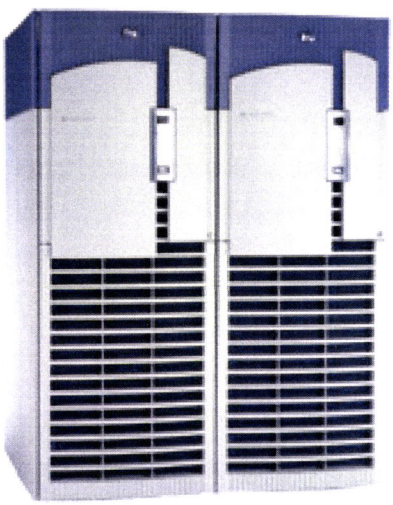
Universidade de Évora

Departamento de Gestão de Empresas
Mestrado em Organização e Sistemas de Informação

Dissertação de Mestrado

Gestão da Continuidade



Um guia para a protecção dos Sistemas de Informação

Apresentada por
Lic° Nuno Ricardo Azevedo Silva Jardim

Orientador
Professor Doutor António Serrano

Évora 2004

Esta dissertação não inclui as críticas feitas pelo júri

Gestão da Continuidade

Um guia para a protecção dos Sistemas de Informação

Dissertação apresentada à
Universidade de Évora
para a obtenção do grau de
Mestre em Organização e Sistemas de Informação

Orientador
Professor Doutor António Serrano

Évora
2004

Esta dissertação não inclui as críticas feitas pelo júri

Agradecimentos

A presente obra não teria sido possível sem a contribuição de inúmeras pessoas.

Gostaria de deixar de forma bem vincada a minha mais profunda gratidão para com o Professor Doutor António Serrano, pelo excepcional apoio, incondicional disponibilidade e, sobretudo, pela sua soberba orientação.

O meu reconhecimento vai também para o Professor Doutor Carlos Zorrinho e Professora Doutora Palmira Lacerda pelas suas contribuições generosas na prossecução dos objectivos a que me propus atingir no decorrer do Mestrado.

Não posso deixar de agradecer a todos os meus colegas e restantes docentes pelo estimulo e amizade que sempre me dispensaram.

Tenho que agradecer à minha expressão viva, pois foi também ela responsável pelo presente sucesso.

Aos meus pais e irmão aqui fica a minha especial palavra de gratidão por tudo o que por mim sempre fizeram. Em especial uma palavra de carinho para com o meu ascendente que sem a sua empenhada contribuição cognitiva este trabalho não teria sido possível.

Um reconhecimento especial para a invent que continua a dar grandes lições de cultura organizacional e a demonstrar que é a melhor das organizações onde é meu privilégio colaborar.

A todos desejo uma longa e prospera vida com muita saúde.

Bem hajam.

Évora, Out. 2004

Resumo

A Gestão da Continuidade expande-se por todas as unidades de negócio da organização, incluindo o departamento de Tecnologias de Informação, e muitas vezes estende-se para além das fronteiras organizacionais, de forma a incluir parceiros tecnológicos.

No que diz respeito aos Sistemas de Informação o planeamento de Gestão da Continuidade do negócio requer o desenvolvimento e implementação de procedimentos e tecnologias alternativas de forma a assegurar que a informação crítica para a organização continua sempre disponível e que as funções críticas da organização são rapidamente restauradas, quando ocorrerem interrupções súbitas e imprevistas, nas quais é negado o acesso à informação.

Os procedimentos de recuperação devem ser definidos de forma a gerir os colaboradores da organização, assegurando a sua segurança e preparando-os para executarem todos os procedimentos alternativos, num Centro de Processamento de Dados redundante, equipados com os Sistemas de Informação e Comunicação necessários para a reposição da capacidade operacional da organização.

A protecção da informação e a recuperação de desastres são os pontos chave na Gestão da Continuidade do negócio, temas desenvolvidos ao longo da presente dissertação.

A protecção da informação refere-se à componente de desenvolvimento e implementação de sistemas, procedimentos e soluções que asseguram o acesso contínuo à informação dentro da organização. O processo de recuperação de desastres engloba todos os procedimentos complementares de forma a garantir que os Sistemas de Informação, as aplicações críticas e a informação são restaurados de forma rápida e eficaz em caso de ocorrência de um evento com impacto negativo na organização.

Abstract

Nunca antes a disponibilidade da informação e aplicações foi de tão vital importância, e, consequentemente, nunca antes a prática disciplinada da Gestão da Continuidade foi tão crítica para o sucesso organizacional - e sua sobrevivência. As forças sociais e de negócio do séc. 21 fazem com que o acesso imediato à informação seja uma necessidade crítica para qualquer organização. Desenvolvimento de produtos para suporte da informação, vendas de combustível e marketing optimizam a produção fazendo a ponte na relação com os clientes. Consequentemente, os armazéns de informação continuam a expandir, enquanto cada vez mais colaboradores trabalham fora das paredes organizacionais e o comércio local alcança as fronteiras regionais e internacionais, transformando um simples dia de negócio num *continuum intemporal.*

Never before has the availability of data and applications been so vitally important and, consequently, never before has the disciplined practice of Managed Availability been so critical to business success - and survival. The business and social forces of the 21st century have made ready access to information a critical necessity for any organization. Data supports product development, fuels sales and marketing, optimizes production and bridges customer relationships. Consequently, data stores continue to expand, while more employees work outside corporate walls and even local commerce reaches across regional and international boundaries, transforming the business day into a timeless continuum.

Palavras Chave / Key Words

Alta Disponibilidade, High Availability

Gestão da Continuidade, Business Continuity Management

Planeamento Recuperação de Desastres, Disaster Recovery Plan

Sistemas de Informação, Information Systems

Índice

I – Introdução

1.1 Escolha do Tema

O presente opúsculo pretende reunir um conjunto de orientações e criar uma metodologia no que diz respeito a uma temática cada vez mais importante para a sobrevivência das organizações, a Gestão da Continuidade.

O tema da presente dissertação, no âmbito do Mestrado de Organização e Sistemas de Informação, tem como objectivo fundamental levar o conhecimento a todos os que se interessam pela presente temática e contribuir de forma modesta para suscitar uma reflexão nos quadros de mudança e estratégia global das organizações.

"Não estou interessado no futuro.
Estou interessado no futuro do futuro."

Robert Domiger, 1996

1.2 Problema

Avaliação da necessidade de uma Gestão da Continuidade

A maioria das pessoas pensa imediatamente em fogos, inundações ou terramotos como casos de desastre, mas um desastre do ponto de vista organizacional interagindo com os Sistemas de Informação, pode ser qualquer evento que de uma forma súbita interrompa um serviço ou corrompa os dados em toda a estrutura de um Centro de Processamento de Dados, uma incursão que escava profundamente e danifica toda uma estrutura de rede e comunicações, ou mesmo um acto de plena sabotagem.

Segundo Weygant (2001) uma arquitectura tolerante a desastres deve proteger os Sistemas de Informação contra a indisponibilidade aplicacional não planeada e contra possíveis interrupções de serviços, na forma de uma implementação redundante na qual é efectuada uma distribuição dos nós/sistemas de um *cluster* de tal maneira que na eventualidade de um desastre no Centro de Processamento de Dados principal os restantes componentes do *cluster,* integrados no ambiente tolerante a desastres não são afectados.

Para se avaliar a necessidade de uma solução de Recuperação de Desastres *(Disaster Recovery)* é necessário pesar-se os seguintes factores:

- **Riscos de desastre** - Áreas propícias a tornados, inundações, fogos ou terramotos requerem por excelência uma solução de recuperação de desastres. Algumas indústrias devem considerar riscos adicionais que não apenas os desastres naturais ou acidentes tais como as actividades terroristas e sabotagens.

  O tipo de desastre ao qual uma organização está sujeita, quer seja devido à sua localização geográfica ou natureza do seu negócio, irá determinar qual o conjunto de soluções de recuperação de desastres que a organização deverá implementar. Se a organização estiver localizada numa região sujeita a terramotos, como por exemplo algumas zonas no Japão, a organização não deverá colocar todos os seus sistemas alternativos ou nós de backup na mesma cidade onde estão localizados os nós primários do cluster dado que este tipo de desastre poderá afectar toda uma vasta área geográfica metropolitana.

  A frequência do tipo de desastre também desempenha um papel importante ao se determinar o tipo de solução de recuperação de desastres. Uma organização mais depressa se protege contra um possível tornado, que poderá ocorrer numa determinada época do ano, do que se protege contra um vulcão que não entra em actividade à mais de 100 anos.

- **Vulnerabilidade do negócio** – Qual o período de tempo em que uma organização se consegue manter indisponível? Algumas unidades de negócio da organização podem voltar à produção ao fim de um ou dois dias de interrupção dos serviços. No entanto outras deverão regressar à produção numa questão de minutos! Desta forma algumas componentes da organização apenas necessitam de protecção local contra pequenas falhas de sistemas, enquanto que as componentes organizacionais críticas precisam não só de protecções contra falhas locais como também de protecção no caso de falha de um Centro de Processamento de Dados completo.

É de suma importância considerar-se o papel dos Centro de Processamento de Dados no contexto da organização.

Uma determinada organização poderá no entanto considerar todos os servidores de produção da sua linha de montagem como sendo os mais críticos para o negócio e definir que os mesmos precisam de protecção contra um determinado desastre. Mas se o desastre mais provável de ocorrer na área geográfica onde a organização está situada for um terramoto, iria colocar fora de produção não só os servidores da linha de montagem como a própria linha de montagem. Verifica-se então que neste tipo de cenário um plano de recuperação de desastres não será eficaz, a não ser que contemple uma nova linha de montagem num site alternativo e remoto e que um *failover* local poderá ser um nível de protecção mais adequado a esta situação.

Por outro lado se uma organização tem um centro de processamento de encomendas que se situa numa zona geográfica propícia a inundações no inverno e a mesma organização perde milhares de dólares por minuto enquanto os seus sistemas de processamento de encomendas estão indisponíveis, verifica-se que uma solução de recuperação de desastres é a mais apropriada neste tipo de situação.

A rápida mudança nas organizações é uma nova norma. A maneira como as organizações operam está a evoluir à medida que novas e melhores tecnologias ficam disponíveis.

Segundo Sikich (2003) a habilidade para responder de forma eficaz na gestão das interrupções de serviço de forma atempada é agora um factor decisivo na sobrevivência de uma organização. A decisão de se implementar uma solução de recuperação de desastres deve assim depender do balanço entre o risco de ocorrência de determinados tipos de desastres e a vulnerabilidade do negócio no caso da sua ocorrência.

Dados estatísticos que justificam uma análise do problema

O comércio electrónico tornou imperativo a total disponibilidade do negócio e respectivos serviços. Caso contrário a organização poderá sofrer graves implicações - perdas de revenues, diminuição da credibilidade no mercado, desvalorização das acções e da produtividade. Notícias de organizações que perdem milhões de dólares na capitalização de mercado em poucas horas ou em poucos dias devido a falhas nas plataformas de e-Commerce são comuns nos nossos dias.

As estatísticas do U.S. Bureau of Labor (2002) mostram que das companhias que sofrem um desastre convencional apenas 6% sobrevivem a longo prazo, 43% nunca voltam ao activo e 51% acabam por fechar em menos de dois anos.

A seguinte tabela gerada a partir de pesquisas conduzidas pelo grupo Contingency Planning Research e Contingency Planning & Management apresenta valores interessantes do ponto de vista de custo hora/downtime:

Industry	Application	Average cost per hour of downtime (US$)
Financial	Brokerage	$ 7,840,000
Financial	operations	$ 3,160,000
Media	Credit card sales	$ 183,000
Retail	Home shopping (TV)	$ 137,000
Retail	Catalog sales	$ 109,000
Transportation	Airline reservations	$ 108,000
Entertainment	Tele-ticket sales	$ 83,000
Shipping	Package shipping	$ 34,000
Financial	ATM fees	$ 18,000

fonte: Contingency Planning Research (2002)

Hoje em dia estes valores estão naturalmente agravados.

De acordo com Musaji (2001) o aumento dos lucros na nossa economia é imposto com base nas novas soluções dos Sistemas de Informação e serviços. Na sua opinião os diferenciadores chave são os factor de especialização, motivação e os colaboradores "de ponta" que no seu conjunto determinam a capacidade de competitividade e o crescimento das organizações. Este crescimento está directamente associado a um nível de satisfação dos clientes cuja lealdade é a fundação para o sucesso.

Mas antes do dia 11 de Setembro 2001, NY verifica-se que muitos dos *senior managers* encontravam-se cépticos acerca do investimento na Continuidade do negócio, *(Business Continuity)*. Neste momento todos entendem a gravidade da situação e os riscos associados e preocupam-se com as suas capacidades de sobrevivência organizacional. Do ponto de vista de algumas organizações a Gestão da Continuidade do negócio não é mais uma opção ou um luxo mas sim uma maneira de se negociar e de se estar no mercado. A Gestão da Continuidade pronuncia a diferença entre a organização que se mantém

activa, em produção versus a que tem que encerrar as actividades por incapacidade de sobrevivência.

Desta forma o planeamento para a Gestão da Continuidade deverá ser diligente e parte integrante das responsabilidades dos *Business Managers* contemporâneos. Também deverá existir a consciência adquirida através dos contínuos *merges* e aquisições dos nossos dias de que um programa válido para a Continuidade do negócio é normalmente uma peça importante das negociações, se não mesmo um requisito obrigatório.

A Gestão da Continuidade não deve ser vista como uma proposição do estilo tudo ou nada dado que mesmo o mais pequeno dos esforços, tal como o armazenamento de *backups* num *site* remoto, pode num determinado momento poupar à companhia valores muito significativos em termos de potenciais perdas. Determinadas soluções de Continuidade oferecem às organizações um conjunto completo de soluções que vão desde a replicação por *hardware* dos dados mestres para as organizações, passando pela computação *fault-tolerant* até à infra-estrutura completamente redundante.

As referidas soluções integram invariavelmente toda a fase de arquitectura e desenho das soluções, fases de implementação e suporte contínuo em produção. De acordo com os dados existentes no mercado internacional dos Sistemas de Informação existem soluções que abrangem múltiplas áreas da continuidade tais como as soluções integradas de Alta Disponibilidade *(High Availability)* para todas as vertentes *UNIX* em distintos ambientes *Non-Stop Computing*.

As soluções devem de um modo claro:

- Identificar e minimizar todos os possíveis riscos nas áreas chave do negócio e utilizarem as melhores práticas e tecnologias na indústria.
- Medir o impacto de downtime no negócio para se determinarem os níveis óptimos de investimento e respectivas localizações.
- Determinar estratégias de continuidade para os processos individuais do negócio, sobre os vários cenários possíveis: Tecnologias IT que suportam as estratégias óptimas de modo económico, desenvolvimento das infra-estruturas e implementações que suportem os processos críticos ao negócio e as operações críticas para uma recuperação em *"modo de sobrevivência"*.
- Regressar ao *"business as usual"* .

1.3 Objectivos

No decorrer da presente dissertação verifica-se a oportunidade de abordar o tema da alta disponibilidade dos Sistemas de Informação, e as várias soluções tolerantes a falhas e em conjunto integrar e documentar a problemática da Gestão da Continuidade dado que os temas encontram-se interligados.

Desta forma o tema central da tese de mestrado integra não só a alta disponibilidade de um ponto de vista científico na gestão dos *clusters mission critical* bem como referencia a necessidade e predisposição da Continuidade do negócio em termos organizacionais. Com a presente tese de mestrado irá ser proposta uma metodologia para a implementação da Continuidade no negócio e criado um manual de referência que aborda o tema da criticidade de negócio e os meios existentes no mercado internacional dos SI´s/TIC´s para a reposição dos serviços e sistemas considerados críticos pelas organizações.

Será criado um modelo de referência na Gestão da Continuidade e definido um conjunto de processos que possibilitam às organizações manterem-se activas assegurando a capacidade operacional de toda a infra-estrutura e informação crítica em caso de eventos adversos com impactos significativos para a produção (calamidades físicas, sabotagens, desastres naturais, etc.).

Será proposta uma metodologia que considera um contínuo ciclo de avaliação, planeamento, implementação e suporte que deve integrar toda a tecnologia e conjunto de serviços necessários por forma a garantir o funcionamento das plataformas nas situações mais adversas.

Durante a tese será igualmente demonstrado que a Gestão da Continuidade do negócio não é apenas uma peça específica de tecnologia, produtos ou serviços, nem consiste numa implementação específica de alta disponibilidade, recuperação de desastres ou numa solução tolerante a falhas, mas sim um conjunto de processos distintos e integrados que permitem à organização a sua sobrevivência!

1.4 Metodologia

Para alcançar os objectivos pretendidos com a presente dissertação foram efectuadas investigações a diversos níveis sendo a fase de análise a mais crítica para o seu desenvolvimento.

A investigação consistiu num estudo bibliográfico detalhado do funcionamento dos processos de Gestão da Continuidade do negócio em análise e das diversas soluções e arquitecturas de Sistemas de Informação existentes para os ambientes críticos.

A fase complementar passou por diversas etapas onde a experiência profissional foi dos factores determinantes para a elaboração do presente trabalho.

1.5 Resultados Esperados

Como resultados ao abordar o tema da Gestão da Continuidade, no seu conjunto de processos organizacionais, pretende-se demonstrar que a integração destes temas não são uma proposição do estilo "tudo ou nada", mas antes de mais um espectro de processos que abrangem todas as melhores práticas de uma indústria. Tais como rotinas diárias de *backups*, onde as *tapes* são armazenadas de forma segura em salas protegidas, bem como as diversas arquitecturas e os diversos planos em grande escala de Continuidade do negócio, que podem invocar não só um sistema em *standby* como também activar processos internos com a utilização de sistemas alternativos e Centros de Processamento de Dados geograficamente dispersos.

Pretende-se também definir ao longo da presente tese de Mestrado uma metodologia que possibilita validar que as soluções de Continuidade do negócio garantem às organizações a continuidade operacional seja qual for a situação existente, que podem ser desde falhas aplicacionais a problemas com a operação dos sistemas, falhas de segurança ou mesmo desastres em grande escala. As soluções propostas devem ser aplicadas no processamento de unidades de negócio críticas para as organizações. Apenas como referência alguns exemplos de unidades críticas de negócio, dependendo das organizações, são os centros de processamento de facturação e sistemas de *home banking*.

Ao longo da presente tese de Mestrado vão ser sugeridos métodos de gestão aplicacional que providenciam soluções integradas que permitem às organizações minimizar os riscos de *downtime* bem como possibilitar a recuperação dos serviços de forma rápida, segura e em tempo útil, com o objectivo principal da organização regressar às operações de uma forma transparente e sem grandes sobressaltos para o utilizador final.

II – Gestão da Continuidade

2.1 Âmbito e impacto

De acordo com Varghjese (2002) o Homem tentou sempre evadir-se das forças da natureza e da destruição que causam. A industrialização e o rápido avanço tecnológico conduziram a novas ameaças e um tremendo aumento das suas capacidades de impacto. Como tal, o Homem desenvolveu estratégias para ultrapassar ou minimizar esses impactos e os esforços tem sido canalizados para o planeamento de desastres.

Alias, o planeamento de contingência tem estado junto da humanidade desde que os Faraós Egípcios armazenaram cereais para a "grande fome".

Mas as novas realidades forjaram novos requisitos! Moldados pelas complexidades organizacionais, pelos recursos disponíveis e pelos aceitáveis retornos dos investimentos, ROI, tais requisitos incluem a partilha de informação, capacidades para uma rápida e eficaz recuperação em caso de catástrofe como a perda de informação e um alto nível de disponibilidade - todos termos relativos no léxico comum da Gestão da Continuidade.

As organizações lutam hoje para encontrar soluções que são a "resposta certa" para a integridade da informação e contra as interrupções nas operações, chegando eventualmente a um firme planeamento de processos analíticos na execução das novas realidades numa Gestão da Continuidade.

2.1.1 Quando um desastre ocorre o planeamento marca a diferença na capacidade de sobrevivência de uma organização!

Serias consequências e interrupções podem ser evitadas através de uma Gestão da Continuidade do negócio. Segundo Syed (2004), o planeamento para a Gestão da Continuidade pode ser considerado uma disciplina que prepara uma organização para manter a Continuidade de negócio durante um desastre através da implementação de um plano de contingência.

Poderá ser um acontecimento tão inocente como o de uma equipa de construção que acidentalmente perfura uma parede de pedra subterrânea que suporta um rio. Ou tão sinistro como um bombardeamento terrorista a um arranha-céus ou tão súbito como um terramoto ou tão devastador como um furacão.

A imperdoável natureza da disponibilidade contínua dos negócios, segundo Barnes (2001), e dos processos baseados na Internet vai muito para alem das complexidades técnicas na recuperação de plataformas computacionais ou redes de comunicação. Os cenários de interrupções de serviços - tais como furacões, fogos, falhas de energia ou cheias foram suplantados por actos de terrorismo, ataques com negação de serviços, violência no local de trabalho e um conjunto adicional de ameaças inimagináveis duas décadas atras.

Em qualquer momento que aconteçam os eventos naturais ou causados pelo homem os mesmos interrompem os ciclos de processamento de dados e uma coisa é certa: as organizações perdem dinheiro!

As verbas avultadas perdidas nestas situações estão proporcionalmente relacionadas com o grau de preparação das organizações para lidarem com situações de interrupção de serviços e de processamento nos seus Centro de Processamento de Dados. Um plano de recuperação de desastres actual, bem documentado e bem ensaiado marca a diferença entre um regresso às transacções normais de uma forma suave e transparente para o utilizador ou o facto de uma organização ter que lidar com uma situação que pode ter repercussões graves e devastadoras e que se faz sentir por meses, ou que pode mesmo ditar o fim da organização.

Qualquer evento que interrompa o negócio cuja origem seja a perda de informação ou a negação de acesso à informação é classificado como um desastre. Uma definição utilizada de forma mais comum ao se referir um desastre segundo Levinson e Granot (2002) é a de um evento que cause a morte e/ou extensos danos a propriedades, que se sobrepõe à capacidade de resposta usual. Neste caso um plano de recuperação de desastres funciona como um mapa para a recuperação na ocorrência destes eventos. O seu objectivo não é a duplicação de uma organização, em vez disso pretende aumentar as hipóteses de sobrevivência e diminuir os efeitos das perdas.

Uma sucessão de desastres de causas naturais e de desastres causados pelo homem, onde podemos salientar nos últimos anos o terramoto em São Francisco, as cheias em Chicago e os atentados ao World Trade Center são apenas alguns dos exemplos que vieram provocar uma onda crescente de interesse acerca da recuperação de desastres.

Frequentemente não são estes eventos que ditam aos líderes organizacionais que devem investir no planeamento de recuperação. De uma forma geral as acções são despoletadas a mandado de instituições financeiras, ou podem ser o resultado de uma auditoria externa ou mesmo por vezes a ameaça de um processo por parte dos accionistas da organização. Mas mesmo quando uma organização reconhece os benefícios do planeamento de recuperação de

desastres, muitos dos seus executivos não têm um sentido de urgência apurado para porem em prática o plano até à primeira ocorrência de um desastre.

Nessa altura poderá eventualmente ser tarde demais!

A realidade é que qualquer organização em que o seu negócio se baseie em Sistemas de Informação, o que na realidade inclui a maioria das organizações dos nossos dias, necessita de um plano de recuperação de desastres actualizado. Isto é especialmente aplicável para as pequenas e médias organizações que ao contrário das grandes organizações possuem recursos limitados. Estas pequenas e médias organizações são frequentemente as primeiras a sucumbir a um desastre.

2.1.2 Requisitos para o desenvolvimento de um Plano de Recuperação de Desastres

Os melhores planos de controlo de desastres não conseguem prevenir a ocorrência de situações de emergência catastróficas. Segundo Hiles (2004) os procedimentos de resposta aos eventos que a maior parte das organizações desenvolvem ou que são exigidos por lei, lidam apenas com os aspectos inicias dos desastres como combate a incêndios, evacuações, segurança de vidas humanas, etc. - o que pode estabilizar a situação e no geral cobrem as primeiras horas da emergência. Mas não lidam com a recuperação a longo prazo, que pode eventualmente demorar vários meses.

Por norma existem apenas alguns passos que qualquer organização deve executar para criar o seu próprio plano de recuperação de desastres: o primeiro passo é obter o apoio dentro da chefia da organização e a sua sensibilização para o facto, o segundo passo é a criação do plano de recuperação de desastres e por fim o terceiro e último passo é o de se testar e pôr em prática o planeamento efectuado.

A obtenção de suporte por parte do *management* é essencial dado que um plano de recuperação de desastres custa dinheiro e afecta toda a organização. A obtenção deste suporte pode por diversas razões ser difícil de se obter. Alguns *managers* ficam relutantes ao investir em algo que provavelmente e preferencialmente nunca vão precisar. Outros por sua vez são optimistas demais e acreditam que os desastres são coisas que só acontecem a outras organizações. E ainda existem outros que acreditam estarem preparados para o facto embora na verdade não o estejam.

Para se ultrapassar este ponto sensível de objecção por parte dos gestores de topo ao planeamento de recuperação de desastres é necessário aumentar a

sua sensibilidade para o risco que correm e alertar para os impactos causados por um evento. A maioria dos gestores de topo rapidamente consegue pensar em dois ou mais tipos de desastres que possam interromper o seu negócio e o acesso à informação na sua organização. Contudo existe uma longa lista de eventos críticos que podem causar este tipo de interrupções. Desta forma ao se mostrar aos gestores de topo uma lista com todos estes factores, rapidamente conseguem identificar mais algumas ameaças ao seu negócio.

Além da identificação dos riscos é também manifestamente importante substanciar-se o custo total do *downtime* na moeda local ao se responder à seguinte questão, "Qual o valor total de perdas que a organização consegue suportar se as aplicações críticas não estiverem disponíveis?". Numa eventual organização a falha dos sistemas de vendas online pode representar €50.000 por dia em vendas perdidas, o que perfaz um total de €250.000 de vendas perdidas no final de uma semana de trabalho, ao qual se devem acrescentar os custos adicionais de empregados parados por não poderem executar as suas tarefas.

