UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

THIAGO RODRIGO DE FREITAS

PLANO DE CONTINGÊNCIA DE NEGÓCIOS E SERVIÇOS
TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2013

THIAGO RODRIGO DE FREITAS

PLANO DE CONTINGÊNCIA DE NEGÓCIOS E SERVIÇOS

Trabalho de Conclusão de Curso apresentado ao Departamento Acadêmico de Eletrônica como requisito parcial para obtenção do grau de Tecnólogo no Curso Superior de Tecnologia em Sistemas de Telecomunicações da Universidade Tecnológica Federal do Paraná.

Orientador: Professor Alexandre Jorge Miziara

CURITIBA
2013

TERMO DE APROVAÇÃO

THIAGO RODRIGO DE FREITAS

PLANO DE CONTINGÊNCIA DE NEGÓCIOS E SERVIÇOS

Este trabalho de conclusão de curso foi apresentado no dia 11 de outubro de 2013, como requisito parcial para obtenção do título de Tecnólogo em Sistemas e Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. O aluno Thiago Rodrigo de Freitas foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Dr. Jamea Cristina Batista
UTFPR

_____
Prof. Dr. Simone Crocetti
UTFPR

_____
Prof. Alexandre Miziara
Orientador - UTFPR

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

AGRADECIMENTOS

Agradeço a Deus pela oportunidade de estar se graduando em uma Universidade tão renomada como é a Universidade Tecnológica Federal do Paraná. Aos meus pais, irmãos e outros integrantes que sempre estiveram ao lado prestando apoio durante o curso e inclusive durante a elaboração desse projeto.

Aos amigos que fizemos e nos acompanharam durante o curso. A todos os professores que passaram seus conhecimentos durante esses anos e em especial ao professor Alexandre Miziara que foi meu orientador e a professora doutora Jamea Cristina Batista Silva que me ajudaram ao longo do projeto.

RESUMO

FREITAS, Thiago. **Plano de Contingência de Negócios**. 2013. 50 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamentos Acadêmicos de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Este trabalho tem como objetivo descrever e documentar o desenvolvimento de uma solução em infraestrutura e contingência para qualquer empresa, a fim de promover e difundir a ideia de estruturas e planos como esse, evitando problemas com a perda de dados de serviços e aplicações, podendo dessa maneira dar continuidade ao negócio e, além disso, mostrar como os Projetos de Contingência são desenvolvidos demonstrando a estrutura de tarefas, objetivos do projeto, dimensionando respectivas tecnologias e serviços críticos. O Plano de Contingência é uma prática comum em países desenvolvidos, é uma maneira de aumentar o valor da empresa em questão de ações e prover o acesso continuo em casos de falhas de sistemas e serviços críticos, o objetivo é de tornar claro para o leitor de que é possível ter um Plano de Contingência com um custo menor, podendo implementar por empresas de pequeno porte.

Palavras-chave: Contingência. BCP. Planos de Negócio. Recuperação de Desastre.

ABSTRACT

FREITAS, Thiago. **Business Contingency Plans**. 2013. 50 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamentos Acadêmicos de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

This work has the main goal to provide documentation and describe the development of a infrastructure solution and contingency plan for any interested company, trying to promove and disseminate the idea of plans and structures like these to solve or avoid problems like loss of data or services and applications, providing the business continuity and after that, show how this kind of Contingency happens, dimensioning the technologies and critical services. The Contingency Plan is an ordinary practice on developed countries, it is a way to increase the value of the company and give continue access in case of failures of critical systems, the main goal of this work is become clearly that is possible have one Contingency Plan with a low coast and can be implement on small companies.

Key-words: *Contingency. BCP. Business Plans. Disaster Recovery*.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Plano de Contingência de Negócios e Serviços é um tema atual, decorrente da alta eminência de grandes empresas buscarem alternativas de contingência em seus sistemas e aplicações a fim de implementar com segurança e tecnologia nas áreas de maior risco, alternativas e operações viáveis para proteger o lucro.

Isso pode ser percebido devido a um estudo da Marsch European que mostra todas estatísticas sobre os planos de contingência no mundo. Para melhor compreensão (MARSH EUROPEAN, 2008).

Derivada da palavra em inglês BCP (*Business Continuity Plans*) ou Plano de Contingência de Negócios, devido à experiência e vivência na área é possível dizer que visa à criação de um documento corporativo para que seja possível mensurar as áreas de maior risco da empresa e quantificar o impacto da área, caso a mesma venha a sofrer algum dano, seja através de um desastre natural (furacão, tempestades, tsunami, terremoto, tornados), protesto ou greve, economia em risco, erros críticos de aplicações que demandam a possibilidade de perda de dados e etc. (AMARO, 2004).

O plano deverá cobrir e mensurar todas as áreas de TI (Tecnologia da Informação), analisando e definindo um plano para todos seus processos, implementando de tal forma o BCP de modo que possa minimizar os impactos na área de segurança de ti como podemos ver na figura 1.

Figura 1: Ciclo da segurança de TI em Planos de Contingência
Fonte: (REMMERS, 2012)

Conforme a figura 1, o ciclo de um Plano de Contingência ou *Business Planning* se resume a analise do plano, ajuste, implementação, treinamento e cuidado, monitoramento e o relatório final.

O termo BCP (*Business Contingency Plans*) ou no português Plano de Continuidade de Negócios foi criado pelos Norte-Americanos devido à necessidade de sempre manter tudo funcionando, já que manter o negócio funcionando significa lucro contínuo. Geralmente esse tipo de projeto é implementado com outras ferramentas de gestão, como o *IT Infrastructure Library* (Biblioteca de Infraestrutura de TI) mais conhecido como ITIL que atua na parte comportamental dos indivíduos e visão estratégica de projetos como o *Project Management Institute* (Instituto de Gerenciamento de Projetos) mais conhecido pela sigla PMI.

Porém hoje em dia, o continente que se mostra mais preparado para o uso do BCP é o continente Europeu, que possuí cerca de 70% das grandes empresas com mais de 1000 funcionários. A Europa também se mostra o continente mais preocupado com problemas críticos como incidentes naturais, ataques cibernéticos, e toda essa preocupação também se mostraram decorrente a problemas anteriores. (MARSH EUROPEAN, 2008).

A implementação de novas tecnologias ou de ideias inovadoras podem poupar dinheiro aos cofres das grandes corporações e por isso os dados e levantamentos do projeto devem ser quantificados de maneira correta, sempre se perguntando que tecnologias podem ser utilizadas para cada tipo de contingência, se existe a possibilidade da migração de serviços críticos e instáveis para outros, melhores e atuais.

Vários fatores devem ser considerados em um plano de contingência, descrito logo abaixo de acordo com (INSTITUTO DE INFORMÁTICA, 1999).

- Avaliar os impactos no negócio, ou seja, para cada processo identificado, avaliar o impacto que a sua falha representa para a organização, levando em consideração também as interdependências entre processos. Como resultado deste trabalho será possível identificar a maioria dos processos críticos para a sobrevivência da organização;
- Identificar riscos e definir cenários possíveis de falha para cada um dos processos críticos, levando em conta a probabilidade de ocorrência de cada falha, provável duração dos efeitos, consequências resultantes, custos

inerentes e os limites máximos aceitáveis de permanência da falha sem a ativação da respectiva medida de contingência;

- Identificar medidas para cada falha, ou seja, listar as medidas a serem postas em prática caso a falha aconteça, incluindo o contato com a imprensa;
- Definir ações necessárias para a operacionalização das medidas cuja implantação dependa da aquisição de recursos físicos e/ou humanos (por exemplo, aquisição de gerador e combustível para um sistema de contingência de energia elétrica);
- Estimar custos de cada medida, comparando-os aos custos incorridos no caso da contingência não existir;
- Definir forma de monitoramento após a falha;
- Definir critérios de ativação do plano, como tempo máximo aceitável de permanência da falha;
- Identificar o responsável pela ativação do plano, normalmente situado em um alto nível hierárquico da companhia;
- Identificar os responsáveis em colocar em prática as medidas de contingência definidas, tendo cada elemento responsabilidades formalmente definidas e nominalmente atribuídas. Deve também existir um substituto nominalmente definido para cada elemento. Todos devem estar familiarizados com o plano visando evitar hesitações ou perdas de tempo que possam causar maiores problemas em situação de crise. A equipe responsável deverá ter a possibilidade de decidir perante situações imprevistas ou inesperadas, devendo estar previamente definido o limite desta possibilidade de decisão;
- Definir a forma de reposição do negócio aos moldes habituais, ou seja, quando e como sair do estado de contingência e retornar ao seu estado normal de operação, assim como quem são os responsáveis por estas ações e como este processo será monitorado.

Após a área de Gerenciamento de Riscos mensurar os possíveis danos causados, deve-se analisar a quantidade de investimento para que haja a cobertura total dos serviços e sites ou apenas das áreas críticas conforme cada empresa.

Com o Plano de Contingência pronto e aprovado pelos diretores existe o último procedimento que é o teste em si o qual deve ser previamente agendado e

acordado um dia onde será realizado o teste comportamental de todos os indivíduos da empresa ou de um setor.

Dessa forma é possível prevenir qualquer perda de dados ou parada de produção que resultaria em prejuízos para empresa. Mesmo que com o custo elevado, o BCP vem a ser uma ótima saída estratégica para os negócios.

1.1 PROBLEMA

Mesmo hoje em dia, grandes empresas investem em aprimoramentos tecnológicos para que o lucro corporativo seja maior, implementando novas ideias que asseguram muitas vezes uma maneira eficiente de crescimento.

O mercado atual é muito competitivo e cada vez mais existe a necessidade de produzir mais com menos. Alguns riscos eminentes decorrentes de ações humanas podem vir a impactar empresas, áreas ou mesmo países inteiros.

Alguns problemas decorrentes disso são os desastres naturais, como furacões de alta escala, grandes terremotos, tsunamis, entre outros, são motivos assustadores com que fizeram as multinacionais se preocuparem com ambientes de contingência.

O BCP de maneira geral não é algo fácil de ser mensurado, necessita estudo de casos, compreendimento completo de aplicações que podem ser muito complexas e existem razões geopolíticas e sociológicas sobre como implementar a necessidade do Plano de Contingência de Negócios não apenas em grandes corporações, mas sim, em todas as empresas.

Outras questões serão levantadas no TCC, tais como:

- Compreender o funcionamento de projetos BCP;
- Como projetar planos de contingência;
- Propostas do uso de uma nova tecnologia.
- Realizar testes de BCP e *Disaster Recovery*.
- Como é mensurado a criticidade dos sistemas e aplicações.

Por fim, a inserção dessa metodologia e o receio de alguns países e economias de investirem recursos para que exista o BCP se tornam barreiras na implementação de projetos como esse.

1.2 JUSTIFICATIVA

É uma maneira de demonstrar que projetos assim são possíveis no Brasil, trazendo também para o seu contexto político e socioeconômico maneiras viáveis da implementação do mesmo.

Devido à vivência na criação e participação de projetos como esse, a expectativa é que além de trazer um projeto inovador, se torne viável mostrar soluções inovadoras de mercado, planos estratégicos e um novo conceito do mercado exterior para o mercado brasileiro.

