguradora. O cliente paga uma taxa de adesão inicial e tem um custo de manutenção mensal fixo para ter seu risco reduzido.

Assim pode-se concluir que as estratégias de mitigação de riscos, recuperação de desastres e contingência são acessíveis aos mais diversos ramos de empresas e aos mais diversos níveis de organização e, depende exclusivamente de cada empresa saber qual estratégia pode ser encaixada ao seu orçamento.

2.2 Aplicação do PDCA

Como comentado na Seção 1.3, o método de base utilizado foi o PDCA, que estrutura projetos visando uma melhoria contínua. Assim, busca-se um ganho de qualidade. O passo a passo para a estruturação do PRD está detalhado nesta seção, com informações adicionais relevantes a cada etapa do projeto.

Fica claro que o sequenciamento das etapas segue uma forma lógica e é adaptável aos mais variados casos em que pretende se aplicar o tema deste trabalho. É importante comentar que antes de seguir as etapas descritas abaixo, deve-se ter uma política clara sobre quais serão os propósitos e objetivos do plano que se está desenvolvendo, para servir de foco e limitar as milhares de possibilidades das quais um PRD pode abranger.

2.2.1 Análise de Riscos

Quando se trata de analisar riscos, podemos imaginar uma vasta gama de incidentes que podem ocorrer, mas acima de tudo, devemos saber filtrar quais são os riscos que possuem maior probabilidade de ocorrer e também avaliar o seu nível de impacto.

Esta primeira etapa de identificação de riscos é fundamental para o desenvolvimento de uma estratégia coerente e eficaz de continuidade de negócios. A partir do momento que se sabe o tipo de ameaça que se está lidando, pode-se elaborar um plano de contingência para tal ameaça de acordo com a análise de impacto e, assim, definindo uma estratégia. Pode-se dizer que a análise de risco envolve uma análise das probabilidades de ocorrer ameaças avaliadas à empresa e uma análise da vulnerabilidade da mesma quanto a tais ameaças.

Durante a etapa de análise de riscos, podem-se ter diferentes classificações sendo elas naturais ou ambientais, causadas pelo homem ou ainda de infraestrutura. Como exemplos de ameaças ambientais, são citados incêndios, enchentes, terremotos, tempestades e até mesmo pandemias.

Incêndios são a causa de maior recorrência. Foi avaliado que 44% das empresas que sofrem tipo de incidente significante com fogo no local de trabalho não se recuperam completamente por não possuírem um plano de contingência (SNEDAKER, 2007). A mitigação desta ameaça possui fácil acessibilidade. Podem ser instalados *sprinklers* e extintores devem ser dispostos nas paredes. Temos ainda o uso de gases como o FM200 que é inserido em um dispositivo de combate e prevenção de incêndio. Este gás interrompe a combustão afetando o oxigênio disponível. Têm-se, ainda, treinamentos especializados para parte dos funcionários os quais, em caso de necessidade, devem liderar os restantes dos funcionários por rotas de fugas pré-definidas. Simulações são recomendadas visando uma melhor preparação para uma situação real. Quanto ao início do incêndio, as causas podem ser diversas: pontas de cigarro, faíscas elétricas geradas por um dimensionamento elétrico ruim ou mesmo sobrecarga da rede em dias de tempestade.

Enchentes, terremotos e tempestades dependem muito da posição geográfica onde sua empresa se encontra. Enchentes e tempestades estão atreladas. Na cidade de São Paulo, por exemplo, é comum ocorrerem enchentes do período que vai de dezembro a março, em regiões específicas, devido ao alto índice pluviométrico desta época do ano (INMET). Locais altos oferecem menores riscos a este tipo de ameaça ou locais afastados de rios e córregos. Já terremotos oferecem baixo risco ao Brasil devido ao seu posicionamento geográfico em relação às placas tectônicas.

As ameaças humanas podem ser acidentais ou intencionais. Incêndio foi citado anteriormente e também pode ser causado por uma pessoa. Entre outras possibilidades, temos sabotagem, vandalismo, roubo de arquivos, ataques virtuais, terrorismo e até mesmo ataques químicos. A abordagem destas ameaças vai depender do escopo do plano em que se está visando estabelecer. Ameaças específicas e de baixíssima ocorrência podem ficar fora de fora do plano como terrorismo, que apesar de apresentar riscos, nem sempre pode ser prevenido.

Falhas causadas pela infraestrutura predial podem ser previstas e evitadas. Alguns exemplos simples podem ser citados como queda de energia elétrica, falhas em sistemas de segurança como dispositivos controladores de incêndio ou até mesmo falha na rede de comunicação. À parte destas categorias de ameaças citadas temos ainda greves que podem afetar direta ou indiretamente uma corporação. Supondo que haja greve do sindicato dos funcionários e os mesmo impeçam os funcionários de entrar no prédio, deve haver uma medida de contingência para este caso como *home office* (trabalho em casa). Também podem ser citadas ainda greves de transporte público que podem impossibilitar boa parte dos funcionários de chegar ao trabalho.

2.2.2 Análise de Impacto nos Negócios

O objetivo desta análise é identificar quais são as funções ou processos críticos para o funcionamento do negócio e analisar as consequências da interrupção dos mesmos. Classificar as funções como críticas e não-críticas é essencial para que se possa determinar o tempo de recuperação destas funções. Funções críticas devem ter um tempo de reestabelecimento de operações bem menor do que funções não-críticas, pois sua interrupção gera os maiores impactos à empresa.

Snedaker (2007) define alguns conceitos importantes utilizados na BIA:

- *Recovery Point Objective* (RPO) pode ser definido como a maior quantidade de tempo em que se pode perder dados devido a interrupção de sistemas críticos. É importante

definir com clareza este parâmetro de forma que se tenha tempo hábil para recuperar os dados atrasados durante o RPO num momento de contingência em que os sistemas serão reestabelecidos;

- *Recovery Time Objective* (RTO) pode ser definido como o maior período de tempo em que os sistemas e funções críticas podem ser recuperados. Inicia-se logo após um incidente que leva a empresa a entrar em contingência;
- *Work Recovery Time* (WRT) é o período seguinte ao RTO. Durante esta etapa, a empresa está funcionando com operações parciais. Os sistemas críticos já estão no ar e os demais sistemas e processos começam a ser reestabelecidos, assim como o *backlog* ou trabalho acumulado;
- *Maximum Tolerable Downtime* (MTD) é constituído pela soma do RTO e do WRT, ou seja, é o máximo de tempo em que a empresa pode ficar sem sua funcionalidade 100% normal.

Para ilustrar melhor os conceitos acima definidos, uma simulação do funcionamento de uma empresa é apresentada na Figura 5.