Segundo Fulmer (2000) apenas dois dias depois de uma falha total do Centro de Processamento de Dados, uma organização média perde 30% das suas capacidades para executar as suas actividades essenciais. Ao quinto dia, 70% das capacidades estão perdidas e ao decimo dia uma organização típica está a funcionar apenas a 10% da sua capacidade. Estes níveis de perda são mais graves e ocorrem bastante mais cedo no sector financeiro.

O planeamento de recuperação de desastres providencia alguns benefícios financeiros adicionais à cabeça, tais como o baixar do valor dos prémios de seguros para as interrupções de serviços, bem como outros seguros adicionais.

Finalmente é importante o desenvolvimento de um plano de projecto que permita durante toda a fase do planeamento um tempo razoável para o seu próprio desenvolvimento e no qual devem estar definidos todos os recursos disponíveis e orçamentos necessários para se atingirem os vários pontos chave no decorrer do projecto, bem como a integração de métricas que permitam medir o grau de sucesso do projecto.

Após a aprovação para se avançar com o planeamento de recuperação de desastres inicia-se o trabalho pesado para se concretizar o plano. Nesta altura as organizações que não precisaram aceder a serviços externos de consultoria para a aprovação por parte da administração do plano de recuperação de desastres, devem agora começar a considerar a hipótese de formarem ou contratarem no exterior um especialista em recuperação de desastres.

Dado que o planeamento de contingência e a Continuidade de negocio como entidades formais são relativamente recentes, o grande problema com que as organizações se deparam é a falta de standards ao implementarem e gerirem uma plano de recuperação de desastres. Kuong (1998) reforça a noção de que os standards são necessários para virtualmente todos os aspectos e actividades complexas envolvidas num plano de Gestão da Continuidade. Ao procurar a colaboração externa a organização deve ter em linha de conta a experiência prévia dos consultores e as suas habilitações, nas quais devem estar contidas uma vasta experiência em projectos e serviços em organizações semelhantes.

Uma das certificações disponíveis no mercado é a *CBCP, Certified Business Continuity Professional* que é emitida pelo *Disaster Recovery Institute International* com a sede em St. Louis, Missouri. Para poder passar o certificado a DRII requer um elevado grau de compreensão da indústria, bem como a participação nas áreas de desenvolvimento do planeamento e uma experiência mínima de dois anos.

Mesmo com a utilização de consultores externos à organização mantêm-se as necessidades de uma estreita colaboração entre os consultores externos e os colaboradores da organização designados para participarem no desenvolvimento de um projecto global de Gestão da Continuidade do negócio da organização. No caso de um eventual desastre serão sempre os colaboradores da organização os primeiros a reagir à ameaça e não os consultores externos.

Ao se definir um plano de Gestão da Continuidade e segundo Yourdon (2002) deve ser contemplado o impensável, ou seja a identificação e gestão de riscos que nunca foram considerados. O processo de criação do planeamento de recuperação de desastres consiste essencialmente em sequências de perguntas e respostas. Quais são as aplicações críticas que devem ser protegidas? Quais os vários riscos e quais os potenciais efeitos? Existem métodos alternativos, tais como métodos de processamento manual que possam ser utilizados para a execução do negócio em curtos períodos de tempo? Qual o *downtime* que a organização consegue suportar antes da activação do plano? Quais os processos críticos para se implementarem no plano?

Outra parte importante do planeamento é a da criação da equipa de recuperação de desastres que irá activar e implementar o plano se os serviços de acesso à informação forem interrompidos. Os membros óbvios são as pessoas com características técnicas dentro da organização, incluindo os especialistas de sistemas, aplicações, comunicações e redes. Existem membros dos quais a participação não é assim tão óbvia e dos quais são de salientar as pessoas do departamento de compras, que tenham acessos aos orçamentos

necessários à compra de equipamento, os responsáveis pelas instalações que podem dirigir mudanças rápidas para os sites alternativos, tais como os *Recovery Sites* onde as aplicações críticas devem ser restauradas de forma rápida e eficaz. Também devem ser incluídos os Recursos Humanos que podem e devem alertar as famílias em caso de vítimas e os responsáveis pelas comunicações que devem manter os empregados e os meios de comunicação constantemente informados acerca do que se está a passar.

É necessário que estas pessoas tenham um envolvimento sério no projecto e façam parte da equipa. Se um desastre ocorrer serão em grande parte estes os responsáveis pelo sucesso ou falha na recuperação.

Quando todos estes membros forem seleccionados devem ser efectuados novos conjuntos de perguntas e respostas. Quem é o responsável por declarar o desastre e como é que a declaração dentro da organização deve ser efectuada? Como é que a equipa deve ser contactada especialmente se o desastre ocorrer num fim de semana ou fora de horas? Qual o local de convergência para começarem a implementar o plano de recuperação de desastres?

Como é que a organização responde a uma interrupção de acesso aos Sistemas de Informação que se prolonga para além do período definido na recuperação?

A organização é detentora de contractos alternativos com outras entidades para uma recuperação das aplicações críticas que necessitam de acesso a um site alternativo, caso não possuam um?

Após estas e várias outras questões terem sido exaustivamente respondidas durante o processo de planeamento e ainda mais importante passadas a papel, o plano de recuperação de desastres terá que ser implementado e ensaiado. Segundo Rothstein (1995) os ensaios de um plano de Continuidade são tão críticos como o desenvolvimento do próprio plano em si. Sem os ensaios, o plano de continuidade é pouco mais do que um exercício de especulação - ou mesmo uma futilidade. De que outra forma poderia uma organização assegurar a eficácia do plano, se não fosse por intermédio de ensaios regulares: Vivendo de facto uma catástrofe?

Invariavelmente o ensaio irá apontar lacunas e falhas no plano de recuperação de desastres que devem ser preenchidos e corrigidos. Detalhes que à partida possam parecer pequenos e de menor importância podem prejudicar gravemente o processo de recuperação. Uma organização, por exemplo, tinha previsto restaurar as comunicações telefónicas num site alternativo mas ao efectuarem o ensaio depararam com a questão de que

ninguém tinha encomendado os telefones. As linhas estavam lá mas os telefones não existiam.

Durante o ensaio faz sentido a presença de um consultor externo que possa efectuar o papel de observador para que o feedback final seja completo e objectivo.

Após o ensaio o *feedback* deverá ser integrado no plano.

O ensaio de um plano de recuperação de desastres não deverá acontecer apenas uma vez. Bell (1995) refere que os ensaios devem ser efectuados frequentemente para testar a capacidade de resposta e prontidão do grupo de trabalho. Os ensaios devem acontecer de forma periódica a intervalos definidos ou em alturas em que ninguém o esteja a prever. As melhores organizações conduzem vários níveis de ensaio a cada quatro meses e um ensaio global uma vez por ano.

Os ensaios vão de apenas exercícios de secretária, no papel, até à fase em que toda a organização se desloca para o site alternativo e recuperam-se as aplicações críticas e os respectivos dados. Juntamente com os ensaios o próprio plano de recuperação de desastres deve ser revisto de forma regular e actualizado periodicamente, ou seja, deverá ser um documento vivo!

Obviamente deverá ser actualizado sempre que se mudar um membro da equipa, sempre que forem adicionadas ou removidas aplicações e sempre que for implementado um novo equipamento crítico à produção. Contudo mesmo que não existam alterações o plano deverá ser revisto a cada três ou quatro meses pela equipa de recuperação de desastres para identificarem pequenos pormenores e pequenas alterações que possam ter passadas despercebidas. O plano não deve ser revisto pela pessoa que o desenvolveu, preferencialmente deverá ser revisto por alguém com um ponto de vista adicional, objectivo e crítico.

Segundo Bell (1995) a preparação é o que marca a diferença. A preparação subentendida como ensaios requer que as responsabilidades sejam identificadas e que se mantenham claras e que o entendimento dos procedimentos no plano seja real. A falta de ensaios e planos desactualizados e fora de prazo são as duas maiores fraquezas num plano de recuperação de desastres. Nada é mais arrepiante do que se descobrir no pior momento que o plano foi desenvolvido em 1988 ensaiado em 1992 e que nenhuma das aplicações críticas e as pessoas identificadas pelo plano já não fazem parte da actual organização.

O planeamento de recuperação de desastres não é um processo trivial. Está cheio de potenciais armadilhas que podem passar despercebidas mesmo aos melhores intencionados e às pessoas mais inteligentes na organização. Os gestores de planos, certificados pelas entidades responsáveis e com experiência no ramo podem ajudar as organizações a evitar essas potenciais armadilhas. Da mesma maneira estes consultores com experiência tipicamente possuem relações que podem identificar outros recursos que a organização poderá não possuir, tais como acessos a sites alternativos.

Independentemente da ajuda externa o planeamento de recuperação de desastres é um processo essencial para as organizações.

Colocado de uma forma simples, poderá ser um assunto de sobrevivência organizacional!

Ao acompanhar-mos o sucesso a longo prazo das organizações verificamos o aumento na importância da aquisição de seguros contra vários tipos de desastres. Neste caso um seguro poderá ser uma forma de planeamento de contingência que poderá trazer de volta à produção uma organização que passe por um estado de recuperação perante um desastre, de uma maneira eficiente e com o menor esforço financeiro possível. De acordo com a actual situação mundial, Yourdon (2002) identifica a presente década como a década da segurança. A probabilidade de sobrevivência a um desastre aumenta na proporção directa da qualidade do planeamento e preparação para a ocorrência desse mesmo desastre. Um processo de recuperação bem delineado irá providenciar à organização um plano compreensivo de recuperação perante a calamidade e se o mesmo abordar a recuperação das funções críticas da organização com procedimentos detalhadamente definidos e identificação das respectivas pessoas e acções, o plano resultará numa recuperação de sucesso.

O aumento do grau de preparação irá também reduzir o impacto na operação do dia-a-dia da organização. Os requisitos necessários para se regressar ao processamento normal dentro do IT estarão bem definidos e uma acção decisiva baseada num planeamento avançado irá certamente minimizar a interrupção de serviços e consequentemente eliminar a incapacidade de negociar da organização.

2.1.3 Modelo na Recuperação de um Desastre

A Gestão da Continuidade do negócio é uma função crítica à sobrevivência da organização. É uma metodologia e um conjunto de processos que identificam os requisitos essenciais, condições, pessoas e procedimentos para a continuação e restauro das operações.

A Gestão da Continuidade do negócio é muitas vezes definida como o restabelecer das operações, a Continuidade do negócio, recuperação de desastres ou mesmo como plano de contingência.

Todos estes termos implicam a recuperação de um evento não planeado e inesperado. A ocorrência poderá ser tão pequena como uma curta falha de energia ou a passagem de um furacão que destrói toda uma região. Para cada tipo de cenário o processo de Gestão da Continuidade do negócio terá que definir as estratégias de recuperação em que o objectivo principal é o de assegurar o restabelecimento das funções críticas ao negócio. O processo é utilizado na identificação de pessoas e dos procedimentos necessários à recuperação.

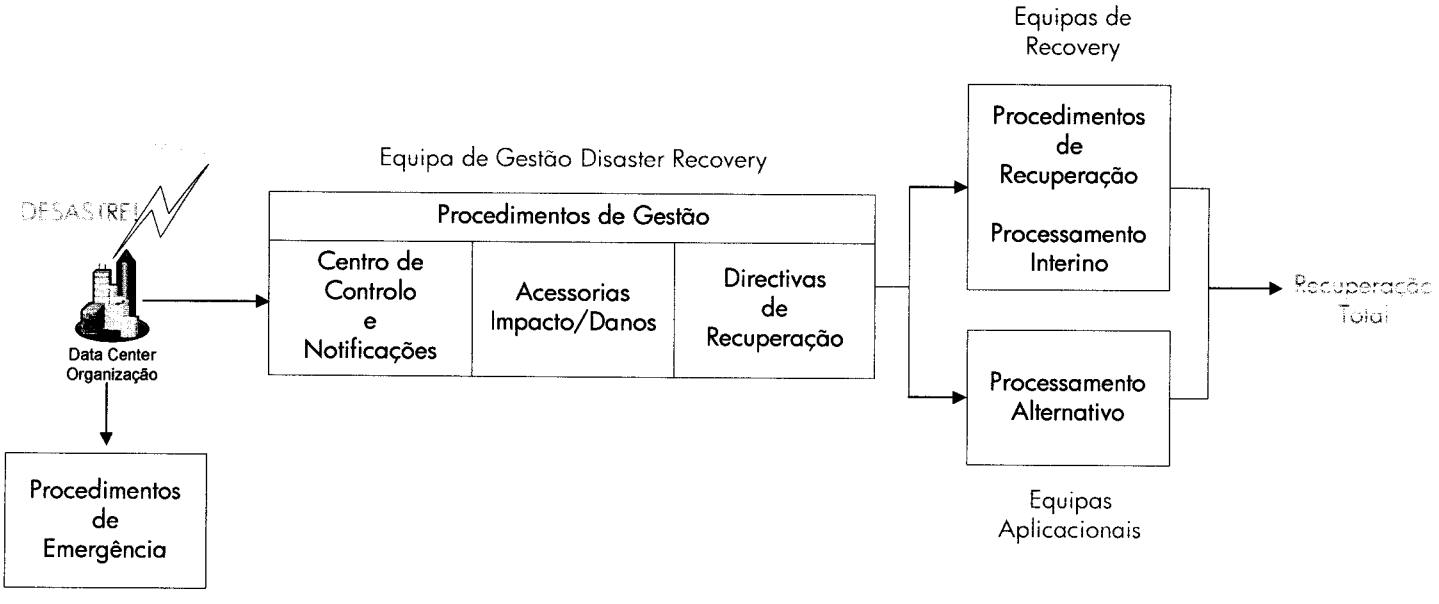


Figura 2.1: Visão geral do fluxo dos processos de recuperação.

A recuperação de um desastre envolve uma série de acções relacionadas que apontam no final para uma reposição das operações na sua normalidade.

A sequência será a seguinte:

- Ocorrência de um desastre.
- Evocação imediata dos procedimentos de emergência para a protecção de vidas e ao mesmo tempo minimizar o impacto do desastre.
- A Equipa de Continuidade do Negócio/Recuperação de Desastres é notificada e reúne num local pré definido para o efeito.
- A Equipa de Continuidade do Negócio/Recuperação de Desastres averigua os danos causados e avalia o impacto. Considera várias alternativas de recuperação e emite uma directiva de recuperação.
- As Equipas de Recuperação entram em acção para restabelecer os processamentos alternativos das aplicações críticas utilizando processos e recursos pré definidos e se necessário novas instalações.
- Entretanto as Equipas das Aplicações iniciam o processamento alternativo das aplicações consideradas críticas, com a utilização dos procedimentos de recurso alternativos até a capacidade de processamento total ou parcial estar novamente disponível.
- Assim que o processamento interino é estabelecido a Equipa de Recuperação de Desastres inicia os passos necessários para a restauração total e perfeita normalização das operações.

2.2 Relação entre processos ITSM

Um processo de Gestão da Continuidade deve incluir escaladas, notificações, contingências e procedimentos de recuperação que minimizam a interrupção total ou parcial dos serviços dos utilizadores. Segundo Kuong (2002) é necessário a revisão do programa existente na organização considerando mais do que apenas as mundanas e provavelmente já bem estabelecidas protecções aos serviços e tecnologias de informação.

O processo de Gestão da Continuidade do negócio está directamente relacionado com várias partes do modelo de referência do *IT Service Management (ITSM)*. As áreas do modelo referência do *ITSM* que interagem com a Gestão da Continuidade do negócio são a Gestão de Disponibilidades, Gestão dos Níveis de Serviço, Gestão de Problemas e Gestão de Alterações.

A gestão de disponibilidades, ou *availability management*, é um processo contínuo de monitorização da disponibilidade dos sistemas e aplicações, que eventualmente se traduz em *uptimes*. Esta informação também poderá ser de grande valor para a Gestão da Continuidade do negócio, ao se reflectir na maneira como é gerida a preparação de uma resposta adequada a um potencial problema, ou em contrapartida aos problemas gerados com *downtines*, que poderão ter duas vertentes distintas, neste caso *downtimes planeados* ou *downtimes não planeados* e imprevistos que afectam o normal funcionamento dos Sistemas de Informação dentro da organização.

Outra área de interacção é a relação existente entre a Gestão da Continuidade do negócio e a gestão dos níveis de serviço, ou *service level agreement*. Os *service levels agreements* são desenvolvidos e implementados de acordo com as necessidades e os vários níveis de criticidade aplicacionais da organização. A Gestão da Continuidade do negócio deve suportar estes *SLA´s* de forma a que os procedimentos de recuperação possam garantir o *que* está definido contratualmente. Existem circunstâncias especiais onde ficam claramente definidos nos *SLA´s* potenciais perdas e degradação de performance caso se contemplem vários cenários de recuperação.

Por sua vez a gestão de problemas servirá como fonte de informação no caso de falhas recorrentes e na indicação de possíveis causas dos problemas. O *problem management* deverá interligar as condições e os critérios dentro do processo de Gestão da Continuidade do negócio de forma a indicar quando um problema passa a potencial desastre. Estas condições são tipicamente referenciadas como desastres em evolução onde a sua duração poderá ser permanente.

Existe ainda a interacção entre a Gestão da Continuidade do negócio e a gestão de alterações ou *change management*. Ao mesmo tempo que acontecem alterações nos Sistemas de Informação e as mesmas são contabilizadas no processo de *change management*, o processo de Gestão da Continuidade do negócio terá necessariamente que ser revisto e alterado nos pontos referidos pelo *change management*. A interacção também se verifica no sentido oposto, neste caso durante o decorrer dos testes e procedimentos de Gestão da Continuidade do negócio terá que obrigatoriamente ser dado feedback ao *change management* para actualização do mesmo.

Conforme verificamos a Gestão da Continuidade do negócio é um processo emergente ao nível das organizações que consiste na interacção entre os vários processos *ITSM* de modo a que o planeamento da Continuidade do negócio possa permitir a recuperação com sucesso de todos os processos críticos à organização.

O planeamento deverá sublinhar todas as condições, procedimentos, pessoas e equipas necessárias para responderem de forma imediata e eficaz, a fim de se restabelecerem e recuperarem a organização de um evento que afecte de forma parcial ou total a sua capacidade de produção. Fulmer (2000) também refere que em situações de emergência é essencial que as todas decisões sejam tomadas de imediato para se controlar a ameaça existente à organização. Em situação de emergência a organização deve voltar a laborar as funções vitais ao negocio o mais rapidamente possível, dado que na altura de um desastre, a única coisa que todas as organizações têm em comum a trabalhar contra elas é o tempo! Tempo perdido traduz-se em clientes insatisfeitos, perda de negócio e muito mais.

Em alguns casos a Gestão da Continuidade do negócio pode ser entendida como uma extensão da Gestão da Disponibilidade dos serviços. No caso de um sistema ficar indisponível por um período de tempo superior ao aceitável a situação poderá rapidamente transitar de um problema de disponibilidade de sistemas ou de aplicação para um problema de continuidade do negócio. O processo de Gestão da Continuidade do negócio deverá garantir desta forma a continuidade operacional o mais rapidamente possível.

A ilustração abaixo indicada apresenta a sequência de acções após uma interrupção de serviços ter sido definida como um desastre. Os utilizadores muito provavelmente terão que efectuar todos os seus procedimentos e tarefas por métodos alternativos, que podem consistir em processamentos manuais ou a utilização de *PCs stand-alone*. Enquanto o Centro de Processamento de Dados principal não é novamente restabelecido um site alternativo poderá ser activado para que o processamento alternativo possa decorrer dentro da medida do possível, perante a gravidade do impacto e perante a capacidade de planeamento de recuperação da organização.

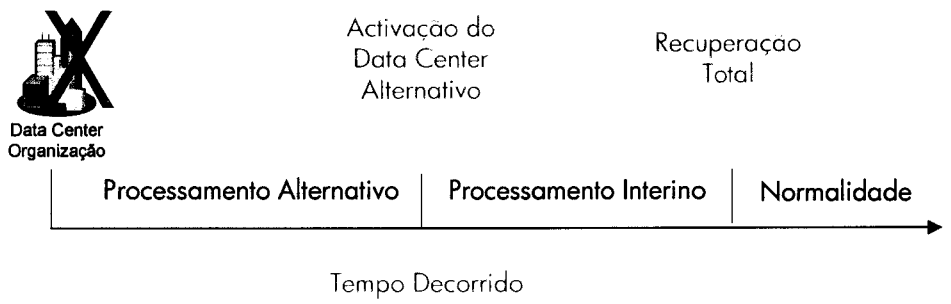


Figura 2.2: Processamento alternativo, interino e restabelecimento da normalidade operacional.

2.3 Metodologia para a Gestão da Continuidade

As ameaças são reais e os desastres podem ocorrer com base em fontes distintas. Os desastres naturais e os que ocorrem com base em falhas humanas, prolongadas falhas de energia, fogos, sabotagens e mesmo ameaças de bombas são potenciais geradores de problemas. Está mais do que provado que os desastres não ocorrem só das 09:00h às 18:00h e de segunda a sexta-feira. É importante ter-se a percepção de que os desastres podem evoluir e mesmo acontecer! Numa suposição inicial uma falha num sistema poderá não ser muito grave, mas se o mesmo sistema não ficar reparado em tempo útil, poderá rapidamente ser gerada uma escalada e um novo desastre comercial.

Qualquer que seja a origem de uma perda na capacidade de processamento da organização, mesmo que por um (in)determinado período de tempo, podem existir consequências reais e devastadoras para a organização. Como tal todas as organizações devem estar preparadas para possíveis ocorrências destes factos.

A melhor protecção é o desenvolvimento de uma metodologia para a Gestão da Continuidade do negócio que pode numa primeira aproximação de âmbito geral ser dividida em quatro módulos. O primeiro módulo será o da identificação dos objectivos de continuidade e de recuperação; o segundo o da identificação dos requisitos essenciais para suporte dos objectivos definidos no primeiro; o terceiro será o do desenho e desenvolvimento do próprio plano e da arquitectura que irá suportar a infra-estrutura, bem como a identificação de todas as soluções necessárias para a implementação de uma recuperação com sucesso; o quarto módulo será constituído pelos ensaios e manutenção dos processos e do plano de recuperação de desastres.

Desta forma indicam-se os módulos integrados na estrutura de gestão:

- Âmbito, Objectivos de Recuperação e Gestão de Risco
- Requisitos Funcionais
- Desenho, Formação e Desenvolvimento do Plano
- Ensaios, Manutenção e Revisões de Planeamento

A informação que se segue tem como objectivo referir as actividades de cada um destes quatro módulos, dado que a partir do ponto 2.3.1 será apresentada em detalhe a metodologia proposta.

No plano de continuidade do negócio os objectivos de recuperação devem ficar claramente definidos com uma identificação objectiva dos possíveis tipos de interrupção de serviços e os vários cenários de recuperação de desastres que serão abordados pelo plano, bem como os que eventualmente não vão ser contemplados. Roessing (2002) refere que muitas vezes os planos de continuidade são baseados apenas em alguns cenários específicos de desastres e não suportam cenários que não foram contemplados, sugerindo que os desastres não são disciplinados e o caos não segue um mapa. O senior management deve desta forma definir os objectivos de recuperação e validar os esforços do planeamento. A definição e âmbito do plano também inclui a extensão do planeamento de recuperação. Por outras palavras o plano deverá referir falhas de sistemas e redes, unidades de negócio e funções críticas, aplicações, Centro de Processamento de Dados bem como todos os componentes e processos críticos para a organização.

Em conjunto com os esforços para se validarem as ocorrências de possíveis desastres deve ser efectuada uma análise de risco para se identificar e reduzir todos os potenciais perigos dentro da organização. Com base nos riscos identificados são então tomadas medidas que permitem à organização a diminuição dos riscos ou mesmo a completa eliminação dos mesmos. Não faz sentido o desenvolvimento de um plano elaborado de Continuidade do negócio se a própria organização tiver demasiadas exposições que podem à partida ser prevenidas ou minimizadas.

Antes de se efectuar o planeamento para protecção de todo o ambiente e consequente recuperação dos serviços, a organização deverá garantir que todas estas as medidas para evitar os potenciais desastres estão em pleno funcionamento. Desta forma uma revisão do estado actual de todo o ambiente deve ser efectuada de modo a se garantir que os riscos são minimizados.

De seguida avança-se com o processo para se determinar o impacto de um determinado desastre numa organização, denominado *Business Impact Analysis (BIA)*. Através desta análise é identificado o impacto financeiro e operacional para cada unidade de negócio dentro de períodos de tempo pré-definidos. Com base neste critério as unidades de negócio são classificadas em diversas categorias e grau de criticidade e de acordo com o tipo de organização. Cada unidade de negócio e respectivas aplicações são analisadas para se determinar o impacto relativo na organização caso a mesma esteja indisponível. Desta forma as funções de negócio e respectivas aplicações devem ser agrupadas em categorias tais como críticas, vitais, importantes ou pouco relevantes.

Definem-se de seguida todos os requisitos necessários para se suportarem as diversas funções e aplicações críticas da organização identificadas de acordo com o BIA. Esta informação identifica as pessoas, os processos e os requisitos para o suporte crítico e vital da organização.

Baseado nos requisitos de recuperação e na janela de recuperação as alternativas ao processamento normal devem ser definidas de modo a que melhor se consiga garantir os diferentes tipos de recuperação de acordo com os vários cenários. Henderson (2003) alerta para o facto que frequentemente os planos podem ser desenvolvidos de forma fechada numa perspectiva "silo approach" em de vez se utilizar uma perspectiva global ao nível da organização. Neste tipo de aproximação os planos resultantes variam em detalhe e não é incomum encontrar departamentos com excelentes procedimentos de recuperação e outros sem qualquer tipo de planeamento.

Dependendo do tipo de desastre deve ser implementada a estratégia específica de recuperação e alternativas redundantes. A partir deste ponto devem ser determinados os critérios para se desenvolver o plano de recuperação de desastres e da continuidade do negócio. Também devem ser identificadas as equipas de projecto, estruturas e as várias linhas temporais críticas e de recuperação. A garantia dos requisitos de recuperação e dos objectivos são complementares e interdependentes de acordo com a metodologia escolhida. O plano de recuperação de desastres deverá ser desenvolvido utilizando a metodologia correcta tendo em conta as necessidades de Continuidade do negócio da organização.