Até um tempo atrás, as multinacionais tinham o costume de ter grandes *datacenters* ou lugares próprios para se armazenar informações e servidores em lugares diferentes do globo para poder manter contingência de serviços e hoje este conceito vai além e é aplicável a qualquer área de risco seja uma aplicação, um serviço ou um ambiente.

Ao longo dos anos, não somente devido à necessidade da criação de estruturas que comportem contingência, mas também no desenvolvimento de planos estratégicos a fim de maximizar os ganhos e mantê-los, os Planos de Contingência de Serviços foram sendo criados e implementados.

Como a grande chance de existir áreas de risco ou aplicações críticas em uma empresa, o tratamento desse problema é algo que se torna muito necessário e na maioria das vezes mensurável.

O plano de contingência deve ser desenvolvido envolvendo todas as áreas sujeitas a catástrofes, tanto as de sistema de informática quanto as de negócio e não deve ser de exclusiva responsabilidade da área de Tecnologia da Informação da organização. Seus itens deverão estar documentados e a atualização desta documentação deve ser feita sempre que necessário. Testes periódicos no plano também são necessários para verificar se o processo continua válido.

Um plano de contingência mais elaborado normalmente tem um custo elevado, pois envolve alocação de pessoas, sites alternativos, hardware redundante subutilizado, entre outros.

1.3 OBJETIVOS

Apontar e relatar a partir da vivência, planos de contingência como projetos mandatórios em qualquer empresa, demonstrando e citando ações preventivas, considerando o custo benefício que um programa como esse pode oferecer.

1.3.1 Objetivos Gerais

Demonstrar a necessidade de planos de contingência para empresas multinacionais ou de médio porte, mostrando e apresentando os benefícios da implementação do mesmo, trazendo planejamentos de baixo custo e de alto custo.

1.3.2 Objetivos Específicos

1. Identificar a necessidade do uso do BCP;
2. Identificar áreas de risco;
3. Identificar medidas em caso de falha e possíveis soluções;
4. Avaliar impacto nos negócios;
5. Demonstrar a visão estratégica de mercado;
6. Demonstrar as áreas de TI que são impactados diretamente;
7. Planejar a criação de um Plano de Contingência;
8. Mostrar serviços e programas que podem ajudar no BCP sem um alto custo.

1.4 METODOLOGIA

A metodologia utilizada é em parte experiência devido à vivência com a prática da criação de um Projeto de Contingência e a estudos realizados por outras empresas nessa área. Através de pesquisa foi possível confirmar teses que podem ser observadas na prática e com isso complementar o que existe.

Identificando dessa maneira, as melhores abordagens sobre o tema, trazendo sobre o assunto aquilo que há de recente no mercado além de mostrar na prática como o projeto acontece deixando exemplos práticos sobre como tudo funciona.

2 PLANO DE CONTINGÊNCIA DE NEGÓCIOS

Durante alguns anos, grandes corporações sofreram com desastres naturais de alta escala ou mesmo protestos políticos ou protestos, levaram tempo para perceber que esses eventos que ocorriam privavam da manutenção do fluxo de lucro, já que sempre ouve perda financeira.

As grandes multinacionais, principalmente as americanas, começaram a se voltar em projetos que visavam à manutenção e a continuidade do negócio e dessa maneira, mesmo que algo exterior viesse a impactar a empresa, com algumas medidas de prevenção isso poderia ser minimizado.

Para Amaro (2004),

> O plano de contingência deve ser parte da política de segurança de uma organização complementando assim o planejamento estratégico desta. Nele são especificados procedimentos pré-estabelecidos a serem observados nas tarefas de recuperação do ambiente de sistemas e negócios, de modo a diminuir o impacto causado por incidentes que não poderão ser evitados pelas medidas de segurança em vigor.

A ideia foi implementada com sucesso nas empresas, para ter alta disponibilidade em seus serviços, as grandes multinacionais começaram a investir cada vez mais. É possível dizer que a criação de um Plano de Contingência dura um longo tempo além de possuir um investimento considerável de acordo com a estrutura da corporação.

Devido à vivência obtida na criação de um Plano de Contingência, é possível falar que esse tipo de projeto está longe de ser algo simplório, precisam-se levantar todos os requisitos da empresa, aplicações, problemas, segurança até que seja possível mensurar e quantificar todas as áreas criticas.

O que se percebe é que esses planos são uma área restrita e perigosa no mercado, onde serviços agregados à área de tecnologia de informação estão relacionados a uma criticidade imensa dentro das corporações, cada vez mais serviços e aplicações não podem falhar fazendo com que fossem desenvolvidas essas estratégias a fim de evitar esses problemas. (WALLACE; WEBBER, 2004)

Para assegurar os serviços, áreas e recursos emergenciais, todos os responsáveis e envolvidos diretamente na entrega do serviço final começaram a se preocupar com o BCP e isso pode ser visto através da figura 2:

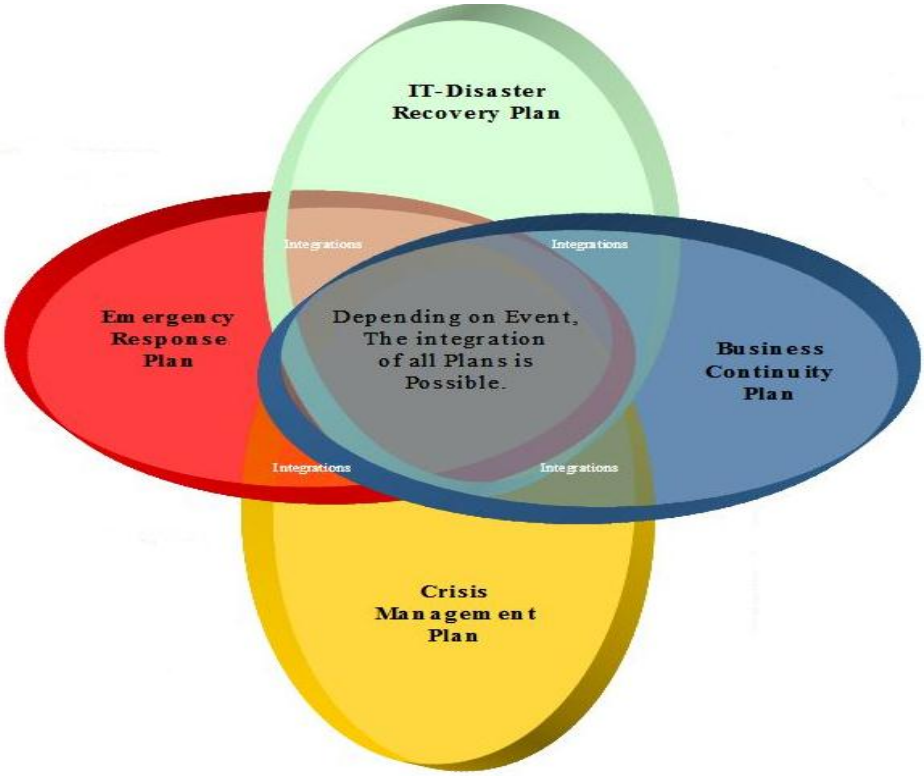


Figura 2: Áreas Emergências de TI

Fonte: Autoria Própria.

O BCP pode possuir outros fins, na tentativa de levar a empresa a ter maior credibilidade e mais investimentos, o plano de contingência pode significar aos acionistas um investimento certo devido ao lucro contínuo dessa maneira pode-se evitar: Segundo o (INSTITUTO DE INFORMÁTICA, 1999).

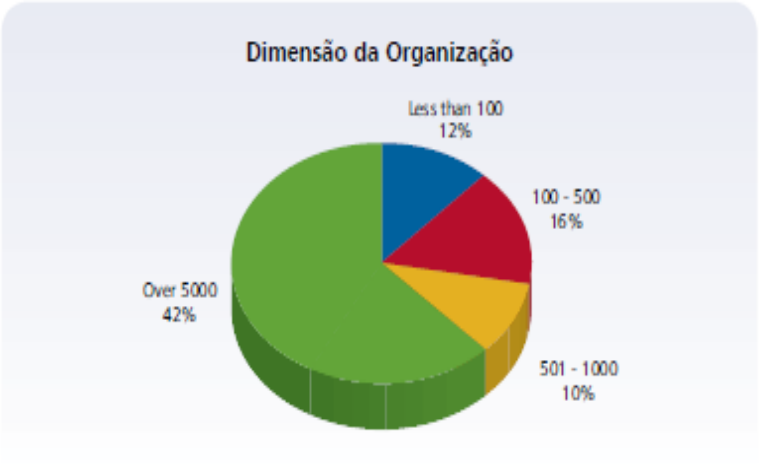
- A fuga de acionistas;
- Perdas de receita;
- Sanções governamentais;
- Problemas jurídicos para os dirigentes;
- Abordagens maliciosas da imprensa;
- Fuga de funcionários para os concorrentes;
- Em casos extremos, o fechamento da empresa.

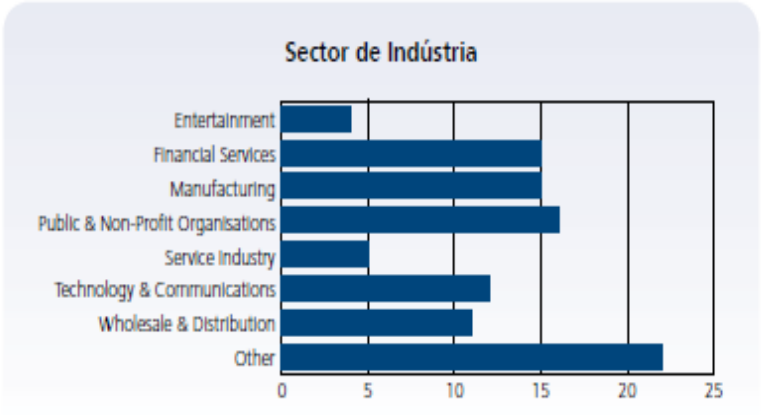
O plano de contingência deve ser parte da política de segurança de uma organização complementando assim o planejamento estratégico. Nele são especificados procedimentos pré-estabelecidos a serem observados nas tarefas de

recuperação do ambiente de sistemas e negócios, de modo a diminuir o impacto causado por incidentes que não poderão ser evitados pelas medidas de segurança em vigor (INSTITUTO DE INFORMÁTICA, 1999).

Cada dia mais o termo BCP ou esses planejamentos são implementados nas companhias pelo mundo, a prática recorrente das multinacionais se deve pelo fator de mitigar a perda de dinheiro.

Isso pode ser melhor observado nas estatísticas a seguir que de acordo com o Benchmarking da Marsh, apenas multinacionais adotam projetos de contingência. Isso se deve não apenas pelo valor do investimento e ações da empresa, mas também na necessidade de negócio, operacionalidade, segurança e confiabilidade conforme mostrada na Figura 3:





Quando analisamos os dados europeus podemos afirmar que foram principalmente as empresas com mais de 1000 empregados que responderam a este inquérito, com um total de 62%, ao passo que apenas 12% das empresas têm menos de 100 empregados.