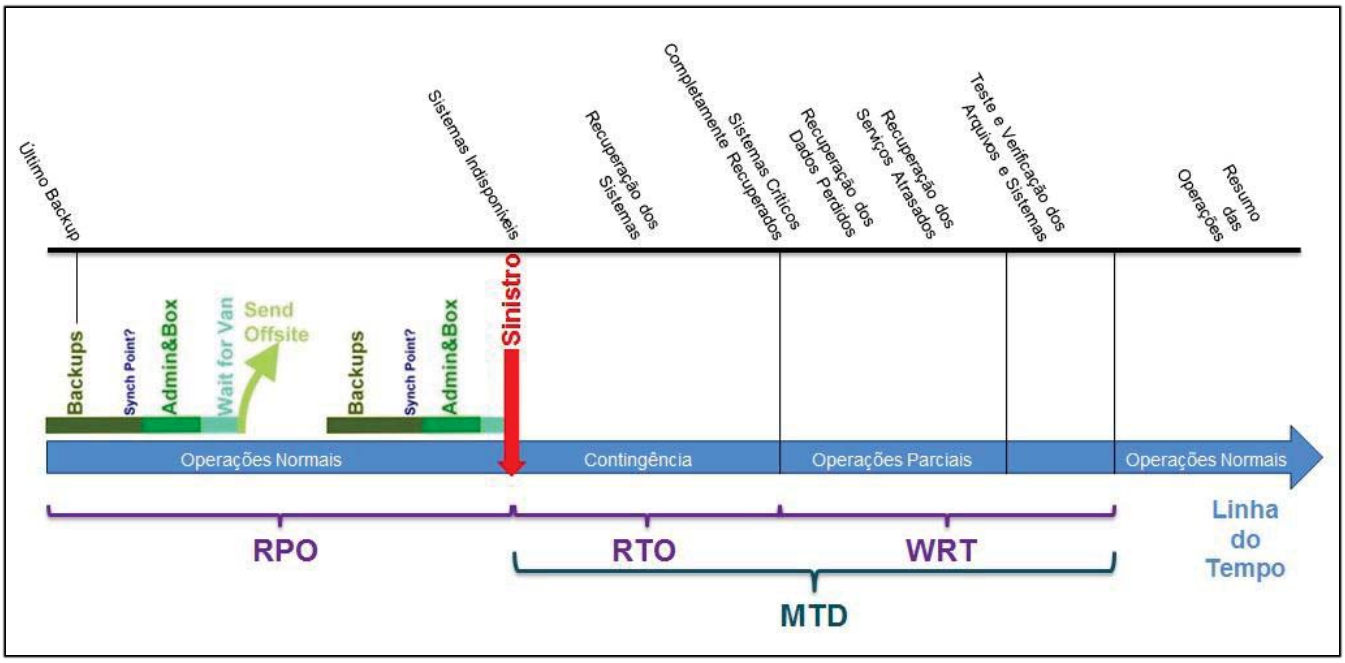


Figura 5 – Exemplo de emprego das definições da análise de impacto nos negócios

Nesta simulação, supõe-se que uma empresa mantenha o seu DC, e como opção de segurança de dados, faça cópias de *backups* diários em fitas. O trâmite comum diário seria

executar os *backups*; marcar um ponto de sincronização dos dados, ou seja, retira uma imagem do atual estado do sistema (semelhante a quando se cria um ponto de restauração em sistema operacional *Windows*); guardar as fitas em malas de segurança; aguardar pela van para transportar as fitas para um *offsite*, sendo este próprio ou terceirizado.

Imaginando a pior hipótese possível, supõe-se que ocorra um sinistro no prédio da empresa que impossibilite o funcionamento dos negócios no momento imediatamente antes da van deixar o local com as fitas contendo os *backups* diários. Dado que os *backups* são diários, ou seja, a cada 24 horas é feito um novo *backup*, como margem de segurança, pode-se dizer que o RPO seja de 48 horas. Como pode ser notado no exemplo acima, o sinistro ocorreu no pior momento possível trazendo para a empresa uma perda de dados próxima às 48 horas do RPO.

Com a indisponibilidade dos negócios, é declarado o estado de contingência e o PRD entra em ação. Esforços são feitos pelo time de contingência e seus colaboradores de forma que os sistemas críticos sejam recuperados, sendo que estes tem prioridade por serem fundamentais para que o negócio volte ao seu funcionamento, pelo menos parcial. Recuperados tais sistemas, temos pela Figura 5, o RTO, que compreende o espaço de tempo entre o sinistro e a recuperação dos sistemas críticos. Com os negócios funcionando com operações parciais, iniciam-se os esforços para recuperar os demais sistemas, que possuem RTO maior do que os sistemas críticos. Recuperados todos os sistemas, é feita a recuperação dos dados perdidos e *backlog*. Para finalizar e validar o funcionamento normal das operações é feito um teste e uma consequente verificação dos sistemas. O período de tempo compreendido entre a recuperação dos sistemas críticos e o funcionamento normal dos negócios corresponde ao WRT. Com o teste e verificação validados, ocorre o resumo normal das operações.

Tendo pronta a análise de impacto dos sistemas e funções críticas do negócio, deve ser gerado um relatório expondo tal análise de forma que se possa passar à próxima etapa em que se seleciona a estratégia a ser empregada no seu PCN.

2.2.3 Seleção da Estratégia

Quando se pensa em estratégias de mitigação de risco de TI, temos alguns sistemas que conhecidos que são amplamente usados. Para o caso de desastre que leve à perda do prédio, por exemplo, temos a opção de utilizar *sites* alternativos, ou seja, um local específico que conterá uma estrutura que será acionada em caso de desastre, como um DC de recuperação de

dados. Os dados que serão armazenados neste *site* alternativo podem ou não ser síncronos com o DC principal. Quanto menor o tempo de atraso ou de diferença do tempo de dados entre os dois DCs, mais caro será sua solução e as tecnologias empregadas.

O *site* alternativo mais caro é o completamente espelhado que possui replicação síncrona de dados. Costuma ser utilizada por empresas que necessitam ter uma alta disponibilidade de serviços, como bancos. Quando usados de forma redundante, desligando o DC principal, o DC *backup* é automaticamente ativado e toma o lugar do principal.

Temos ainda as opções de *Hot Sites, Warm Sites* e *Cold Sites*. Snedaker (2007) alega que *Hot Sites* são espaços alugados com fornecedores geralmente especializados que manterão uma cópia da configuração do DC principal de seus clientes. Dados são replicados para os mesmos de maneira assíncrona mas com um tempo de atraso muito curto, chegando a menos de 2 horas. *Warm Sites* são espaços menos preparados que *Hot Sites* e são recomendados para que se recuperem funções ou sistemas menos críticos. Seu tempo de recuperação dos sistemas é maior devido à menor estruturação do ambiente. Não necessariamente é mantido por um terceiro. Como exemplo, cita-se uma sala que contém um servidor de *backup* de dados críticos. Em caso de acidente, este é acionado e os dados críticos que se tem *backup* serão reestabelecidos em questão de horas. *Cold Sites* é o tipo de solução mais barata. São utilizados quando não existe uma urgência em retomar determinados serviços ou funções pois quando ocorre um incidente, este tipo de *site* costuma estar *off-line* e esforços são feitos para a preparação do local e retomada dos serviços. Este tipo de solução costuma levar mais de um dia para recuperar todos os sistemas.

Além de opções de *sites*, temos as opções de replicação dos sistemas de discos. Dentre as mais utilizadas podemos citar os sistemas RAID (*Redundant Arrays of Inexpensive Disks*). A Figura 6 apresenta uma ilustração deste sistema que possui algumas variações e que basicamente funciona como uma replicação do disco original para um ou mais discos podendo ou não estarem alocados na mesma máquina (SNEDAKER, 2007).