É imperativo que os membros da equipa de projecto e todas as pessoas envolvidas percebam a terminologia e a aproximação aos processos de Gestão da Continuidade do negócio. Como referência neste guia processual podem existir várias definições de termos semelhantes e a organização deverá assegurar que todos os membros trabalham com base nos mesmos critérios. As *workshops* são métodos eficazes para se formalizar um *kick off* do projecto e para de forma continuada formar todos os membros das equipas da importância na continuidade do planeamento e das suas responsabilidades no seu sucesso.

No seguimento da metodologia um plano de recuperação de desastres, integrado no processo de Gestão da Continuidade do negócio, é desenvolvido para suportar as funções críticas ao negócio. O plano deverá incluir notificação de eventos, escaladas e a própria execução do plano. Um plano de Projecto deverá identificar as dependências e os potenciais bottlenecks. Os procedimentos de recuperação devem ser escritos e definidos de forma clara e abordar todos os cenários críticos com probabilidades de ocorrência.

O plano deverá então passar a uma fase de ensaios e ser revisto de forma regular pelos gestores de projecto e pelo próprio responsável e gestor da Continuidade do negócio.

Nunca é demais referir que um *plano* é apenas útil até à ultima vez que foi testado com sucesso!

De acordo com Roessing (2002) cerca de 85% dos planos de Continuidade do negócio falham quando são testados a primeira vez. Posto de uma forma simples, estes planos demonstram falhas fundamentais que podem impedir a ocorrência da recuperação dentro dos prazos definidos. Ainda de acordo com Roessing (2002) mais de 50% dos planos de Continuidade do negócio nunca são ensaiados. Isto indica que as falhas do plano não foram expostas e que os planos quase de certeza irão falhar na execução de uma recuperação atempada.

Os ensaios devem ser conduzidos de forma regular com todas as pessoas chave envolvidas e os seus respectivos backups. Para cada ensaio devem ser medidos os objectivos e os factores críticos de sucesso do plano bem como a correspondente documentação de suporte. Cada ensaio deverá incluir os diversos tipos de cenário e podem ser efectuados de forma planeada, ou podem ser executados de surpresa. Para cada ensaio existe uma carga significativa de planeamento seguido de uma reunião *post-mortem*. Durante cada ensaio existem lições que devem ser retiradas e potenciais melhoramentos a efectuar ao plano de recuperação de desastres.

O plano integral de recuperação de desastres deverá ser continuamente actualizado e monitorizado de forma regular. Strohl (2002) enfatizam a expressão de que os planos são documentos "vivos" e que devem ser mantidos actualizados e ensaiados para serem de facto úteis. Os updates devem ser efectuados de forma expedita e sempre que alguma alteração significativa ocorra na organização. Deverá também ter como base um critério de avaliação. O *feedback* dos ensaios que foram conduzidos anteriormente servem como *input* para a integridade e eficácia do plano. A cada alteração significativa no ambiente de Sistemas de Informação da organização é obrigatória a actualização do plano de recuperação de desastres.

No seguimento das alterações o plano de recuperação de desastres deverá ser revisto numa base periódica e de acordo com os objectivos desenvolvidos e os que devem ser abordados. Estas revisões periódicas vão identificar potenciais falhas ou exposições dentro da documentação ou nos próprios procedimentos de recuperação. Segundo Kuong (2002) se uma assessoria for conduzida por auditores ou consultores independentes, existe uma oportunidade única para

se providenciar um valor adicional e melhorar as hipóteses da organização estar preparada para uma eventualidade ou potenciais ataques que possam provocar danos e perdas irreparáveis.

O desenvolvimento de um bom plano de recuperação de desastres tem que ser baseado numa aproximação estruturada. Este processo irá preparar a organização para potenciais auditorias referentes à sua capacidade de sobrevivência e continuidade do negócio.

O diagrama representa apenas as várias etapas e fases no desenvolvimento e implementação do plano de recuperação de desastres.

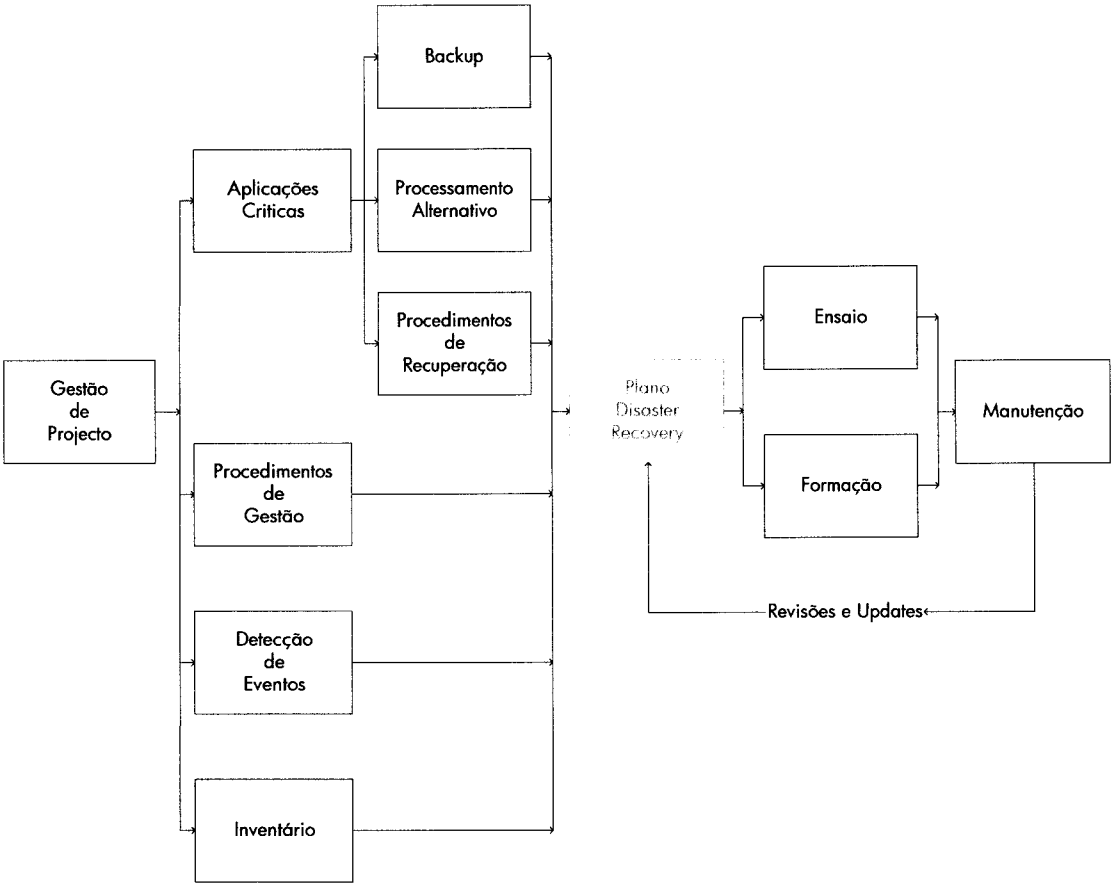


Figura 2.3 Fases do plano de recuperação de desastres

Define-se em seguida a metodologia que se considera essencial seguir como referência na aproximação cuidada à Gestão da Continuidade do negócio.

2.3.1 Princípios do Plano de Recuperação de Desastres e de Continuidade

É imperativo para o sucesso do projecto de planeamento da Continuidade do negócio que exista um compromisso da gestão de topo para com a totalidade do programa. Isto inclui o patrocínio e a participação de um gestor de topo enquanto membro activo do programa.

O planeamento da Continuidade do negócio deve ser visto como uma decisão de negócio e não uma decisão técnica. O propósito do programa ao ser definido deve assegurar que o mesmo é uma necessidade da organização e do negócio e não apenas um objectivo do IT.

A fundação para uma boa Gestão da Continuidade do negócio deverá focar primeiro as decisões de negócio, identificando funções críticas e quais as verbas que a organização está disposta a perder e quanto está disposta a investir para minimizar as perdas.

Propósitos:

- Obtenção do compromisso e patrocínio da gestão de topo.
- Definição de objectivos do programa de Gestão da Continuidade do negócio.
- Definição do alcance e objectivos do plano de recuperação de desastres.
- Definir objectivos temporais e janelas de recuperação.
- Definir os desastres mais prováveis e os pouco ou menos prováveis.
- Definir e classificar os desastres de acordo com uma escala i.e. menores, maiores e catastróficos.
- Definir e classificar as funções de negócio como sendo críticas importantes, adiáveis ou menos importantes.

O alcance do plano de recuperação de desastres ao ser definido deve ser validado por toda a organização. Os tipos de desastre que o plano vai contemplar devem ser identificados bem como todos os desastres que não vão ser contemplados. Devem também ser respondidas perguntas, tais como: Qual o *downtime* tolerável dada a perda de funções vitais para a organização? Em que medidas serão diferentes uma interrupção de serviços de um pequeno desastre? Ou um grande desastre de um desastre catastrófico?

Os impactos nas funções de negócio são definidos em categorias e de acordo com critérios pré-definidos como perda de rendimentos, perdas de salários ou deterioração da imagem da organização. Deve ficar identificado quem tem o papel principal na aprovação de uma determinada função em detrimento de outra.

Todas estas áreas precisam ser estudadas e analisadas antes de se iniciar o plano de recuperação de desastres. O gestor da Continuidade do negócio e o gestor patrocinador do projecto devem assegurar que todas estas questões são respondidas antes de se avançar com o planeamento.

Inputs:

- direcção da gestão e expectativas
- alcance do plano de recuperação de desastres
- perdas aceitáveis (intangíveis e tangíveis)

Ferramentas:

N/A - não aplicável

Outputs:

- plano de projecto de alto nível com resultados e conclusões

Métricas:

- informação validada pela gestão de topo.

2.3.2 Condução de uma Análise de Riscos e Prevenção de Desastres

Não de um ponto de vista teórico mas sim pratico, Hiles (2002) refere que a maneira correcta de se efectuar uma gestão de risco significa escolher, corresponder, cruzar e trabalhar a informação de casos e exemplos complexos e construir a análise com base nas melhores práticas da organização.

Este passo é importante pois define o propósito da Gestão da Continuidade do negócio e dos processos que o suportam. Porquê ir em frente e desenvolver um plano de recuperação de desastres elaborado quando a organização está vulnerável a potenciais riscos e desastres que podem ser evitados? O ambiente corrente deverá ser avaliado para assegurar que todas as medidas preventivas apropriadas estão prontas para evitar ou minimizar potenciais desastres. Isto deve incluir sistemas de supressão de incêndios, pavimentos elevados, segurança física, segurança de sistemas e outras ameaças de alto risco.

A análise de risco é um processo utilizado para a identificação dos riscos e vulnerabilidades na organização. Em conjunto com a revisão para definição dos processos que podem evitar e impedir desastres, é feita uma análise de risco que identifica as potenciais ameaças para a organização e define a probabilidade dessas ameaças afectarem toda ou parte da organização, o que é conhecido como risco. Por exemplo, uma organização localizada numa falha terrestre pode ter uma probabilidade maior ou um risco mais elevado de ser afectada por um terramoto do que uma organização que está localizada a milhas da falha terrestre ou numa pedreira.

A análise de risco é o processo de identificação das probabilidades de ocorrência de uma determinada ameaça e a identificação das vulnerabilidades nas funções de negócio para com a ameaça. Deve ser determinado o grau de eficácia de um determinado controlo em deter as potenciais ameaças e limitar o custo associado ao risco, minimizando desta forma o impacto que possam ter na organização.

Propósitos:

- Identificação de potenciais ameaças.
- Avaliação da probabilidade das ameaças.
- Avaliação das medidas correntes de prevenção de desastres.
- Avaliação dos controlos de risco em funcionamento para mitigar as ameaças.

- Determinação do impacto para a organização sem controlos adequados.
- Análise do valor para a organização dos controlos adicionais.
- Implementação dos controlos adicionais para mitigar e reduzir riscos.

As ameaças são agrupadas em duas categorias: Naturais e causadas pelo Homem. As ameaças naturais consistem em eventos como tornados, furacões e tremores de terra. As ameaças criadas pelo Homem incluem tumultos, erro de programação, sabotagem, greves, bombas e actividade terroristas. Para cada ameaça, é necessário determinar uma probabilidade de ocorrência, tanto com ou sem controlo. A organização precisará então determinar quais os riscos que está disposta a aceitar e quais os que quer e deve controlar.

É importante pôr em prática a gestão de riscos e prevenção de desastres para assegurar a organização que não assume um nível de risco inaceitável.

Inputs:

- riscos e ameaças
- histórico de informação
- ambiente actual
- políticas, processos e procedimentos correntes

Ferramentas:

- Annual Loss Exposure
- Controled Risk Analysis and Management Method (CRAMM)

Outputs:

- avaliação de risco
- relatório com recomendações para melhorias

Métricas:

- controlo de risco para mitigar a ameaça.

2.3.3 Condução de uma Análise de Impacto no Negócio (BIA)

Tipicamente, a Continuidade do negócio e o plano de recuperação de desastres identificam e processam métodos de recuperação de aplicações e de funções críticas para a organização. A recuperação não é uma situação de *business as usual*, mas sim uma situação de recurso, em *survival mode*.

De forma a se identificarem as funções críticas para a organização deve ser elaborada uma *Análise de Impacto no Negócio*. O *BIA* vai identificar as aplicações, que por sua vez são agrupadas em categorias, calculando os custos financeiros e operacionais para a organização caso as mesmas não estejam disponíveis por períodos de tempo definidos.

Propósitos:

- Definição da metodologia e dos processos a utilizar com o BIA.
- Identificação das funções de negócio a analisar.
- Definição de critérios para as funções e categorias.
- Desenho e validação das questões de entrevista.
- Condução de entrevistas.
- Análise da informação e validação dos resultados necessários.
- Desenvolvimento das conclusões e apresentação de um relatório final.

A análise é feita por entrevistas, com questões chave sobre perdas intangíveis, como imagem, moral dos empregados e sobre perdas tangíveis, como perda de rendimentos ou de valor de mercado.

Baseados em critérios pré-definidos para as várias categorias e na informação das entrevistas, cada função de negócio da organização vai ser colocada numa determinada categoria. A criticidade de recuperação dessa função é baseada na sua categoria. Tipicamente, a organização vai construir o seu plano de recuperação de desastres para suportar primeiro a recuperação de funções críticas e vitais para a organização, e só depois as restantes.

A entrega final é um relatório que define e atribui uma escala de prioridades às funções de negócio segundo as categorias pré-definidas. O relatório identifica também quaisquer potenciais *workarounds* ou alternativas no processamento e identifica o conjunto de requerimentos mínimos para todas as funções vitais, necessárias ao funcionamento da organização.

Inputs:

- critério de perda
- input para definições de categorias
- lista de funções

Ferramentas:

- questionários
- entrevistas
- análise

Outputs:

- lista de funções segundo grau de criticidade
- lista de requerimentos de recuperação para o processamento das funções vitais

Métricas:

- alcançar a definição e o critério de perdas aceitáveis

2.3.4 Determinação das Opções de Backup e Sites Alternativos

Tendo como base os requerimentos para a recuperação das funções críticas e vitais para a organização, ficam imediatamente disponíveis uma variedade de opções de backup e alternativas para o processamento das funções críticas. Nenhuma opção é mutuamente exclusiva pois está dependente do tipo de desastre e do tipo de interrupção existente. Dependendo do tipo de desastre, falha e das implicações para o negócio uma ou mais destas opções podem ser consideradas apropriadas. O objectivo passa por determinar quais as opções de backup e alternativas que são mais apropriadas para se efectuar o processamento alternativo das funções vitais para a organização.

Exemplificando:

- De forma a se processar a aplicação de salários, um processo manual poderá ser utilizado por um período de duração não superior a uma semana; de uma a três semanas poderá recorrer-se a uma agência de serviços para processamento dos salários; para um período superior a três semanas é necessário um *hot-site* comercial.

- Para todos os pequenos desastres a opção de recuperação poderá passar por não se fazer nada até à 24ºhora. Nesse caso, o plano de recuperação de desastres será activado e todas as opções disponíveis serão revistas. - Não é uma boa opção, dado que um pequeno problema poderá transformar-se rapidamente num desastre comercial.

Propósitos:

- Identificação das opções de backup para as funções críticas.
- Avaliação e determinação das opções de backup para os vários cenários.
- Definição das opções de backup para as funções críticas.
- Desenho dos procedimentos para invocar as opções de *backup*.

As estratégias de *backup* e alternativas de processamento são métodos de operações redundantes para as instalações, operações de sistemas e aplicações críticas em caso de desastre. A alternativa de recuperação é o método seleccionado para a recuperação das funções críticas ao negócio a seguir a ter sido declarado um desastre. Algumas alternativas possíveis podem ser o processamento manual, utilização de escritórios/agências de serviços ou de um Centro de Processamento de Dados alternativo (*hot* ou *cold-site*). As alternativas de recuperação são normalmente definidas no seguimento de uma *Análise de Risco* e de uma *Análise de Impacto no Negócio*.

Um Centro de Processamento de Dados alternativo é definido como uma localização, que não a instalação principal, utilizada para se processar informação ou conduzir funções críticas de negócio em caso de desastre. A capacidade de recuperação é definida como todos os componentes necessários para se efectuar uma recuperação com sucesso. Estes componentes podem incluir um site alternativo, mudanças no processo de controlo, reencaminhamento de redes e outros.

Para cada área do plano de recuperação de desastres devem existir múltiplas opções de backup e alternativas. Isto inclui unidades de negócio, Sistemas de Informação, utilizadores, *call centers*, etc.

Devem ser implementadas na infra-estrutura dos Sistemas de Informação opções de recuperação para a maioria das falhas dos componentes de *hardware*. Os seguintes exemplos podem ser utilizados como opções de backup e alternativas redundantes:

- ***Clusters*** implica a utilização de múltiplos sistemas, interligados de maneira a formarem um sistema virtual sólido com capacidades redundantes, que pode continuar a fornecer serviços após falha de um componente ou mesmo após a falha total de um dos sistemas no cluster.

- ***Remote Electronic Vaulting*** é a transferência de informação para uma instalação de armazenamento *off-site* via um circuito de dados electrónico, em vez da utilização de suportes de armazenamento magnéticos. São tipicamente utilizados para actualizações de informação crítica e suplementares aos *full backups* periódicos.

- Utilização de tecnologia ***Fault Tolerant***. Um sistema é considerado *Fault Tolerant* quando possui componentes de *hardware* redundantes. Este tipo de sistema apenas permite a protecção contra falhas de *hardware*. Ser-se *Fault Tolerant* não significa que o sistema nunca falhe.

- ***Shadow File Processing*** é uma abordagem ao *backup* de informação onde são mantidas cópias duplicadas dos dados num *CPD* remoto, em tempo real.

As instalações de recuperação devem conter todos os equipamentos, Sistemas de Informação, consumíveis, circuitos de dados e voz para se conduzir e processar todas as transacções necessárias às funções críticas do negócio.

- ***Comando*** ou ***centros de controlo*** é uma instalação com ênfase nas linhas de comunicação para se avançar com a activação do plano de recuperação de desastres. Tipicamente é uma instalação temporária usada pela equipa de gestão para começar a coordenar o processo de recuperação e é usado até o local alternativo estar operacional.

- Um ***hot-site cooperativo*** é um *hot-site* que é propriedade de um grupo de organizações disponível para cada membro do grupo caso aconteça um desastre.

- ***Crate-ship, drop-ship,*** ou ***quick-ship*** é uma opção contratual em que uma substituição ou mesmo um equipamento alternativo é entregue à organização dentro de um prazo de tempo definido e numa localização alternativa.

- Um ***cold-site*** é uma instalação que contêm tudo excepto os equipamentos e a informação. Por exemplo, uma instalação *cold-site* poderá estar equipada com ar condicionado, energia, *halon*, pavimentos elevados, etc. Os equipamentos e recursos têm que ser obtidos e instalados no *cold-site* para se retomar as funções críticas de negócio. Existem muitas variações de *cold-sites* dependendo das instalações de comunicação, sistemas de *UPS* ou da mobilidade.

- Um ***hot-site comercial*** é uma das opções de *backup* mais utilizadas hoje em dia. Esta opção fornece uma instalação de *backup* que contêm todo o equipamento e recursos para se recuperar as funções críticas de negócio. Uma configuração predefinida é contratada através de um valor de subscrição. Outros valores a incluir podem ser o valor para declaração de desastre e a utilização dos Sistemas de Informação.

- Um ***hot-site interno*** fornece o mesmo ambiente que um comercial, descrito acima, mas é propriedade e operado pela organização.

- Um ***cold-site portátil*** ou ***portable shell*** é uma estrutura pronta a funcionar que pode ser transportada para o local de um desastre de forma a se obter e instalar um novo equipamento próximo da localização original.

- Um ***hot-site portátil*** ou ***móvel***, é tipicamente uma unidade móvel grande, como um *trailer*, contendo todo o equipamento necessário de *backup* e periféricos, que é entregue no local do desastre. É então ligado às linhas de comunicação existentes.

- Um ***warm-site*** é um local de processamento alternativo mas que só esta parcialmente equipado, comparado com um *hot-site* que está completamente equipado.

Acordos e consórcios

- Acordo de consórcio é um acordo feito por um grupo de organizações semelhantes, com o objectivo de partilharem instalações, para se efectuar o processamento de dados e ou partilha de escritórios, no caso em que um dos membros do consórcio sofre um desastre.

- Acordo recíproco, ou de ajuda mútua, é um acordo entre duas organizações com Sistemas de Informação compatíveis, permitindo que uma das organizações utilize o excesso de capacidade de processamento da sua semelhante em caso de desastre.

- Escritório de serviços é uma unidade de processamento do IT que fornece a capacidade de processamento, normalmente para se efectuar um tipo de processamento especializado, como o de salários.

- Serviço de armazenamento *off-site* fornece uma localização segura e remota em relação à localização primária do Centro de Processamento de Dados e no qual são armazenados sistemas alternativos de *backups* de *hardware*, *software*, dados, documentos, equipamentos e consumíveis.

A capacidade de processamento *stand-alone* é um processamento tipicamente executado num servidor ou num PC mas que não requer nenhuma ligação a um *mainframe* ou a qualquer outro tipo de servidor central.

Os procedimentos de operações temporários são procedimentos pré-determinados, que dinamizam as operações dos sistemas mantendo-se desta forma um nível de controlo e de auditoria aceitável durante uma situação de desastre. O processamento alternativo representa todo o conjunto dos procedimentos utilizados para o processamento das funções críticas ao negócio enquanto as operações estão a ser restauradas e normalizadas.

Inputs

- janelas de recuperação
- downtime aceitável
- requerimentos de recuperação

Ferramentas:

- ferramentas de análise

Outputs:

- objectivos de recuperação
- lista de opções de backup
- procedimentos de suporte
- contratos

Métricas:

- atingir os objectivos dos tempos de recuperação

2.3.5 Equipas de Recuperação de Desastres

Imediatamente a seguir a um desastre ter sido declarado a equipa de Continuidade do negócio deve reunir-se, avaliar os estragos e o âmbito do impacto e decidir quais os passos de recuperação a implementar de acordo com o grau de calamidade do desastre. As equipas de recuperação executam então os procedimentos de recuperação adequados.

Uma parte importante do planeamento de recuperação de desastres consiste na instalação das equipas de recuperação e detalhe claro do que cada equipa deve fazer. Existem diferentes tipos de desastres com circunstâncias distintas. O desafio ao se definir os procedimentos de recuperação é serem genéricos o suficiente para cobrirem todo um leque alargado de possibilidades e ao mesmo tempo, serem específicos e detalhados para que o plano possa ser genuinamente útil e implementado com sucesso.

Propósitos:

- Definição das estruturas das equipas de recuperação de desastres.
- Definição das funções das equipas de recuperação de desastres.
- Definição de líderes, dos seus *backups* e da totalidade dos membros.
- Definição do *charter* das equipas e procedimentos de recuperação.

Dependendo das necessidades de negócio a estrutura das equipas de recuperação de desastres poderá ser diferente. Para cada equipa existe um líder, o seu *backup* e os membros da equipa. Um *charter* é definido para cada equipa, para além da definição dos papéis e responsabilidades.

As equipas de recuperação são responsáveis por executarem todas as acções necessárias para a completa recuperação de um desastre, dentro da sua área de responsabilidades. Cada equipa deve definir os seus procedimentos de recuperação pertinentes ao seu papel na organização.

Inputs:

- necessidades do negócio
- requerimentos de recuperação

Ferramentas:

- template dos procedimentos de recuperação

Outputs:

- organização das equipas de recuperação
- charter e membros das equipas de recuperação
- procedimentos de recuperação

Métricas:

- N/A - não aplicável

2.3.6 Desenho e Desenvolvimento do Plano de Recuperação de Desastres (PRD)

Esta é claramente a tarefa mais árdua na definição de todo o conjunto dos processos de recuperação, contudo a mais importante! É aqui que os procedimentos são desenvolvidos de forma a suportarem as funções críticas do negócio. Como são definidos, sob que circunstâncias devem actuar e quem os vai implementar são factores importantes a definir e que devem ficar claros. Só após a sua total elaboração são então validados pelas várias unidades de negócio e pela gestão de topo na organização.

Propósitos:

- Determinação da estrutura e metodologias.
- Definição da agenda e dos processos de notificação incluindo listas de telefones.
- Definição dos processos de escalonamento.
- Incorporação no plano de políticas e objectivos de *recuperação* chaves para a organização.
- Estabelecimento do quadro de referência necessário ao processo de fluxo de recuperação de desastre.
- Estabelecimento do quadro de referência necessário para os procedimentos de recuperação.
- Definição dos passos de recuperação.
- Definição dos processos de restauração incluindo os critérios de aceitação.

Devem ser determinadas as estruturas e metodologias de desenvolvimento do plano. Isto inclui a estrutura e todos os componentes do próprio plano de projecto para gestão *do* plano de recuperação de desastres associado. Cada *Equipa de Recuperação* deve ser responsável pelas suas respectivas secções, o que inclui listas de notificação, os procedimentos necessários para se efectuar o processamento alternativo e os respectivos procedimentos de recuperação claramente detalhados.

