Plano de Recuperação de Desastres para os SISTEMAS de IT

Políticas de Continuidade e Recuperação
Análise de Risco
Domínios de Recuperação a Considerar

Trabalho Final de Curso 2010/2011

Alunos:

Sandra Trindade Frias 20080471
Paulo Viseu 20081810

Professor Orientador:

Pedro Malta

Índice

Introdução 3
1. Objectivos 4
1.2. Planeamento 5
Subscrição de Serviços 6
Outras alternativas de backup de Data Centers: 10
1.3. Manutenção do Plano de Disaster Recovery 11
1.4. Teste ao Plano de Disaster Recovery 12
1.5. Comité de desastre 14
1.6. Quando termina um desastre? 15
1.7. Fraude e Crime 16
2. Objectivos Específicos 17
Alternativas de Cenários e Plano de Recuperação 18
2.1. Recuperação Baseada em Procedimentos de Backup 19
Fluxo de Actividades do Plano 20
2.2. Comité de Desastre 21
2.3. Avaliação de Incidentes 23
2.4. Declaração de Desastre 24
2.5. Operações de Recuperação 24
2.6. Solução de Backup 25
Backup On-line 25
Ferramentas de backup de dados locais: 26
2.7. Recuperação Baseada na Utilização de Site Alternativo 27
3. Conclusão 30
4. Referências 33
5. Anexos 33

Introdução

O plano de Recuperação de Desastres (DRP – Disaster Recovery Plan) é o processo, politicas e procedimentos relacionados à recuperação ou a manutenção de infra-estrutura tecnológica essencial para uma organização.

Uma solução de recuperação de desastre consiste na recuperação dos sistemas a partir de uma emergência, causando o mínimo impacto para a organização, garantindo a continuidade de negócio.

Como principal objectivo pretende-se identificar os domínios de recuperação que permitem endereçar a preservação do negócio em face de uma interrupção elevada dos sistemas de TI, fornecendo operações alternativas durante os processos de recuperação, do controlo, e do retorno à situação normal mais tarde, sem sentir a experiência de uma perda substancial da capacidade de processamento.

O planeamento para atingir este objectivo envolve um conjunto de tarefas perfeitamente identificadas, tais como, preparação, testes, e actualização das acções necessárias para a protecção contra efeitos de falhas críticas dos sistemas.

A finalidade do plano de recuperação pós-catástrofe é reduzir a confusão e realçar a habilidade da organização de tratar a crise.

1. Objectivos

O objectivo principal da implementação de uma solução de Disaster Recovery (DR) é fornecer uma maneira organizada de tomar decisões quando um evento de desastre ocorre.

O primeiro objectivo do plano de recuperação pós-catástrofe é fornecer a capacidade dos processos críticos utilizarem "locais" diferentes para manterem o negócio, e garantir o retorno ao local preliminar e ao processamento normal dentro de um prazo que minimize as perdas à organização, executando procedimentos de recuperação rápidos.

Obviamente, quando um evento disruptivo ocorre, nenhuma organização se pode dar ao luxo de criar e executar um plano de recuperação durante a ocorrência. Consequentemente, a capacidade prévia de planeamento e de teste que foi feita anteriormente, determinará a capacidade da mesma organização suportar um desastre.

Os objectivos do Disaster Recovery Plan (DRP) são múltiplos mas cada um é importante.
Podem incluir os seguintes:

- Proteger da falha dos serviços informáticos;
- Minimizar os riscos que ocorrem no atraso da prestação dos serviços informáticos aos processos de negócio;
- Garantir a fiabilidade dos sistemas de "backup" através e testes e simulações;
- Minimização a necessidade de tomadas de decisão (as acções estão previamente planeadas) durante um desastre;

Os passos no processo de planeamento de desastres são os seguintes:

- Planeamento para o desastre e criação de planos para suportá-lo;
- Implementação;
- Manutenção dos planos actuais e actualização dos mesmos;

A avaliação da necessidade de uma implementação de um plano de Disaster Recovery deve ser feita com base nos seguintes factores:

- Riscos de desastre. Desastres naturais ou acidentes;
- Vulnerabilidade do negócio. Qual o período de tempo máximo que uma organização se consegue manter indisponível;
- Os custos de downtime. O investimento na Gestão da Continuidade deve ser encarado como um seguro.

1.2. Planeamento

O planeamento para o desastre e criação de planos para suportá-lo constitui um dos passos mais importantes.

Um dos elementos essenciais para um bom planeamento de um sistema de Disaster Recovery é o meio de processamento de serviços de backup.

Os tipos de processos mais comuns são:

- Subscrição de serviços
- Centros múltiplos
- Serviço de escritórios

- Outras alternativas de backup de Data Center

Subscrição de Serviços

Outro cenário alternativo é a subscrição de serviços. Neste cenário a prestação de serviços por empresas externas providencia uma alternativa de backup e de centro operacional.

Subscrição de serviços é provavelmente a solução alternativa mais utilizada.