No caso de Portugal também foram principalmente as empresas com mais de 1000 empregados a responderem ao inquérito com um total de 46%, ao passo que 29% das empresas têm menos de 100 empregados.

Estes resultados são indicativos das condições de mercados prevalentes, onde o BCM é mais provável que seja um problema nas grandes empresas. Isto é devido não só à consciência da necessidade de ter um Plano de Contingência, mas também às economias de escala, bem como a capacidade de tomar a longo prazo uma posição financeira desfrutada por as grandes empresas.

O inquérito apresenta respostas de uma ampla variedade de indústrias. No entanto, a maioria das respostas pertence a Organizações Públicas e sem fins lucrativos (16%), Instituições Financeiras (15%) e Fabrico (15%). Esta inclinação é susceptível de ser causada pela consciência gerada a partir da regulação e o impacto de eventos reais nestas indústrias.

No caso de Portugal as principais Indústrias que responderam foram: Retalho/ Grossista (17%), Serviços (17%) e Tecnológicas & Telecomunicações (17%).

Figura 3: Estatística de Organizações que adotam a utilização do BCP
Fonte: (MARSH EUROPEAN, 2008).

Apesar disso, os planos de contingência não são luxos apenas das grandes corporações, devido ao crescimento da tecnologia existem inúmeras maneiras de que se tenha contingência, utilizando recursos disponíveis no mercado e de uma maneira altamente viável e de alto custo beneficio podendo ser visto logo abaixo: (INSTITUTO DE INFORMÁTICA, 1999).

1. Manter *backup* regular das bases de dados;
2. Manter um site de contingência sempre atualizado;
3. Possuir ferramentas seguras para acesso aos dados remotamente para o caso da impossibilidade de chegar até o prédio da empresa (VPN ou *Virtual Private Network* ou acesso discado, por exemplo);
4. Ter cópias completas e atualizadas de servidores vitais para o funcionamento da empresa (principalmente os que requerem muito tempo para reconstituição);
5. Manter senhas em local seguro, mas de fácil acesso a pessoas chaves da empresa no caso de uma emergência.

Os procedimentos simples são a prova de que é possível haver contingência sem um alto custo, prevenindo assim, incidentes que possam derrubar uma aplicação ou fazer parar todo um ambiente de trabalho. Isso também mostra que essas soluções tecnológicas se mostram cada vez mais viáveis, possibilitando pequenas empresas terem ambientes que funcionem dessa forma.

Um plano de contingência mais elaborado normalmente tem um custo elevado, pois envolve alocação de pessoas, sites alternativos, *hardware* redundante subutilizado, etc. Normalmente o site alternativo possui recursos menores do que o site de produção, visando reduzir custos e atendendo apenas o suficiente para manter os serviços vitais da empresa. A partir de uma análise é possível mensurar o que é realmente importante para a empresa, comparando os custos para se criar a contingência de um determinado item e o eventual prejuízo gerado pela falta da contingência deste mesmo item (WATKIN, 1997).

O bom entendimento das áreas de risco juntamente com os responsáveis por cada aplicação traduzem o problema e as criticidades para dentro do escopo do plano.

3 CRIAÇÃO DE UM DOCUMENTO DE CONTINGÊNCIA

A criação de um plano de contingência geralmente respeita uma determinada ordem durante a execução de um plano, os procedimentos atendam passo a passo todos os movimentos descritos a serem realizados.

O Plano de Contingência deve ser constituído por uma série de ações determinadas relacionadas com o sistema para recuperar em caso de falha. A sua complexidade e profundidade deve ser necessária e suficiente para a complexidade desses mesmos sistemas, sem desperdícios ou excesso de informação que pode ser prejudicial numa situação crítica (INSTITUTO DE INFORMÁTICA, 1999).

Esses tipos de ações podem ser melhores observadas na Figura 4:

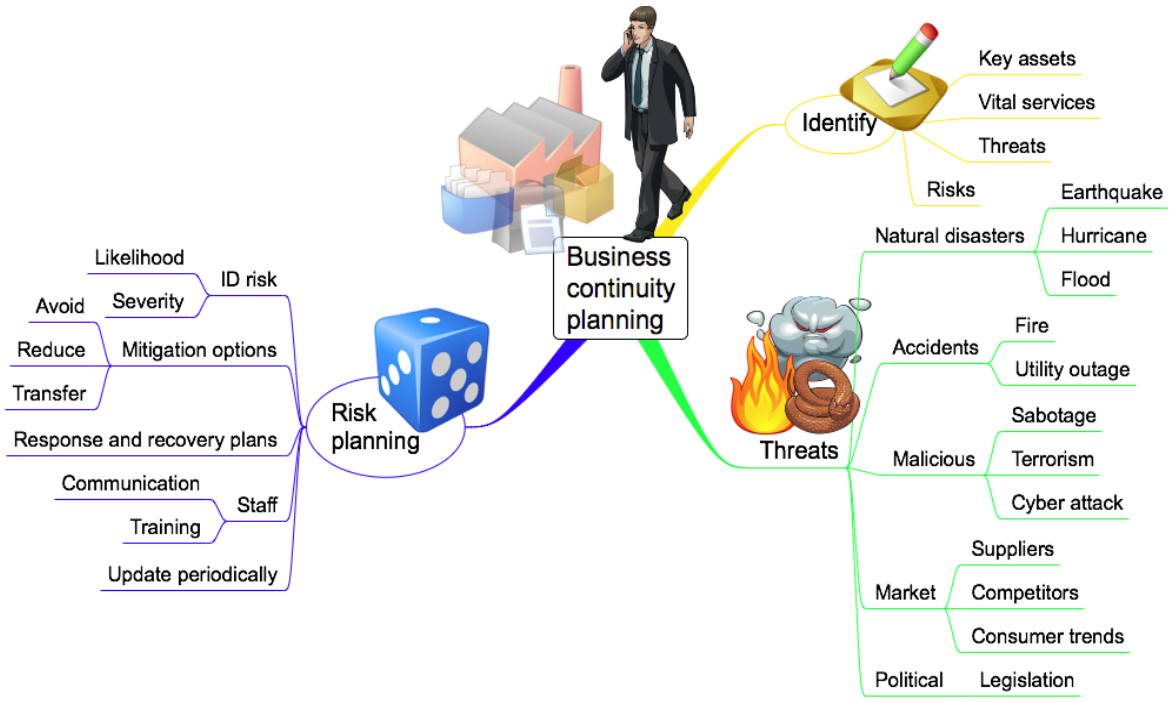


Figura 4: Tarefas á serem definidas para o BCP
Fonte: Autoria Própria

Essas ações são tomadas a partir de três diretrizes conforme a Figura 4 para se determinar um plano de contingência é necessário:

- A identificação dos riscos: onde são encontrados as pessoas chaves e serviços vitais para o negócio;

- A área de ameaças: Acidentes, problemas políticos, terrorismo, ataque cibernético;
- Planejamento de risco: Amizade, ID de segurança, treinamento, comunicação.

O Plano de Contingência deve concentrar-se nos acidentes de maior probabilidade e menos catastróficos e não nos acidentes mais catastróficos que podem ser, ou não, menos prováveis e deve ser construído a partir de cenários prováveis, previamente definidos. De forma global, as ocorrências negativas mais comuns são a existência de vírus destruidores de dados e sistemas, a perda de disco rígido, a perda de um servidor da rede ou de uma ligação em rede, a alteração do software, a falha de ar condicionado e de energia de forma mais geral, as fugas de extintores de incêndio que danifiquem o hardware, as avarias na Unidade Central de Processamento de um computador, entre outras (INSTITUTO DE INFORMÁTICA, 1999).

Além disso, um plano de contingência deve ser:

1. Desenvolvido por um profissional que conhece todas as áreas e que tenha uma visão ampla de tecnologia;
2. Desenvolvido em conjunto com profissionais que tenham visão na área de negócios;
3. Envolvimento de todas as áreas;
4. Envolvimento de todos os especialistas das aplicações críticas;
5. Envolvimento da área financeira, orçamento;
6. Estipular datas, cronogramas, testes;
7. Nomes de todos envolvidos e pessoas chaves;
8. Planejamento e cursos (todos os membros da corporação devem saber o conteúdo e procedimentos que deveram ser realizados).

Pode ser que de acordo com o tamanho da empresa, o BCP seja divido em várias fases e partes, respeitando uma sequência lógica do negócio podendo separar ou não por tecnologia. Por exemplo: é possível existir um BCP para aplicações críticas, outro para *Data Centers* (Locais de infraestrutura reforçada com os servidores e aparelhos de rede), Contingência de contatos e e-mail (*EXCHANGE* Servidor de *e-mail* da *Microsoft*), Telecomunicações e etc.

3.1 PRIMEIRA ETAPA NA CRIAÇÃO DE UM PLANO DE CONTINGÊNCIA

Durante o processo de criação de um BCP, alguns procedimentos sempre são constantes:

- Nomear os integrantes de um grupo para a criação do BCP;
- Definir o gestor responsável da equipe;
- Integrar todas as áreas da empresa para que saibam da criação do documento;
- Ter apoio dos diretores.

Com a equipe definida, deve-se começar a criação do documento em si. A atuação da equipe deve ser pró-ativa, mensurando as possíveis áreas críticas assim como os serviços da empresa, e deve ser elaborado a fim de deixar claro (INSTITUTO DE INFORMÁTICA, 1999).

- Os objetivos de desempenho do plano, isto é, o plano destina-se a assegurar um funcionamento pleno de todos os processos, dos processos críticos para o negócio, ou tem apenas por objetivo assegurar um funcionamento minimalista da organização;
- A metodologia e periodicidade de reporte em relação aos trabalhos de elaboração do plano.

Após uma pesquisa sobre as áreas afetadas que deverão receber o plano de contingência, é criado um documentado mostrando isso, além de trazer um breve levantamento financeiro de quanto deve custar para empresa.

Quando tudo for assinado, deverá ser colocado em prática o desenvolvimento do plano.

3.2 SEGUNDA ETAPA NA CRIAÇÃO DE UM PLANO DE CONTINGÊNCIA

Durante a fase dois, deverão ser identificados todos os processos necessários do BCP e quais aplicações ou sistemas deveram ser incluídos, para cada processo, deve ser mensurado o nível de criticidade, avaliando o impacto e a chance de que erros possam ocorrer.