Inputs:

- objectivos de recuperação
- alcance do plano
- classificação das funções de negócio

- definições e classificação de desastre
- organização das equipas de recuperação

Ferramentas:

- template do plano de recuperação
- software de processamento de texto
- software gráfico
- software de cálculo

Outputs:

- plano de recuperação

Métricas:

- O plano atinge os objectivos de recuperação!

2.3.7 Definição do Processamento Alternativo para as Funções Críticas

Cada função crítica de negócio deve ser avaliada para determinar se os procedimentos para o processamento alternativo são necessários e possíveis de se colocar em prática no período existente entre o desastre e a recuperação, seja a recuperação efectuada num *site* alternativo ou no Centro de Processamento de Dados principal.

Para as funções críticas seleccionadas os procedimentos para o processamento alternativo são desenhados e desenvolvidos de forma a serem executados enquanto as novas instalações dos Sistemas de Informação são restauradas.

Os procedimentos alternativos são uma forma de processamento de aplicações e funções críticas ao negócio sem a presença das normais instalações do Centro de Processamento de Dados. Em alguns casos existirão apenas procedimentos manuais ou a utilização de sistemas baseados em PC's *standalone*. Seja qual for a forma para se executar os procedimentos alternativos é necessário que os mesmos mantenham a continuidade da

informação. Na implementação de métodos e procedimentos alternativos não deve existir perda de informação como resultado da execução do processamento alternativo. Assim sendo, tem que ser considerada a implementação de uma forma de integração da informação, gerada no processamento alternativo, no sistema usual após a restauração do processamento normal.

Propósitos:

- Identificação das funções críticas para o processamento alternativo.
- Desenvolvimento das opções para processamento alternativo.
- Desenvolvimento dos procedimentos para o processamento alternativo.
- Desenvolvimento dos procedimentos para se regressar do processamento alternativo ao processamento normal.

Os procedimentos alternativos identificam passo-a-passo como deve ser efectuado o processamento alternativo das funções críticas ao negócio com que recursos e utilizando opções diferentes. Os procedimentos alternativos devem incluir verificações de integridade, linhas temporais, limiares e planos de ensaio. Devem incluir também os procedimentos de actualização e manutenção.

Inputs:

- funções críticas
- alternativas para o processamento de funções críticas

Ferramentas:

- ferramentas de processamento alternativo

Outputs:

- linhas temporais para funções críticas
- procedimentos alternativos

Métricas:

- relatórios e verificações da integridade da informação

2.3.8 Formação em *Recuperação de Desastres* e na *Continuidade*

É fundamental a implementação de um plano de formação em recuperação de desastres de forma a que a organização consiga assegurar que todas as pessoas recebem a formação adequada e essencial para a execução do plano. Embora um grande número de pessoas necessite de formação em recuperação de desastres, nem todas precisam do mesmo tipo de formação. O plano de formação deve ser mantido o mais simples possível e ao mesmo tempo satisfazer as distintas necessidades de formação. No mínimo, o plano de formação deve incluir objectivos, programas, cronogramas e administração da formação.

Propósitos:

- Desenho do plano de formação em recuperação de desastres.
- Desenvolvimento das actividades de formação específicas.
- Desenvolvimento das técnicas e ferramentas de avaliação.

Os planos de formação devem ser específicos, simples e completos. As actividades devem estar logicamente associadas a um ou mais dos objectivos gerais de recuperação. Os objectivos específicos devem descrever todas as actividades críticas que os formandos devem executar em caso de desastre. Com base na formação ministrada os formandos devem ser capazes de desempenhar com sucesso a totalidade das suas responsabilidades numa activação do plano de recuperação de desastres.

São utilizados formulários, *checklists*, notas e outras ferramentas para a avaliação do programa de formação.

Inputs:

- plano de recuperação
- papéis e responsabilidades
- processo de fluxo de recuperação de desastre
- objectivos do programa de formação

Ferramentas:

- cursos de formação com exercícios
- cenários
- critérios de avaliação

Outputs:

- avaliações dos formandos
- recomendações aos formandos

Métricas:

- atingir a totalidade dos objectivos do plano de formação

2.3.9 Ensaios do Plano de Recuperação de Desastres e de Continuidade

Um objectivo vital para a sobrevivência da organização é a existência do plano de recuperação de desastres, em papel, outro completamente distinto é a sua implementação e alcance com sucesso de todos os seus objectivos! Os ensaios são absolutamente vitais para o sucesso e capacidade de uma organização conseguir responder e recuperar de forma positiva a operacionalidade face a um evento catastrófico. Palavras como «ensaios» ou «exercícios» são preferíveis a «testes», porque a palavra «testes» tem conotação negativa. Implica «passar/chumbar». Não se pode chumbar um ensaio de recuperação de desastres. O mero facto de se estar a conduzir um ensaio planeado, com ou sem aviso, é considerado um sucesso. A palavra ensaio será utilizada durante toda esta secção.

Propósitos:

- Desenho do programa para os vários ensaios de recuperação.
- Desenvolvimento dos cenários de ensaio.
- Planeamento e calendarização dos ensaios, com e sem aviso.
- Desenvolvimento de técnicas de avaliação.

- Desenvolvimento da garantia de qualidade dentro do programa de ensaio.
- Condução de *briefings*.
- Desenvolvimento e distribuição dos relatórios *post-mortem* com as lições aprendidas, pontos a melhorar, etc.

Os ensaios são utilizados para a validação de todos os procedimentos do plano de recuperação de desastres. Isto inclui os procedimentos de notificação e de escaladas, listas de telefones, procedimentos de recuperação e procedimentos alternativos. Os ensaios servem também para validar que todos os bens essenciais, sistemas e hardware, documentação e todos os dados e informação necessárias estão disponíveis *off-site* e que os mesmos estão prontos para entrada em produção em caso de desastre. De igual forma os ensaios servem para assegurar que todos os elementos das várias equipas estão devidamente formados.

Ensaios contínuos reforçam os pontos chave e aumentam o compromisso com todo o processo.

Um plano de ensaio determina quais as áreas de recuperação e quais os processos que são ensaiados, com que frequência, potenciais cenários, critérios de medida, factores críticos de sucesso, pessoas envolvidas incluindo observadores e quais os objectivos e propósitos de cada ensaio. Formulários, *checklists* e estratégias de *briefing* devem ser desenvolvidas para avaliar os resultados finais.

Inputs:

- plano de ensaio
- procedimentos de recuperação
- procedimentos alternativos
- objectivos do ensaio
- responsabilidades e papéis

Ferramentas:

- Variadas: cassetes áudio, vídeos e cenários

Outputs:

- lições aprendidas
- relatório *post-mortem*

Métricas:

- atingir a totalidade dos objectivos do ensaio

2.3.10 Manutenção e Revisão do Plano de Recuperação de Desastres

O conteúdo do plano de recuperação de desastres deve ser revisto periodicamente. Isto ocorre segundo um cronograma pré-definido e a acção deve ser iniciada por um ou mais dos indivíduos que são responsáveis pela integridade do plano. Indivíduos que não estão directamente relacionados com o desenvolvimento do plano devem conduzir e participar nestas revisões. Isto fornecerá um olhar objectivo que é o que se pretende numa fase de revisão do planeamento.

Como nota, as pessoas que desenvolveram o plano não devem fazer a sua revisão.

Uma revisão objectiva com indivíduos das várias equipas, de auditoria interna, gestão do IT ou de consultores externos é tipicamente a melhor forma de se identificar os pontos fracos no plano. Para além das revisões periódicas o plano deve ser actualizado como parte do processo de Gestão da Mudança e com base em todas e quaisquer outras alterações com impacto na operacionalidade da organização.

Propósitos:

- Atribuição de responsabilidade pela manutenção do plano.
- Estabelecimento de procedimentos e cronogramas de manutenção e revisão do plano de recuperação de desastres.
- Integração do processo de manutenção do plano no processo de gestão da mudança.
- Criação de uma lista de distribuição.

A equipa de Gestão da Continuidade do negócio deve assegurar que os responsáveis nos processos de Gestão de Mudança estão directamente envolvidos nas actualizações do plano de recuperação de desastres. Isto também deve funcionar ao contrário, ou seja, à medida que forem sendo feitas actualizações à infra-estrutura e aos Sistemas de Informação devido às necessidades do planeamento de recuperação de desastres, a equipa de Gestão da Continuidade do negócio deverá notificar os responsáveis pela Gestão da Mudança, ou seja, as duas equipas devem trabalhar em conjunto e com objectivos comuns.

Tipicamente todos os planos de recuperação de desastres são considerados de natureza confidencial e as cópias devem ser seguidas e controladas. Os responsáveis pela manutenção do plano são responsáveis por controlar e distribuir as cópias actualizadas do plano, que devem ter um número ou identificador da versão, para assegurar que todos os membros têm a mesma versão, a versão actual.

Inputs:

- revisão da agenda
- lista de revisores
- objectivos e critérios de revisão
- plano de recuperação de desastres
- resultado dos ensaios

Ferramentas:

- N/A – não aplicável

Outputs:

- recomendações para melhorias ou mudanças
- lista de assinaturas dos revisores, geralmente exigida para efeitos de auditoria

Métricas:

- descobrir potenciais falhas no plano
- atingir os objectivos e cronograma de revisão

2.4 Políticas de Gestão na Continuidade

Em tempos incertos, é especialmente importante a organização estar preparada para o pior. Segundo Laye (2002) no evento de um desastre, os gestores devem executar as directivas e políticas organizacionais que devem ao mesmo tempo devem ser claras, inequívocas e elaboradas para atingirem o máximo beneficio para a organização.

De acordo com Henderson (2002) numa situação de emergência são necessárias decisões rápidas com respostas e medidas apropriadas dado que frequentemente não existe tempo para organizar e analisar as varias alternativas. Ao mesmo tempo deve existir um indivíduo no comando e que no caso de não estar disponível deve ser utilizada uma "cadeia de comando", para a implementação das políticas da organização no caso de uma ocorrência.

Solidificar e documentar as Políticas de Continuidade da organização são segundo Myers (1999), a chave para deter os custos exponenciais de desenvolvimento e a forma correcta de se terminar o projecto em tempo útil. Na sua opinião devem também ficar definidas todas as regras e suposições em que o plano deve ser baseado de modo a prevenir uma possível caça as bruxas durante a fase de desenvolvimento do plano.

A metodologia na presente dissertação considera não só as pessoas, processos de negócio e recursos como elementos essenciais no plano de continuidade do negócio, como também a sua integração nas políticas de Gestão da Continuidade, seguidamente propostas:

Política I : A organização assume o compromisso de planear e gerir a continuidade.

Isto é absolutamente crítico para o sucesso na Gestão da Continuidade do negócio.

A organização deve assegurar que todos os colaboradores e gestores compreendem o significado e valor deste planeamento. Sem um entendimento generalizado o plano poderá falhar.

Princípios e melhores práticas:

- assegurar que a Gestão da Continuidade do negócio é um objectivo chave para a sobrevivência da organização
- obter o compromisso da gestão de topo
- obter um gestor patrocinador do projecto
- criar a consciência de recuperação na organização
- obter o patrocínio de todas as unidades de negócio

Implicações:

- os esforços de planeamento podem falhar
- alteração na percepção de valores
- dificuldades na obtenção do apoio e cooperação das várias unidades de negócio

Benefícios:

- compromisso da gestão de topo assegura a importância do plano
- aumento do moral dos empregados ao colaborarem na protecção dos valores e dados críticos da organização
- reconhecimento dos membros chave do projecto e das equipas de recuperação

Política II : Definição dos objectivos de recuperação claros e realistas contemplando o alcance e extensão do plano de continuidade.

Com base nesta política devem ser definidos os objectivos de recuperação bem como a total extensão do plano. Os objectivos e janelas de recuperação devem ser realistas visando contemplar todas as funções críticas e vitais ao negócio. Existe uma relação directa entre o custo de *downtime* e o custo da protecção, assim sendo, o plano de recuperação de desastres deve definir claramente quais os tipo de desastres que o plano irá abordar, ou não. Devem ser definidas todas as componentes e unidades de negócio críticas para a organização abrangidas pelo plano.

Princípios e melhores práticas:

- alinhar o processo de recuperação para apoiar os objectivos de negócio
- assegurar que o impacto no negócio e o investimento na recuperação têm uma relação directa
- comunicação e validação dos objectivos e tempos de recuperação
- definição dos desastres que o plano de recuperação de desastres irá abranger e os que não são abrangidos
- reforçar o alcance dos esforços do planeamento

Implicações:

- expectativas desalinhadas
- o processo de recuperação poderá não suportar as necessidades de negócio
- noção errada de que o plano de continuidade é à prova de falhas

Benefícios:

- objectivos claros
- alcance dos esforços definidos
- expectativas acordadas e definidas
- esforços de recuperação coordenados

Política III : A gestão de risco e medidas de prevenção são postas em prática.

É vital garantir que todos os processos de gestão de risco e que todas as medidas que possam impedir ocorrências de desastres, ao serem identificadas, sejam postas em prática para minimizar potenciais riscos e prevenir desastres, com o objectivo de se garantir que um potencial desastre é controlado e/ou prevenir que o mesmo cause mais danos.

Princípios e melhores práticas

- assegurar que o ambiente é construído e operado de forma a se prevenir potenciais desastres

- à medida que a infra-estrutura e as necessidades de negócio mudam deve ser assegurado que são tidos em conta novos riscos e exposições

Implicações

- passagem por falhas de energia ou outro tipo de interrupções que podem ser evitados
- pequenos desastres podem fugir rapidamente ao controlo

Benefícios

- controlo de desastres evitáveis e previsíveis
- desvalorização e impedimento de potenciais desastres

Política IV : Desenvolver o plano de recuperação e de continuidade de forma a suportar a total recuperação das funções críticas ao negócio.

Partindo do princípio que todas as funções de negócio são críticas para a organização, é necessário ter em atenção que em caso de desastre a organização encontra-se numa situação de sobrevivência e não de *business as usual.*

As funções de negócio que têm um impacto mais significativo na organização, quer financeiras, quer operacionais ou ambas, devem ser recuperadas primeiro. Todas as funções de negócio devem ser avaliadas e medidas de forma a assegurar a existência de prioridades e *rankings* apropriados caso seja necessário uma recuperação total.

Isto pode incluir no planeamento a elaboração e distribuição de cartas de confiança previamente preparadas para os clientes chave.

Princípios e melhores práticas:

- investir em métodos adequados, preventivos, proactivos e de recuperação para as funções críticas de negócio
- definir e comunicar todas as funções de negócio e qual o seu valor crítico para a organização

- garantir que os clientes chave são assegurados quanto ao processo de continuidade

Implicações:

- desconhecer-se quais as funções que têm que ser recuperadas primeiro
- recuperação de funções de negócio menos críticas antes das críticas

Benefícios:

- as expectativas são claramente definidas e acordadas
- minimização de perdas significativas em termos financeiros, legais e operacionais

Política V : Ensaios regulares do plano de recuperação e de continuidade do negócio.

Uma vez desenvolvido o plano de recuperação de desastres é imperativo que o mesmo seja ensaiado de forma regular. Existem inúmeras técnicas para ensaiar planos de continuidade, desde simples exercícios escritos, apenas no papel, até ensaios completos ou de «pull-the-plug». As equipas de Gestão da Continuidade do negócio e de recuperação de desastres têm que estar directamente envolvidas nos ensaios, onde devem também participar observadores externos para avaliarem de forma imparcial a globalidade das operações.

Os factores críticos de sucesso e objectivos dos ensaios devem ser definidos como parte do processo de planeamento.

Os ensaios planeados não devem ter uma duração superior a seis horas, se possível menos, devem ser seguidos de um *briefing* e de uma reunião *post-mortem*. Todas as lições aprendidas, novas informações, etc... devem ser actualizadas no plano de recuperação de desastres. Os ensaios devem ser planeados, com ou sem aviso e serem tão simples como a evacuação de um prédio para desactivação das linhas telefónicas ou tão complexos como a mudança total de instalações e arranque dos serviços alternativos.

Princípios e melhores práticas:

- definição clara dos objectivos de ensaios e critérios de sucesso
- condução de ensaios regulares, planeados com e sem aviso
- condução de ensaios parciais e completos
- utilização de várias técnicas de ensaio

Implicações:

- os processos e procedimentos podem não funcionar
- as equipas de recuperação poderão não saber o que fazer
- configurações incorrectas/não existentes, conhecimentos insuficientes, falta de informação
- a própria recuperação da simulação do desastre pode não funcionar
- os consumidores podem perder a confiança no IT da organização
- visibilidade negativa

Benefícios:

- o potencial de uma recuperação com sucesso é alto
- reforça a aprendizagem e o compromisso
- demonstra valor para a organização
- identifica os potenciais pontos fracos no plano de recuperação de desastres

Política VI : As novas implementações e mudanças nos Sistemas de Informação são integradas no plano de recuperação e de continuidade.

Como compromisso contínuo para com o processo de Continuidade do negócio é vital considerar o impacto dos novos sistemas e das novas aplicações críticas nas estratégias da organização e no plano de recuperação de desastres existente. É de suma importância, quando se desenha uma nova arquitectura ou uma nova solução aplicacional crítica para o negócio, a actualização imediata do plano de recuperação de desastres.

Princípios e melhores práticas:

- garantir que os planos de Gestão da Mudança são implementados tendo em conta a Continuidade do negócio
- definir procedimentos de recuperação para as novas aplicações, novos sistemas e configuração de redes

Implicações:

- os procedimentos de recuperação das últimas alterações podem não estar integrados no plano de recuperação de desastres
- implementação de novos componentes sem planos de contingência, de continuidade ou de suporte

Benefícios:

- a continuidade é um componente crítico no ambiente de operações
- as estratégias do plano de recuperação de desastres desempenham um papel vital no desenho e lançamento de decisões para as novas implementações

Política VII : Actualização e revisão periódica do plano de recuperação e continuidade.

O plano de recuperação de desastres pode por inúmeros motivos ficar rapidamente desactualizado. Uma metodologia deve ser definida e colocada em prática para planear e agendar revisões periódicas do plano, para assegurar a validade e eficácia do mesmo. É recomendado que os revisores do plano não sejam os mesmos que o desenvolveram ou testaram. É também fundamental que a revisão seja objectiva e efectuada por várias entidades de departamentos diferentes e em conjunto com o grupo de gestão, grupos de auditoria interna ou uma terceira parte consultora.

Esta política na recuperação de desastres inclui também a gestão das revisões e do processo de distribuição do próprio plano.

Princípios e melhores práticas:

- definir e agendar revisões regulares do plano de recuperação de desastres
- assegurar que os revisores não são os mesmos que desenvolvem o plano; para isso devem ser utilizados grupos de trabalho distintos e objectivos nas revisões e ensaios
- assegurar as actualizações do plano na integração e no processo de Gestão de Mudança dos Sistemas de Informação
- definição e documentação das revisões, *tracking* e lista de distribuição

Implicações:

- o plano de recuperação de desastres poderá estar ultrapassado e desta forma ser irrelevante
- procedimentos incluídos no plano podem não ser de fácil utilização por pessoas não envolvidas no início do planeamento
- indivíduos possuírem múltiplas revisões desactualizadas do plano

Benefícios:

- mantém o plano de recuperação de desastres como um documento vivo
- assegura a manutenção e actualização do plano
- efectuam-se acções de informação do propósito do plano e dos seus benefícios para toda a organização
- assegura que todos os membros têm a mesma versão, a actual, do plano de recuperação de desastres

2.5 Funções e Responsabilidades

É importante definir de modo claro as funções e as responsabilidades dos vários elementos e equipas que se revelam fundamentais no processo de recuperação de desastres. A indefinição das equipas e das suas respectivas responsabilidades dará origem a um caos desnecessário que irá prejudicar uma recuperação atempada, organizada e com sucesso. Esta área demonstra um elevado potencial de visibilidade positiva, mas o inverso poderá ser considerado.

Deste modo as várias unidades de negócio têm que trabalhar em conjunto com o processo de Gestão da Continuidade do negócio, dado que todas as unidades de negócio serão afectadas directa e indirectamente pelo processo global de Gestão da Continuidade e pelos seus componentes.

Uma vez que o processo atravessa fronteiras organizacionais requer elevados padrões de definição, planeamento e validação por todos os que se encontram envolvidos. Um dos factores críticos de sucesso nesta área consiste no nível de patrocínio e empenho da gestão de topo na organização. De acordo com a visão de Janco (2004) algumas destas funções são únicas, dado que a maior parte das funções não implicam a necessidade de envolvimento a tempo inteiro, com excepção dos dois cargos de liderança: o Gestor da Continuidade e o Coordenador da Continuidade.

É importante referir que apenas num processo de Gestão da Continuidade do negócio as funções atribuídas podem ser executadas a tempo parcial após a conclusão do planeamento. Excluindo o gestor e o coordenador da continuidade esta situação é aplicável depois do desenvolvimento do plano de recuperação de desastres e de um ensaio geral dos vários processos alternativos e do próprio plano terem sido executados por pelo menos uma ocasião.

Caso ocorra um desastre que justifique a activação do plano de recuperação de desastres todos os elementos das equipas de recuperação devem entrar em acção. É por este motivo que na maior parte das vezes, a não ser que ocorram acidentes diários ou outras interrupções de serviços, os elementos das equipas de recuperação não precisam actuar de modo exclusivo nesta actividade. E, no caso em que ocorrem acidentes ou interrupções diárias dos serviços a sua resolução não deve ser da responsabilidade das equipas de recuperação dado que representam problemas que devem ser resolvido de outra forma.

Segue-se uma aproximação do que se entende por funções e responsabilidades identificadas no processo de Gestão da Continuidade do negócio.

2.5.1 Gestor da Continuidade

Função

O gestor da continuidade é funcionalmente responsável pelos planos de contingência, recuperação, continuidade e restabelecimento dos serviços que devem ser definidos, comunicados, executados, documentados e ensaiados. A sua função consiste na gestão do processo de continuidade do negócio de modo a assegurar a operacionalidade contínua das funções críticas ao negócio e assegurar a minimização de potenciais perdas para a organização.

Responsabilidades

- contacto com a gestão de topo
- funcionalidade do plano de continuidade do negócio
- sucesso do processo de recuperação e de continuidade
- comunicação e manutenção de alertas
- integração do processo nas várias unidade de negócio da organização

Áreas de resultados chave

- assegurar a existência de um plano de contingência de modo a minimizar prejuízos financeiros
- assegurar a existência de um plano de contingência de modo a minimizar prejuízos operacionais
- assegurar a exequibilidade do plano de recuperação de desastres
- obter aceitação e aprovação por parte dos auditores internos

2.5.2 Coordenador da Recuperação

Função

O coordenador da recuperação e continuidade do negócio é responsável pela operacionalidade, ensaios e revisão do plano de recuperação de desastres e

continuidade dos serviços. Actua como facilitador durante a execução e activação de um plano de recuperação de desastres.

Responsabilidades

- coordenação de todos os processos de recuperação
- formação dos membros das equipas de recuperação da organização
- coordenação e liderança de todos os exercícios de simulação das equipas relativos aos planos de contingência
- agilização de todos os processos de recuperação
- ligação com o gestor da continuidade do negócio
- definição e desenvolvimento do plano de Gestão da Continuidade do negócio
- contratação de serviços

Áreas de resultados chave

- assegurar o envolvimento de todos os membros das equipas de recuperação
- assegurar toda a logística do processo de recuperação
- elaborar os relatórios de *status* para o gestor da continuidade do negócio

2.6 Equipas de Recuperação

As equipas de recuperação desenvolvem todas as acções necessárias à recuperação dos serviços dentro das suas áreas de responsabilidade, após a ocorrência de um desastre. Para cada área de negócio deve existir uma equipa de 5 a 7 elementos e um chefe de equipa bem como o seu *backup*.

Segundo Janco (2004) as equipas de recuperação devem operar sob a liderança de uma equipa de gestão que monitoriza e coordena os esforços de recuperação. Cada equipa é definida com base nas suas funções para com a disponibilização dos processos de Gestão da Continuidade do negócio.

A equipa de Gestão da Continuidade do negócio é constituída pelo gestor da continuidade do negócio, pelo coordenador da recuperação e pelos líderes das várias equipas de recuperação constituídas para o efeito.

Cada equipa de recuperação divide-se nas seguintes secções:

- chefe de equipa
- chefe de equipa alternativo ou *backup*
- membros da equipa
- escala da equipa

Responsabilidades dos chefes das equipas.

- são responsáveis pela gestão das actividades das equipas
- são responsáveis pelas actividades que envolvem a avaliação de danos e prejuízos, coordenação com outras equipas de recuperação, decisões sobre acções de recuperação a empreender, manutenção de registos e elaboração de relatórios dos *status* de recuperação
- cada chefe das várias equipas de recuperação é membro activo da equipa de Gestão da Continuidade do negócio

Responsabilidades do chefe de equipa substituto ou de backup.

- funciona como chefe de equipa em caso de indisponibilidade do chefe de equipa.

Responsabilidades dos vários membros das equipas.

- são responsáveis pela execução das acções de recuperação
- um ou mais elementos por cada área funcional ou operacional devem estar representados na equipa
- o número de elementos necessários para uma determinada área depende das circunstâncias apresentadas
- alguns elementos podem integrar mais do que uma equipa, especialmente em pequenas organizações
- dependendo do tipo e dimensão do acidente nem todos os membros da equipas podem ser necessários

2.6.1 Equipa de Recuperação de Instalações

Funções

A responsabilidade da equipa de recuperação de instalações consiste na verificação da avaliação dos danos no local, minimização de outras perdas e recuperação dos recursos possíveis de serem restaurados, reparação e segurança das instalações danificadas, preparação e manutenção do *site* alternativo para os Sistemas de Informação e preparação dos processos de restauro, coordenação de entradas e saídas do *site* alternativo em conjunto com a equipa de gestão de recuperação de desastres.

Possíveis membros da equipa:

- planejadores e gestores de instalações (ar condicionado, electricidade, chãos elevados, sistema de segurança, detecção de incêndios/sistemas de supressão), bem como os responsáveis pela concepção do centro de processamento de dados principal e alternativo
- operações de IT
- departamentos financeiro, jurídico e de seguros com ligação a representantes comerciais
- especialistas em engenharias
- auditores internos
- gestores de segurança

2.6.2 Equipas de Administração

Funções

A função mais importante das equipas de administração consiste em servirem de fornecedores. Por norma, as equipas de administração funcionam como fornecedores de recursos aos membros da equipa de Gestão da Continuidade do negócio e não de apenas meros utilizadores. As suas responsabilidades podem incluir o transporte, segurança, seguros, disponibilização de verbas para despesas, passagem de informação aos colaboradores e à área de relações públicas.