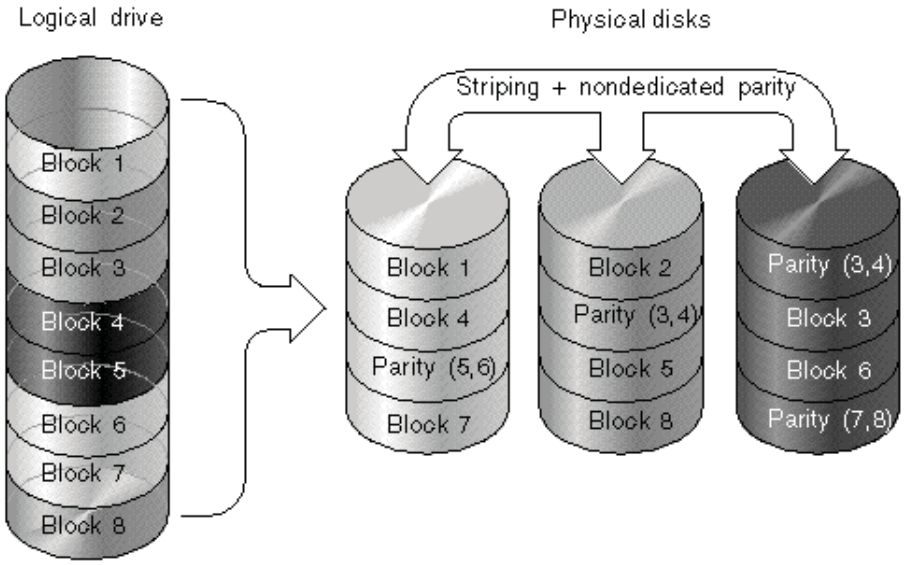


Figura 6 – Exemplo de Composição RAID5 (Fonte: DRIVE SOLUTIONS)

Um novo conceito que vem tomando mais força a cada dia é o *clustering*, que consiste em utilizar a "nuvem" de computadores, ou seja, servidores virtuais (SNEDAKER, 2007). Têm-se um servidor físico e este físico dá acesso a duas réplicas virtuais redundantes entre si. Quando o usuário visa acessar estes servidores, cai diretamente em um dos servidores virtuais. Este sistema oferece uma disponibilidade maior dos sistemas (Figura 7). Outra alternativa bastante utilizada e citada na Seção 2.2.2 é o *backup* em fita. Empresas costumam fazer *backups* de seus servidores diários, semanal e mensalmente. Estes *backups* armazenam uma imagem do estado do servidor em determinada data e funcionam como ponto de restauração em caso de necessidade. Vamos supor que um usuário tenha excluído uma pasta importante, uma restauração pode ser feita a partir dos dados das fitas de *backup*. Estas fitas não devem ser armazenadas no mesmo prédio do DC devido ao risco de perdê-las por qualquer incidente que cause danos ao DC e, que possivelmente também destrua os dados copiados.

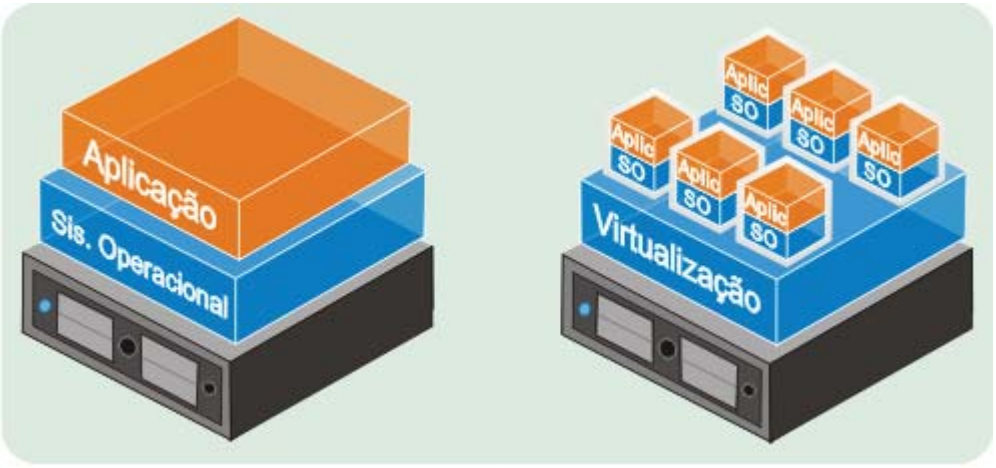


Figura 7 – Representação de virtualização de servidores (Fonte: ITS)

Dadas algumas opções de estratégia e solução de backup, é importante ter em mente que cada empresa deve escolher a solução que apresenta o melhor custo-benefício compatível com as suas necessidades.

2.2.4 Desenvolvimento e Execução do Plano

Como todo projeto e procedimento, o PRD deverá ser documentado. Existem métricas a serem seguidas para a elaboração deste plano que conterá o passo a passo do momento da contingência. Deve haver uma definição bem clara sobre quem são os responsáveis por tomar decisões durante a fase de contingência. Este é um dos propósitos do plano de contingência.

Antes que em qualquer tipo de emergência se resolva acionar o PRD, deve-se ter uma definição clara do momento em que estes planos devem ser acionados. Para tais propósitos que são criadas algumas equipes com o intuito de não só coordenar o momento da contingência, mas também definir se há a necessidade de ativar o plano.

Algumas equipes com atividades específicas devem ser formadas para que a recuperação do desastre ocorra de forma organizada e menos impactante possível. Uma Comitê de Gerenciamento de Crises, obrigatoriamente, deverá ser formada tendo a responsabilidade de determinar se empresa entra ou não em contingência dado o nível de um determinado incidente ocorrido. Se um incêndio se inicia em uma sala no prédio da empresa, deve-se avaliar se este incêndio para ou não o funcionamento dos negócios. O DC é o ambiente mais crítico para o departamento de TI, logo, se um incêndio se inicia e não pode ser contido rapidamente, a empresa deve necessariamente entrar em contingência pois o funcionamento da empresa inteira está prejudicado neste caso.

Além da Comitê de Gerenciamento de Crises, existem equipes opcionais que poderão ser definidas, tornando a organização dos esforços de recuperação mais eficazes. Poderão ser definidas: a Equipe de Notificação, que será responsável pela comunicação à todos os funcionários sobre o estado de contingência, assim como contatar as famílias de possíveis envolvidos em acidentes; a Equipe de Resposta a Emergências, que deverá atuar em conjunto com a Comitê de Gerenciamento de Crises, mas com a função de entrar em contato com as principais autoridades para que se tomem as providências necessárias quanto ao incidente ocorrido; a Equipe de Mídia ou Imprensa, que terá como principal função divulgar informações aos meios de comunicação sendo que todo e qualquer contato com meios externos deverá ser feito exclusivamente por esta equipe. Outros times específicos poderão ser definidos ficando a critério da organização decidir qual configuração de times tornará o fluxo de trabalho mais eficaz. Estas equipes específicas são válidas quando se visa criar um PCN. Quando se trata de um PRD, somente a Comitê de Gerenciamento de Crises é essencial.