Na figura 5 se observa um exemplo das áreas avaliadas e aplicações da empresa, sempre priorizando a informação da criticidade para o negócio em si:

Scorecard / assessment	Position in league table	Overall criticality	Confidentiality rating	Integrity rating	Availability rating	Critical timescale
Brazil.P1 (CA6503) [3]	1	C Highly critical	B Very serious harm	B Very serious harm	A Extremely serious harm	2-3 days
Brazil.iSMS (CA7510) [2]	2	D Critical	B Very serious harm	A Extremely serious harm	B Very serious harm	A week
Brazil.NFe (CA7576) [2]	3	D Critical	C Serious harm	A Extremely serious harm	B Very serious harm	A week
Brazil.ADP_Expert (RS7683) [1]	4	D Critical	B Very serious harm	D Minor harm	B Very serious harm	A week
Brazil.BudgetControlSystem (RS7911) [1]	5	D Critical	C Serious harm	C Serious harm	B Very serious harm	A week
Brazil.PW (CA7577) [2]	6	D Critical	C Serious harm	A Extremely serious harm	D Minor harm	A month+
Brazil.CPJLegal (RS8636) [1]	7	D Critical	D Minor harm	B Very serious harm	D Minor harm	A month+
Brazil.PWSped (RS8225) [1]	8	E Important but not critical	E No significant harm	C Serious harm	C Serious harm	A month+
Brazil.ControleAcesso (CA7656) [1]	9	E Important but not critical	D Minor harm	C Serious harm	D Minor harm	A month+
Brazil.QAT (RS2617) [4]	=10	E Important but not critical	E No significant harm	C Serious harm	D Minor harm	A month+
Brazil.CaixasPMB (CA7491) [2]	=10	E Important but not critical	E No significant harm	D Minor harm	C Serious harm	A month+
Brazil.Bora (CA7508) [2]	=10	E Important but not critical	C Serious harm	E No significant harm	D Minor harm	A month+
Brazil.LIMS (RS2989) [4]	=13	F Of regular importance	D Minor harm	D Minor harm	D Minor harm	A month+
Brazil.NEXO (RS3252) [4]	=13	F Of regular importance	D Minor harm	D Minor harm	D Minor harm	A month+
Brazil.ISOSystems (CA7457) [2]	=15	F Of regular importance	D Minor harm	D Minor harm	E No significant harm	A month+
Brazil.E-Taf (CA7490) [2]	=15	F Of regular importance	E No significant harm	D Minor harm	D Minor harm	A month+
Brazil.ConsumerDB_ArcLight (RS8639) [1]	=15	F Of regular importance	D Minor harm	E No significant harm	D Minor harm	A month+
Brazil.BTL_System (CA6325) [2]	=18	F Of regular importance	D Minor harm	E No significant harm	E No significant harm	A month+
Brazil.LEA (CA7662) [1]	=18	F Of regular importance	E No significant harm	E No significant harm	D Minor harm	A month+
Brazil.AcessoSeguro (CA8638) [1]	=18	F Of regular importance	E No significant harm	D Minor harm	E No significant harm	A month+
Brazil.FORPONTO (RS4759) [4]	21	F Of regular importance	E No significant harm	E No significant harm	E No significant harm	A month+
Maximum ratings		C Highly critical	B Very serious harm	A Extremely serious harm	A Extremely serious harm	2-3 days

Figura 5: Exemplo de Definição de Criticidade dos Programas
Fonte: Autoria Própria

De posse dos dados das áreas necessárias, um estudo sobre cada área, tecnologia e aplicação devem ser realizados. Aplicações ou sistemas que tem alto impacto na empresa e que possuam alto nível de criticidade devem receber a atenção completa da empresa, funcionários e do plano de contingência.

Soluções técnicas deveram ser discutidas com essas áreas procurando alternativas e métodos que possam minimizar os impactos dessas aplicações em caso de risco ou falha. É nesse momento em que as soluções são diferenciadas de acordo com o tamanho da empresa e da criticidade.

Em pequenas empresas, o BCP pode vir a quantificar as áreas de riscos e geralmente soluções técnicas resolvem o problema. Soluções como:

- Backup dos dados;
- Servidores virtuais ou VHD (*Virtual Hard Disk*);
- Dados e documentos importantes em *Cloud* (nuvem de dados que podem ser acessados á qualquer momento e em qualquer lugar utilizando conexão com a internet);
- Possuir acessos seguros a documentos e aplicações corporativas;
- Acesso via *Active Directory* (Diretório de Dados responsável por permitir acesso ou bloquear usuários indesejados).

Geralmente nesses casos, existe a criação de um fluxograma que deve ser aprovado pelos gerentes, para garantir o bom entendimento como pode ser observado na figura 6:

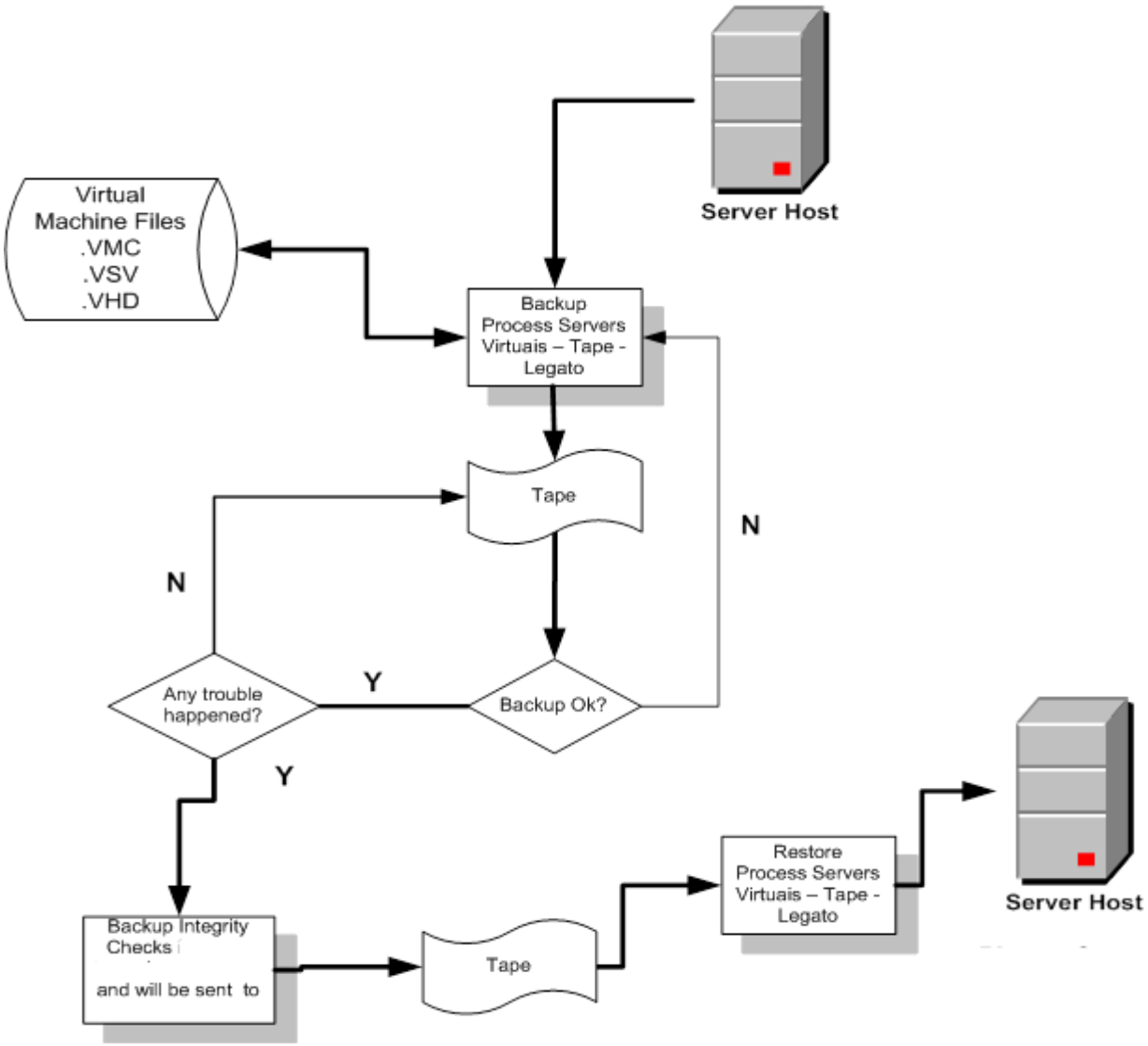


Figura 6: Exemplo de Fluxograma para verificação dos processos
Fonte: Autoria Própria

Mas em grandes empresas, saídas de contingências assim nem sempre são o suficiente. Em um banco, por exemplo, onde transações bancárias não podem jamais deixar de serem comutadas, devem existir no mínimo três bancos de dados diferentes (tecnologias diferentes) e utilizando métodos de nó ou falhas chamadas de *Redundant Array of Independent Drives* (Conjunto de Discos Independentes e Redundantes) ou simplesmente de RAIDS que permitem que o mesmo banco de dados em um servidor possa estar espelhado em outros e se um falhar, outro servidor assumiria de imediato não perdendo pacotes de dados ou trazendo alguma diferença para o usuário.

O problema, que soluções tecnológicas como essas não são baratas, mas é algo estritamente necessário.

Devido a problemas em países que possui alto índice de desastre natural, como tsunamis, furacões, vulcões, as grandes multinacionais investem em sites ou lugares de contingência. Para um *Data Center* construído no Japão, por exemplo, deve haver pelo menos 3 *data centers* similares que possam proteger os dados através de contingência caso aconteça algo á aquele determinado lugar.

Essa ideologia de contingência entre ambientes ou locais diferentes pode ser observada na Figura 7, onde são mostradas cidades diferentes ligados por fibra ótica podendo convergir entre elas através de um sistema de nuvem implementado por várias empresas.

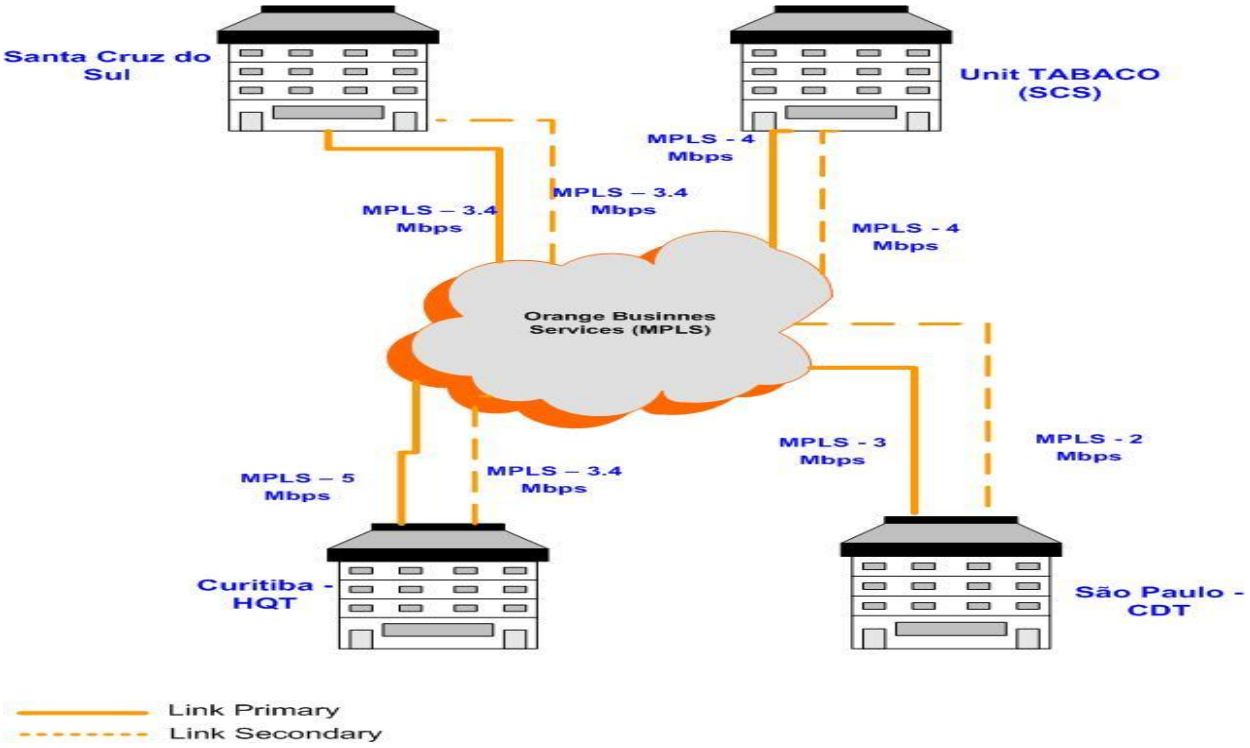


Figura 7: Exemplo de Ambientes e Lugares em contingência
Fonte: Autoria Própria

A ideia é muito difundida nas multinacionais e os *data centers* sempre se situam em lugares completamente distantes um dos outros, a capacidade ou qualidade desses *data centers* também possuí um determinado nível de importância.