Possíveis membros da equipa:

- manager
- transporte
- financeiro
- recursos humanos
- segurança
- relações públicas
- seguros
- departamento jurídico
- compras
- administrativo

2.6.3 Equipas de Recuperação de Sistemas

Funções

As principais funções das equipas de recuperação de sistemas consistem em assegurarem o restabelecimento dos serviços de aplicações e funções críticas, o levantamento dos meios de informação e dos recursos necessários fora do local de armazenamento e assegurarem a existência de *staff* adequado e disponível para a operação alternativa aos Sistemas de Informação no seguimento de um desastre.

Possíveis membros da equipa:

- administradores de sistemas
- supervisores / managers
- analistas de sistemas e aplicações
- técnicos de hardware
- engenheiros
- dispatcheres
- operadores
- gestores da bandoteca

2.6.4 Equipa de Recuperação de Comunicações Dados/Voz

Funções

As responsabilidades da equipa de recuperação de comunicações de dados/voz consistem na reparação, recuperação e restauro dos serviços de comunicação de dados e voz para as funções de negócio críticas. Devem trabalhar em colaboração com outras equipas para redireccionar o tráfego de informação, assim como cooperar com outros fornecedores de comunicações e estabelecer um interface com os membros das várias equipas de recuperação.

Possíveis membros da equipa:

- manager de comunicações dados/voz
- analistas de comunicações dados/voz
- administradores de redes
- engenheiros de redes

2.6.5 Equipa de Recuperação e Comunicação com os Utilizadores

Funções

A equipa de recuperação e comunicação com os utilizadores é responsável pela manutenção e actualização da informação no que se refere aos recursos necessários para as aplicações dos utilizadores consideradas críticas. Deve funcionar como um elo de comunicação contínuo entre o local onde se encontram os utilizadores e o site alternativo dos Sistemas de Informação, assegurando que os requisitos de processamento dos utilizadores e que as suas prioridades são transmitidas às *Equipas de Recuperação de Sistemas* e às restantes equipas. Esta equipa é também responsável pela negociação das prioridades tal como definido na política da organização.

Possíveis membros da equipa:

- representantes dos utilizadores locais e remotos
- suporte às aplicações
- programação de sistemas

2.6.6 Equipa de Controlo de Informação

Funções

A equipa de controlo de informação será de maior ou menor dimensão consoante o nível do acidente. Fornece um fluxo de *input, pickup e balancing* da informação e de distribuição para o site alternativo. Podem ser necessários recursos de entrada de dados. Esta equipa deve gerir a biblioteca/bandoteca e adquire o material necessário como tapes e cartridges.

Possíveis membros da equipa:

- manager de controlo de informação
- operadores de supervisão de entrada de informação
- distribuição e controlo de qualidade
- responsáveis e fornecedor de formulários
- colaborador responsável pela atribuição de funções no site alternativo
- técnicos de tapes

2.6.7 Equipa de Recuperação de Aplicações

Funções

A equipa de recuperação de aplicações é responsável pela recuperação das aplicações. Esta equipa pode ser dividida em sub-equipas dependendo dos ambientes. Estas sub-equipas podem ser compostas da seguinte forma: Sistemas *UNIX* e *Windows, SAP, Oracle*, etc... Coordenam o seu trabalho com as restantes *equipas de recuperação de desastres* para reposição dos serviços e das aplicações. Esta operação pode incluir a recuperação de *logs* de transacções, operações *roll forward/back*, ou outros requisitos aplicacionais. As equipas devem também funcionar como interface com a *Equipa de Comunicação com o Utilizador*, de modo a assegurarem que a informação do *status* da situação chega aos utilizadores.

Possíveis membros da equipa:

- manager(s) da aplicação
- suporte à aplicação

III – Soluções de Sistemas e Tecnologias de Informação que suportam a Continuidade

3.1 Benefícios para a Organização

Um ambiente que se encontre implementado numa plataforma tecnologicamente redundante e que permita a disponibilidade de serviços na ordem dos 99.95% (quatro horas de *downtime*/ano) a 99.999% (5 minutos), permite que os vários tipos de *downtime* sejam minimizados e controlados resultando num ambiente produtivo com uma maior estabilidade e um maior nível de alta disponibilidade.

As organizações ao criarem os *packages* de *software aplicacional* com os vários conjuntos de aplicações críticas para o negócio e transformarem estes *packages* de *software* crítico em soluções *Mission Critical*, implementados em ambientes de alta disponibilidade, conseguem retirar todos os benefícios que advêm deste tipo de soluções. Um ambiente *mission critical* consiste desta forma numa combinação de *hardware*, sistemas operativos e o *middleware* correspondente à componente de *software* aplicacional, implementados de forma redundante em *clusters* que trabalham em conjunto de modo a minimizar os impactos e falhas nos serviços disponibilizados.

Segundo Weygant (2001) a alta disponibilidade caracteriza um Sistema de Informação que é desenhado de forma a evitar a perda de serviços, reduzir e gerir falhas e ao mesmo tempo minimizar a indisponibilidade aplicacional. Para Piedad & Hawkins (2000) o termo alta disponibilidade significa uma redução no *downtime* aplicacional, planeado ou não, que é sentido pelos utilizadores ou pelas próprias aplicações. Os *downtimes* não planeados incluem todos os acontecimentos imprevistos que causam um impacto negativo nos Sistemas de Informação com a negação temporária do acesso à informação. Os *downtimes* planeados são todos os eventos geridos de forma controlada tais como *backups offline*, *upgrades* de sistemas, revisões de *patches* ou alterações nas configurações de *hardware*.

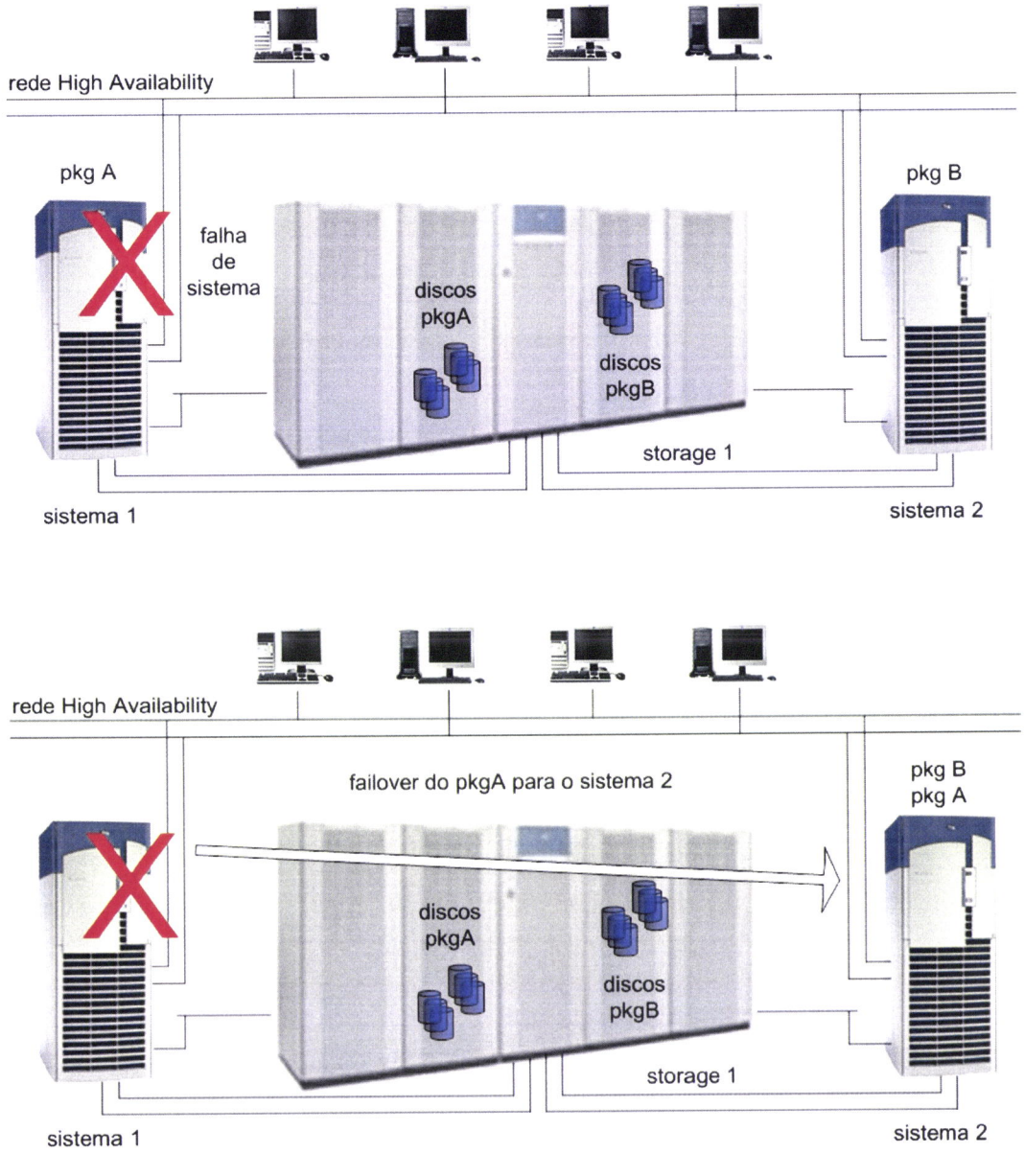
Weygant (2001) refere também que a alta disponibilidade é expectável quando a vida, a saúde e o bem estar, incluindo o bem estar económico de uma organização, dependem disso.

A alta disponibilidade implementa-se numa primeira fase com base na utilização de um espaço de *storage* partilhado e endereços *IP* flutuantes ou re-alocáveis, para permitirem o acesso aos *packages* de *software* críticos a partir de um único ponto de acesso, independentemente do sistema onde se encontre a correr. Desta forma obtém-se a livre movimentação dos *packages* de *software* entre os vários sistemas no *cluster*. Este tipo de solução permite que se efectuem alterações de forma independente em cada um dos sistemas no *cluster* enquanto se mantêm a total disponibilidade aplicacional.

3.2 Soluções e Arquitecturas Tolerantes a Desastres

Ao se considerar, por exemplo, um centro de processamento de facturação onde falhas de energia possam ser comuns durante os invernos rigorosos, ou ao se considerar os Sistemas de Informação que gerem uma Bolsa de Valores onde um falha de sistema causa um significativo impacto financeiro, verificamos que para este tipo de organização, e muitas mais com características semelhantes, é importante que os sistemas fiquem protegidos não só contra os chamados "ponto de falha", mas também contra os múltiplos pontos de falha. Ou mesmo protegidos contra uma falha total que condiciona o funcionamento do próprio Centro de Processamento de Dados. Um Centro de Processamento de Dados num contexto de recuperação de desastres é um conjunto de sistemas, discos e redes com proximidade física entre si.

Figura 3-1 Implementação de uma Arquitectura de Alta Disponibilidade

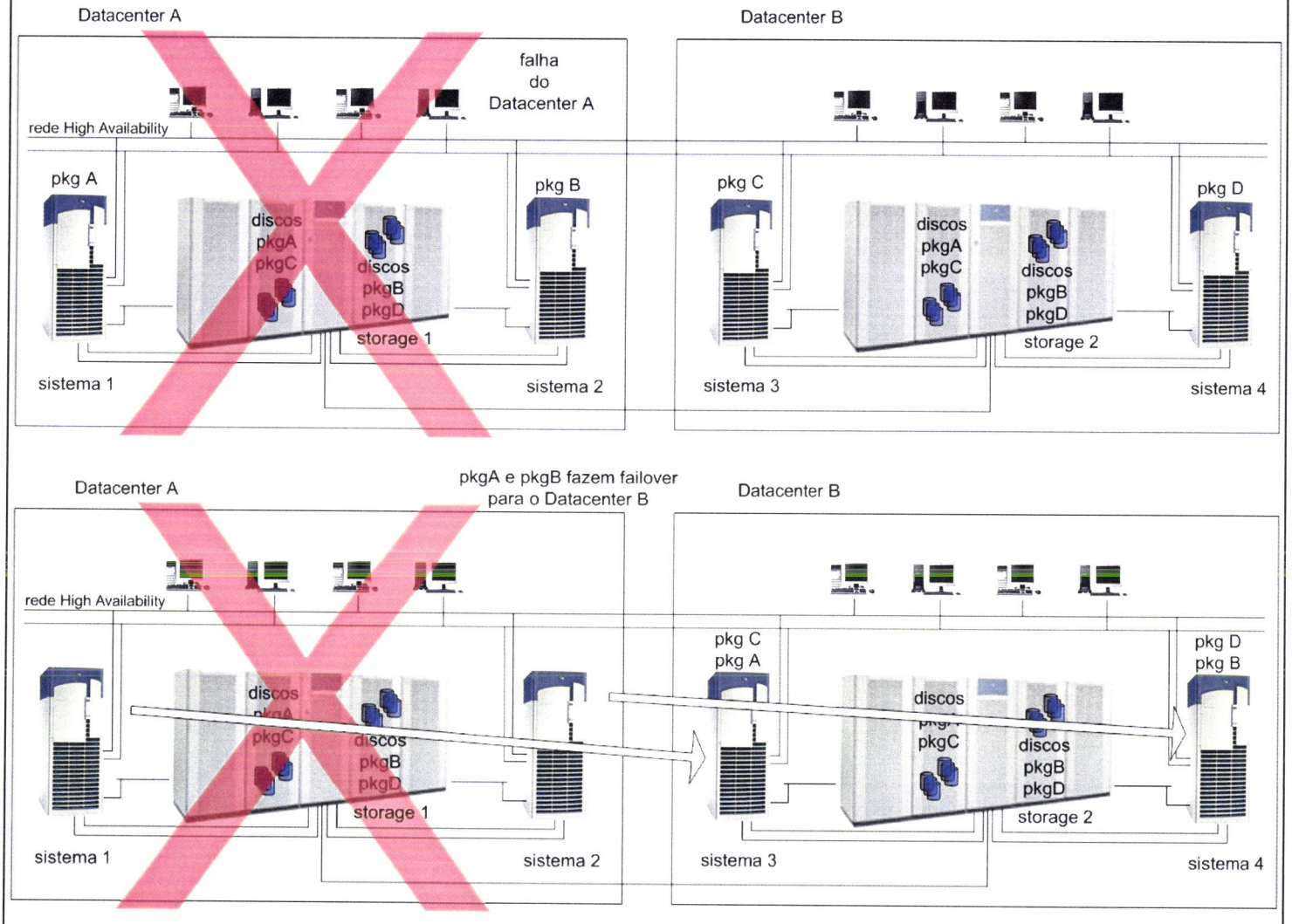


Para algumas organizações este tipo de protecção poderá não ser suficiente!

Gordon (1999, citado por Everitt, 2001) define o termo *cluster* em termos de coesão interna - homogeneidade - e isolação externa. A criação de *clusters* que são capazes de resistir a múltiplos pontos de falha ou a totais interrupções de serviço requerem um tipo de arquitectura denominada *Disaster Tolerant*. Esta arquitectura disponibiliza a capacidade de transferência dos serviços e aplicações mission critical para uma parte alternativa do *cluster* após a ocorrência de um determinado tipo de desastre.

De forma geral um *cluster Disaster Tolerant* providencia um *failover* automático em caso da falha completa de um Centro de Processamento de Dados.

Figura 3-2 Implementação de uma Arquitectura Disaster Tolerant



Esta é a "espinha dorsal" das soluções *Mission Critical, Disaster Tolerant Clusters* abordadas na presente dissertação.

Devem ser referidas as perspectivas e os pontos que justificam que para uma protecção contra múltiplos pontos de falha um *cluster* deve estar geograficamente disperso, e que os nós do *cluster* devem estar em salas separadas, espalhadas pelos andares de um edifício ou preferencialmente em edifícios separados ou cidades distintas.

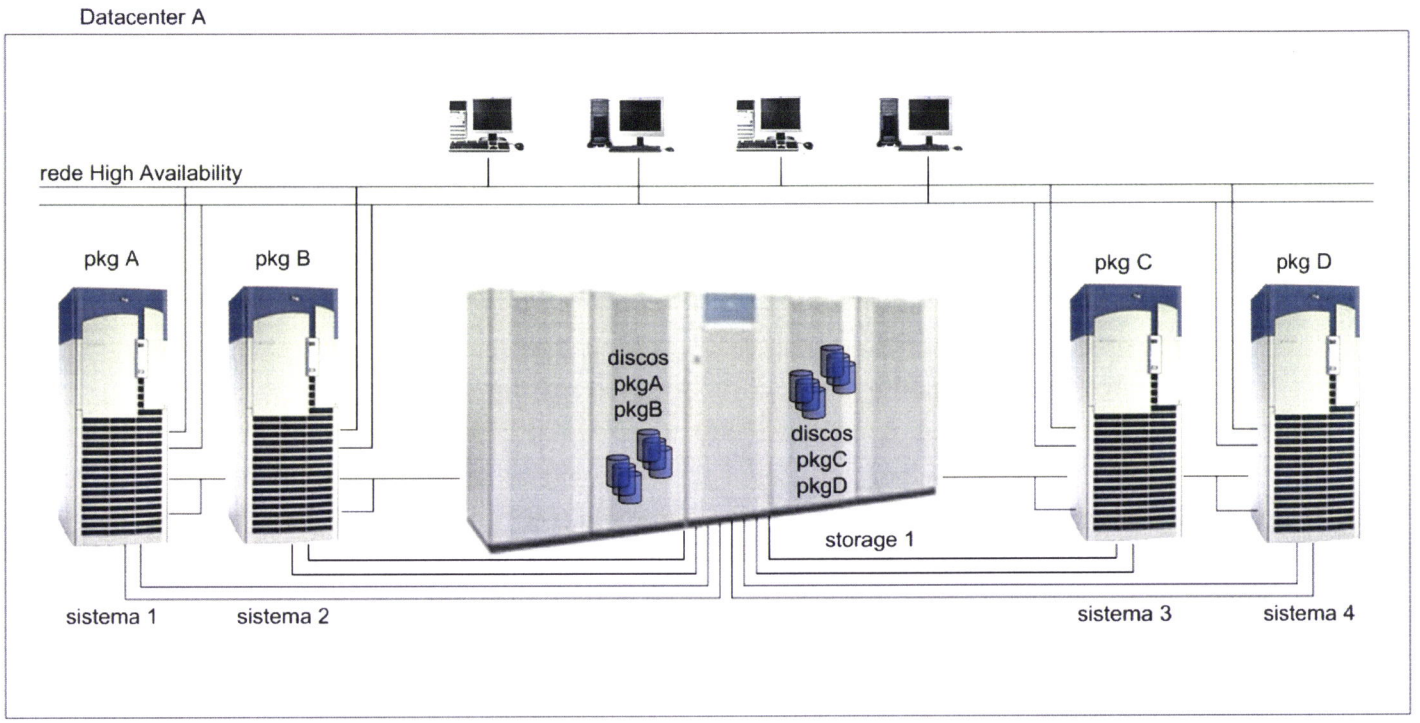
A distância entre os nós do *cluster* está dependente do tipo de desastre do qual é necessária a prevenção e do tipo de tecnologia utilizada para se replicar a informação.

É importante referir que, segundo Piedad & Hawkins (2000), nas arquitecturas cliente/servidor em *cluster* cada recurso computacional pode ser um cliente, um servidor ou ambos em diferentes alturas.

3.2.1 Clusters Locais

Um *cluster local* tem todos os nós localizados num único Centro de Processamento de Dados e não é um *cluster Disaster Tolerant*. Como a maioria dos clusters de alta disponibilidade são *clusters locais*, são incluídos aqui apenas como linha de base para comparação com as arquitecturas *Disaster Tolerant*.

Figura 3-3 Implementação de um Cluster Local

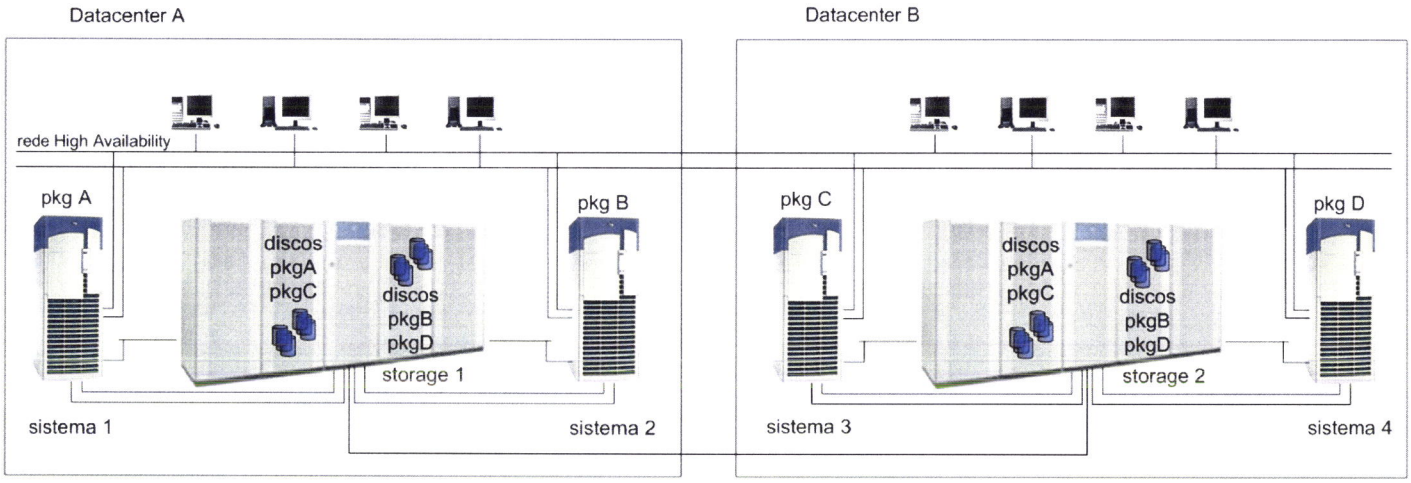


3.2.2 *Extended Campus Clusters*

Um *extended campus cluster* tem todos os sistemas alternativos localizados num segundo Centro de Processamento de Dados redundante. Os Centro de Processamento de Dados podem estar em salas separadas, edifícios adjacentes, ou em edifícios separados por curtas ou médias distâncias. A palavra "*campus*" implica que a organização possui um leasing sobre o terreno, ou sobre os edifícios adjacentes, de maneira que não precisa de uma autorização externa para cavar trincheiras e passar toda a estrutura de cabos, ou para efectuar o reencaminhamento dos circuitos de energia necessários para a implementação de um *extended campus cluster*.

Os *campus clusters* são ligados entre si através de uma ligação de alta velocidade que garante o acesso de rede entre os nós do *cluster* de modo a que todas as premissas de um ambiente *Disaster Tolerant* sejam cumpridas. A distância entre os nós num *extended campus cluster* é apenas limitada pela tecnologia de replicação de dados.

Figura 3-4 Implementação de um *Extended Campus Cluster*



Os requisitos de arquitectura para um *extended campus cluster* são:

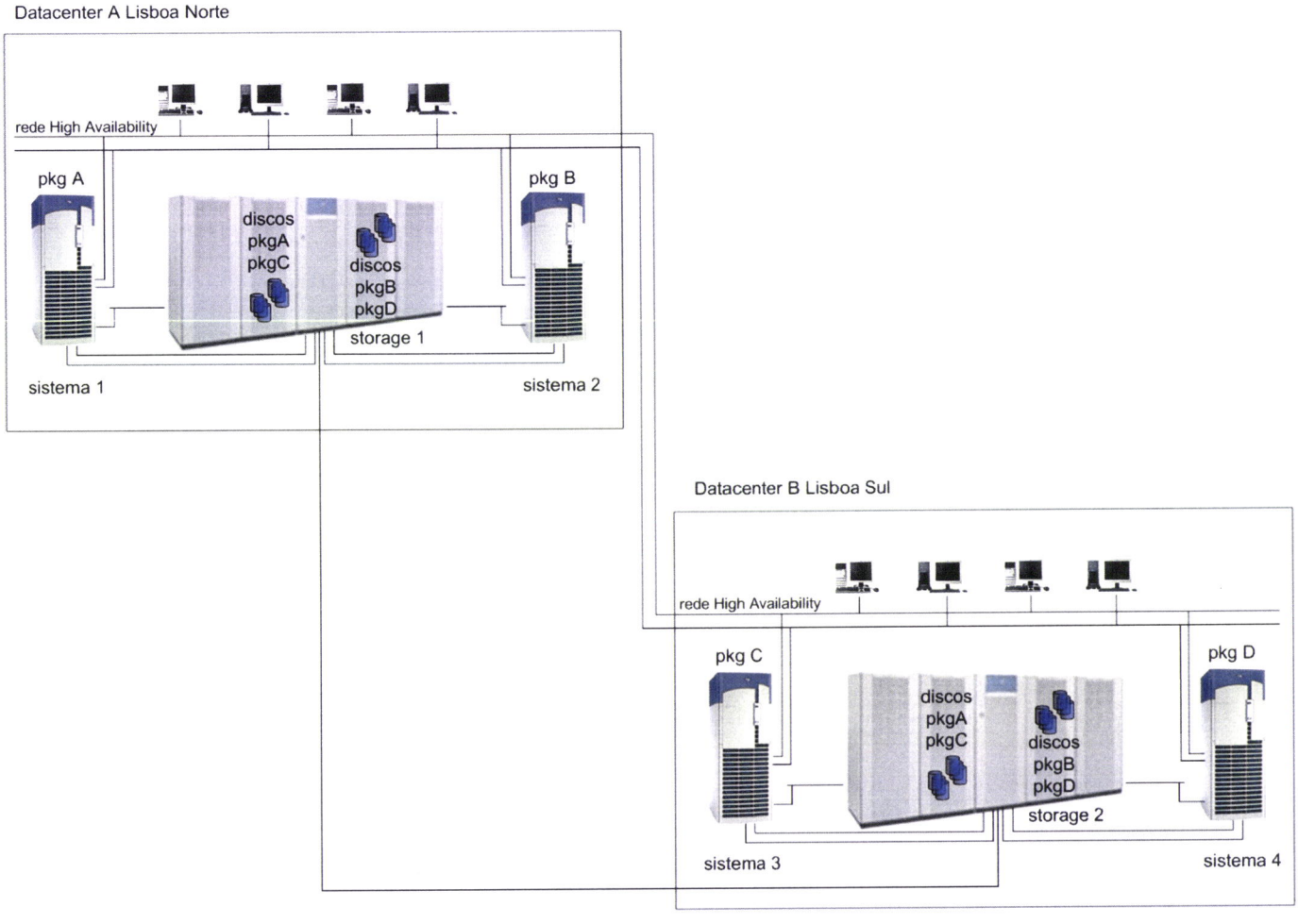
- Discos redundantes com a utilização de replicação de dados. Três exemplos são o *Symmetrix Remote Data Facility, SRDF* da EMC, que replica e sincroniza os dados entre dois *disk arrays* Symmetrix, o *Continous Access, CA* por parte da HP para a replicação por hardware dos sistemas de *storage XP* e o *MirrorDisk/UX* que replica por *software* os dados entre discos de qualquer tipo.