Dependendo do tamanho da organização ou empresa que se está implantando o PRD ou PCN, pode ser mais prático dividir o seu plano em níveis de acordo com a criticidade do incidente ocorrido. Pode-se determinar níveis como criticidade baixa média ou alta, por exemplo. Critérios devem ser claramente estabelecidos como gatilhos para cada criticidade que representa um plano, delineando uma forma diferente de agir em cada caso. Cabe à Comitê de Gerenciamento de Crises determinar em qual plano o incidente se adequa.

2.2.5 Testes e Manutenção do Plano

Completada a etapa de desenvolvimento do plano de continuidade de negócios, o próximo passo é validá-lo. A melhor forma de fazer a validação de um plano é testando-o mesmo de forma que se encontrem falhas ou *gaps* nos procedimentos de atuação, ou mesmo algum passo que necessite uma revisão por não demonstrar ser a melhor opção.

É comum tanto em prédios corporativos quanto em fábricas que algumas simulações sejam feitas visando mitigar possíveis riscos como simulação de evacuação do prédio em caso de incêndios ou qualquer outro acidente relevante.

Para que estes testes ocorram de forma efetiva, parte dos funcionários deverão fazer treinamentos. Estes treinamentos deverão conter escopo, metodologia e objetivos bem definidos. De nada adianta um funcionário saber o que fazer num momento de emergência mas não saber como fazê-lo, como por exemplo, o uso de extintores de incêndio que, se não forem manuseados da forma correta, podem ser uma ameaça ao usuário.

Cada equipe mencionada na seção 2.2.4 pode ter treinamentos em conjuntos e/ou treinamentos específicos. Da mesma forma que o seu plano necessitará de uma revisão periodicamente, os treinamentos realizados também devem ser revisados buscando possíveis melhorias ou necessidades apontadas em treinamentos anteriores. Além de serem revisados, os treinamentos devem ser refeitos periodicamente para que todos os funcionários estejam sempre atualizados.

Como dito anteriormente, os treinamentos servem com uma base para se obter melhores resultados durante os testes propriamente ditos. O responsável pelo desenvolvimento e execução dos testes deve ter em mente que testar um plano de recuperação de desastres traz um determinado nível de indisponibilidade dos serviços, com um custo relativo, mas que quanto mais completo for o teste, melhor será a precisão dos resultados. Existem quatro tipos de testes convencionalmente conhecidos. Segundo Snedaker (2007):

- Procedimento passo a passo (*Paper Walkthrough)* é o teste que traz o menor impacto ao funcionamento dos negócios da empresa. Este procedimento deve ter um objetivo definido com causas teoricamente simples, sempre objetivando tratar um risco específico. Em geral, escolhe-se o maior risco com maior probabilidade de acontecer e monta-se um esquema de teste para por em prática o seu plano de contingência. Uma simulação de fogo no prédio é um exemplo de procedimento passo a passo, pois é uma situação que tem uma probabilidade razoavelmente alta de ocorrer e que traz impactos consideráveis ao funcionamento da corporação;
- Exercícios funcionais são utilizados para se testar uma parte específica do plano. Funciona muito bem junto com o procedimento passo a passo. Recomenda-se definir um cenário e as equipes deverão entrar em ação de acordo com as suas respectivas responsabilidades que constam no plano. Este teste pode levar de duas a três horas e tem como objetivo por em prática as responsabilidades de cada time e fazê-los trabalhar em equipe;
- Exercícios de campo são mais realistas que os exercícios funcionais e também trazem um custo muito maior à empresa por trabalhar com um tempo de parada maior. Neste teste, autoridades de emergência também são envolvidas trazendo mais realismo ao cenário adotado. *Gaps* e falhas que não foram percebidas no plano se tornam mais facilmente identificáveis neste tipo de simulação.
- Interrupção total é o teste que traz mais impacto à empresa por interromper, de fato, funções críticas do funcionamento do negócio. Pode ser efetivo para testar o

funcionamento de *sites* de recuperação, efetuando a "virada" do funcionamento de um DC do site primário para o secundário.

Durante a execução destes testes, recomenda-se que seja disponibilizada uma cópia do teste para todos os envolvidos. Os membros das equipes devem ter completa ciência das suas responsabilidades para que os resultados sejam os mais precisos possíveis. Trabalhar com listas de checagem pode ser uma ótima forma de avaliar o andamento do teste. Ao finalizar o mesmo, um relatório deve ser feito apontando o procedimento, os objetivos e os resultados, assim como as lições aprendidas e possíveis problemas encontrados.

Mais difícil do que se elaborar um PRD/PCN é mantê-lo atualizado. Principalmente quando a TI é envolvida, qualquer mudança pode se tornar impactante no plano previamente desenvolvido fazendo com que este se torne inválido. Sistemas operacionais e *softwares* são atualizados com frequência, *hardwares* são alterados com versões mais modernas, funcionários especialistas em determinadas ferramentas podem sair da empresa ou serem movidos de área. Todas estas situações podem afetar a validade do plano, assim, fazem-se necessárias revisões periódicas do plano baseadas numa base de todas as mudanças que possam ocorrer no mesmo.

A maneira mais simples de manter um PRD sempre atualizado é incorporando regras à formalização de novos componentes que são inseridos na atual estrutura da empresa. Sugere-se que membros das equipes relacionadas ao PRD façam parte do Comitê de Mudanças da organização de forma que seja possível identificar possíveis mudanças efetuadas nos itens de configuração da TI (*hardwares, softwares,* conectividades etc.), impactantes não só ao ambiente produtivo mas também ao plano de contingência. Mudanças que afetem um possível site de recuperação devem ser tratadas com atenção para que se tenha compatibilidade dos sistemas com *sites* principal e secundário.

3 PESQUISA-AÇÃO

3.1 Descrição do Objeto de Estudo

Uma empresa brasileira foi escolhida para que este estudo de caso seja desenvolvido e a chamaremos neste trabalho de Corporação. A Corporação é um dos maiores grupos empresariais brasileiros, formada pelas seguintes empresas: a Empresa A, que atua na distribuição de gás GLP; a Empresa B, que atua na distribuição de combustível; a Empresa C, que atua na indústria química e a Empresa D, que atua no ramo de armazenamento de granéis líquidos. Possui 75 anos de história e cerca de 9 mil funcionários.

Falando individualmente das empresas, a Empresa A foi a empresa que originou o grupo em 1937. Tem forte atuação no mercado sendo a maior distribuidora de GLP no Brasil com 23% de participação do mercado brasileiro em 2010. Distribuem GLP a cerca de 11 milhões de brasileiros utilizando frota própria. A Empresa B é a segunda maior distribuidora de combustíveis do Brasil tendo 21% de participação no mercado brasileiro em 2011 e uma rede de postos de 6,1 mil revendedores. A Empresa C é uma empresa química sendo uma das maiores produtoras de óxido de eteno na América Latina, assim como seus produtos derivados. Possui unidades industriais no Brasil, no México, e na Venezuela, nos Estados Unidos e no Uruguai e escritórios comerciais na Argentina, na China, na Bélgica e nos Estados Unidos. Quando se trata de armazenagem de granéis líquidos, a Empresa D lidera o mercado neste quesito. Ao final de 2011 possuía uma capacidade de armazenagem de 664 mil metros cúbicos.