As classificações por camadas foram criadas para descrever, de modo consistente, o nível de exigência requerida de infraestrutura local destinada a manter as operações de um centro de processamento dados (CPD). Assim, a classificação da topologia Camada considera como um todo o local destinado a hospedar um CPD, sendo restringida pela classificação do seu subsistema mais fraco.

Datas Centers em geral são classificados em quatro camadas mostrados conforme o quadro 1 abaixo: (UPDATE INSTITUTE, 2006)

Nível	Requisitos
1	• Caminho de distribuição único não-redundante que serve os equipamentos de TI. • Componentes de capacidade não-redundantes. • Infraestrutura do local básico garantindo disponibilidade 99,671%.
2	• Cumpre todos os requisitos da Camada 1. • Infraestrutura do local com componentes de capacidade redundante, garantindo a disponibilidade de 99,741%.
3	• Cumpre todos os requisitos da Camada 1 e Camada 2. • Múltiplos caminhos de distribuição independente, servindo aos equipamentos de TI. • Todos os equipamentos de TI devem ser dual-alimentados e totalmente compatíveis com a topologia da arquitetura do local • Infraestrutura local paralelamente sustentável, garantindo a disponibilidade de 99,982%.
4	• Cumpre todos os requisitos Camada 1, Camada 2 e Camada 3. • Todos os equipamentos de refrigeração são independentes e dual-alimentados, incluindo os de esfriamento e de aquecimento, ventilação e sistemas de ar-condicionado(HVAC). • Infraestrutura local tolerante a falhas, com instalações de armazenamento e distribuição de energia elétrica, garantindo a disponibilidade de 99,995%.

Quadro 1: Classificação de Datas Centers
Fonte: (TELECO, 2005)

Através dessa abstração de cenário é possível imaginar o quanto é caro um plano de contingência de alto porte, porém esses planos estratégicos são necessários para multinacionais manterem seus serviços sempre ativos durante qualquer distúrbio no planeta terra. Com isso também é possível notar que não é somente uma aplicação ou alocação de um espaço que vem a somar nos números financeiros necessários para o investimento, mas toda a sua infraestrutura.

Durante a fase dois todos os itens devem ser verificados podendo assim definir qual será a melhor situação de acordo com a criticidade de negocio de cada empresa.

Para cada processo crítico devem identificar-se:

- Todos os riscos possíveis de falha.
- A probabilidade de ocorrência de cada falha.
- A duração provável dos efeitos.
- As consequências resultantes da ocorrência de cada falha e os custos inerentes.
- Os limites máximos aceitáveis de permanência da falha, sem ativação da respectiva medida de contingência.

3.3 TERCEIRA ETAPA NA CRIAÇÃO DE UM PLANO DE CONTINGÊNCIA

A fase três consiste na identificação das medidas cabíveis para prevenção, remediação ou total contingência para cada falha, nessa fase são construídos cenários de prováveis falhas para mensurar as aplicações e sistemas.

Durante esse processo, geralmente muitos contratos são revistos com as prestadoras de serviços das empresas, pois empresas de tecnologia podem oferecer serviços melhores ou um suporte de acordo com o contrato.

Consequentemente, nessa fase os testes de possíveis cenários são de suma importância e com isso é definido as ações necessárias para a operacionalização das medidas a serem tomadas conforme quadro 2 (INSTITUTO DE INFORMÁTICA, 1999).

Falha	Medida
Falta de Água	Dependendo do seu impacto no negócio da Organização: - Prever quantidades e formas de armazenamento - Definir critérios de racionamento - Identificar áreas a desativar (por exemplo, cantinas).
Vazamento de Gás	Dependendo do seu impacto no negócio da Organização: - Prever quantidades e formas de armazenamento - Definir critérios de racionamento - Identificar áreas a desativar (por exemplo, cantinas).
Controle Ambiental	Alguns equipamentos carecem, para o seu correto funcionamento, de determinadas condições de temperatura e humidade. Prevendo uma eventual falha nos mecanismos de controle e reposição dessas condições, deve: - Criar-se meios alternativos para fornecer essas condições mínimas de funcionamento - Definir períodos mais curtos de funcionamento no sentido de minimizar a degradação das condições ambientais. - Haver meios de controlar e vistoriar sempre esses dispositivos.
Combate a incêndio	Estes sistemas, se existirem, devem ser colocados em forma de controle manual. Se considerado necessário, prover o eventual reforço de meios mecânicos de combate a incêndio.
Lixo	Numa eventual hipótese de falha na coleta de lixos, devem ser definidas e postas em prática, formas de acondicionar esses lixos, ou mesmo de destruí-los, sem prejuízo para o meio ambiente.
Transportes	Uma eventual falha ao nível dos transportes pode pôr em causa a possibilidade de acesso das pessoas ao seu local de trabalho, inviabilizando desse modo o funcionamento da Organização. Deve, assim, equacionar-se a viabilidade de planejar formas de transporte alternativas, através de meios da própria Organização ou outros. Porém, caso esta falha resulte, por exemplo, de falhas de abastecimento de combustíveis a um nível mais global, um planeamento de contingência da Organização será ineficaz, se não existirem medidas a outro nível que garantam um abastecimento em função das necessidades e prioridades nacionais.
Combustíveis	Este tipo de falha deve ser encarado de forma mais global, uma vez que as medidas para a sua minimização e/ou anulação não poderão ter resposta ao nível de uma Organização isoladamente. Independentemente da ocorrência de qualquer falha devem ser feitas cópias redundantes de toda a informação, incluindo dados, aplicações, sistema

	operativo, SGBD e outros sistemas de gestão em uso. Estas cópias devem ser guardadas em locais diferentes. Deve assegurar-se que, caso estas cópias venham a ser utilizadas, existe sempre, pelo menos, uma cópia fiel de toda a informação no seu estado original. Deve igualmente ter-se o cuidado de efetuar o startup ou começo do sistema passo a passo e monitorar adequadamente o correto funcionamento de cada componente que foi sendo integrada.
Produção de resultados Errados	Definir procedimentos tendentes a verificar a correção da informação produzida.
Dados corrompidos	Definir procedimentos que, a espaços definidos e em momentos cruciais do processamento, permitam verificar a correção e coerência dos dados e decidir pela continuação ou interrupção do processamento.
Falha de um processo	Encarar a hipótese de desenvolver sistemas alternativos (sejam pequenas aplicações minimalistas que possibilitem a execução das funções nucleares do processo, seja através da ativação de processos manuais). - Prever a necessidade de publicação de disposições legais que permitam antecipar ou retardar prazos e datas, nas situações críticas em que não seja previsível pôr em funcionamento mecanismos alternativo.
Falha de um processo (Consumível)	Estimar as necessidades e proceder à aquisição de consumíveis, prevendo, não só eventuais falhas no seu abastecimento, bem como um eventual aumento do consumo destes produtos, na sequência, por exemplo, da ativação de processos alternativos de troca de informação.
Falha nos sistemas central de processamento	Avaliar a possibilidade de recurso a um centro alternativo, próprio, ou de parceria com Clientes ou Fornecedores - Encarar a possibilidade de desenvolver aplicações minimalistas que possam ser executados noutros sistemas (por exemplo, desenvolver um sistema de cálculo alternativo, de emissão de cheques, etc.)
Falha na rede local	Listar as tarefas/atividades afetadas por esta falha e definir formas alternativas de envio e recebimento de informação adequada a cada caso.
Falha dos sistemas	Definir e pôr em prática mecanismos de monitorização que permitam identificar de imediato este tipo de ocorrências - Cortar as comunicações com o exterior, até à reparação da falha.

Quadro 2: Identificação de Falhas e Possíveis Medidas de Contingência.

3.4 QUARTA ETAPA NA CRIAÇÃO DE UM PLANO DE CONTINGÊNCIA

Esta é a última fase na criação de um plano de contingência, é nela onde é criado um sistema de suporte para dar ajuda e prestar atendimento a todo o ambiente criado pelo plano, além de estarem diretamente vinculadas às aplicações acabam também se tornando agente ativo na resposta a um problema.

Após a definição das equipes, os testes são feitos como:

- Acionamentos dos gerentes e pessoas responsáveis de cada área.
- Identificação das medidas cabíveis, mostradas passo a passo no plano de contingência.
- Restauração do sistema e normalização do ambiente.