- Interfaces de rede redundantes instalados e configurados de modo a utilizarem caminhos diferentes. Isto protege o *cluster* de um acidente que possa afectar ambos as redes ao mesmo tempo.
- A energia eléctrica para cada Centro de Processamento de Dados deverá ser fornecida por circuitos diferentes. Algumas organizações podem requerer o fornecimento de energia a companhias diferentes, protegendo-se desta forma contra uma falha de energia ou acidentes pontuais que possam cortar a energia a todos os nós do *cluster*.

3.2.3 *Metropolitan Clusters*

Um *metropolitan cluster* é um *cluster* que tem os nós principais e os nós alternativos do *cluster* localizados em diferentes partes de uma cidade ou em cidades adjacentes. Ao aumentar a distância entre os nós do *cluster* aumenta-se a probabilidade da disponibilidade dos nós alternativos para *failover* no evento de um desastre.

Figura 3-5 Implementação de um *Metropolitan Cluster*

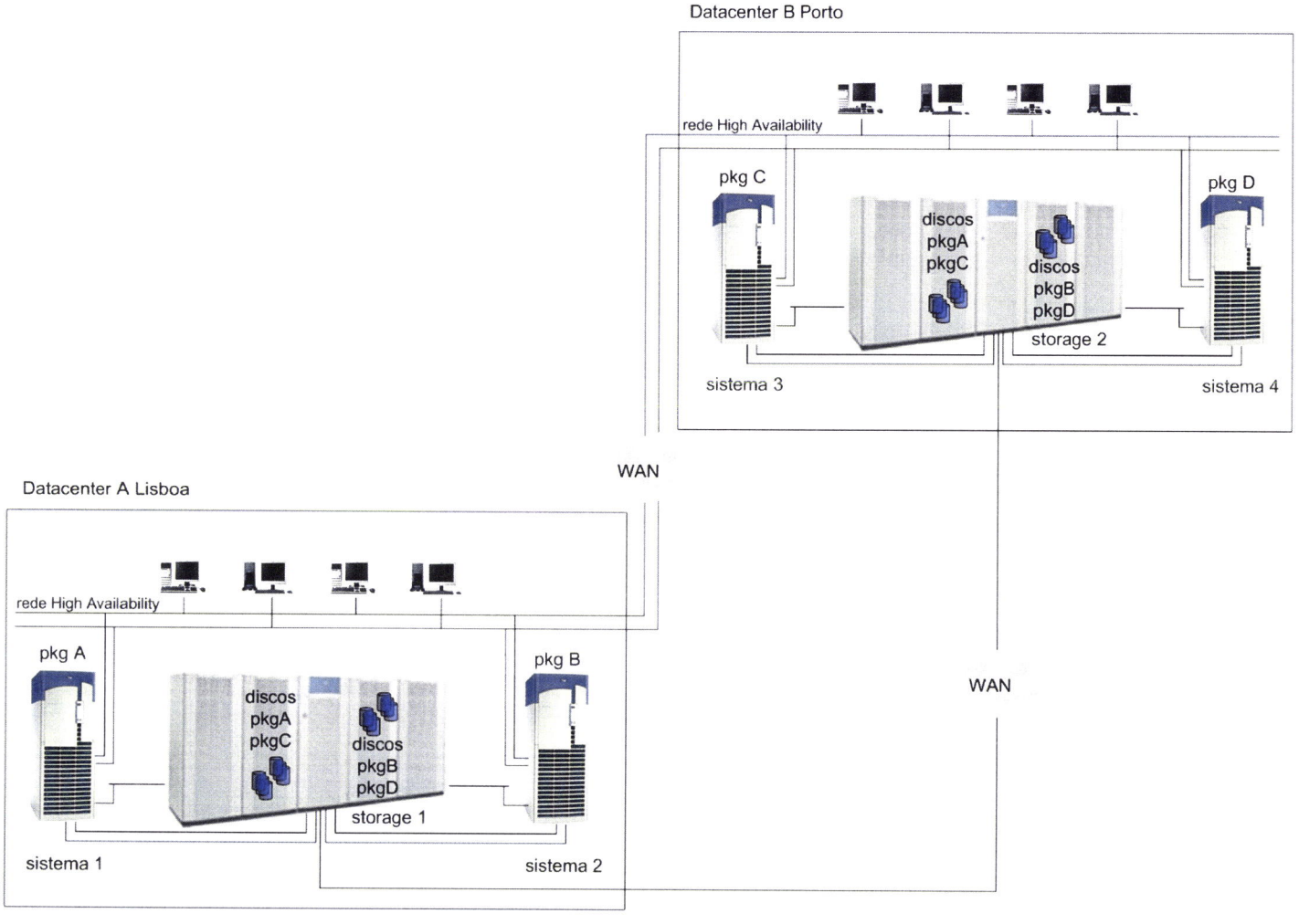


Os *metropolitan clusters* são muito semelhantes aos *extended campus clusters* com a excepção de que os *metropolitan clusters* frequentemente precisam de licenças das autoridades locais ou do governo para a passagem de toda a estrutura da cabos de rede e de replicação de dados. Isto pode aumentar o grau de complexidade do desenho e de implementação de um *metropolitan cluster*. Os requisitos de arquitectura são os mesmos que para os *extended campus clusters*. E como nos *campus clusters* a distância que separa os nós no metropolitan cluster é limitada apenas pelas tecnologias de replicação de dados e de rede existentes.

3.2.4 *Continental Clusters*

Um *continental cluster* tem os nós principais e alternativos do *cluster* separados por distâncias superiores a 100 km de modo a que a ligação *WAN (Wide Area Network)* do tipo T1 ou T3/E3 têm que ser contratadas a operadoras de telecomunicações. É uma solução extremamente cara de se arquitectar e de se implementar.

Figura 3-6 Implementação de um *Continental Cluster*



As principais características para a definição de uma *WAN* num *continental cluster* são:

- A ligação física deverá ser composta por uma ou mais linhas geridas por um ou mais operadores. Os operadores não conseguem garantir a mesma fiabilidade que um cabo físico dedicado, dado que a distância gera uma latência e um delay temporal na replicação dos dados, que por sua vez pode criar um problema com a integridade da informação.
- Ferramentas como *Transaction Processing Monitors, TPM* ou ferramentas de replicação de bases de dados que trabalham através da *WAN* são necessárias para garantir a replicação consistente da informação.
- Questões operacionais tais como a gestão das diferentes equipas nos dois Centros de Processamento de Dados, com procedimentos diferentes e a própria gestão dos ensaios de *failover* são mais complicados quanto maior for a distância entre os nós do *cluster*.

3.3 Factores Críticos na Gestão de uma Solução Tolerante a Desastres

3.3.1 A Necessidade de Protecção da Informação

A protecção da informação e a total recuperação de desastres são peças fundamentais na solução de Continuidade do negócio e consistem no tema principal desenvolvido ao longo deste documento. Marcus & Stern (2003) referem claramente que a alta disponibilidade não pode ser alcançada meramente ao se instalar uma peça de *software* de gestão para ambientes de alta disponibilidade.

A protecção da informação é um factor vital e deve definir-se na concepção dos Sistemas de Informação e dos procedimentos que asseguram um acesso contínuo à informação dentro da organização. A recuperação de desastres por sua vez e conforme já referido consiste num processo complementar que assegura uma rápida recuperação dos Sistemas de Informação e de todas as aplicações e funções críticas ao negócio perante a ocorrência de um desastre com grande impacto na organização.

A protecção dos Sistemas de Informação e o acesso de forma contínua aos dados são obtidos numa primeira fase através da eliminação dos vários pontos de falha nos servidores, sistemas de armazenamento de dados e redes. O *hardware*, o *software* e redes redundantes em conjunto com fontes alternativas de electricidade tornam os Sistemas de Informação mais resistentes a falhas. Mas o ciclo de actualização de cópias da informação e os vários métodos de replicação da informação estão directamente relacionados com os custos associados à indisponibilidade dos sistemas, aplicações e informação, e do que poderá ser considerado pela organização como aceitável no intervalo de tempo que pode existir desde a última cópia ou *backup* da informação, o início de uma ocorrência adversa grave, até à reposição completa de todos os serviços e informação.

Num passado muito próximo a capacidade de recuperação de desastres correspondia apenas à capacidade de restaurar a informação da organização eventualmente num outro local para se regressar ao processamento das funções de negócio. Tradicionalmente os planos de recuperação de desastres estavam apenas orientados para os Sistemas de Informação críticos, incluindo contabilidade financeira, planeamento de recursos da organização (ERP's), assim como outras aplicações de negócio de grandes dimensões. Estas aplicações estão frequentemente localizadas num Centro de Processamento de Dados e corriam/correm em *batches* ou em sistemas de processamento de transacções online (OLTP) durante as horas de expediente da organização. Entre os *batches* e o processamento no horário de expediente, as bases de dados, os ficheiros e grande parte da informação podiam/podem ser duplicadas e as cópias transferidas para outros Centro de Processamento de Dados através da *WAN*, ou através de outro tipo de suporte tais como tapes magnéticas.

Actualmente os planos de recuperação de desastres enfrentam novos desafios.

As organizações de média e grande dimensão tornaram-se dependentes dos Sistemas de Informação nas suas operações e rotinas diárias. Desta forma as organizações que necessitam de um plano de recuperação de desastres bem como o número dos sistemas críticos aumentaram significativamente. As organizações aperceberam-se por intermédio de vários factores de que a indisponibilidade dos seus Sistemas de Informação têm um impacto fortemente negativo e imediato nas suas receitas e lucros, que prejudicam os serviços fornecidos aos clientes, a própria reputação da organização e gera uma diminuição de produtividade, tal como os seguintes exemplos claramente demonstram:

- As falhas nos sistemas de ecommerce, nos sistemas *point-of-sale*, ou nos sistemas de *epayment* tornam a organização inoperacional durante a ocorrência da falha.

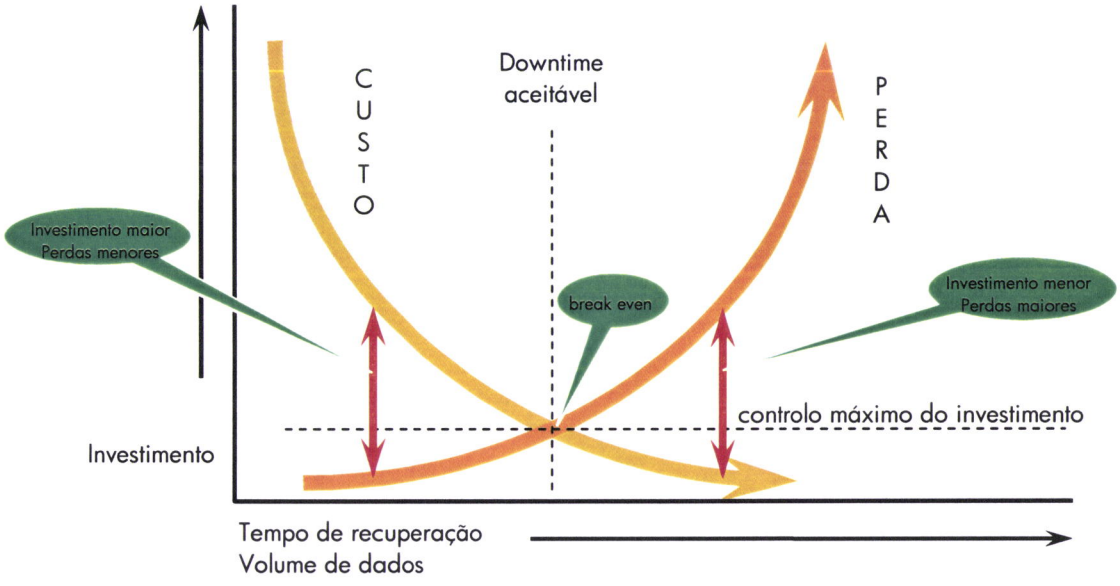
- Interrupções no restabelecimento de serviços na gestão de inventários, assim como de modernas tecnologias nas cadeias de abastecimento tornam as redes das organizações vulneráveis às interrupções dos serviços.

- Quando aplicações tão simples como o *email* estão indisponíveis as organizações não conseguem comunicar com os seus clientes ou parceiros comerciais.

3.3.2 Redundância versus Custos

Os *managers* da Gestão da Continuidade do negócio são responsáveis pelo equilíbrio entre os custos versus o grau de redundância implementado nos Sistemas de Informação. A eliminação dos pontos de falha das arquitecturas dos Sistemas de Informação significa a aquisição e manutenção de sistemas ou peças redundantes. As melhores práticas ditam que o grau de resistência e segurança deve ser proporcional aos custos e consequências do tempo de paragem imprevisto e do valor no acesso atempado e constante à informação.

Figura 3-7 Investimento versus perdas



Quando por exemplo numa organização de serviços financeiros os sistemas em tempo real ficam indisponíveis dá-se um impacto severo e imediato nos interesses centrais da organização. Neste tipo de organização os imensos investimentos em Sistemas de Informação são por vezes proibidos pela regulamentação, mas muitas vezes considerados como um custo básico do negócio.

Outras aplicações podem dificultar as operações da organização mas não de um modo tão severo. Por exemplo, o pagamento mensal de salários ou as aplicações de *time-reporting* podem não ser consideradas críticas para as operações diárias na maior parte das organizações. No que se refere aos serviços cuja indisponibilidade durante horas ou mesmo alguns dias não causam um impacto negativo na organizações uma simples rotina de *backups* e um armazenamento *offsite* da informação e das aplicações pode revelar-se adequado. Nestes últimos casos uma despesa maior associada à criação de um Centro de Processamento de Dados com um elevado nível de redundância pode ser perfeitamente dispensável.

À medida que as organizações revêem os seus planos de recuperação de desastres verificam que as melhorias efectuadas nas infra-estruturas têm implícitas a possibilidade de uma evolução nos sistemas para formatos de maior resistência a baixo custo. A tendência actual para uma consolidação de armazenamento de storage, que anteriormente era distribuído por vários locais com ligações directas aos servidores, levou ao aparecimento de novas arquitecturas mais flexíveis e de novas soluções para a protecção da informação, como por exemplo a disponibilidade de acesso a *Storage Area Networks, SAN*, que estão agora disponíveis para gestão dos sistemas de armazenamento dos Sistemas de Informação.

Dentro de uma rede de armazenamento de dados dedicada podem ser replicadas grandes quantidades de informação, incluindo bases de dados departamentais, de modo a ficarem protegidas contra eventuais falhas dos equipamentos. De acordo com a capacidade e velocidade necessárias a informação é transferida para sistemas de storage em locais alternativos para uma maior segurança.

3.3.3 Eliminação dos Pontos de Falha

Os sistemas críticos são considerados resistentes e seguros quando os pontos de falha são minimizados ou totalmente eliminados. A documentação de todos os elementos redundantes claramente identificados em todos os sistemas e sub-sistemas chave da organização, juntamente com os procedimentos que produzem as cópias de segurança da informação, que devem estar disponíveis no caso de serem necessários, são peças fundamentais para o plano de recuperação de desastres.

Os sistemas com um elevado nível de disponibilidade têm que ser concebidos com todos os componentes redundantes. O conhecimento prévio do tempo médio entre falhas dos sub-sistemas, tais como no fornecimento de energia ou *drives* de suporte magnético, pode aumentar significativamente a fiabilidade da solução através da implementação dos componentes críticos redundantes. Se uma fonte de energia falhar uma segunda ou terceira deve entrar imediatamente em funcionamento. Os responsáveis pela arquitectura da solução devem implementar apenas componentes com capacidades *hot-swapable* de modo a se executar a substituição de um destes componentes avariados sem a necessidade de paragem do sistema.

No Centro de Processamento de Dados a recuperação do processamento e do armazenamento da informação é garantida por técnicas de *failover* e por conjuntos de discos redundantes e independentes, conforme já referido, os servidores no *cluster* podem direccionar o *failover* aplicacional para outro sistema mantendo desta forma as aplicações *online*. A informação armazenada numa *SAN* é assim redireccionada e acedida para um servidor alternativo. Para os sistemas de armazenamento a tecnologia de redundância mais elementar é baseada no *RAID*. Discos que apresentem falhas podem ser *hot-swapped* e o seu conteúdo reconstruído a partir dos restantes discos no *RAID*. Os sistemas de armazenamento inteligentes podem automaticamente detectar o possível aparecimento de erros e pró-activamente duplicar a informação para um dispositivo redundante antes da eventual falha do disco.

A redundância consiste também numa estratégia para fontes de energia, ligações de rede e mesmo para o próprio *staff* do IT. Quando possível os responsáveis pelo planeamento das instalações devem definir a localização de um Centro de Processamento de Dados de modo a que as redes da organização possuam múltiplas ligações independentes à Internet.

Do mesmo modo todas as instalações devem ser planeadas no sentido de existirem diferentes fontes de energia e devem ser concebidas com recursos locais incluindo geradores de energia.

Os procedimentos bem documentados e a formação dos colaboradores reduz o risco de falhas humanas. Para além destas possibilidades o plano de recuperação de desastres deve especificar quais os métodos de comunicação e equipamentos que devem estar disponíveis para dar suporte às equipas alternativas de profissionais.

A existência de métodos de comunicação alternativos é particularmente importante uma vez que estes sistemas sofrem cargas severas aquando da ocorrência de um desastres Os planos de segurança de sistemas e aplicações são importantes para evitar a violação dos sistemas e também a redução dos erros humanos.

A utilização de novas técnicas podem conduzir à redução drástica do tempo de paragem. Por exemplo, a maioria dos sistemas de *storage* possuem hoje capacidades de cópias *Point-in-Time*. Enquanto as aplicações de negócios continuam a ler e a actualizar a informação *online* uma cópia dessa informação pode ser criada e utilizada com outros objectivos. Desta forma as janelas de *backup* podem ser completamente eliminadas através da utilização das cópias *point-in-time* para os *backups online* com a utilização de suportes magnéticos. Por motivos de disponibilidade estas cópias *point-in-time* podem também ser utilizadas para ensaios aplicacionais ou ensaios de performance.

3.4 Factores Críticos de Sucesso na Protecção da Informação

3.4.1 O Benefício na Replicação da Informação

De acordo com Serrano (2004) "a informação é sobretudo um recurso estratégico da organização, superior a qualquer outro factor de produção, pois facilita a combinação e a utilização de outros factores produtivos."

Um plano de recuperação de desastres inicia-se com a suposição da indisponibilidade total ou parcial de um Centro de Processamento de Dados, ou seja a negação do acesso à informação, e, de que para sobreviver a organização terá que realizar a replicação ou *backups point-in-time* da informação, recorrendo a soluções de *backup* em suportes magnéticos ou a novos métodos para replicar a informação em tempo real. A evolução da replicação da informação depende da distância relativa do Centro de Processamento de Dados alternativo e dos métodos de replicação utilizados, que podem ser por *hardware* em modo síncrono ou assíncrono.

A replicação da informação à distância consiste numa importante estratégia do plano de recuperação de desastres para a mitigação dos desastres. As técnicas para replicação da informação de forma síncrona são muitas vezes utilizadas para se replicar a informação dentro de uma universidade, de uma área metropolitana ou de uma região, enquanto que os métodos em modo assíncrono devem ser utilizados para replicar a informação que se encontra a grande distância, ou em casos de grandes alterações no conteúdo da informação em curtos intervalos de tempo e de forma constante.

3.4.2 Replicação da Informação em Modo Síncrono

A informação pode ser replicada através de sistemas de *mirroring* se os Centro de Processamento de Dados estiverem relativamente perto. No caso dos sistemas de *storage* e sistemas de base de dados que suportam aplicações OLTP, a performance poderá ser mantida através de uma replicação em modo síncrono.

A informação pode ser replicada e armazenada num segundo Centro de Processamento de Dados enquanto o software *OLTP* mantém uma transacção em suspenso, levando a que essa transacção só possa ser terminada quando for recebida a confirmação tanto do sistema local como do sistema remoto.

A vantagem da replicação da informação em modo síncrono consiste na velocidade e no grau de prontidão da recuperação. Caso o Centro de Processamento de Dados primário sofra uma paragem todas as transacções completas estão armazenadas no Centro de Processamento de Dados alternativo.

Assumindo que tanto os servidores como o software aplicacional estão disponíveis o *failover* de um Centro de Processamento de Dados para outro pode dar-se numa questão de segundos ou minutos.

3.4.3 Replicação da Informação em Modo Assíncrono

Quando a informação é replicada a grandes distâncias as técnicas de modo assíncrono são as mais correctas. As técnicas em modo assíncrono correspondem à replicação da informação para um Centro de Processamento de Dados distante mas onde se poderá gerar um atraso temporário na transmissão da informação. As transacções são realizadas no site local e terminam sem ser necessário a confirmação da recepção por parte do Centro de Processamento de Dados alternativo.

As técnicas em modo assíncrono são necessárias porque os efeitos de latência causados pela distância provocam uma elevada diminuição da performance.

As técnicas em modo assíncrono são também utilizadas quando uma aplicação não é de natureza transaccional. Um processo diário ou um procedimento de análise semanal do mercado não necessitam de ser replicados em tempo real numa base contínua. As replicações da informação podem ser efectuadas para os sites alternativos mediante *checkpoints* ligados ao calendário de utilização da aplicação.

Uma replicação em modo assíncrono exige uma maior análise dos custos de paragem. Para algumas aplicações, a transmissão de um *snapshot point-in-time* diário para o Centro de Processamento de Dados alternativo, coordenado com as transferências dos registos de transacções horárias, poderá ser o suficiente para a recuperação atempada do sistema, por ex.: algumas horas para carregar o *snapshot* mais recente e depois aplicam-se os registos das últimas transacções.

Na concepção de um plano de replicação da informação a primeira preocupação da organização deverá ser a distância a que se irá localizar o Centro de Processamento de Dados alternativo. Distâncias de centenas ou milhares de quilómetros ditarão uma solução em modo assíncrono.

O passo seguinte deverá consistir na avaliação por parte dos responsáveis do planeamento dos dois objectivos diferentes na recuperação: o Tempo de Recuperação e o Ponto de Recuperação. Os dois métodos, síncrono e assíncrono, podem ser concebidos de modo a realizarem ambas as operações de recuperação de forma rápida. O ponto de recuperação que indica a quantidade de processamento que poderá ser perdido, pode ser desenvolvido a partir de técnicas de replicação em modo assíncrono que podem desta forma gerar alguma perda prevista de informação.

3.4.4 Largura de Banda e Latência

A largura de banda é um dos aspectos fundamentais na rede e corresponde à sua capacidade para transferir informação medida em bits por segundo. A latência consiste no tempo que a informação demora a ser transferida de um local para outro através da rede; sendo medida em segundos.

Por norma, os bits de informação deslocam-se a uma velocidade constante - a velocidade da luz na fibra óptica - mas é acrescentada alguma latência quando os *packets* são processados por *routers* e direccionados para o seu destino.

Enquanto a velocidade da luz pode parecer infinitamente mais rápida, em distâncias continentais e globais as latências tornam-se um factor importante. A latência aumenta na fibra óptica à velocidade de 2ms por 125mi num círculo. A latência mínima de uma viagem circular de costa a costa dos EUA (do Centro de Processamento de Dados A para o Centro B e regresso) é de 50ms; uma viagem circular à volta do mundo e regresso ao ponto de origem demora cerca de 200ms, no mínimo.

No caso dos sistemas de processamento de transacções de elevada performance quaisquer milissegundos de atraso adicional podem revelar-se inaceitáveis. A latência é um desafio particularmente difícil porque, ao contrário da largura de banda, um maior investimento não consegue reduzir a latência.

IV – Gestão Aplicacional em Ambientes Críticos

4.1 Âmbito para o Desenho de Funções Aplicacionais Críticas

Segundo Hunt (1999) não se deve ficar preso a uma peça de tecnologia em particular e a abordagem deve ser feita no sentido de se escolher sempre a melhor opção nas situações complexas, com um ajuste claro aos problemas correntes e ambientes específicos. Gamma (1995) concorda ao adicionar que o desenvolvimento deve ser especifico ao problema entre mãos mas deverá ser suficientemente generalista para adaptar-se a novos requisitos e problemas futuros, com o objectivo de minimizar eventuais alterações necessárias em futuras adaptações.

Desta forma e tendo em mente estes princípios o presente capítulo pretende apresentar uma metodologia generalista o suficiente para potencializar o desenvolvimento e migração de aplicações para ambientes *mission critical* centrando-se principalmente nos seguintes pontos:

- Automatização das operações aplicacionais
- Controlo da velocidade do *failover* aplicacional
- Desenvolvimento de aplicações para correr em vários sistemas
- Recuperação das ligações dos clientes aplicacionais
- Gestão de falhas aplicacionais
- Minimização do *downtime* planeado

Devem ser tidas em linha de conta duas estratégias no desenvolvimento de aplicações integradas em ambientes *mission critical*:

- Concepção das aplicações de modo a gerirem *reboots* ou *panics* de sistemas

  Na alteração de uma aplicação para a integração num ambiente com requisitos *mission critical* é necessário determinar-se qual o estado corrente da aplicação após um *panic* do sistema. Num ambiente de alta disponibilidade devem estar claramente definidos os procedimentos para o reinicio aplicacional. Os procedimentos de reinicio e paragem da aplicação devem ser automatizados de forma que não seja necessário qualquer intervenção humana durante os procedimentos de paragem ou arranque aplicacionais.