3.2 Situação Atual e Descrição do Problema

A matriz da Corporação está situada na cidade de São Paulo. Nela estão reunidas as direções administrativas de todos os negócios do grupo, incluindo a área de TI. Apesar do grupo conter quatro negócios principais (ou empresas) que funcionam de forma independente, o departamento de Tecnologia da Informação da Corporação funciona para todo o grupo tomando as decisões relevantes, sendo que funções minoritárias que não impactam diretamente nos negócios da Corporação são tomadas pelas equipes de TI de cada negócio.

O departamento de TI da Corporação está subdividido em cinco áreas: Sistemas Corporativos e Desenvolvimento, Centro de Competência Oracle, Infraestrutura, Service Desk e Governança. Totalizando 240 profissionais.

A área de Sistemas Corporativos é responsável pela administração, manutenção e evolução de todos os sistemas e interfaces com os negócios, bem como pelo desenvolvimento (programação) dos sistemas corporativos e satélites da Corporação.

A área de Centro de Competência Oracle exerce a mesma responsabilidade da área de sistemas, porém focada no ERP Oracle EBS.

A área de Infraestrutura se subdivide ainda pelas equipes de Arquitetura, Produção, Segurança da Informação, Suporte e Telecomunicações sendo responsável por manter, suportar, monitorar todas as questões relacionadas à infra. A equipe de Arquitetura é responsável pelos ambientes de banco de dados e ERPs (*Enterprise Resource Planning*) e Sistemas Satélites que são sistemas que suportam os ERPs. A equipe de Produção é responsável pelo acesso e monitoração do DC, por *backups* e *restores* (recuperação) de dados, pelos processos automatizados e pela monitoração dos *links* de comunicação de todas as filiais com a matriz. A equipe de Segurança da Informação é responsável pela elaboração de políticas, pelo correio eletrônico, pelas questões de segurança de rede e acesso à internet. A equipe de Suporte é responsável pelos servidores, *storages* (armazenamento), sistemas operacionais e virtualização de servidores. A equipe de Telecomunicações é responsável por telefonia, pelo tráfego de dados, voz, pela conectividade e pela topologia das conexões.

Toda essa gama de aplicações e sistemas são armazenados no DC. Do ponto de vista da TI, este é o coração da empresa pois o DC deve funcionar 24 horas por dia. A todo o momento ocorre envio e recebimentos de dados, aplicações são acessadas, faturamentos e baixas bancárias são realizadas, contas são pagas entre outras atividades. Logo é de suma importância que este Data Center possua o máximo de disponibilidade possível.

A área de Service Desk é responsável pelo processo de suporte a todos os usuários da Corporação e encaminhamento de soluções onde é necessária atuação das demais equipes da TI.

A área de Governança é responsável por fornecer um modelo (*framework*) de estrutura organizacional de TI, processos, papéis e responsabilidades, que garanta o alinhamento aos negócios, a maximização dos benefícios, uso adequado dos recursos, gerenciamento apropriado dos riscos e das finanças da TI.

O DC da Corporação se encontra no primeiro andar do edifício corporativo e possui parâmetros de segurança que consistem de uma porta corta-fogo em caso de incêndio, sendo esta feita de vidro, e leitor biométrico e de crachá para que o acesso seja validado. É necessário, também, atravessar uma câmara separada por duas portas, sendo que a segunda só se abre após o fechamento da primeira.

Dentro do DC, a preocupação com a circulação de ar ideal é sempre constante. Os *racks* com servidores ficam enfileirados formando corredores, assim, em corredores intercalados, as máquinas ficam viradas uma de frente para as outras e uma de costas para as outras. Este *layout* gera uma diferença de temperatura no fluxo de ar fazendo com que caracterizem corredores quentes e frios entre as fileiras dos *racks* (Figura 8). Visando uma melhor circulação de ar e um melhor desempenho das máquinas, os corredores frios foram enclausurados. O piso de todo o ambiente é de fórmica, sendo elevado por 27 cm para que ocorra circulação de ar no subsolo por onde passa o cabeamento. Nos corredores frios, o teto é feito de gesso e nos corredores quentes foram instaladas placas perfuradas que aspiram o ar quente fazendo o mesmo passar por uma evaporadora seguido de uma tubulação por onde ele é insuflado pelo piso elevado para os corredores frios, novamente.

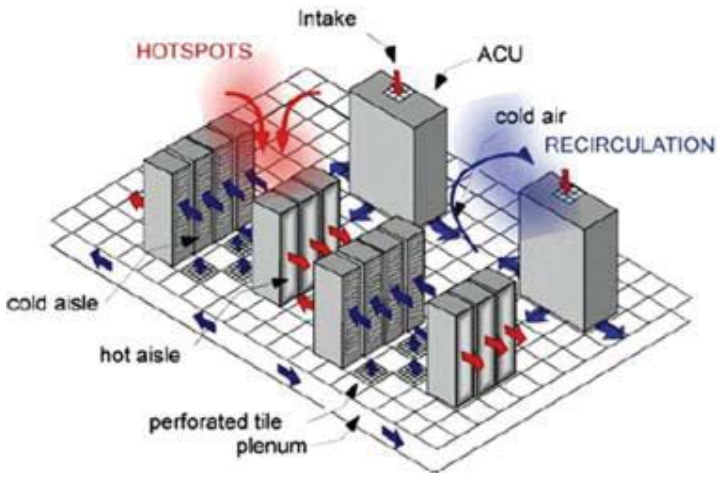


Figura 8 – Layout típico de DC (Fonte: López e Hamann, 2011)

A climatização do ar é feita por cinco equipamentos de ar condicionado de capacidade de 15 TR cada, operando em configuração (N+1), ou seja, sempre há um equipamento em *stand by* para o caso de algum equipamento que esteja ativo venha a falhar. Estes equipamentos possuem alimentação elétrica proveniente de três quadros de alimentação. Os *racks* possuem alimentação proveniente de quatro quadros de energia elétrica, todos com fontes redundantes.

O sistema de combate a incêndio é composto por um sistema de detecção de fumaça de alta sensibilidade e um sistema de combate com gás extintor FE-25.

Na atual configuração da estratégia de mitigação de risco da empresa, a única forma de proteção e recuperação dos dados é por meio de *backups* que são realizados diariamente, semanalmente e mensalmente. Assim, se algum acidente catastrófico acontecer com o DC, o

operação dos negócios estará comprometido podendo trazer grandes riscos à empresa. Para solucionar tal adversidade, um plano de recuperação de desastres e continuidade foi planejado e desenvolvido e seu detalhamento é comentado a seguir.

3.3 Solução do Problema

O plano de recuperação de desastres da Corporação foi desenvolvido com o intuito de criar um plano que estruture de maneira sistêmica ações para que a empresa possa retomar o processamento normal de suas aplicações críticas, dentro de um espaço de tempo adequado aos requisitos dos negócios. Outro motivador foi por sua não existência constituir um grande risco de continuidade de negócios da companhia e consequentemente riscos de prejuízos financeiros e de imagem.