Para ficar claro e bem definido, a invocação dos processos e quem deverá tomar as ações cabíveis, as regras de criação de um plano de contingência deverão apresentar ou estar inserido dentro do projeto um diagrama de invocação conforme mostrado na figura 8:

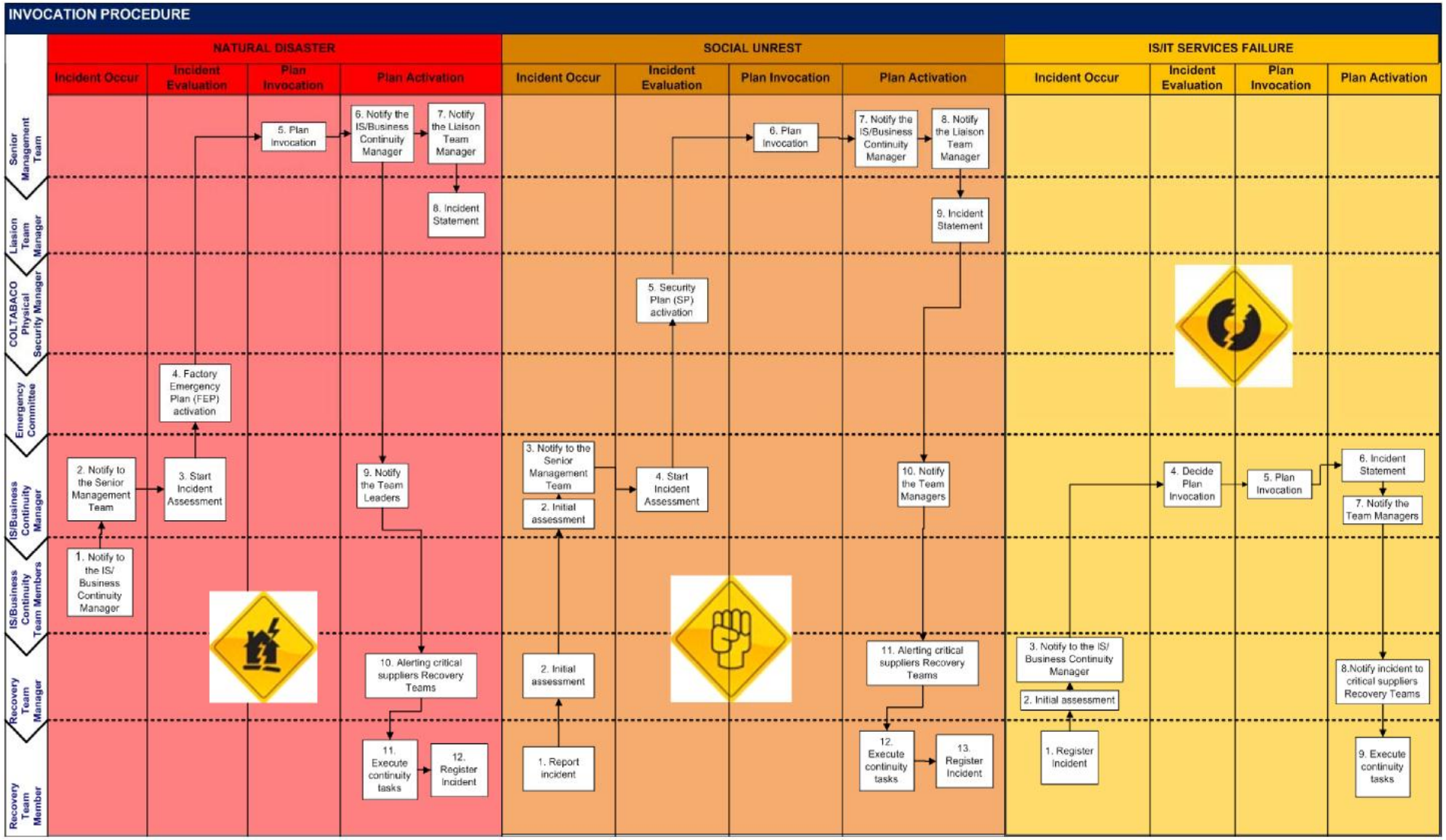


Figura 8: Diagrama de atividades em caso de incêndio, terrorismo e falhas.
Fonte: Autoria Própria

4 RECUPERAÇÃO DE DESASTRE

Diferentemente do Plano de Contingência de Negócios, o *Disaster Recovery* ou Recuperação de Desastres visa apenas a recuperação do ambiente ou negócio, decorrente de uma catástrofe como furacões, vulcões sem medir, por exemplo, os serviços, aplicações, tecnologias e etc.

Porém como a necessidade de haver tanto a parte de desastre natural como a de serviços, o *Disaster Recovery* acaba sempre fazendo parte de qualquer plano.

O quadro 3 á seguir mostra uma série de atividades genéricas que devem ser desempenhadas na invocação de um processo de Recuperação de Desastre para a melhor compreensão de como o processo funciona.

Tarefas	Descrição	Conteúdo	Responsabilidade	Dependências
1	Notificar o Gerente de BCP.	Notificar ao Diretor responsável pelo BCP.	Gerente do BCP	Nenhuma
2	Notificar os Seniors de cada área e aplicação.	Notificar o Gerente Senior sobre a situação	Gerente do BCP	1
3	Começar a descrição e a verificação do incidente.	Identificar a causa e o impacto do incidente	Gerente do BCP E Times de Recuperação de Desastre	2
4	Emergência Plano de Ativação do BCP	O lugar deverá ser colocado em emergência ativando as devidas pessoas responsáveis descritos no BCP.	Emergencial Reunião para decidir se existe a necessidade da invocação do plano.	3

5	Plano de Invocação	Gerente Senior responsável pelos Deve invocar o BCP para a área afetada correspondente de acordo com o negócio.	Gerente Senior	4
6	Notificar todos os empregados	Notificar os times e empregados das áreas afetadas	Gerente Senior	5
7	Gerente de Incidente	Deve prover um prazo de reestabelecimento da normalidade.	Gerente de Incidentes	6
8	Alerta Critico de suprimentos	Provendo quaisquer eventuais fontes de suprimentos.	Time de Recuperação	7
9	Executando as Tarefas de Contingência	Execução de todas tarefas que devem estar escritas no BCP.	Time de Recuperação	8
10	Voltar a normalidade	Registra o incidente, volta a normalidade, e volta o funcionamento complete de todas áreas.	Time de Recuperação	9

Quadro 3: Procedimentos de Recuperação de Desastre
Fonte: Autoria Própria

Á partir do Quadro 3 é possível compreender como funcionam as invocações do plano de contingência de negócios, cada área, cada tarefa devem ser muito bem especificas com o objetivo de dizer com facilidade de entendimento a responsabilidade de cada um.

Com esse tipo de planejamento no escopo do projeto, fica fácil e rápido para agir em caso de eventuais desastres naturais, inclusive contra o terrorismo.

5 PLANO DE CONTINGÊNCIA DE SERVIÇOS

O plano de contingência de serviços basicamente se resume a utilização de aplicações que possam viabilizar e dar suporte a contingência. As aplicações devem ser estritamente pensadas e analisadas, devem ser discutidas com a área técnica a fim de permitir e tornar possível a contingência através de aplicações.

Como sugestões levantadas para contingência de serviços, seram levantada algumas soluções e possibilidades, como:

1) Soluções de Servidores virtuais (*Virtual Machine*, Hyper-V);
2) Soluções de Banco de Dados (SQL Server, Sybase, Oracle);
3) Soluções de acesso remoto;
4) Soluções em Nuvem.

As diferentes soluções podem ser apresentadas de acordo com a estratégia de negócio, essas soluções devem ser mensuradas e testadas em cada empresa a fim de proporcionar a completa ou parcial cobertura de uma aplicações.

5.1 SOLUÇÕES DE SERVIDORES VIRTUAIS

Algumas das soluções desenvolvidas mais importantes dos últimos tempos é a criação de máquinas virtuais que possibilitam a criação de múltiplos servidores em uma mesma máquina.

Uma máquina virtual é um software de ambiente computacional em que um sistema operacional ou programa pode ser instalado e executado. Com isso se torna possível ter um computador e criar múltiplas instancias dentro da mesma (TECMUNDO, 2012).

A máquina virtual irá alocar, durante a execução de sistemas operacionais, uma quantidade definida de memória RAM. Ela normalmente emula um ambiente de computação física, mas requisições de CPU, memória, disco rígido, rede e outros recursos de hardware serão todos geridos por uma “camada de virtualização” que traduz essas solicitações para o hardware presente na máquina. (TECMUNDO, 2012)

As máquinas virtuais são capazes de “enganar” os programas e sistemas operacionais, pois eles acreditam que estão sendo executados diretamente no hardware físico, e não dentro de uma simulação. Por isso, eles podem ser instalados da mesma forma que seriam dentro do sistema operacional. (TECMUNDO, 2012)

Com isso as máquinas virtuais trazem inúmeras vantagens podendo assegurar que as aplicações e serviços atuem de forma singular e separada uma das outras, além da facilidade de deslocamento, cópia e transferência de arquivos.

Aos profissionais que cuidam da parte de gerenciamento, se torna fácil a recuperação dos dados e otimização dos sistemas, já que as máquinas virtuais são altamente mutáveis. Em caso de falta de memória, por exemplo, basta acrescentar mais memória utilizando os recursos da própria máquina virtual.

Mas uma das principais vantagens da máquina virtual é poder testar diversos sistemas operacionais sem precisar particionar o HD. Dessa forma, você poderá instalar versões antigas do Windows, Linux, ou qualquer outro sistema sem fazer alterações no disco rígido. (TECMUNDO, 2012)

A partir disso o termo VM (*Virtual Machine*) tem sido empregado gradativamente nas empresas devido às inúmeras vantagens, algumas empresas se tornaram forte no segmento apresentando soluções de ciência da computação possibilitando ainda mais a convergência de serviços. Os melhores aplicativos para criação de máquinas virtuais no momento são:

a) VMAware;
b) Windows Server Hyper-V;
c) Virtual Box;

5.2 SOLUÇÃO DE BANCOS DE DADOS

Considerando os principais bancos de dados hoje em dia como Oracle, SQL Server, Sybase e DB2 Mainframe é possível dizer que existe um alto investimento para contingência. Isso se deve, pois os bancos de dados geralmente suportam aplicações criticas como transações, aplicativos que precisam comitar acessos e ainda questões de segurança, parte financeira, RH entre outros de uma corporação inteira.

Devido a essa criticidade, empresas como Oracle, IBM e Windows vem criando diversas possibilidades de contingência, conceitualmente as soluções são muito parecidas.

Uma das principais características dos bancos de dados é a utilização de *Fail Over Cluster* que basicamente significa um nó para precaver falhas. Os Failovers são sistemas que compreende dois ou mais computadores ou sistemas no qual trabalham em conjunto para executar aplicações ou tarefas(MICROSOFT, 2012).

Segue a demonstração na Figura 9:

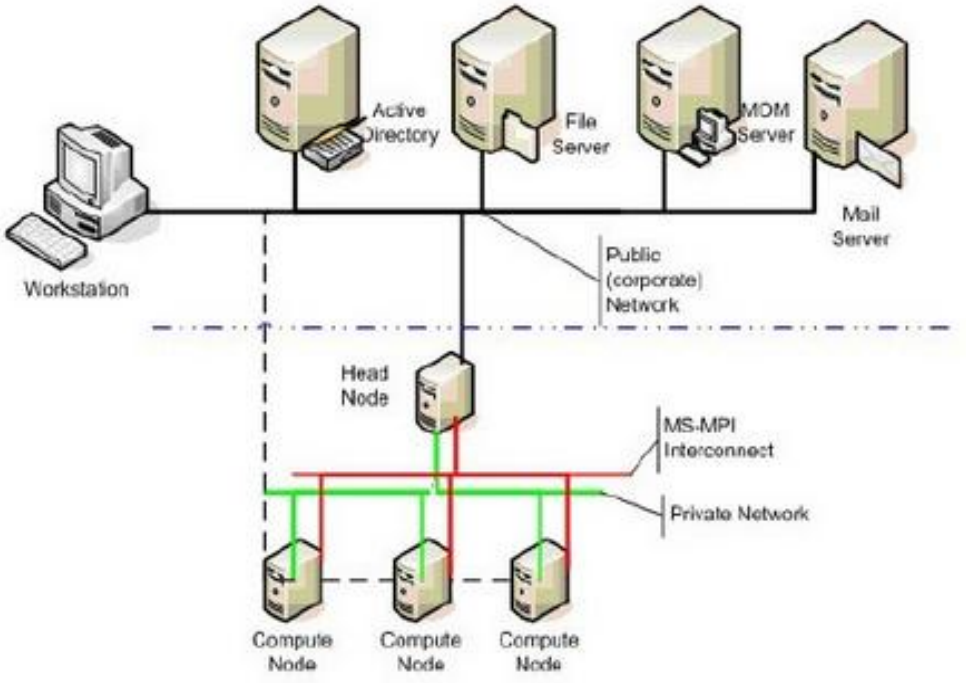


Figura 9: Fail Over Clusters – Sistemas de nós
Fonte: (MICROSOFT, 2012)

Além da contingência que os clusters podem proporcionar, os bancos de dados o utilizam por questões performáticas, em bancos de dados existem três tipos de clusters: (MICROSOFT, 2012)

a) *Shared All* – Onde a memória e os discos são compartilhados por cada nó;
b) *Shared Disc* – Onde apenas os discos são compartilhados pelo nó do cluster;
c) *Shared Nothing* – Onde cada nó tem a sua própria memória e discos.