Existem três tipos standards de subscrição de serviços:

- Hot site
- Warm site
- Cold site

Hot Site

Este serviço é a melhor solução para a implementação de um sistema de Disaster Recovery.

Um Hot Site consiste numa réplica integral da realidade do Data Center actual configurado com a energia eléctrica, aquecimento, ventilação e ar condicionado e todos os sistemas operacionais.

As aplicações necessárias para suportar as transacções remotas são instaladas nos servidores e mantidas actualizadas como mirror do sistema em produção.

Teoricamente os utilizadores dos sistemas terão acesso constante a informação dos últimos backups, de forma a iniciarem o funcionamento num curto espaço de tempo.

Este tipo de site requer manutenção constante de hardware, software, informação, e aplicações de forma a assegurar que o site é uma réplica do site em produção.

As vantagens de um site deste tipo são inúmeras:

- Disponibilidade 24 Horas / 7 dias
- Exclusividade de utilização
- O site estará imediatamente (ou dentro das tolerâncias admissíveis de tempo) disponível após o evento ocorrer.
- O site pode apoiar uma interrupção por um breve período (ex: manutenção do sistema de produção), bem como um compromisso a longo prazo.

Algumas das desvantagens do Hot Site são as seguintes:

- É a alternativa mais dispendiosa;
- É comum que os prestadores de serviços sobre dimensionem as suas capacidades de processamento;
- Todos os sistemas de segurança e mecanismos que são exigidos no site principal devem ser duplicados no Hot Site. O acesso ao mesmo deve ser controlado e deve estar-se ciente da segurança e metodologia implementada pelo prestador de serviço.

Warm Site

Tal como um Hot site, também está prontamente disponível um conjunto de equipamentos replicados do Data center de produção, com energia eléctrica, ar condicionado e conectividade à rede de comunicações.

Para activar o processamento remoto para este tipo de site, as aplicações e dados terão de ser restauradas a partir de backups previamente elaborados.

As vantagens para este tipo de site, por oposição ao Hot Site, são essencialmente os seguintes:

- Este tipo de configuração será consideravelmente mais barato do que um Hot site.
- Uma vez que este tipo de site requer menos controle e configuração, existe uma maior flexibilidade na escolha do local.
- A utilização dos recursos administrativos é mais baixa do que com a manutenção de um Hot site.

A principal desvantagem de um warm site, em comparação com um hot site, é a diferença de quantidade de tempo e esforço que terá para começar a produção no novo site.

Se a operação de Recovery não for extremamente urgente e crítica, esta pode ser uma alternativa aceitável.

Cold Site

Um cold site é o menos preparado de qualquer uma das três opções, mas é provavelmente a mais comum das três.

Um cold site difere dos outros dois na medida em que está pronto para receber os equipamentos a serem levados durante uma emergência, mas nenhum hardware existe no local.

O cold site consiste num espaço disponível com energia eléctrica e ar condicionado, mas os equipamentos devem ser levados para o local, e será necessário a instalação das aplicações. As linhas de comunicação podem estar disponíveis ou não.

Um Cold Site não é considerado um recurso adequado para Disaster Recovery, por causa do tempo necessário para colocar em produção todos os sistemas, excepto se existirem contratos de serviços adicionais com os diversos fornecedores das soluções de forma a garantir uma reposição rápida (que garanta os cenários de recuperação) de todo os sistemas que compunham o Data Center. Torna-se no entanto impossível realizar testes exaustivos de Disaster Recovery, o que torna muito difícil prever o sucesso em caso de desastre.

Centros Múltiplos

A variação aos sites anteriormente mencionados é chamada de centros múltiplos, ou duplicação de sites. No conceito de centro múltiplo, o processo é distribuído por vários centros de operações, criando uma abordagem à distribuição e partilha de redundância de recursos disponíveis. Estes múltiplos centros poderiam ser propriedade e gerência da mesma organização (in-house sites) ou usados em conjunção com algum tipo de acordo de reciprocidade.

As vantagens são principalmente financeiras, pois o custo é contido. Além disso, este tipo de site permite a partilha de recursos e de apoio entre os vários sites.

A principal desvantagem é que uma catástrofe de grandes proporções poderia facilmente ultrapassar a capacidade de Recovery dos sites. Além disso, múltiplas configurações poderiam ser difíceis de administrar.

Outras alternativas de backup de Data Centers

Existem outras alternativas para as já anteriormente mencionadas. Muitas vezes uma organização pode usar uma combinação destas alternativas, para além da utilização de um dos cenários anteriores.