Diante das premissas do projeto estavam: definir a estratégia de *site backup* para o PRD, reduzir os riscos associados à infraestrutura, simplificar a arquitetura e esforço de recuperação, definir as equipes para atuação em momentos de crise e aprimorar processos que suportem a recuperação dos ambientes. Consta ainda na política que o PRD será acionado em caso de indisponibilidade total ou parcial do DC principal. O acionamento do mesmo caberá ao Comitê de Gerenciamento de Crises e a estratégia de recuperação das aplicações será efetuada de forma gradativa sendo da mais crítica para a menos crítica, sendo que o funcionamento do site *backup* terá o mesmo desempenho do DC principal.

A análise de risco deste projeto apurou alguns possíveis cenários em que o plano contemplaria uma estratégia de mitigação. A partir desta configuração de estratégia de mitigação de risco, foram definidos três possíveis cenários para o primeiro teste inicial do plano visando-se obter uma validação do mesmo. Dos cenários colocados em tópico, foram abordadas as seguintes possibilidades: sem DC e com prédio, com DC e sem prédio e sem DC e sem prédio.

A primeira medida definida como estratégia de continuidade de negócios para os casos sem DC, foi a contratação de uma empresa terceirizada especializada em DCs. Esta empresa aluga seu espaço para seus clientes de forma que eles possam construir seus DCs *backup* em um local seguro fora do prédio da própria empresa. Esta estratégia adotada é caracterizada como uma estrutura *Hot Site*.

A infraestrutura da empresa conta com 12 MW de energia disponível, duas linhas de alimentação independentes e redundantes de 34,5 kV em sua configuração final e distribuição redundante dos painéis elétricos. Possui sistemas UPS's (*Uninterruptible Power Supply*) de

última geração e alta eficiência. Possui geradores com capacidade total de 14 MW com autonomia de 200 horas sem abastecimento. Os sistemas de refrigeração são redundantes sendo os *racks* de servidores dispostos em corredores quentes e frios totalmente confinados, garantindo uma melhor eficiência. A instalação tem capacidade para disponibilizar 1920 TR. A área construída destinada a DCs corresponde a 3200 m² com um piso elevado de 1 metro de altura e pode suportar até 40 mil servidores.

Para o DC da Corporação, especificamente, foi utilizada uma área de 90 m² com sistema de climatização utilizando 12 máquinas em regime 2N, ou seja, 12 ligadas e 12 em *standby* como *backup*. A alimentação de energia elétrica é feita através de 26 pontos de energia que funcionam em regime N+1, disponibilizando 90 kVA. Destes, são utilizados 83,17 kVA (92,4% do total).

Dentro da TI da Corporação, foi feito um levantamento sobre quantas pessoas seriam necessárias em um momento de contingência para que se fosse possível ativar o *site backup* e que não se tivesse a infraestrutura predial. Estimou-se que 34 pessoas seriam necessárias, sendo destas: 12 da equipe de Arquitetura, 6 da equipe de Produção, 8 da equipe de Suporte, 4 da equipe de Telecomunicações, 4 da equipe de Segurança da Informação. Tendo fechado este número de funcionários necessários, foi avaliada a infraestrutura e capacidade da empresa terceirizada para abrigar e fornecer estações ou espaço de trabalho para todos. Desta avaliação foi apurado que a empresa terceirizada dispunha de três salas de 12 m² (6 x 2 m²) com quatro baias cada, contendo um ponto de rede cada baia. Cada sala possuía uma linha telefônica VOIP e dois pontos de rede. Além dos pontos de rede, o acesso à internet era feito via *wi-fi*, disponibilizado pela própria empresa. Se necessário, a empresa disponibilizaria ainda mais três salas de reuniões para o trabalho da equipe de contingência. Todos os *hardwares* necessários para que os funcionários possam trabalhar são de responsabilidade da Corporação. Não é possível deixar estações pré-montadas nas salas disponibilizadas pois esta empresa terceirizada lida também com outros clientes, não só a Corporação, assim, outros clientes podem necessitar destas salas que são disponibilizadas.

Como pode ser notado, a infraestrutura da empresa terceirizada não supre a demanda de estações de trabalho para funcionários que a Corporação necessitava. Portanto, os cenários avaliados que consideravam a perda do prédio matriz da Corporação foram excluídos da pauta de testes, colocando como principal premissa somente a virada de funcionamento das aplicações críticas do DC principal para o DC *backup*.

A BIA foi realizada com o auxílio de uma consultoria. Esta análise utilizou as entrevistas como principal método de obtenção das informações relevantes para identificar os

sistemas críticos das empresas. Foram realizadas cerca de 100 entrevistas com as áreas de negócio de todas as empresas da Corporação. Nas entrevistas foi utilizado um questionário para levantamento de informações com os negócios. O material resultante foi consolidado passando por uma validação do resultado pela TI da corporação e dos negócios. Dessa forma foi possível identificar os principais processos críticos dos negócios e os impactos referentes a todas as interdependências que estes processos críticos estão atrelados.

Como resultado da BIA, foi apurado que a Corporação possui 243 sistemas sendo que destes, 93 são de alta criticidade, 75 são de média criticidade e 75 são de baixa criticidade. A Tabela 1 traz mais detalhes sobre a divisão dos sistemas.

Tabela 1 – Divisão Detalhada dos Sistemas por Negócio

Unidade de Negócio	Sistemas Criticidade Alta	Sistemas Criticidade Média	Sistemas Criticidade Baixa
Corporação	11	8	11
Informática Corporativa	45	8	14
Empresa A	13	31	36
Empresa B	9	5	2
Empresa C	6	9	4
Empresa D	9	14	8
Total de Processos	**93**	**75**	**75**

Como pode ser notado na Tabela 1, a Informática Corporativa foi colocada no mesmo patamar das empresas por conter sistemas e processos que funcionam para a própria TI independente das outras áreas da empresa.

É de suma importância comentar que as diferenças de criticidade dos sistemas representam RTOs diferentes. A tabela 2 exemplifica o critério de RTO adotado pelo Comitê de Gerenciamento do Projeto.

Tabela 2 – Definições dos tempos de recuperação (RTO)

Criticidade Alta	Criticidade Média	Criticidade Baixa
0-4h	4-10h	>10h

Ainda dentro do tópico do primeiro cenário, foram avaliadas algumas possiblidades de cenários mais específicos que causassem a perda do DC principal ou da sua funcionalidade normal impactando nos negócios mas que não comprometessem a infraestrutura predial. Dentre eles foram levantadas as possibilidades de falha:

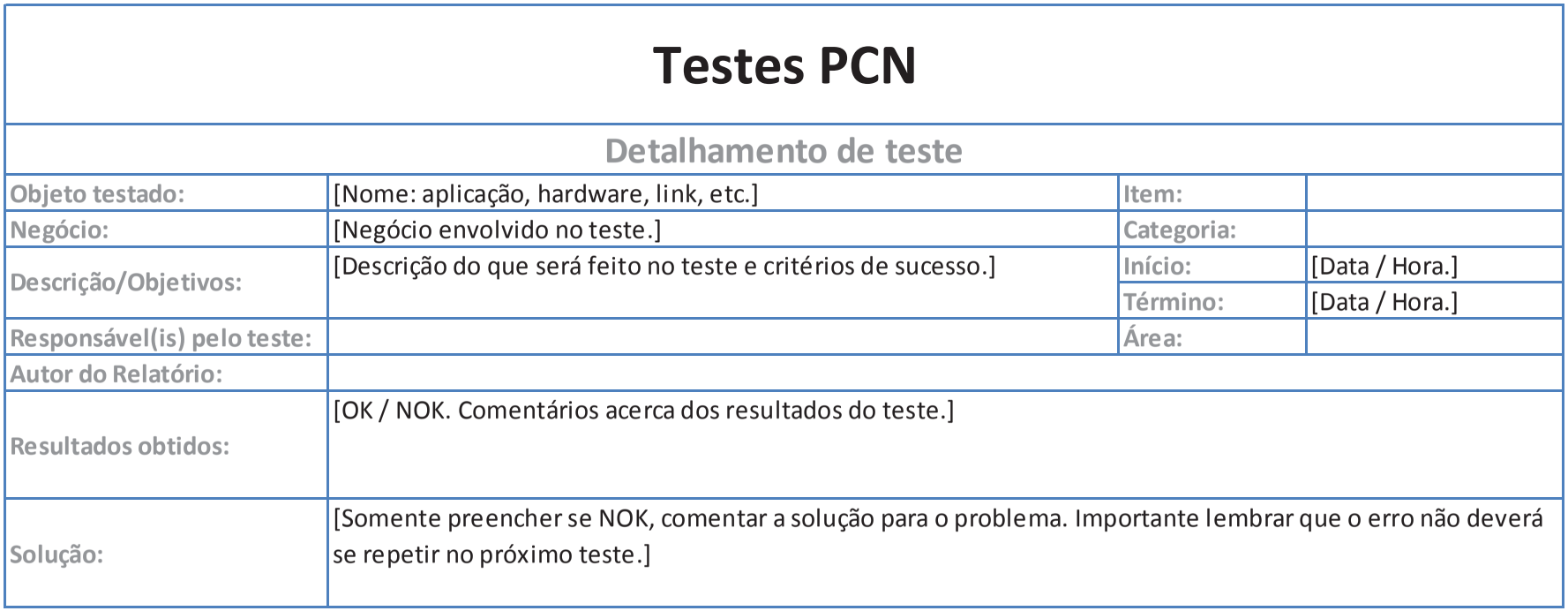
- Falha de aplicação crítica: pode gerar indisponibilidade para os usuários prejudicando o trabalho;
- Falha de servidores: pode impactar uma ou mais aplicações;
- Falha de *link* com as operadoras: pode prejudicar a comunicação da Corporação com as diversas filiais espalhadas pelo Brasil impactando o tráfego de dados (envio e recebimento);
- Falha de *appliance*: inclui falhas em *switches*, roteadores, *core*, *firewall* e outros filtros de linha e de rede. Pode impactar tanto comunicação de *links* quanto servidores e aplicações;
- Falhas de acesso: pode prejudicar o trabalho de todos os funcionários da Corporação pois impacta nos *logins* e acessos de pefis dos usuários de toda a empresa;
- Falha de energia elétrica: pode ameaçar o DC com possíveis sobrecargas, falhas no fornecimento da rede, *blackout* etc. Geradores e UPSs podem evitar que o DC seja desligado mas se a previsão de tempo para retorno da energia for muito longo, é mais barato transferir o funcionamento do DC principal para o DC *backup* fazendo com que se minimizem os gastos com combustíveis para manter os geradores ligados;
- Ausência de equipe técnica: a falta de recursos para colocar os sistemas de volta no ar no DC *backup* pode ser uma grande ameaça ao andamento da recuperação dos negócios da empresa;
- Problemas com fornecedores: a impossibilidade de contatar fornecedores, seja de aplicação, *hardware* ou *appliance*, pode trazer preocupação no que tange a rápida recuperação dos sistemas;
- Incêndio no DC: uma dos acidentes mais comuns em prédios , os incêndios podem destruir o DC causando um grande impacto à empresa;
- Incidente operacional: casos como sabotagem, erro humano e vandalismo devem ser incluídos como possíveis cenários por impactarem de alguma forma o ambiente produtivo.

Tendo em vista as possíveis causas, foi montado o plano de teste. O tipo de teste selecionado pelo Comitê de Gerenciamento do Projeto foi o *paper walkthrough* para que se possa ter uma primeira avaliação da condição e efetividade do plano criado. Serviu de incentivo, ainda, para se ganhar experiência e maturidade.

Este plano foi dividido pelas quatro empresas mais a Informática Corporativa. Os sistemas foram testados individualizando cada empresa. Cada teste foi realizado em um final de semana diferente devido à precaução para que não houvesse impacto no ambiente produtivo (cargas de faturamento) das empresas. Em cada teste, a comunicação entre o DC principal e o DC *backup* foi cortada para que o teste não trouxesse qualquer tipo de impacto ao DC principal e seu ambiente produtivo. Vale comentar que tal medida foi tomada como mera preocupação pois não ocorre tráfego de dados do *site backup* para o *site* principal, somente o oposto, caracterizando a configuração Ativo-Passivo. O escopo do primeiro teste realizado foi validar todas as aplicações de alta criticidade que constavam no *site backup* na sua total funcionalidade, sem envolver o usuário final, ou seja, os analistas técnicos testaram as funcionalidades de todos os sistemas e aplicações envolvidos. Os testes foram registrados por meio de um formulário exemplificado na Figura 9.

A responsabilidade de acionamento do plano cabe ao Comitê de Gerenciamento de Crises, como dito na Seção 2.2.4, sendo que este consiste de 5 membros sendo os quatros gerentes executivos das 4 empresas do grupo mais o gerente executivo da TI da Corporação. Foi definida, também no primeiro plano criado, a Equipe de Resposta a Emergências que é composta por todos os membros levantados, durante a etapa de análise de risco, como necessários no momento de contingência.

Na tabela 3 são apresentados os resultados obtidos. Para efeitos de esclarecimento, a Informática Corporativa e a Empresa D não puderam ter todos os seus sistemas testados devido a uma falha de replicação e atraso na montagem de dois servidores que continham sistemas críticos. Sendo assim, a Informática Corporativa teve 87% dos seus sistemas testados e a Empresa D, 89%.



Testes PCN

Detalhamento de teste

Objeto testado:	[Nome: aplicação, hardware, link, etc.]	**Item:**	
Negócio:	[Negócio envolvido no teste.]	**Categoria:**	
Descrição/Objetivos:	[Descrição do que será feito no teste e critérios de sucesso.]	**Início:**	[Data / Hora.]
		Término:	[Data / Hora.]
Responsável(is) pelo teste:		**Área:**	
Autor do Relatório:			
Resultados obtidos:	[OK / NOK. Comentários acerca dos resultados do teste.]		
Solução:	[Somente preencher se NOK, comentar a solução para o problema. Importante lembrar que o erro não deverá se repetir no próximo teste.]		