Na figura 10 é demonstrado como funcionam os nós de *Cluster (*Desambiguação*)*:

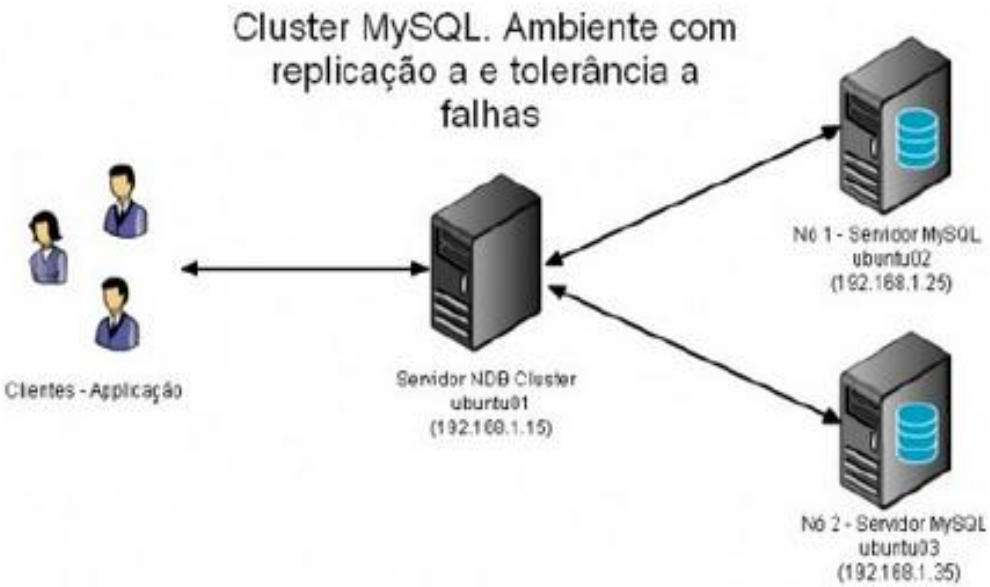


Figura 10: Replicação de Nós
Fonte: (MICROSOFT, 2012)

Além disso, outras solução que se tornou possível com a implementação de *clusters* é as replicações de dados que nada mais é que concentrar os dados em um lugar e replicar para os demais conforme a figura 11:

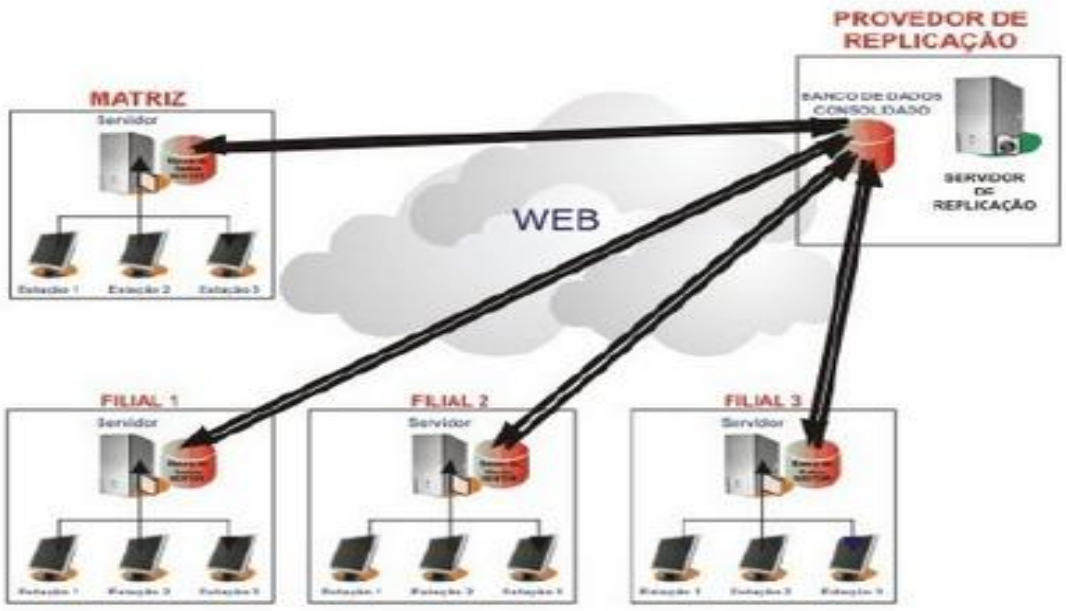


Figura 11: Replicação de Dados
Fonte: (ABASESUL, 2012)

Existem quatro tipos de replicação:

1) Replicação síncrona: onde todas as réplicas possuem sempre os mesmos dados;
2) Replicação assíncrona: onde as réplicas podem ser sincronizadas depois que uma alteração nos dados é feita;
3) Replicação MultiMaster: onde é possível realizar leitura e gravação em qualquer réplica;
4) Replicação Master/Slave: onde apenas a réplica master permite gravação, enquanto as demais réplicas só permitem leitura.

Uma outra solução tecnológica foi criada pela Microsoft, o conceito de *mirroring* ou no português espelhamento. Essa técnica nada mais é que repetir os dados de um servidor em outro.

Um dos servidores ficará atualizando o outro, um terceiro servidor atuará em modo witness que significa testemunha, assim que o servidor principal cair ou sofrer algum problema o servidor dois é levantado automaticamente trazendo contingência para o serviço em 50ms aproximadamente conforme mostrado na figura 12:

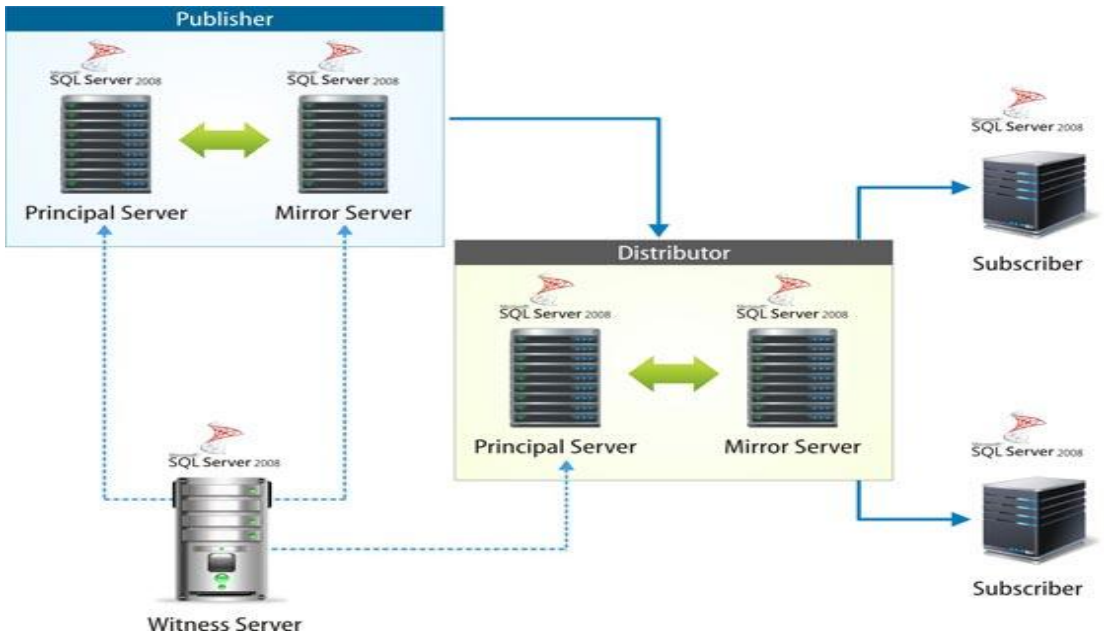


Figura 12: Modo Mirroring
Fonte: (MICROSOFT, 2012)

5.3 SOLUÇÕES DE ACESSO REMOTO

Mais uma vez se tratando de contingência algumas soluções se mostram altamente aplicáveis e exercidas na maioria das multinacionais, o *home office* ou trabalhar em casa por exemplo. O termo é empregado para tipos de trabalhos onde não é preciso um lugar físico, porém se tratando de contingência, os empregados das multinacionais costumam acessar suas máquinas de casa.

Devido ao atual mercado e através da experiência profissional, as empresas investem pouco para ter esse tipo de contingência, se mostrando altamente promissor, os custos para tal implementação se mostra com um alto custo beneficio.

Alguns dos aplicativos mais utilizados para tal acesso são:

1) Citrix – Aplicativo utilizado para conexão remota, possibilidade de acesso por tablets e celulares;
2) Remote Desktop da Microsoft – conexão através de ip com a sua máquina física, porém é necessário a máquina física estar ligada e operante.

5.4 SOLUÇÕES EM NUVEM

Computação nas nuvens é essa a tradução para o termo *Cloud Computing*. O princípio segue a linha do armazenamento de dados e informações na internet, acessível, assim de qualquer ponto. Por isso a utilização da palavra nuvem. Entenda as vantagens e benefícios que a Cloud Computing pode agregar.

Computação nas nuvens (*Cloud Computing*) é todo o conceito que se tem hoje do que é computação (processamento, armazenamento e softwares) só que dessa vez armazenado na rede, podendo ser acessado remotamente através da internet. É como dizer que a rede é um grande computador (SISNEMA, 2009).

Existem quatro tipos de implementações de nuvem: (ALECRIM, 2013).

1) Privado - As nuvens privadas são aquelas construídas exclusivamente para um único usuário (uma empresa, por exemplo). Diferentemente de um data center privado virtual, a infraestrutura utilizada pertence ao usuário, e, portanto, ele possui total controle sobre como as aplicações são implementadas na nuvem;

2) Público - As nuvens públicas são aquelas que são executadas por terceiros. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento, o que pode parecer ineficiente a princípio. Porém, se a implementação de uma nuvem pública considera questões fundamentais, como desempenho e segurança, a existência de outras aplicações sendo executadas na mesma nuvem permanece transparente tanto para os prestadores de serviços como para os usuários;

3) Comunidade - A infraestrutura de nuvem é compartilhada por diversas organizações e suporta uma comunidade específica que partilha as preocupações (por exemplo, a missão, os requisitos de segurança, política e considerações sobre o cumprimento). Pode ser administrado por organizações ou por um terceiro e pode existir localmente ou remotamente;

4) Híbrido - Nas nuvens híbridas temos uma composição dos modelos de nuvens públicas e privadas. Elas permitem que uma nuvem privada possa ter seus recursos ampliados a partir de uma reserva de recursos em uma nuvem pública. Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja flutuações rápidas na necessidade dos recursos. A conexão entre as nuvens pública e privada pode ser usada até mesmo em tarefas periódicas que são mais facilmente implementadas nas nuvens públicas.