- Backup em sites móveis;
- In-house ou fornecimento externo de substituição de hardware;

Matriz de características dos serviços:

Características	**Hot Site**	**Warm Site**	**Cold Site**
Réplica integral do Data Center	√	√	
Não existem equipamentos no local. Recebe os equipamentos do site original em caso de desastre			√
Aplicações de suporte as transacções remotas instaladas nos servidores e actualizadas	√		
As aplicações e dados são restauradas a partir de backups previamente elaborados, para activar o processamento remoto		√	
Instalação das Aplicações			√
Acesso a informação dos últimos backups.	√		

Disponibilidade 24 Horas / 7 dias	√		
Site imediatamente disponível após um evento ocorrer.	√		
Alternativa mais dispendiosa	√		
Duplicação de todos os mecanismos de segurança do site principal	√		

1.3. Manutenção do Plano de Disaster Recovery

Uma semelhança comum a todos os planos de Recovery é a rapidez com que se tornam obsoletos pelas mais variadas razões. A empresa pode reorganizar-se e unidades empresariais críticas podem ser diferentes do que quando o plano foi elaborado pela primeira vez.

Mais frequentes são as mudanças na rede ou nas infra-estruturas de IT, que resultam em alterações na localização ou configuração de hardware, software e outros componentes.

Os motivos podem também ser administrativos. Planos de Disaster Recovery muito complexos não são facilmente actualizáveis, perda de interesse pelo processo, ou alterações de funcionários podem afectar o seu envolvimento.

Seja qual for o motivo, devem ser empregues técnicas para a manutenção do plano desde o início, para garantir que o plano se mantém actual e utilizável.

É importante fomentar a manutenção de procedimentos na organização utilizando descrições de funções de forma a criar uma responsabilização pelas actualizações.

Também se devem criar procedimentos de auditoria que possam apresentar relatórios regulares sobre o estado do plano.

É necessário assegurar que as várias versões do plano sejam arquivadas e não confundidas com a mais actualizada. Deve substituir-se as versões mais antigas do texto, com versões actualizadas em toda a empresa, quando um plano é alterado ou substituído.

1.4. Teste ao Plano de Disaster Recovery

Efectuar um teste ao plano de Disaster Recovery é fundamental. Por exemplo: um sistema de backup não pode ser considerado operacional enquanto não forem efectuados testes de recuperação total da informação nele armazenado.

Tipicamente um plano de Disaster Recovery é um conjunto de elementos meramente teóricos até que tenha sido efectivamente testado e certificado. O plano de teste deve ser criado e os ensaios devem ser realizados de forma regular.

Para além dos motivos para testes mencionados anteriormente, existem outras razões específicas para testar o plano, principalmente, para informar os órgãos administrativos da capacidade da empresa em recuperar totalmente.

Outras razões específicas para a realização de testes são:

- O teste verifica o rigor dos processos de recuperação e identifica deficiências;
- Testar permite preparar e treinar os funcionários para executar as suas tarefas de emergência;
- Os testes verificam a capacidade de processamento do site de recuperação;

A funcionalidade de um plano de recuperação vai determinar directamente a capacidade de restabelecer a situação original antes do desastre.

O plano não pode ser um documento que reúna informação desactualizada. Tem que reflectir a real capacidade da organização permanentemente actualizada onde conste:

- Os passos específicos do plano
- Quem irá participar na realização do teste
- A assignação de tarefas aos funcionários
- Os recursos e serviços necessários (hardware, software, documentação, etc.)

Alguns conceitos fundamentais serão aplicados na realização de testes. Fundamentalmente o teste não deve perturbar o normal funcionamento do negócio. Além disso, o nível de testes a efectuar deverá ser implementado gradualmente, começando num nível fácil e ir aumentando de acordo com os resultados obtidos pela equipa interveniente. É importante lembrar que o motivo pelo qual se efectua o teste é para encontrar pontos fracos no plano de execução.

Devem documentar-se os problemas encontrados durante a realização do teste e actualizar o plano de acordo com o necessário.

Existem cinco tipos de testes a planos de Disaster Recovery ordenados por prioridades, do mais simples ao mais complexo.

Conforme a organização avança através dos testes, cada teste é progressivamente mais preciso e adequado à realidade da organização.

Alguns tipos de testes, por exemplo, os últimos dois, exigem grandes investimentos de tempo, recursos e coordenação para serem implementados:

- Checklist.
- Walk-through estruturado.
- Simulação.
- Paralelo.
- Interrupção Total.

Nível	Tipo	Descrição
1	Checklist	São distribuídas cópias do plano para revisão pelos órgãos de gestão.
2	Walk-through Estruturado	Órgãos de gestão por unidade de negócio reúnem-se para rever o plano.
3	Simulação	Todo o pessoal de suporte é reunido para executar uma sessão prática.
4	Paralelo	Teste aos sistemas críticos que correm em paralelo no site alternativo.
5	Teste de interrupção Total	Encerramento do processo normal de funcionamento para uma simulação de um cenário real de desastre.

1.5. Comité de desastre

O comité de desastre da recuperação será claramente definido com o mandato para executar os procedimentos de recuperação em caso de desastre.

A tarefa principal da equipa é a de manter o funcionamento das funções críticas pré-definidas no site alternativo de backup.