Figura 9 – Modelo do formulário de registro dos testes

Tabela 3 – Resultados dos testes com sistemas de alta criticidade

Unidade do Negócio	Sistemas OK	Sistemas NOK	Total Testado por Negócio	OK (%)
Corporação	10	1	11	91%
Informática Corporativa	33	6	39	85%
Empresa A	8	5	13	62%
Empresa B	9	0	9	100%
Empresa C	6	0	6	100%
Empresa D	7	1	8	88%
Total	**73**	**13**	**86**	**85%**

3.4 CONTRIBUIÇÕES

O autor deste trabalho participou diretamente nas seguintes atividades:

- Auxílio no levantamento das aplicações do projeto;
- Levantamento dos tempos de recuperação de cada aplicação (RTO);
- Levantamento e análise de todos os parâmetros de infraestrutura do DC da empresa terceirizada e do DC principal da Corporação;
- Elaboração do modelo padronizado (*template*) de preenchimento dos procedimentos de *start/stop* das aplicações;
- Elaboração do fluxo atualizado com a inserção do processo de mudanças do *site backup*;
- Levantamento dos itens de configuração referentes ao *site backup*;
- Participação das reuniões do Comitê de Mudanças da TI da Corporação;
- Participação da etapa de definição de cenários de teste;
- Elaboração do formulário de avaliação dos testes ilustrado na Figura 9;
- Contribuição na elaboração da escrita do PRD;
- Coleta e apuração dos dados obtidos nos testes.

4 CONCLUSÃO

4.1 ANÁLISE DOS RESULTADOS

Este trabalho buscou apresentar a importância de se elaborar um PRD. Analisou-se a estrutura de uma empresa na sua forma mais completa e também avaliou-se sua complexa estrutura.

Analisando os dados, pode-se creditar o sucesso de 100% de funcionalidade aos sistemas da Empresa C por serem 100% virtualizados e, portanto, possuírem uma cópia fiel do DC principal. A Empresa B possui somente um servidor físico, o que contribuiu também para uma funcionalidade absoluta de seus sistemas. A Empresa A possuiu apenas 62% devido à queda de seu ERP, o que afetou a funcionalidade direta de outros sistemas que se comunicam com este ERP.

Servindo o propósito de corrigir e validar a atual configuração do DC do *site backup*, a avaliação geral do teste tendo 85% de sucesso foi muito satisfatória e, objetivando-se uma melhoria contínua, foram estudadas soluções para melhorar a taxa de sucesso do próximo teste que visa englobar todos os sistemas da Corporação. Perante a análise dos analistas especialistas de cada sistema, apurou-se que a desinstalação e reinstalação das aplicações e sistemas que são de alta criticidade para a Corporação iria solucionar os problemas de comunicação entre aplicações interdependentes melhorando a porcentagem de sucesso obtida no próximo teste.

Como próximos passos, visa-se a elaboração de mais dois testes, sendo um integrado com todos os sistemas disponíveis no ambiente produtivo e outro caracterizado por uma interrupção total dos sistemas, que indicará a real eficácia do plano elaborado.

Um PRD é válido enquanto seus testes apresentarem resultados satisfatórios e seu gerenciamento deve ser realizado com maestria trazendo a segurança necessária para a empresa.

4.2 CONSIDERAÇÕES FINAIS

Como dito anteriormente, deve-se ressaltar a importância de manter o PRD sempre atualizado efetuando as devidas mudanças de acordo com as mudanças de postura, configuração e sistemas da organização.

Por fim, ressalta-se que este estudo atingiu seu propósito inicial, apresentando métricas para se elaborar um PRD e, ainda, validou este plano com um teste, aplicando as métricas descritas neste trabalho.

REFERÊNCIAS

BALARINE, O. F. O. **Tecnologia da Informação como vantagem competitiva**. RAE-eletrônica, Vol. 1, Número 1, 2002. Disponível em: <http://www.rae.com.br/eletronica/index.cfm?FuseAction=Artigo&ID=1059&Secao=INFORMAÇÃO&Volume=1&Numero=1&Ano=2002>. Acesso em 22/10/2012.

BROWN, A.; DOWLING, P. **Doing research/reading research:** a mode of interrogation for teaching. Londres: Routledge Falmer, 2001.

CUMMINGS, M ; HAAG, S.; MCCUBREY, D. J. **Management Information Systems for the Information Age**. McGraw-Hill Companies, Inc., 2005, 592 p.

DRIVE SOLUTIONS. **Raid Arrays**. Disponível em: <http://www.drivesolutions.com/datarecovery/raid.shtml>. Acesso em 26/10/2012.

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

INMET. **Gráfico das normas climatológicas**. Disponível em: <http://www.inmet.gov.br/html/clima/graficos/plotGraf.php?chklist=4%2C&capita=saopaulo%2C&peri=99%2C&per6190=99&tempmed=4&saopaulo=37&Enviar=Visualizar>. Acesso em 08/11/2012.

ITS: THE IT SOLUTION CENTER. **Virtualização**. Disponível em: <http://www2.itssolucoes.com.br/virtualizacao>. Acesso em: 27/10/2012.

JEFFERY, M.; LELIVELD, I. **Best practices in IT portfolio management**. MIT Sloan Management Review, v. 45, n. 3, p. 41-49, 2004.

LAURINDO, Fernando José Barbin et al. **O papel da tecnologia da informação (TI) na estratégia das organizações**. *Gest. Prod.*, 2001, vol.8, no.2, p.160-179. ISSN 0104-530X.

LÓPEZ, V.; HAMANN, H. F. **International Journal of Heat and Mass Transfer:** Heat transfer modeling in data centers. Vol. 54, Issues 25-26, 2011, p. 5306-5318.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. **Um estudo empírico do impacto da governança de TI no desempenho organizacional.** Prod., 2012, p. 0-0. ISSN 0103-6513.

MAIZLISH, B.; HANDLER, R. **IT portfolio management: step by step**. John Wiley & Sons, 2005.

McAFEE, A. **Do you have too much IT?** MIT Sloan Management Review, v. 45, n. 3, p. 18-22, 2004.

McFARLAN, F. W. **Information technology changes the way you compete**. *Harvard Business Review*, v. 62, n. 3, p. 98-103, 1984.

MOEN, R.; NORMAN, C. **Evolution of the PDCA Cycle**. Disponível em: < http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf>. Acesso em 03/12/2012.

MORAES, R. O.; LAURINDO, F. J. B. **Um estudo de caso de gestão de portfolio de projetos de tecnologia da informação**. *Gest. Prod.*, 2003, vol.10, no.3, p.311-328. ISSN 0104-530X.

RAMOS, Rodrigo de Oliveira. **Aplicação de um modelo de análise da tecnologia da informação em empresa de telecomunicações.** 2007. Trabalho de Graduação (Graduação em Engenharia Mecânica) – Faculdade de Engenharia do Campus de Guaratinguetá, Universidade Estadual Paulista, Guaratinguetá, 2007.

SNEDAKER, S. **Business Continuity and Disaster Recovery Plan for IT Professionals.** Burlington: Syngress Publishing, Inc., 2007. 449 p.

WEILL, P. ; ROSS, J. **A Matrixed Approach To IT Governance**. *MIT Sloan Management Review*, v. 46, n. 2, p. 26, 2005.