- As aplicações não devem utilizar informações específicas de sistema de forma a ser possível o *failover* para outros sistemas:

  - a aplicação não deve utilizar referências ao *uname*() ou *gethostname*().

- a aplicação não deve utilizar referências ao *SPU ID.*
- a aplicação não deve utilizar referências aos *MAC Addresses.*

4.2 Automatização das Funções Aplicacionais

Uma das primeiras regras (não a primeira) para se atingir um nível de alta disponibilidade nos Sistemas de Informação consiste em minimizar as intervenções manuais. Caso seja necessário uma intervenção de um utilizador num terminal, consola ou GUI para dar entrada de comandos numa aplicação ou sistema aplicacional, esse utilizador torna-se um elemento chave nas operações do sistema. Mas podem decorrer horas até um utilizador conseguir ter acesso a uma consola para efectuar as tarefas necessárias de *startup* ou *recover.* Por diversos motivos o *hardware* pode estar localizado numa área distante onde não existam utilizadores formados ou num local onde fora das horas normais de funcionamento exista uma necessidade de ligação via *modem* e o acesso ter sido de alguma forma barrado.

Se as operações estiverem automatizadas não se perde tempo desnecessário na reposição dos serviços aplicacionais.

Dois princípios devem ser tidos em linha de conta ao se automatizar o failover de aplicações:

- Isolar os utilizadores de potenciais problemas
- Definição dos procedimentos automáticos de *startup* e *shutdown* das aplicações

É fundamental o conhecimento prévio do que ocorre quando uma aplicação é reiniciada de forma abrupta, bem como se são necessárias alterações à resposta aplicacional na integração em ambientes de alta disponibilidade.

4.2.1 Protecção dos Utilizadores de Potenciais Problemas

Sempre que possível os utilizadores finais devem estar isolados de potências problemas. Para isso é necessário ter em atenção os seguintes pontos:

- Não deverá existir intervenção por parte dos utilizadores para o restabelecimento das ligações às aplicações quando estas se perdem devido a paragens súbitas de servidores

- Quando possível os utilizadores devem ser avisados acerca de atrasos devido à realização de *failovers*
- Minimizar a reentrada de informação
- Concepção dos Sistemas de Informação com folga de recursos para minimizar a deterioração de performance junto dos utilizadores

4.2.2 Definição dos Procedimentos de Startup e Shutdown

O reinicio das aplicações deve ser executado sem intervenção manual. Se a aplicação necessitar que se faça um *switch* num determinado componente, a automatização do reinicio aplicacional não é possível de se efectuar. Os procedimentos para o *startup, shutdown* e monitorização das aplicações devem ser criados de forma a que estas funções sejam efectuadas automaticamente. Estes procedimentos devem verificar erros e enviar informações sobre o *status* aplicacional para o *software* de controlo e monitorização. O *startup* e o *shutdown* devem ser orientados através de linhas de comando integradas em *scripts* e não devem funcionar de modo interactivo.

Num ambiente de alta disponibilidade o *software* responsável pela gestão do *cluster,* deve em caso de falha de um dos nós do *cluster* reiniciar as aplicações num sistema alternativo.

As aplicações por sua vez devem permitir o seu reinicio com base em dois princípios:

- Devem possibilitar o reinicio e recuperação a partir de um sistema alternativo ou no mesmo sistema caso exista uma opção de reinicio da aplicação.

- Deverá ser possível reiniciar as aplicações se as falhas ocorrerem durante o seu *startup,* assumindo que a origem da falha possa ser resolvida.

Os administradores das aplicações devem aprender a realizar o *startup* e o *shutdown* das aplicações através dos comandos apropriados de gestão do *cluster.* Se a aplicação for inadvertidamente encerrada, iniciar-se-á um procedimento de *failover* não pretendido.

De modo a reduzir um possível impacto junto dos utilizadores a aplicação não deve abortar em caso de erro, uma vez que este procedimento provocaria um *failover* para um sistema alternativo no *cluster.* As aplicações devem determinar o tipo de erro e empreender as acções específicas de recuperação.

É necessário a existência de um mecanismo de monitorização das actividades aplicacionais de modo a que o *software* de controlo reconheça uma falha da aplicação. Esta acção pode ser realizada de um modo simples através de um *script* que acciona o comando ps –ef | grep xxx para todos os processos pertencentes à aplicação.

4.3 Controlo de Velocidade do Failover Aplicacional

Que medidas podem ser tomadas de modo a se garantir um rápido *failover*?

Existem várias medidas e opções que podem ser implementadas de modo a diminuir o tempo de *failover* se ocorrer uma falha que provoque a transferência da aplicação para outro sistema.

Destacam-se as seguintes:

- Replicação de *filesystems Non-Data*
- Avaliação da utilização de *Raw Devices, online JFS* ou *VXVM*
- Minimização de perda de informação
- Utilização de transacções reiniciáveis
- Utilização de *checkpoints*
- Design para múltiplos servidores
- Design para sites com informação replicada

4.3.1 Avaliação da Utilização de Raw Devices, Online JFS ou VXVM

Os *filesystems* com ficheiros *non-data,* como por exemplo os ficheiros binários devem ser duplicados e não partilhados pelos vários sistemas no *cluster.* Deve existir uma cópia dos executáveis da aplicação por sistema do *cluster,* em vez de uma única cópia num *filesystem* partilhado. Mas a informação/dados deve ser mantida num conjunto de discos partilhado acessíveis a todos os sistemas do *cluster.* Após o *failover* se o conjunto dos discos partilhados estiverem configurados como *filesystems,* passam invariavelmente pelo processo de recuperação de *filesystems, fsck,* antes de se poder aceder à informação. Para reduzir este período de recuperação podem ser utilizados *raw devices* ou o *VXFS* ou *VXVM* em caso de configurações com *filesystems,* desta forma a recuperação será sempre mais rápida.

Se a aplicação utilizar grandes volumes de informação para *datafiles* poderão ser utilizados *raw devices* em vez de filesystems. Os *raw devices* não precisam de *fsck* eliminando-se desta forma uma passo demorado na recuperação e *failover*.

Ao se utilizarem *filesystems* deverá ser usado o *VXFS* ou o *VXVM* dado que este tipo de *filesystems* oferece uma recuperação significativamente mais rápida do que o *HFS*. No entanto a performance do *VXFS* ou *VXVM* pode variar consoante a aplicação.

4.3.2 Métodos para Minimizar a Perda de Informação

O objectivo é o de minimizar a quantidade de informação que poderá ficar perdida no momento de um *crash*. É impossível prevenir a perda total de informação na ocorrência de uma falha, no entanto, é necessário implementar certas medidas de modo a minimizar a quantidade de informação que se poderá eventualmente perder.

Minimizar a Quantidade de Informação em Memória

Toda a informação alocada em memória física, contexto *in-memory*, será perdida na ocorrência de uma falha. A aplicação deve ser concebida de modo a minimizar a quantidade de informação em memória física, a não ser que esta informação possa ser facilmente recalculada. Quando a aplicação é reiniciada deve calcular ou carregar a partir de disco toda a informação que necessita em memória.

Um das métricas de velocidade no *failover* consiste no cálculo de tempo que a aplicação demora a reiniciar no sistema normal após um *reboot*. A aplicação inicia-se imediatamente, ou existe uma série de passos pelos quais a aplicação deve passar antes do utilizador final conseguir acesso? O ideal será a aplicação reiniciar rapidamente sem a necessidade de cálculo de estruturas ou tabelas de informação que devem estar residentes em memória.

A preocupação com a *performance* pode ditar a manutenção da informação na memória física em vez da sua transferência para disco. No entanto, o risco associado à perda desta informação deverá ser pesado contra o impacto de *performance* no *destage* desta informação para disco.

Mas a informação lida a partir dos discos partilhados e carregada em memória física que é utilizada apenas como informação *read-only* poderá ser sempre mantida em memória.

Manutenção de Logs de Pequena Dimensão

Quase todas as bases de dados permitem que os *logs* sejam carregados em memória de modo a aumentarem a performance *online* do sistema. Claro que quando ocorre uma falha todas as transacções a decorrer e que apenas estavam em memória são perdidas, no entanto, a diminuição da dimensão destes *logs* reduz a quantidade de informação de transacções incompletas em caso de falha. A manutenção da dimensão dos *logs* existentes e o *destage* para disco permite o seu arquivo ou replicação de forma mais frequente, reduzindo-se o risco de perda da informação. Verifica-se, todavia, a existência de um *trade-off* entre a *performance online* e o tamanho dos *logs* da base de dados.

Eliminação da Necessidade de Informação Local

Quando possível deve ser eliminada a existência de informação local.

Num ambiente cliente/servidor de três níveis, o nível intermédio poderá não ter informação local. Esta camada relativa ao "servidor aplicacional" pode neste caso apresentar níveis adicionais de disponibilidade, de *load-balancing* e de *failover*.

No entanto, este cenário exige que toda a informação seja guardada no cliente (nível 1) ou no servidor da base de dados (nível 3).

4.3.3 Utilização de Transacções Restartable e Utilização de Checkpoints

As transacções devem ter a capacidade de serem reiniciadas de forma transparente para que o cliente não seja forçado a fechar as transacções nem ter que reintroduzir a mesma informação em caso de falha de um servidor.

Por outras palavras, se uma falha ocorre no meio de uma transacção não deve ser necessário voltar-se ao início da transacção. Esta característica torna a aplicação mais robusta e reduz a visibilidade dos *failovers*.

Um bom exemplo é o de um trabalho que esteja em impressão. As aplicações de impressão por norma ordenam os trabalhos e só quando um trabalho termina o *scheduler* avança para o seguinte. Se, no entanto, o sistema crashar a meio de uma longa impressão de recibos de vencimento, que já decorre por três longas horas, o que deverá acontecer quando o sistema for reiniciado? A impressão volta ao início reimprimindo todos os recibos, o trabalho reinicia-se a partir do momento em que parou, ou assume que a impressão terminou não continuando a impressão?

O comportamento correcto num ambiente de alta disponibilidade consiste no reinicio do trabalho a partir do ponto onde ficou, assegurando-se desta forma que todos recebem um e apenas um recibo de vencimento.

Outro exemplo consiste numa aplicação em que um funcionário está a registar a informação de um novo colaborador. Suponhamos que esta aplicação exige que os números dos colaboradores sejam únicos e que após a entrada do nome e do número do novo colaborador ocorre uma falha. Uma vez que o número do colaborador já tinha sido introduzido antes da falha a aplicação recusará a sua reintrodução ou será necessário apagar primeiro a informação já parcialmente introduzida? Num ambiente de alta disponibilidade a aplicação deverá permitir o reiniciar da introdução dos dados ou continuar a partir do próximo registo a ser preenchido.

É necessário o desenvolvimento de aplicações que utilizem *checkpoints* para as transacções complexas. Uma transacção única na perspectiva do utilizador pode resultar em várias transacções da base de dados. Apesar deste tema estar relacionado com transacções reiniciáveis é aconselhável gravarem-se os progressos do cliente com a utilização de *checkpoints*, de modo a que se a transacção for interrompida por uma falha de sistema possa ser terminada após a ocorrência do *failover*.

Suponhamos por exemplo que a aplicação que se encontra a correr está a calcular o PI. No sistema principal a aplicação correu até aos 1.000 pontos decimais mas a aplicação ainda não gravou nada para o disco. Nesse momento, dá-se um *crash* do sistema. A aplicação é então reiniciada no sistema alternativo, mas é reiniciada a partir do início. A aplicação vai então recalcular novamente os primeiros 1.000 pontos decimais. No entanto, se a aplicação tivesse gravado em disco os pontos decimais numa base regular a aplicação poderia ser reiniciada a partir do momento em que foi interrompida.

É importante balancear a frequência da realização dos *checkpoints* com a *performance*. O *trade-off* decorrente da realização de *checkpoints* em disco consiste no seu impacto directo na *performance* do sistema. Se forem realizados demasiados *checkpoints* a aplicação torna-se mais lenta, se não se

realizarem todos os *checkpoints* necessários será mais lento o processo de recuperação da aplicação para o estado anterior ao *failover*.

4.3.4 Desenho para Sites com Informação Replicada e Múltiplos Servidores

Ao se utilizarem vários servidores activos os pontos de acesso disponibilizados pelos mesmos, podem providenciar um serviço relativamente transparente para os clientes. No entanto, esta arquitectura requer que o cliente tenha a informação necessária acerca de cada um dos servidores, bem como a definição das prioridades de acesso. Nesta arquitectura, em caso de falha será necessário o acesso à informação partilhada ou replicada.

Em vez de existir por exemplo uma aplicação que efectua o *failover* para um sistema alternativo, suponhamos que a aplicação corre em ambos os servidores ao mesmo tempo. Após uma falha do primeiro servidor, o segundo servidor recebe a carga adicional das transacções aplicacionais do primeiro e elimina-se o período de *startup* da aplicação em caso de falha. Existem variados métodos para a concepção deste tipo de arquitectura mas existem também várias questões relativas a estas implementações.

O método mais simples consiste em duas aplicações correrem numa relação *master/slave*, na qual o *slave* funciona apenas como um *hot standby* do *master*. Em caso de falha da aplicação *master*, a aplicação *slave* existente no segundo servidor apenas precisa determinar qual o estado da informação no momento de falha para poder iniciar as transacções, mas a recuperação da informação teria que ser sempre executada. No entanto, o período de tempo decorrente entre o *fork* da aplicação e a execução com o *startup* inicial seria eliminado.

Outra possibilidade consiste na existência de duas aplicações activas em dois servidores. Por exemplo, no caso de dois servidores aplicacionais alimentarem uma base de dados, estando metade dos utilizadores ligados a um dos servidores aplicacionais e a outra metade ligada ao segundo servidor, neste caso, se um dos servidores aplicacionais falhar todos os utilizadores passariam a estar ligados ao segundo servidor aplicacional que continua em funcionamento e a alimentar a base de dados.

Os sites com informação replicada são uma vantagem em caso de activação do plano de recuperação de desastres após um desastre. Na replicação da informação por *software* ou *hardware* os discos que contêm a informação não são partilhados entre todos os sistemas. No entanto neste tipo de solução

podem existir *trade-offs* de performance associados à replicação da informação. Existem vários métodos para a replicação da informação, que devem ser analisados de forma abrangente pelos responsáveis do desenvolvimento aplicacional e das equipas de planeamento de recuperação de desastres.

Muitos dos produtos *standard* para as bases de dados oferecem hoje a possibilidade de se efectuar uma replicação da informação de forma transparente para a aplicação cliente.

4.4 Desenvolvimento Aplicacional para Ambientes Críticos

No *failover* de uma aplicação para um sistema alternativo como irá a aplicação funcionar nesse sistema?

As secções anteriores apresentavam métodos para assegurar o reinicio automático de uma aplicação bem como um reinicio do modo mais célere possível. Esta secção apresenta agora as metodologias que asseguram a capacidade de uma aplicação correr em vários sistemas.

Os pontos principais são os seguintes:

- Evitar informação específica do sistema
- Atribuição de nomes únicos às aplicações
- Ligação a um *socket* fixo
- Ligação a um endereço IP flutuante
- Cada aplicação tem os seus próprios volumes de discos
- Evitar o *locking* de ficheiros

Evitar a Informação Específica do Sistema

Por norma, quando um sistema é configurado é atribuído um endereço IP a cada interface de rede activo. Estes endereços IPs estão sempre associados ao sistema e são definidos como endereços IPs estáticos.

A utilização de aplicações com características de alta disponibilidade num ambiente *mission critical* pode necessitar de um conjunto adicional de endereços IP, os quais serão atribuídos às próprias aplicações. Neste contexto, os endereços IP associados a uma aplicação com capacidade de *failover* serão chamados endereços IPs flutuantes.

A cada aplicação deverá ser atribuído apenas um nome bem como um endereço IP flutuante. O seguimento desta regra assegura a separação da aplicação em relação ao sistema no qual ela corre, deixando de existir a necessidade do utilizador ter que saber qual o sistema onde a aplicação está a correr. Também agiliza a movimentação da aplicação entre sistemas de um *cluster* para a realização de *load balancing* ou por motivos de *failover*. Se duas aplicações partilharem um endereço IP flutuante, têm que se movimentar em conjunto. Por outro lado, a utilização de nomes e endereços IP independentes permite-lhes uma movimentação separada.

A partir de um acesso externo ao *cluster* os clientes têm que conhecer a forma correcta de se referirem à aplicação. Uma opção consiste em informar o cliente qual o endereço IP flutuante associado à aplicação, a outra opção consiste em atribuir um nome à aplicação como numa função de hostname, e configurar o nome da aplicação no *Domain Name System, DNS*. Em ambos os casos, o cliente estará a comunicar com o endereço IP flutuante da aplicação. No caso da aplicação ser movimentada para outro sistema o endereço de IP mover-se-à também, permitindo ao cliente continuar a utilizar a aplicação sem o conhecimento da sua localização. É necessário ter em atenção que cada interface da rede deve ter um endereço IP estático associado. Este endereço IP não deve ser movido para um sistema alternativo em caso de falha na rede.

Cada aplicação recebe desta forma um endereço IP flutuante separado dos endereços IP estáticos atribuídos ao próprio sistema. Assim, um sistema poderá ter vários endereços IP, um ou vários para o sistema e um para cada aplicação de alta disponibilidade que corre nesse sistema. Deste modo, os endereços IP no âmbito de uma determinada *subnet* serão rapidamente consumidos num ambiente *mission critical* com alta disponibilidade. Neste caso, talvez se verifique a necessidade de adquirir endereços IP adicionais.

A existência de múltiplos endereços IP no mesmo interface de rede é suportada apenas no caso de se encontrarem na mesma *subnet*.

As aplicações devem ser desenvolvidas de modo a permitir que múltiplas instâncias, com nomes próprios e endereços IP possam correr num único sistema em paralelo. Poderá ser necessário invocar a aplicação com um parâmetro que indique qual a sua instância, sob circunstâncias normais, esta acção irá permitir distribuir os utilizadores por vários sistemas, mas ao mesmo tempo permitindo que todos os utilizadores tenham acesso às suas aplicações e serviços em caso de falha e a partir de um único sistema.

Devem ser eliminadas todas as referências aos *SPU IDs* ou *MAC Addresses*. As aplicações devem ser concebidas de modo a não se basearem no *SPU ID* ou nos *MAC addresses* (*link-level*) para a identificação dos sistemas. O *SPU ID* consiste num identificador de *hardware* único, existente na memória não volátil do sistema e que não pode ser alterado. Um *MAC address* consiste num endereço especifico associado a um interface de rede, também conhecido por *LANIC ID*. A utilização destes endereços é um problema comum para os servidores de licenças, uma vez que por motivos de segurança baseiam-se num ID específico de *hardware* para assegurarem que as licenças aplicacionais não são copiadas para múltiplos servidores. Uma das soluções consiste em ter várias licenças instaladas, uma para cada sistema no qual a aplicação deverá correr. Outra solução consiste num mecanismo *cluster-wide* que lista um conjunto de *SPU IDs* ou *nodenames* e se a aplicação estiver a correr num destes servidores o licenciamento fica automaticamente validado.

Existia um conjunto de razões para não se utilizar o *MAC address* que consistia nos seguintes argumentos:

- Os antigos dispositivos de rede existentes entre a fonte e o ponto de destino tais como *routers* tinham que ser manualmente programados com o conjunto endereço IP e *MAC address*. Em caso de *failover*, a solução para este problema consistia em mover o *MAC address* juntamente com o endereço IP para o novo servidor.

- Podiam decorrer cerca de 20 minutos até terminar a actualização da *cache* em todos os dispositivos de rede, devido aos *timeouts* associados a falhas de sistemas. Este problema é solucionado com a utilização do *software* de gestão alta disponibilidade, que actualiza automaticamente as tabelas de *ARPA* com o antigo endereço IP e o novo *MAC address*.

Atribuição de Nomes Únicos às Aplicações e Utilização do DNS

Deverá ser atribuído um único nome a cada aplicação. Este nome deve ser configurado no *DNS* de modo a servir de input para o *gethostbyname*(), tal como a seguir se descreve.

O *Domain Name System* apresenta um *API* que pode ser utilizado para efectuar o mapeamento entre hostnames e endereços IP e vice-versa. Este procedimento é útil para as aplicações que utilizam *sockets BSD*, tais como o *telnet*, que recebe primeiro a informação referente ao nome do sistema destino. A aplicação deve então mapear o nome do sistema para um endereço IP de modo a estabelecer a ligação. No entanto algumas chamadas devem ser efectuadas com precaução.

As aplicações não devem fazer qualquer referência aos *hostnames* oficiais ou a endereços IP estáticos. O *hostname* e o correspondente endereço IP para o referido servidor referem-se ao interface *LAN* principal e ao seu endereço IP estático. Deste modo, qualquer aplicação que se refira a, ou necessite do *hostname* ou do endereço IP primário do servidor não poderá ser integrada num ambiente de alta disponibilidade, onde a identidade de rede no sistema que suporta a aplicação se movimenta de um sistema para outro, mas onde o *hostname* não é movimentado.

Um dos métodos para identificar problemas nesta área consiste em localizar chamadas para o *gethostname(2)* na aplicação. Os serviços devem utilizar a função *gethostname()* com precaução, uma vez que a resposta pode mudar ao longo do tempo se a aplicação migrar entre servidores. As aplicações que utilizem o *gethostname()* para determinar o nome a utilizar numa chamada ao *gethostbyname(2)* devem ser evitadas pela mesma razão. Do mesmo modo, a chamada *gethostbyaddr()* poderá obter diferentes respostas ao longo do tempo se for executada sobre endereços IP flutuantes.

Opcionalmente, a aplicação deverá referir-se sempre ao nome da aplicação e ao endereço IP flutuante e não ao *hostname* ou endereço IP estático. A aplicação deverá chamar o *gethostbyname(2)* especificando o nome da aplicação e não o hostname. A indicação *gethostbyname(2)* devolverá assim o endereço IP da aplicação e este endereço IP será movimentado com a aplicação para o sistema alternativo.

No entanto, o *gethostbyname(2)* apenas deverá ser utilizado para localizar o endereço IP de uma aplicação se o nome da aplicação estiver configurado no *DNS* ou no */etc/hosts*. A melhor aproximação é a de se associar um nome e uma aplicação a um serviço *Misson Critical*. Esta acção vai permitir que cada aplicação e o seu respectivo endereço IP sejam movimentados para outros sistemas sem afectarem outras aplicações. Apenas os endereços IP estáticos devem estar associados ao *hostname* no *DNS*.

Da mesma maneira a utilização da função *uname(2)* numa aplicação está associada ao tema referido que devolve o nome oficial do sistema, o *hostname*.. Por convenção o uname e o *hostname* são os mesmos mas essa situação não terá obrigatoriamente que ser desta forma. Algumas aplicações após o *startup* podem executar a função *uname(2)* como método de validação do sistema onde a aplicação está a arrancar, mas este método não se adequa a um ambiente alta disponibilidade uma vez que o serviço é movido de um sistema para outro e o mesmo não acontece com o *uname* ou o *hostname*.

Desta forma as aplicações devem desenvolver meios alternativos de validação do sistema onde estão a correr, como por exemplo, a validação a partir de uma lista com o conjunto dos *hostnames* num ficheiro de configuração.

Estabelecimento de ligações a sockets fixos com chamada ao bind() antes do connect ()

Ao se criar uma ligação ou binding a um socket do sistema pode-se especificar qual a porta da ligação que irá ser estabelecida ou em alternativa, o *binding* ao *socket* poderá ser atribuído de forma dinâmica. O *binding* dinâmico coloca a questão da atribuição de *sockets* diferentes e no caso da aplicação efectuar um *failover* para outro sistema esta situação poderá criar problemas no restabelecimento das ligações dos clientes à aplicação.

O método recomendado consiste na utilização de *sockets* pré-definidos e fixos em todos os sistemas do *cluster* onde a aplicação deve correr em vez de se atribuírem os *sockets* de forma dinâmica a cada *startup* aplicacional. Deste modo a aplicação devolve sempre o mesmo *socket* independentemente do sistema onde se encontrar a correr. A atribuição dos *sockets* associados a cada aplicação deverá ser implementada no ficheiro */etc/services* de modo a manter sempre o mesmo registo e assegurar que esse *socket* não será utilizado por outra aplicação.

Quando uma aplicação inicia as suas ligações deve primeiro efectuar uma chamada ao *bind(2)* especificando o endereço IP da aplicação, antes da chamada ao *connect(2)*. De outro modo o pedido de ligação será enviado através do endereço IP estático do sistema em vez do endereço IP flutuante da aplicação. O cliente recebe então este endereço IP através da chamada ao *accept(2)*. Se as chamadas não forem efectuadas de forma correcta a situação poderá provocar conflitos no *software* cliente.

Estabelecimento de Ligações a Endereços IP Flutuantes

Quando as ligações entre *sockets* são estabelecidas especifica-se o endereço IP que fica associado ao *socket* nessa ligação. Isto indica o endereço IP que é utilizado na comunicação, de modo a limitar o número de interfaces na comunicação aplicacional com os clientes. Em alternativa uma aplicação pode efectuar um *binding* com *INADDR_ANY* como indicação de que qualquer dos interfaces poderá receber dados na ligação estabelecida.

As aplicações em rede podem estabelecer ligações aos endereços IP estáticos, IP flutuantes ou a um *INADDR_ANY*. Caso exista uma especificação relativa ao

endereço IP estático a aplicação irá falhar quando fizer *failover* e for reiniciada noutro sistema, uma vez que o endereço IP estático não é suposto ser transferido para outro sistema.

Muitas aplicações estabelecem ligações *a INADDR_ANY*, ou seja, irão acusar a recepção de pedidos a partir de qualquer interface de rede do sistema. Este método permite aos clientes enviarem a informação para os endereços IP estáticos ou flutuantes. No entanto a aplicação não consegue determinar qual o endereço IP adequado para as respostas aplicacionais, desta forma irá sempre ser utilizado o endereço IP estático.