Entre as muitas tarefas, esta equipa terá as funções:

- Recuperar a partir dos materiais off-site, ou seja, tapes backup, servidores, workstations, etc;
- Instalação de sistemas críticos, aplicações e dados exigidos pelas unidades de negócio;
- A equipa deve identificar fontes de informação, equipamentos e outros que possam tornar o regresso ao local possível;
- Repor o site original nas condições anteriores à ocorrência do desastre (se possível);
- Retorno para o site original;

1.6. Quando termina um desastre?

A catástrofe não está terminada até que todas as operações sejam devolvidas à sua localização e função normal. Existe uma grande janela de vulnerabilidade quando se retorna a partir do site suplente ao site original para a produção local. Por uma questão de custos deve retornar-se a normalidade logo que existam condições para tal.

Devem ser efectuados os últimos backups do site de contingência e envia-los para o Data Center principal. Após os dados serem restaurados no ambiente principal, a produção poderá ser iniciada.

1.7. Fraude e Crime

Outros problemas relacionados com o evento podem aparecer. Deve ter-se em conta pessoas ou organizações que podem tentar capitalizar financeiramente a organização sobre o desastre, explorando preocupações de segurança ou de outras possibilidades de fraude. Em uma grande catástrofe física, vandalismo e saques são comuns ocorrerem. O plano deverá considerar estas contingências.

2. Objectivos Específicos

É objectivo das empresas providenciar uma forma organizada e consolidada de gestão das actividades de resposta e recuperação dos sistemas de IT de um Data Center após uma interrupção não planeada da operação dos mesmos, assim como recuperar os sistemas de IT críticos no suporte ao negócio em tempo útil, aumentando a resiliência da organização face a um desastre e reduzindo os impactos resultantes da interrupção;

É necessário um levantamento exaustivo das unidades de negócio e respectivas missões, assim como os Processos de Negócio e Internos de Suporte. Estas actividades devem ser desenvolvidas com a realização de entrevistas com todas as Unidades Funcionais.

Partindo da identificação dos respectivos Interlocutores, na fase de Preparação do Projecto, os principais objectivos das entrevistas devem centrar-se:

- Identificação dos Processos Internos de Suporte e de Negócio sob responsabilidade das Unidades e aferição da pertinência dos mesmos para o âmbito do Projecto quanto à sua criticidade. A criticidade dos Processos encontra-se directamente relacionada com a dimensão do impacto causado pela sua interrupção.

- Nível de criticidade das Aplicações e Infra-estruturas, através do seu mapeamento com os Processos a que dão suporte. Inventário de Activos que Integram o Plano de Recuperação;

- Tempos de Indisponibilidade e de Perda de Dados máximos admissíveis, para cada Processo e, consequentemente, o momento (após a ocorrência de um desastre) no qual as componentes tecnológicas (Aplicações e Infra-estruturas) deverão encontrar-se operacionais para

dar cumprimento aos requisitos de continuidade definidos para os Processos;

- Relacionar os resultados obtidos anteriormente e constituir Domínios de Recuperação onde se enquadram conjuntos de Processos com requisitos de recuperação semelhantes.

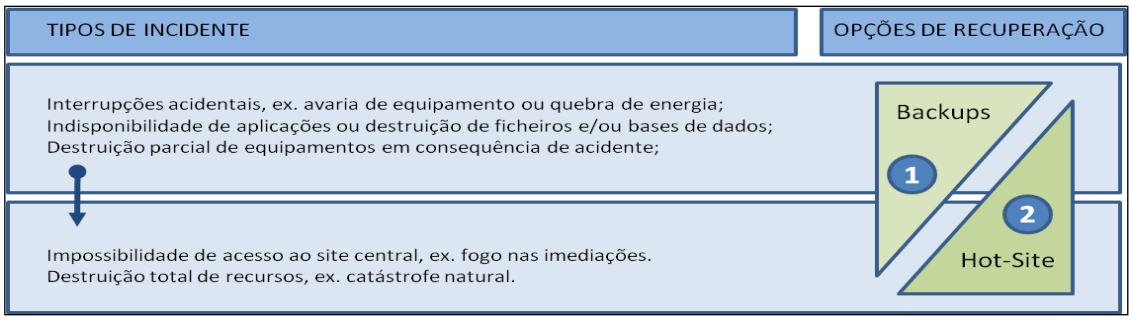
- Apresentação e distribuição dos Questionários de Levantamento de informação;

- Por fim identificar os requisitos que um Plano de Recuperação deverá contemplar face ás alternativa de cenários de recuperação considerados.

Alternativas de Cenários e Plano de Recuperação

A elaboração de um plano de recuperação deve estar associada a ideia de que a protecção dos sistemas de IT do Data se encontra associada ao tipo de incidente que possa afectar a normal operação desses mesmos sistemas e que a conjuntos específicos de incidentes estão associadas estratégias de recuperação distintas.