Com esse tipo de tecnologia, algumas vantagens vêm se mostrando promissoras e muito atraentes como é mostrado abaixo (ALECRIM, 2013).

- O usuário não precisa se preocupar com o sistema operacional e hardware que está usando em seu computador pessoal, podendo acessar seus dados na "nuvem computacional" independentemente disso;

- As atualizações dos softwares são feitas de forma automática, sem necessidade de intervenção do usuário;
- O trabalho corporativo e o compartilhamento de arquivos se tornam mais fáceis, uma vez que todas as informações se encontram no mesmo "lugar", ou seja, na "nuvem computacional";
- Os softwares e os dados podem ser acessados em qualquer lugar, bastando que haja acesso à Internet, não estando mais restritos ao ambiente local de computação, nem dependendo da sincronização de mídias removíveis.
- O usuário tem um melhor controle de gastos ao usar aplicativos, pois a maioria dos sistemas de computação em nuvem fornece aplicações gratuitamente e, quando não gratuitas, são pagas somente pelo tempo de utilização dos recursos. Não é necessário pagar por uma licença integral de uso de software;
- Diminui a necessidade de manutenção da infraestrutura física de redes locais cliente/servidor, bem como da instalação dos softwares nos computadores corporativos, pois esta fica a cargo do provedor do software em nuvem, bastando que os computadores clientes tenham acesso à Internet.

6 VISÃO ESTRATÉGICA DE MERCADO

A visão estratégica do mercado não é algo tão fácil e previsível, a análise fria do mercado e vivência nesse meio pode trazer uma visão clara da utilização e necessidade do Plano de Contingência de Negócios e basicamente é levado em conta o custo beneficio que um plano pode trazer.

Conforme foram citados ao longo do trabalho, inúmeras vantagens podem ser observadas a maioria demanda de um alto custo, mas a implementação de tal serviço permite o aumento da credibilidade empresarial e a estrutura montada pode permitir um crescimento ainda maior.

Devido à vivência com esses projetos, é possível dizer que praticamente 100% das multinacionais aplicam esse tipo de plano e que isso ocorre devido ao Business entender ou compreender a necessidade do BCP para assegurar seus lucros. Outro fator importante, porém escondido é o mercado de ações que torna a empresa com tal planejamento mais rentável.

Essa rentabilidade se deve ao fato de haver uma maior segurança em empresas que possuem esses planos, a chance de problemas externos impactarem os serviços internos é relativamente menor se compararmos com outras que não possuem o serviço.

Não foram encontrados estudos que mostrem a diferença percentual entre empresas que possuem ou não o BCP, mas através da experiência nesse mercado, cerca de mais de 60%. O impacto nos negócios basicamente vem dessa necessidade constante de segurança, o mercado acionista exige o BCP nas multinacionais e por esse motivo o plano de contingência se tornou mandatório nas grandes empresas e hoje em dia é uma prática comum.

Pequenas empresas investem pouco em soluções tecnológicas, mas que podem ser altamente lucrativas, a infinidade de serviços que podem prover a contingência de qualquer lugar e a qualquer momento é enorme.

O mercado atual é muito dinâmico e empresas que não possuem essa visão de mercado acabam falindo, o mercado além de dinâmico é competitivo deixando uma

margem pequena para erros. Esse dinamismo torna tudo muito competitivo e soluções tecnológicas por meios de aplicativos acabam suprindo certa necessidade.

É muito falado de computação em nuvem e tudo parece convergir a esse novo meio de tecnologia principalmente devido as suas características como a interatividade, facilidade e ambientes intuitivo contribuindo para aquisição do mesmo. Ao mesmo tempo em que isso acontece, outra questão importante é levantada.

Muito se fala em segurança da informação e a pergunta que todos vêm fazendo é: Será que devemos colocar dados e informações tão importantes na nuvem de outras grandes empresas e muitas vezes concorrentes como Google, Microsoft?

Será que uma empresa que quer sair na frente do mercado pode olhar os dados de outra empresa?

Com isso acabamos voltando em um assunto muito antigo, a ética pode ser algo difícil de encontrar quando se fala de dinheiro e valores das ações. A competição entre empresas pode ser maléfica em muitos pontos e a ética nem sempre prevalece, toda essa visão de mercado está acontecendo nesse momento e muitos tem medo por não saber o desfecho dessa história.

7 CONSIDERAÇÕES FINAIS

O mercado atual é altamente competitivo e o BCP é aplicável na maioria das multinacionais visando à continuidade do lucro e diminuição no impacto de ações externas como terrorismo e alterações climáticas, o exemplo das multinacionais devem ser passadas as pequenas empresas. A empregabilidade do BCP não deve ser questionada pelo custo, mas sim pelo conceito.

A ideia ou conceito que o BCP prega pode ser feita através de novas soluções tecnológicas demonstradas ao longo do trabalho, trazendo uma possibilidade real para pequenas empresas de investirem em aplicações que possibilitem a contingência em si e com isso melhorando em questão de rentabilidade e investimento.

O planejamento não deve ser visto como perda de tempo e sim como investimento para o futuro dos negócios e mesmo visando o lucro as empresas que seram lembradas são aquelas que possuem dignidade e ética.

Acredito que a partir disso é possível que empresas pequenas possam se basear nos conceitos que os Planos de Contingências podem trazer para a empresa e fica claro o ganho que a empresa pode ter com isso. A necessidade de negócio permite que esse tipo de investimento se torne prática comum.

É possível que no futuro esse trabalho possa servir como base a pessoas que queiram contingência no Brasil a fim de sanar problemas críticos em situações como deslizamentos, chuvas e etc.

REFERÊNCIAS

ABASESUL. **Replicação de Dados** 2012. < http://www.abasesul.com.br/Conteudo/Index/?id=2&idSM=7> Acesso em: 24 de outubro de 2013.

ALECRIM, Emerson. **O que é cloud computing?** 2013. <http://www.infowester.com/cloudcomputing.php> Acesso em: 13 de agosto de 2013.

AMARO, Mariza de O. S. **Sua organização está preparada para uma contingência? Programa de Pós-Graduação de Engenharia de Sistemas e Computação**: UFRJ, 2004. Disponível em: <https://www.mar.mil.br/sdms/artigos/6816.pdf>. Acesso em 21 de junho de 2006.

AT&T. **Business Continuity Plans**. 2013. Disponível em: <http://www.corp.att.com/latin_america_pt/docs/20050517-1-pt.pdf>. Acesso em: 13 de Junho de 2013.

AUSTIN, G. e Colaboradores (2000). **Certified Information System Auditor Review Technical Information Manual**. Rolling Meadows, Illinois. Information Systems Audit and Control Association, Inc.

INSTITUTO DE INFORMÁTICA. **Planos de Contingência de Mercado**. 1999. Disponível em: <http://www.inst-informatica.pt/o-instituto/factos-historicos/publicacoes/guias-tecnicos/ano2000.pdf>. Acesso em: 14 de Junho de 2013.

MARSH EUROPEAN. **As vantagens de ter um Plano de Continuidade de Negócios**. 2008. Disponível em: <http://www.marsh.pt/documents/EstudodaMarshEuropeu.pdf>. Acesso em:26 de Setembro de 2013.

MICROSOFT. **Overview of Fail Over Clusters** 2012. <http://technet.microsoft.com/en-us/library/hh831579.aspx> Acesso em: 13 de agosto de 2013.

REMMERS, Vanessa. **Disaster Recovery Plan Template** 2012. < http://www.disasterrecoveryplantemplate.org/author/m0j0admin/> Acesso em: 24 de outubro de 2013.

SENAC. **Plano de Contingência de Negócios**. 2011. Disponível em: <http://www.facsenac.edu.br/portal/images/documentos/facinfo/plano-contigencia-ti-reagir-desastres.pdf>. Acesso em: 13 de Junho de 2013.

SILVA, W Lopes. **Etapas de elaboração de um plano de contingência para a área de tecnologia da informação em âmbito corporativo.** 2006. Disponível em: <http://www.centropaulasouza.sp.gov.br/pos-graduacao/workshop-de-pos-graduacao-e-pesquisa/anais/2006/comunicacao-oral/gestao-e-desenvolvimento-de-tecnologias-da-informacao-aplicadas/SILVA,%20W.%20Lopes%20da.pdf>. Acesso em: 17 de junho de 2013.

SISNEMA. **Cloud Computing - novo modelo de computação** 2009. <http://sisnema.com.br/Materias/idmat019433.htm> Acesso em: 13 de agosto de 2013.

TECMUNDO. **O que são máquinas virtuais?** 2012. <http://www.tecmundo.com.br/maquina-virtual/232-o-que-sao-maquinas-virtuais-.htm> Acesso em: 12 de agosto de 2013.

TELECO. **Data Center I: Classificações e Normas de Data Centers** 2005. < http://www.teleco.com.br/tutoriais/tutorialdcseg1/pagina_2.asp> Acesso em: 24 de outubro de 2013.

UPDATE INSTITUE. **Data Center Site Infrastructure Tier Standard: Topology** 2006. <http://www.tiaonline.org/standarts> Acesso em: 17 de junho de 2013.

WALLACE, Michael; WEBBER, Lawrence. **The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets**. New York: Amacom Books, 2004.

WATKINS, John. **Justifying the Contingency Plan**. 1997. Disponível em: <http://www.drj.com/new2dr/w2_011.htm>. Acesso em: 14 de junho de 2013.

GLOSSÁRIO

Cloud Computing – Computação na nuvem, utilização de um sistema pela internet incluindo sistema operacional e aplicativos.

Continuidade do Negócio - Continuidade do negócio é o processo pró-ativo de planeamento que assegura que uma organização pode sobreviver a uma crise organizacional, com identificação das funções chave e das possíveis ameaças a essas funções e da continuação das mesmas independentemente do desenrolar das circunstâncias.

Disaster Recovery - processo que, durante uma crise organizacional, tem lugar no sentido de minimizar a interrupção do negócio.

***Firmware* -** Software embebido em chips de memória que permite que a informação se mantenha mesmo com o equipamento desligado (por exemplo, o BIOS dos computadores pessoais).

Métricas - Medidas com que se podem avaliar os processos, recursos e produtos.

Plano de Contingência - No contexto geral é um plano para fazer face à perda ou à deterioração dos serviços essenciais devidos á um problema num sistema automatizado. De forma geral, um plano de contingência descreve as medidas que uma empresa deve tomar incluindo a ativação de processos manuais ou o recurso a contratos, para assegurar a continuidade dos seus processos de negócio essenciais no caso de uma falha no sistema.

Processo - Cadeia (sequencial, cíclica, intermitente ou descontínua) de operações - ações e decisões - executadas para gerar um produto.