Atribuição de Volumes de Discos por Aplicação

Cada aplicação deve ser configurada de modo a utilizar volumes de discos distintos. Um volume de discos consiste num conjunto de discos que pode ser partilhado entre sistemas. Neste caso existe uma maior flexibilidade para *load balancing* e *failover* quando a aplicação está definida com o seu próprio volume de discos. No caso de duas aplicações partilharem os mesmos volumes para armazenamento de dados, estas devem ser movidas em conjunto no caso de *failover*. Para se evitar esta situação a informação aplicacional deve ser armazenada em volumes de discos distintos, por aplicação e em casos aplicáveis, *mount points* diferentes.

De modo a prevenir um acesso inadvertido aos volumes de discos que estão a ser utilizados por uma aplicação no sistema, o *software* de gestão de alta disponibilidade deverá utilizar um mecanismo de acesso exclusivo aos volumes de disco para estabelecer o acesso à informação.

Eliminação da Ocorrência de File Locking

Num ambiente com *NFS* as aplicações devem evitar a utilização de mecanismos de *file locking*. O *file locking* deverá ser evitado pelas aplicações tanto ao nível dos sistemas locais como dos remotos. No caso do *file locking* ser utilizado pelo sistema local e se ocorrer uma falha o sistema alternativo poderá não ter o registo dos *locks* do sistema que falhou e a situação poderá eventualmente causar problemas no reinicio da aplicação. O *file locking* remoto é a pior alternativa das duas situações uma vez que o sistema responsável pelo *locking* pode ser o sistema remoto onde ocorre uma falha. Nesse caso, o *lock* poderá nunca ser libertado provocando a impossibilidade de acesso aos ficheiros da aplicação para obtenção da informação. Num ambiente com *NFS* o *file locking* pode dar origem a grandes *delays* e em caso de falha pode mesmo provocar o atraso no próprio *failover*.

4.5 Restabelecimento das Ligações dos Clientes após o Failover Aplicacional

De que forma é que o *software* cliente restaura as suas ligações à aplicação após uma falha aplicacional ou de sistema?

As aplicações têm que ser desenvolvidas de modo a diferenciarem os erros aplicacionais das perdas de ligação aos servidores. Uma das questões a considerar consiste no restabelecimento das ligações do cliente após uma falha aplicacional. O cenário típico consiste no reiniciar da sessão do cliente e ao mesmo tempo tornar a efectuar o *login*. No entanto, este método não é automatizado. Se por exemplo, um sistema bem implementado falhar e a aplicação *mission critical* demorar menos de cinco minutos a efectuar o *failover*, se os utilizadores após a falha aplicacional e durante o *failover* desistirem de tentar efectuar o *login* passados apenas 2 minutos ao se ausentarem enquanto aguardam pelo reinicio aplicacional regressando apenas 28 minutos depois, o tempo de falha aplicacional percepcionado poderá ser de 30 minutos e não de 5!

Assim, devem ser consideradas o número de tentativas no restabelecimento da ligação, a frequência dessas mesmas tentativas e a notificação do utilizador no caso da perda de ligação e do seu restabelecimento.

Existe uma série de estratégias no que respeita ao restabelecimento da ligação do cliente à aplicação:

- Atribuir a responsabilidade do restabelecimento da ligação à aplicação cliente e não ao utilizador. Se o sistema alternativo estiver a correr a aplicação cinco minutos depois da falha, caso o cliente continue a tentar restabelecer a ligação, cinco minutos depois, a aplicação cliente conseguirá restabelecer a ligação ao serviço reiniciando as transacções ou continuando a partir do ponto em que se encontrava, sendo desnecessária a intervenção por parte do utilizador.

- Caso possuam um arquitectura que inclua múltiplos servidores activos, o cliente pode restabelecer a ligação a um segundo servidor activo. Deste modo o utilizador aperceber-se-á apenas de uma ligeira falha. Neste caso o problema consiste em saber em que momento deverá o cliente estabelecer a sua ligação a um segundo servidor. Durante quanto tempo deverá o cliente tentar estabelecer a ligação ao servidor que falhou antes de se redireccionar para o servidor alternativo ou activo?

Não existem respostas definitivas para estas questões. A resposta depende do tipo de aplicação.

- Utilização de um software *TPM* para Monitorizar o Processamento das Transacções de modo a aumentar a fiabilidade do sistema. As transacções podem ser colocadas em fila de espera de modo a que o cliente não se aperceba das falhas no servidor. Muitos *TPMs* apresentam uma opção de reencaminhamento automático das transacções de modo a alternarem os servidores ou no caso de ser necessário o reprocessamento de uma transacção. Os *TPMs* também asseguram a finalização das transacções apesar de não serem o único mecanismo com capacidade para desenvolver esta função. Após o restabelecimento do servidor, o *software* que monitoriza as transacções restabelece a ligação ao novo servidor activo e continua a efectuar o reencaminhamento das transacções.

- Como alternativa à utilização dos *TPM's* pode ser estabelecida uma fila de espera para os pedidos, denominada *message queueing,* para as situações em que o servidor estiver indisponível. Em vez de se notificar o utilizador da indisponibilidade do servidor, o pedido é encaminhado para a fila de espera e transmitido mais tarde quando o servidor já se encontrar novamente *online*. O *software* que possibilita esta alternativa aos *TPMs* assegura que qualquer tipo de mensagem, não apenas as referentes às transacções, serão entregues e aceites. O *software* de *message queueing* é útil quando o utilizador não necessita de uma resposta do resultado da execução do seu pedido ou transacção, neste caso quando uma aplicação não for interactiva.

4.6 Gestão de Falhas Aplicacionais

As secções anteriores assumiram as falhas aplicacionais não como sendo da própria aplicação mas sim da responsabilidade de um componente do *cluster*, uma falha de *hardware* ou *software*. Esta secção refere-se especificamente a problemas ou falhas aplicacionais. Por exemplo, *bugs* no *software* aplicacional podem causar problemas na gestão dos recursos de sistema, tais como excesso de utilização de *swap* ou da memória física do sistema, podendo dar origem a indisponibilidade dos serviços. Esta secção apresenta alternativas de recuperação da aplicação após este tipo de falhas.

4.6.1 Criação de Aplicações Tolerantes a Falhas

Uma aplicação deverá ser tolerante à falha de componentes. Muitas aplicações possuem múltiplos processos a correr no mesmo sistema. Caso um destes processos falhe, o que acontece aos restantes? Poderá o processo em causa ser reiniciado no mesmo sistema sem afectar as restantes áreas da aplicação?

Preferencialmente, em caso de falha de um processo os restantes processos aplicacionais devem aguardar até que o processo volte a estar *online*. Esta afirmação é válida para processos locais ou remotos. O componente processual em falha pode ser automaticamente reiniciado e reagrupar-se ao processamento aplicacional, reiniciando a sua actividade. Este tipo de falha pode ser detectado e reiniciado em poucos segundos, de modo a que o utilizador final não tenha conhecimento da mesma.

Outra alternativa consiste na execução e fecho da aplicação de forma controlada mesmo em caso de falha de um processo. Se um servidor de base de dados falhar, a base de dados deve estar preparada para fechar de forma controlada, de modo a não ser necessário qualquer tipo de recuperação.

O pior dos cenários acontece quando a falha de um processo aplicacional provoca a falha de todo o sistema. Caso um processo falhe e todos os restantes necessitarem de ser reiniciados, o tempo de paragem será naturalmente elevado.

4.6.2 Monitorização das Aplicações

Todos os componentes de um ambiente *mission critical*, incluindo as aplicações devem ser monitorizados. A monitorização pode ser tão simples como o resultado de um comando executado num sistema ou tão complicada como uma consulta de *SQL* a uma base de dados. Deve existir um método que permita validar o estado da aplicação e verificar que a aplicação se encontra a correr de forma correcta. Caso a aplicação falhe e essa falha não seja automaticamente detectada poderá decorrer demasiado tempo até que um utilizador consiga determinar a origem da sua paragem e proceder-se, consequentemente, à sua recuperação se a mesma não se encontrar automatizada.

4.7 Métodos para Reduzir o Tempo de Indisponibilidade Aplicacional

Os tempos de paragem planeados, por oposição aos tempos de paragem não planeados, devem ser agendados; os exemplos incluem *backups offline*, *upgrades* de *software* ou *hardware* ou substituições em casos de avarias de alguns dos componentes do sistema.

Devem ser considerados, no desenvolvimento dos ambientes e aplicações *mission critical*, tendo em conta os tempos de paragem planeados:

- O tempo necessário para a realização de *upgrades* e instalação de *patches* da aplicação ou sistema operativo.

- A reconfiguração *online* da aplicação de forma a que a informação utilizada pela aplicação possa ser alterada sem necessidade de paragem da aplicação.

As secções seguintes apresentam os métodos de gestão dos diferentes tipos de paragem planeados.

4.7.1 Utilização de Rolling Upgrades

Periodicamente são lançadas novas versões das aplicações e *patches* de sistema que precisam ser actualizados. Qual o período de tempo que decorre até que o utilizador final faça o *upgrade* para estas novas versões? Esta questão refere-se ao tempo de paragem planeado para a realização dos upgrades previstos pela aplicação e sistema.

A seguinte norma conduz à redução do período de tempo necessário para a intervenção dos upgrades:

Para um ambiente menos crítico, o cenário mais comum consiste na paragem de todo o ambiente de produção, *upgrade* de cada sistema para a nova versão de *software* ou *hardware* e no reinicio da aplicação em todos os sistemas afectados. Nos ambientes de maior criticidade este método pode levar a paragens mais prolongada do que o permitido. A alternativa consiste na execução de *rolling upgrades* nos ambientes cliente/servidor. Um *rolling upgrade* permite a instalação ou *upgrades* de *software* ou *hardware* de forma faseada através da execução dos upgrades individuais em cada componente

do *cluster*, permitindo simultaneamente a disponibilização dos serviços nos sistemas alternativos.

Com esta metodologia evita-se o problema da realização de todas as alterações de uma só vez, minimizando o risco de longas paragens. O *trade-off* desta metodologia consiste na necessidade do *software* aplicacional correr com diferentes versões. A aplicação deverá ser concebida de modo a gerir este tipo de situação.

4.7.2 Evitar a Modificação no Formato da Informação entre Versões Aplicacionais

A migração dos dados para um novo formato, entre versões aplicacionais, poderá demorar demasiado tempo e eliminar a hipótese de se efectuar um *rolling upgrade*.

Enquanto, por exemplo, o motor de uma base de dados estiver a correr sobre o sistema principal do *cluster*, o sistema alternativo poderá ser actualizado para uma nova versão da aplicação. Quando esta actualização terminar pode ser efectuada a paragem dos serviços, de forma a mover o servidor da base de dados do sistema principal para o sistema alternativo, recentemente actualizado. O motor da base de dados será então reiniciado no sistema alternativo, enquanto que o sistema principal se encontra pronto para ser actualizado.

No entanto, se a nova versão da base de dados ou da aplicação exigirem um *layout* diferente, a informação poderá não ser lida pela nova versão recentemente actualizada. Desta forma o tempo de paragem terá que ser prolongado, uma vez que a informação terá que ser migrada para o novo *layout*.

4.7.3 Reconfiguração Online das Aplicações

A maior parte das aplicações lê a informação da parametrização referente à sua configuração no momento em que a aplicação é iniciada. Se, para efectuar uma mudança da parametrização, a aplicação tiver que ser reiniciada para ler a nova configuração existirá uma paragem aplicacional potencialmente desnecessária.

De modo a evitar esta paragem, devem ser utilizadas ferramentas de configuração que interajam com a aplicação e executem as mudanças de forma dinâmica e online. A solução ideal consiste na utilização de ferramentas de configuração que interajam com a aplicação de forma a que as alterações sejam realizadas online e com pouca ou nenhuma interrupção sentidas pelos utilizadores finais.

V – Conclusão

5.1 Conclusões Gerais

A dependência cada vez maior dos Sistemas de Informação dita que a organização deve desenvolver um plano de Gestão da Continuidade para sua protecção e sobrevivência. No centro do planeamento de Gestão da Continuidade está a capacidade tecnológica e todos os procedimentos alternativos que asseguram a protecção da informação e colaboradores, de forma a garantir a disponibilidade da informação e quando necessário uma rápida recuperação dos Sistemas de Informação e das funções críticas de negócio.

A magnitude do investimento na protecção da informação e na recuperação de desastres está directamente relacionada com o custo associado à indisponibilidade dos serviços e da informação. Dada a complexidade dos inúmeros factores existentes no processo de Gestão da Continuidade, um grande número de organizações acaba por concluir que por vezes é necessário o acesso a recursos externos com conhecimentos específicos para uma implementação de sucesso de um plano de Continuidade do negócio.

A indisponibilidade dos serviços, planeada ou não, é uma contínua ameaça à Continuidade do negócio dado que a maior parte das organizações operam hoje de forma contínua, ou quase contínua. Enquanto que as noites e os fins de semana, tradicionalmente eram períodos em que os sistemas podiam parar sem grandes consequências ou impacto na organização, hoje o comércio electrónico estende o conceito de "horas úteis de serviço" para 24x7. De qualquer forma existe sempre a necessidade de paragem por motivos óbvios de manutenção dos Sistemas de Informação. Os sistemas precisam de manutenção e upgrades e as próprias aplicações necessitam de manutenção e alterações de forma a se manterem alinhadas com as necessidades do negócio.

Conforme modesto contributo e entendimento expresso na presente dissertação devem ser considerados na Gestão da Continuidade do negócio os seguintes níveis de disponibilidade:

Disponibilidade básica ou elementar (99.5% a 99.8%)
Alta Disponibilidade (99.8% A 99.95%, *downtime* < 4 horas/ano)
Disponibilidade Contínua (99.999%, *downtime* < 5minutos/ano)

Tolerância a Desastres
- Aumento da disponibilidade
- Providencia o failover automático em caso de desastres

Recuperação de Desastres

- não existe aumento de disponibilidade, *per se*
- minutos, horas, dias ou semanas para a recuperação

A volatilidade do negócio acrescenta uma terceira dimensão ao planeamento da Gestão da Continuidade do negócio. Os profissionais do IT em linha com o negócio lutam de forma a prever correctamente quais as necessidades que o mercado vai impor aos Sistemas de Informação. Os erros das previsões saem caro em qualquer uma das direcções, como a seguir se demonstra:

- Perspectivas muito optimistas encorajam o planeamento e um aumento da capacidade de processamento. Quando surgem momentos menos intensos no negócio, os investimentos no IT são subtilizados e o Custo Total de Aquisição, total cost of ownership TCO, sobe de forma proporcional.
- Perspectivas muito pessimistas encorajam um menor investimento nos Sistemas de Informação. Quando surgem momentos dinâmicos no negócio, os Sistemas de Informação podem ser um factor limitativo à capacidade de negociar da organização. Desta forma podem surgir custos oportunistas dada a perda de negócio e o Custo Total de Aquisição sobe novamente.

Em suma os grandes desafios para a Gestão da Continuidade são a mitigação dos riscos de indisponibilidade dos Sistemas de Informação, a volatilidade do negócio e a criação de um conjunto adequado de contramedidas chave que constituem a garantia de competitividade e sucesso da organização na prevenção e protecção de eventos adversos.

5.2 Sugestões para Novos Trabalhos de Investigação

Pese embora o facto deste trabalho ter sido desenvolvido com algumas limitações, verifica-se que são inúmeras as potencialidades de investigação.

Um novo framework sistemático e sensível às mudanças impostas pelas necessidades competitivas enquadrando as novas perspectivas e tecnologias, que permitam soluções mistas e que qualifiquem decisões. As opções são vistas no âmbito da continuidade nos casos extremos.

Um novo framework simplificará as opções e ampliará as decisões para além do âmbito tradicional de forma a incluir novas alternativas.

Glossário

Activação:

- todas as partes dos procedimentos de Continuidade do negócio e de recuperação de desastres foram colocadas em acção.

Alerta:

- estado de notificação para a ocorrência de um desastre e que todos os elementos devem estar em *standby* para a possível activação do plano de recuperação de desastres.

Desastre:

- qualquer interrupção, falha, evento ou problema que torne a infra-estrutura inoperacional. Poderá ter um número de definições das quais as mais evidentes são:

    - **Falha** - evento que ocorre e impossibilita os utilizadores de acederem aos sistemas e às aplicações. O ambiente, falta de electricidade, fogos, inundações, terramotos e falhas de *Hardware* ou *Software* podem gerar estas falhas eventuais.

    - **Desastre** - evento que cria a incapacidade numa organização de efectuar e providenciar as funcionalidades críticas de negócio por um período (in)determinado de tempo.

    - **Falha de sistemas** - interrupção não planeada da disponibilidade dos sistemas em que a origem poderá estar num problema de *Hardware, Software* ou em simples problemas operacionais.

    - **Emergência** - evento súbito e inesperado que requer uma acção imediata dada a ocorrência de uma potencial ameaça para a saúde, segurança, ambiente ou propriedades.

    - **Interrupção de negócio** - acontecimento que poderá ser antecipado como por exemplo, uma greve da função publica ou

poderá não ser antecipado, tal como uma falha energética que provoca a interrupção do normal funcionamento das operações em determinada localização.

- **Crise** - evento crítico que se não for conduzido da maneira correcta poderá ter um impacto catastrófico na organização, quer do ponto de vista da criação de rendimentos, reputação e capacidade de operar.

- **Falha de comunicações** - interrupção não prevista na comunicação electrónica entre um terminal e um processador, ou entre processadores, gerada pela falha de qualquer uma das componentes de *Hardware*, *Software* ou dos componentes de telecomunicações que compõem o *link*.

- **Falha de rede** - interrupção na disponibilidade de acesso aos sistemas com origem numa falha de comunicação que afecta uma rede de computadores, terminais, servidores ou *workstations*.

Funções críticas:

- actividades de negócio ou a informação que não pode ser interrompida ou ficar indisponível, por um determinado período de tempo, dado que a ausência destas funções durante o período de indisponibilidade é responsável por danos consideráveis à organização.

Funções não críticas:

- actividades de negócio ou a informação que pode ficar indisponível numa organização por um período de tempo indeterminado sem que a interrupção cause dados significativos à organização.

Gestão e análise de riscos:

- disciplina que assegura que uma organização não assume uma determinada quantidade de riscos considerados inaceitáveis.

- **Análise de risco** - processo pelo qual se identificam e minimizam todas as exposições aos riscos identificados que possam ameaçar uma organização.

- **Risco** - quantificação referente à probabilidade da ocorrência de um evento, normalmente associados à probabilidade da ocorrência de um evento adverso. Pode ser descrito como baixo risco – médio risco – ou alto risco, dado que alguns riscos embora conhecidos possam ser controlados ou não.

- **Ameaça** - potencial evento indesejado que poderá causar perdas e que poderá causar um impacto devastador na organização.

    - Identifica e modera as possíveis interrupções de serviços nas operações resultantes de potenciais acções humanas tais como terrorismo e sabotagens e empregados descontentes.

    - Identifica e modera ameaças e eventos causados pela natureza que possam originar interrupções de serviços na organização.

- Identifica e modera a potencial perda de recursos na organização em caso de desastre. Tais situações podem incluir a perda de vidas humanas, rendimentos, quota de mercado, estrutura competitiva, imagem da organização e capacidade operacional.

Recuperação:

- agilidade na capacidade de recuperação dos componentes da infra-estrutura dada a ocorrência de uma falha ou desastre. Os tipos de recuperação podem ser qualificados da seguinte maneira:

    - **Recover aplicacional** - directamente associado à recuperação dos serviços de *software* e aplicações da organização e dos respectivos dados, após os Sistemas de Informação terem sido novamente repostos em produção ou substituídos.

    - **Recover das comunicações** - componente da recuperação de desastres que gere a restauração e o reencaminhamento das comunicações de uma organização, as redes e todos os seus componentes.

- **Centro de Processamento de Dados De Recuperação** - componente da recuperação de desastres que gere a restauração dos serviços IT e a capacidade de processamento num Centro de Processamento de Dados alternativo.

- **Procedimentos de emergência** - conjunto de acções que fazem parte de um plano ou um conjunto de procedimentos que devem ser inicializados imediatamente após a ocorrência de um desastre para prevenir a perda de vidas, reduzir as lesões e também com o objectivo de minimizar danos materiais.

- **LAN recovery** - componente da recuperação de desastres que gere especificamente a substituição do equipamento de redes em caso de desastre e a restauração dos dados e *software* essencial para a gestão dessas comunicações.

- **Voice recovery** - processo de restauração dos serviços de comunicação de voz dentro de uma organização após um desastre.

Recuperação alternativa ou **backup options**:

- métodos seleccionados para a recuperação das funções consideradas críticas para o negócio após a ocorrência de um desastre. Dentro do IT algumas alternativas possíveis podem ser o processamento manual, aquisição de serviços, acordos recíprocos ou um Centro de Processamento de Dados alternativo de backup e recuperação de desastres que podem ser definidos como *hot-site, cold-site, mobile shell* ou centro de comandos. Uma recuperação alternativa é normalmente seleccionada após uma análise de risco ou um estudo de impacto para o negócio ou ambos. Baseados nos diversos cenários e nos objectivos de recuperação podem ser escolhidas várias opções.

Recuperação de Desastres:

- capacidade e habilidade na resposta de uma organização a uma interrupção de serviços através da implementação de um plano de recuperação de desastres que permita a recuperação das funções críticas de negócio de uma organização.

- **Plano de Recuperação de Desastres, PRD** - documento que define os recursos, acções, tarefas e os dados necessários na gestão do processo de recuperação no evento de uma interrupção dos serviços na organização. O plano deverá ser desenvolvido de modo a definir os processos de recuperação de todos as unidades de negócio com o objectivo da recuperação dos dados e dos sistemas críticos.

- o planeamento de recuperação de desastres tem como objectivo endereçar todos os aspectos tecnológicos da Continuidade do negócio. O planeamento avançado e as preparações são necessárias para minimizar as perdas e garantir a continuidade das funções consideradas críticas dentro de uma organização no evento de um desastre.

Recovery Point Objective, RPO:

- definição de um período de tempo a partir do qual todos os dados e serviços críticos devem estar novamente disponíveis, para se regressar ao considerado processamento normal dentro da organização. O ***RPO*** é a base a partir da qual toda a *Estratégia de Recuperação* deverá ser desenvolvida.

Recovery Time:

- período correspondente entre a declaração de desastre ou a activação da recuperação de desastres até à recuperação das funções críticas para o negócio.

Bibliografia

Barnes, J.C. (2001) 'A guide to business continuity planning', John Wiley and Sons Ltd, Chichester. ISBN 0-471-53015-8

Bell, J.K. (1995) 'Disaster Survival Planning Workbook'

Business Continuity Institute. (2002) 'Business Continuity Management: A strategy for business survival', Business Continuity Institute, Worcester.

Everitt, B.S., Landau, S. & Leese, M. (2001) 'Cluster Analysis', Arnold Publishers ISBN: 0340761199

Fulmer, K.L. (2000) 'Business Continuity Planning, 2000 Edition : A Step-By-Step Guide With Planning Forms', Rothstein Associates Inc. ISBN 0-9641648-1-7

Gamma, E. (1995) 'Design Patterns' Addison-Wesley Professional ISBN: 0201633612

Henderson, D.M. (2002) 'Emergency Management Plan for Colleges & Universities: A Continuity of Operations Plan'

Henderson, D.M. (2003) 'Emergency Management Plan for Public & Private Schools'

Hiles, A.N. (2002) 'Enterprise Risk Assessment and Business Impact Analysis: Best Practices', Rothstein Associates Inc. ISBN #1-931332-12-6

Hiles, A.N. (2004) 'Business Continuity: Best Practices - World-Class Business Continuity Management', Rothstein Associates Inc. ISBN 1-931332-22-3

Hunt, A. (1999) 'The Pragmatic Programmer: From Journeyman to Master', Addison-Wesley Professional ISBN: 020161622X

Janco Associates (2004) 'Disaster Recovery Planning & Management Job Decriptions'

Kuong, J.F (1998) 'Standards for Establishing an Effective Contingency Planning & Disaster Recovery Function'

Kuong, J.F. (2002) 'How to Audit Your Business Contingency & Continuity Plan to Ensure IT Covers September 11 & New Global Threats'

Laye, J. (2002) 'Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes.'

Levinson, J. & Granot, H. (2002) 'Transportation Disaster Response'

Marcus, E. & Stern, H. (2003) 'Blueprints for High Availability', ISBN: 0471430269

Musaji, Y.F. (2001) 'Auditing and Security: AS/400, NT, UNIX, Networks, and Disaster Recovery Plans'

Myers, K.N. (1999) 'Manager's Guide to Contingency Planning: Protecting Vital Facilities and Critical Operations'

Piedad, F. & Hawkins, M. (2000) 'High Availability: Design, Techniques and Processes', Prentice Hall PTR ISBN: 0130962880

Roessing, R. (2002) 'Auditing Business Continuity Global Best Practices', Rothstein Associates Inc. ISBN #1-931332-15-0

Rothstein, P.J. (1995) 'Disaster Recovery Testing: Exercising Your Contingency Plan', Rothstein Associates Inc.

Sandhu, R.J. & Varghjese, M. (2002) 'Disaster Recovery Planning'

Serrano, A., Caldeira, M & Guerreiro, A. (2004) 'Gestão de Sistemas e Tecnologias de Informação', FCA – Editora de Informática Lda. ISBN 972-722-409-1

Sikich, G.W. (2003) 'Integrated Business Continuity: Maintaining Resilience in Uncertain Times'

Strohl Systems (2002) 'The Business Continuity Planning Guide'

Syed, A. Ph.D. & Syed, A. (2004) 'Business Continuity Planning Methodology'

Weygant, P.S. (2001) 'Clusters for High Availability: A Primer of HP Solutions', ISBN: 0130893552

Yourdon, E. (2002) 'Byte Wars: The Impact of September 11 on Information Technology'

Videos

British Broadcasting Corporation (2002) 'Disaster1: Spiral to Disaster', BBC Worldwide Limited, London.

British Broadcasting Corporation (2002) 'Disaster2: A Major Malfunction', BBC Worldwide Limited, London.

Business Continuity Institute (2001) 'Back to Business: Planning ahead for the unexpected', Merlin Communications, Cirencester, Gloucestershire.

Videotel International (1993) 'Crisis Management', ShandWick Communications, London.