Para o caso de incidentes graves, no sentido de tornarem indisponível o Data Center, e resultantes por exemplo de catástrofes naturais, a estratégia de recuperação deverá assentar na utilização de instalações alternativas (Hot Sites) com equipamento disponível e dados actualizados. No caso de incidentes resultantes de interrupções acidentais que não causem a indisponibilidade total do Data Center, por exemplo avaria de equipamento, a estratégia de recuperação pode assentar em procedimentos de backup de dados e reposição de equipamentos suportados por contratos de manutenção e suporte com os fabricantes e de acordo com o nível de serviço pretendido.



2.1. Recuperação Baseada em Procedimentos de Backup

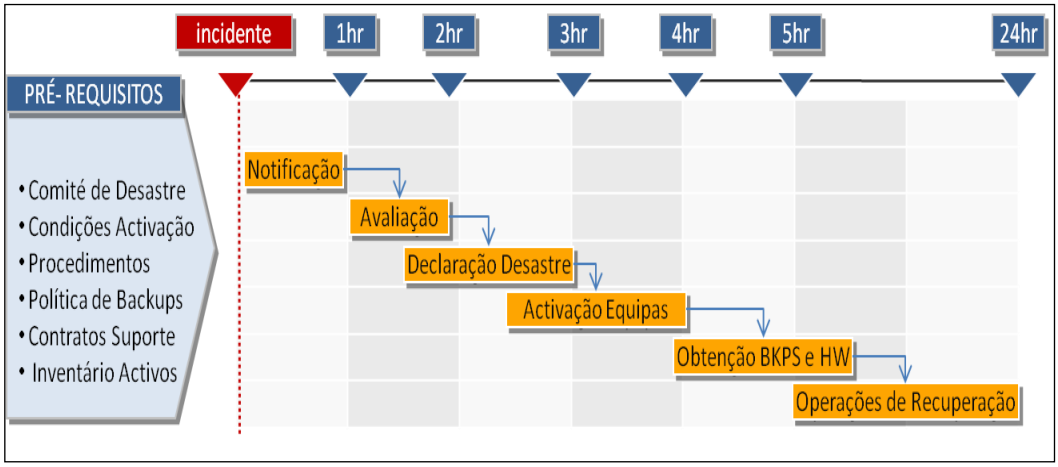
O Plano de Recuperação será desenvolvido de forma a atingir os seguintes objectivos:

- Providenciar uma forma organizada e consolidada de gestão das actividades de resposta e recuperação dos sistemas de IT de um Data Center após uma interrupção não planeada da operação dos mesmos;
- Recuperar os sistemas de IT críticos no suporte ao negócio em tempo útil, aumentando a resiliência da organização face a um desastre e reduzindo os impactos resultantes da interrupção;
- O Plano de Recuperação tem como âmbito a resposta pronta aos seguintes incidentes tipo:
- Qualquer incidente que mantenha a capacidade de recuperação dos sistemas de IT num data center em tempo útil, menos de 24horas;
- Qualquer incidente externo que possa causar uma interrupção do negócio como por exemplo: cortes de energia eléctrica ou dos serviços de comunicações;
- Qualquer incidente que afecte as operações normais dos activos de IT residentes num Data Center mas que permita a sua recuperação por recurso à reposição de hardware e dos backups de aplicações e sistemas;

O Plano de Recuperação tem como base os seguintes pressupostos face a um incidente:

- Os activos de IT existentes num data center foram afectados pelo incidente mas a sua recuperação é possível em menos de 24horas;
- Backups críticos para reposição de sistemas e informação são mantidos fora do site principal com a rotação adequada e estarão acessíveis em caso de incidente;
- Em caso de incidente estará disponível uma equipa técnica/operacional para assumir as responsabilidades de recuperação;
- A recuperação dos sistemas será efectuada de acordo com procedimentos pré-definidos e testados;

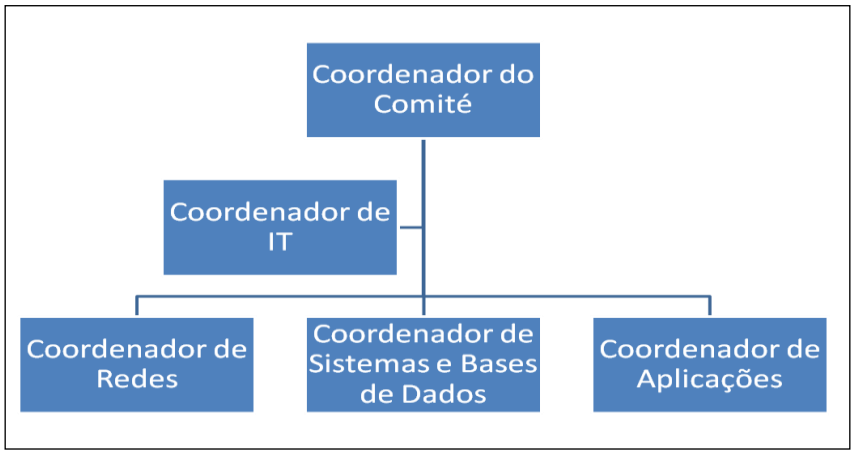
Fluxo de Actividades do Plano



2.1. Comité de Desastre

O Comité de Desastre tem como missão operacionalizar o Plano de Recuperação de Desastre. Após um incidente, funciona como ponto de contacto relativamente aos SI, tendo como responsabilidade de declarar a situação de desastre e colocar em prática o Plano de Recuperação de Desastre.

A constituição do Comité de Desastre é a seguinte:



Os contactos dos membros do Comité de Desastre são os que constam na tabela seguinte:

Função	Responsável	Suplente
Coordenador do Comité de Desastre	Nome Contacto 1 Contacto 2	Nome Contacto 1 Contacto 2
Coordenador de IT	Nome Contacto 1 Contacto 2	Nome Contacto 1 Contacto 2
Coordenador de Redes de Comunicações	Nome Contacto 1 Contacto 2	Nome Contacto 1 Contacto 2
Coordenador de Sistemas e Bases de Dados	Nome Contacto 1 Contacto 2	Nome Contacto 1 Contacto 2

Estes contactos deverão ser actualizados sempre que se verifique alguma alteração, sendo da responsabilidade do Coordenador do Comité de Desastre a garantia da sua validade.

As responsabilidades do Comité de Desastre são as seguintes:

Fase	Responsabilidade	Funções
Antes do incidente	Elaborar e manter actualizado o Plano de Recuperação de Desastre	Coordenador do Comité de Desastre Coordenador de Redes de Comunicações Coordenador de Sistemas e Bases de Dados
	Aprovar e comunicar à Administração o Plano de Recuperação de Desastre	Coordenador do Comité de Desastre
	Garantir a coesão e integração do Plano de Recuperação de Desastre com o Plano de Emergência Interno	Coordenador do Comité de Desastre
	Garantir a existência de meios em permanência para suportar uma declaração de desastre, de acordo com os requisitos	Coordenador do Comité de Desastre
	Garantir a execução dos testes e/ou auditorias anuais ao Plano de Recuperação de Desastre	Coordenador do Comité de Desastre
Durante a situação de incidente	Resposta imediata e avaliação da gravidade da situação	Coordenador do Comité de Desastre Coordenador de Redes de Comunicações Coordenador de Sistemas e Bases de Dados
	Declaração de Desastre	Coordenador do Comité de Desastre
Durante a situação de incidente	Implementação do Plano de Recuperação de Desastre	Coordenador do Comité de Desastre Coordenador de Redes de Comunicações Coordenador de Sistemas e Bases de Dados Coordenador de Aplicações
	Coordenação com o Plano de Emergência Interno	Coordenador do Comité de Desastre
	Comunicação com a Administração	Coordenador do Comité de Desastre

Após o incidente	Revisão crítica do Plano de Recuperação de Desastre, incorporando o conhecimento prático obtido	Coordenador do Comité de Desastre Coordenador de Redes de Comunicações Coordenador de Sistemas e Bases de Dados
	Declaração de Fim de Desastre, e desactivação do Plano de Recuperação de Desastre	Coordenador do Comité de Desastre

2.2. Avaliação de Incidentes

Qualquer pessoa pode iniciar o processo de notificação de desastre. Esta notificação deve ser dirigida a qualquer membro do comité de desastre, que por seu turno informará o Coordenador do Comité de Desastre.

A decisão de activar o Plano de Recuperação de Desastre deverá ser tomada o mais cedo possível, face a um incidente que poderá causar uma interrupção dos sistemas de informação da organização por um período superior a 24horas. Face à ocorrência de um incidente as acções imediatas são as seguintes:

- Garantir a segurança de pessoas, cumprindo rigorosamente o Plano de Emergência Interno;
- Se possível, deslocar um membro do comité de desastre ao local, para aferir a gravidade da situação;
- Usar os meios disponíveis para salvaguardar a integridade de sistemas e dados, sempre que tal não coloque em risco a integridade física dos colaboradores;
- Avaliar a situação: obter inventário dos activos do data center e avaliar estado de operacionalidade dos mesmos; Elaborar lista com deficiências encontradas e estimar tempos de recuperação;

- Informar a Administração;
- Convocar o Comité de Desastre;
- Informar utilizadores / parceiros da degradação expectável nos níveis de serviço praticados;
- Envolver os fornecedores de IT.
- Em caso algum deve haver qualquer comunicação com a imprensa.

2.3.Declaração de Desastre

O Plano de Recuperação de Desastre deve ser activado, quando se verifiquem as seguintes condições de activação:

- O incidente/desastre foi contido, de acordo com os procedimentos do Plano de Emergência Interno, não existindo risco para a integridade física de pessoas;
- Após uma análise do impacto, prevê-se um tempo de recuperação do data center inferior a 24 horas;
- A equipa a envolver está disponível em número suficiente para garantir a eficácia do Plano de Recuperação de Desastre.

2.4.Operações de Recuperação

A equipa técnica que integra o Comité de desastre antes de iniciar qualquer procedimento na Data Center deverá:

- Obter dados de backup a partir do local de armazenamento externo;
- Contactar integradores para reposição de hardware danificado de acordo com contrato de suporte existente;

- Validar disponibilidade de hardware e tapes de backup de acordo com o inventário de equipamentos ou serviços danificados ou degradados elaborada durante a fase de avaliação do incidente;
- Obter a lista com os procedimentos de recuperação previamente definida (Ordem, Infra-estrutura a repor, sistemas que suporta e Macro Procedimentos);

2.5. Solução de Backup

As soluções técnicas que suportarão a opção "Recuperação Baseada em Procedimentos de Backup" podem ser duas:

- "Backup On-line"

- Ferramentas de backup de dados locais e/ou remotos.

Backup On-line

Este é um serviço contratado a um fornecedor deste tipo de serviço (operador ou integrador de serviços) que consiste num processo de backup externo às instalações do Data Center.

O serviço é prestado através de conectividade sobre uma linha dedicada ou sobre um serviço de Internet.

O processo deverá ser totalmente automatizado após a configuração inicial, e transparente para os utilizadores e administradores dos sistemas internos.

Vantagens da solução:

- Processo totalmente automático e/ou manual por ordem do administrador/utilizador;
- Armazenamento de informação incremental (apenas é arquivada a informação nova)
- Possibilidade de acesso em tempo real à informação armazenada;
- Disponibilidade da informação
- Localização da informação é tipicamente replicada em dois locais diferentes;
- Redução de capacidade de "storage" interna.
- Disponibilidade 24 horas por dia, independentemente da disponibilidade de elementos da equipa técnica IT

Desvantagens:

- Pouca capacidade de monitorizar a segurança da informação. É necessário garantir a total confidencialidade da informação armazenada no exterior (segurança na comunicação e encriptação dos dados);
- Dificuldade no controle de testes de reposição (validação da "qualidade" do backup) (deverão existir métodos de controle em função da informação armazenada);

Ferramentas de backup de dados locais:

Consiste numa ferramenta administrada localmente, que efectua, duma forma parametrizada e padronizada, a cópia de informação seleccionada.

Essa cópia pode ser efectuada para diferentes tipos de media: Tapes, discos magnéticos ou discos ópticos.

- Deve ser nomeado um responsável pela tarefa de backup;
- Os sistemas a serem submetidos a backup são os identificados no plano de recuperação;
- Procedimentos de validação da "qualidade do backup" (testes para situações de recuperação)

2.6. Recuperação Baseada na Utilização de Site Alternativo

As soluções técnicas que suportarão a opção "Recuperação Baseada na utilização de site Alternativo" podem ser duas:

- Criação de um "warm site" num local disponibilizado por um provedor de serviço
- Criação de um site remoto em instalações

Warm Site

Este é um serviço contratado a um fornecedor deste tipo fornecimento (operador ou integrador de serviços) que consiste em arrendar um espaço físico num Data Center gerido externamente.

O serviço é prestado através de conectividade sobre uma linha dedicada ou sobre um serviço de Internet.

O processo de transferência da informação para aquele site deverá ser totalmente automatizado após a configuração inicial, e transparente para os utilizadores e administradores dos sistemas internos.

É necessário garantir um contrato exigente relativamente a SLAś com os diferentes fornecedores de hardware e software.

Em caso de ocorrência de uma situação crítica, a informação está totalmente disponível no site remoto e a activação dos contratos de manutenção deverá

ser feita com a premissa de colocar o hardware no local de instalação do espaço contratado.

Vantagens da solução;

- Processo totalmente automático e/ou manual por ordem do administrador/utilizador;
- Armazenamento de informação incremental (apenas é arquivada a informação nova);
- Possibilidade de acesso em tempo real à informação armazenada;
- Disponibilidade da informação
- Localização da informação é tipicamente replicada em dois locais diferentes;
- Redução de capacidade de "storage" interna.
- Disponibilidade 24 horas por dia, independentemente da disponibilidade de elementos da equipa técnica IT

Desvantagens:

- Pouca capacidade de monitorizar a segurança da informação. É necessário garantir a total confidencialidade da informação armazenada no exterior (segurança na comunicação e encriptação dos dados);
- Dificuldade no controle de testes de reposição (validação da "qualidade" do backup) (deverão existir métodos de controle em função da informação armazenada);

Site Remoto

Este é um serviço totalmente controlado pelas equipas técnicas porque consiste em replicar na medida necessária para garantir os serviços mínimos aos processos de negócio.

De acordo com os dados obtidos e já referenciados, consideramos que 50% do negócio é perdido nas primeiras 24 horas de indisponibilidade do Data Center, excepto em alturas consideradas críticas em que o tempo de interrupção não pode ser superior a 4 horas.

Este é o factor principal de cálculo para a disponibilidade do Data Center.

Concluímos que, neste tipo de solução, se deve garantir:

- Replicação de 50% da infra-estrutura considerada crítica no documento de "levantamento de infra-estrutura";
- Sincronização de informação entre os dois sites em tempo real;
- Um contrato exigente relativamente a SLAs com os diferentes fornecedores de hardware e software.
- Devemos garantir, no mínimo, os processos de negócio considerados críticos. Em caso de ocorrência de uma situação crítica, a informação está totalmente disponível no site remoto e a activação dos contratos de manutenção deverá ser feita com a premissa de colocar o hardware no local de instalação do mesmo espaço.

Vantagens da solução;

- Processo totalmente automático e/ou manual por ordem do administrador/utilizador;

- Armazenamento de informação incremental (apenas é arquivada a informação nova)
- Possibilidade de acesso em tempo real à informação armazenada;
- Disponibilidade da informação
- Localização da informação é tipicamente replicada em dois locais diferentes;
- Redução de capacidade de "storage" interna.
- Disponibilidade 24 horas por dia, independentemente da disponibilidade de elementos da equipa técnica IT
- Monitorização totalmente controlada pelas Empresas
- Capacidade de efectuar testes em tempo real sem perder qualidade de serviço;

3. Conclusão

A dependência cada vez maior dos Sistemas de Informação das organizações, leva cada vez mais, a que sejam desenvolvidos planos de Disaster Recovery (DRP) de forma a garantir a operação de uma empresa com o mínimo impacto aos clientes em situações de contingência.

Um Plano de Disaster Recovery deve procurar restabelecer o ambiente de processamento no menor tempo possível a fim de evitar um efeito catastrófico nos negócios, pois a maior ameaça a continuidade de negócio é a indisponibilidade dos serviços.

O desenvolvimento de uma estratégia viável de recuperação constitui um desafio constante, tendo em conta as manutenções e upgrades que os sistemas necessitam. Tendo em consideração a grandiosidade deste desafio para a continuidade de negócio a criação de um conjunto de medidas não deve ser uma iniciativa exclusiva da área de processamento de dados, mas de toda a organização para proteger os interesses da empresa.

No processo de seleccionar uma estratégia de recuperação de desastre, é importante ser efectuada uma check list, de forma a identificar, clarificar processos e responsabilidades:

Check List de Tarefas

Equipa de planeamento	**Estado**
Identificar os membros da equipa para a tomada de decisões e com autoridade para reunir informações a empresa.	
Definir responsabilidades.	
Criação de gráfico organizacional que defina quem é responsável para cada aspecto do planeamento de recuperação de desastres.	
Avaliar os processos de negócios	
Avaliar e classificar (por ordem de importância) todos os processos de negócio.	
Definir quais são os processos de negócios, tecnologia, sistemas e aplicações que devem ser restaurados para que a empresa possa continuar operacional.	
Determinar o nível de protecção contra desastres que se deseja alcançar.	
Determinar que Processos de TI serão incorporados no DRP	
Avaliar os backups existentes e os processos de recuperação.	
Integrar os processos existentes para o DRP.	
Actualizar os processos existentes.	
Implementar e Testar o DRP	
Documentar todas as responsabilidades das pessoas que têm papéis no DRP.	
Implantação de qualquer hardware ou software adicional necessário.	
Teste ao DRP, caminhando através do processo de recuperação de desastres.	
Com base no feedback do walk-through, modificar o DRP para reflectir o processo real.	

Obter a aprovação final do gestor.	
Distribuir os documentos do DRP final para todas as partes envolvidas.	
Manter e armazenar de forma segura offsite cópias impressas de toda a documentação DRP.	
Manter o processo de DRP em curso	
Agendar reuniões regulares da equipa de DRP, para que os diferentes departamentos possam interagir e contribuir para manter o curso do DRP relevante e up-to-date	
Realizar testes regulares ao DRP.	
Agendar actualizações regulares para o DRP para que possam contemplar as mudanças nos processos de negócios ou infra-estrutura de tecnologia.	
Cronograma de avaliações regulares de tecnologia e fluxo de trabalho e actualizar o DRP em conformidade.	
Atribuir a responsabilidade por todas as actualizações do DRP e dos programas de manutenção a pessoas-chave, além de designar uma pessoa central ou pessoas que vai ser responsável pelo cruzamento de quaisquer alterações.	

4. Referências

- Disaster Recovery - Um Paradigma na Gestão da Continuidade - FCA de António Serrano e Nuno Jardim
- http://www-03.ibm.com/systems/itsolutions/disaster-recovery/?lnk=mhso
- http://en.wikipedia.org/wiki/Disaster_recovery
- http://en.wikipedia.org/wiki/Business_Continuity
- http://pt.wikipedia.org/wiki/Recupera%C3%A7%C3%A3o_de_desastres
- http://www.esecuritytogo.com/ccpage.aspx?pageid=6&name=Planning&lid=10&lgid=1
- http://www.dcag.com/webdocs/BC_DR_Job_Descripts.htm

5. Anexos

Anexo 1 – Casos de uso – Sistemas

Anexo 2 – Detecção de desastre e activação do plano

Anexo 3 – Sequências lógicas após declaração de desastre

Anexo 4 – Inventário de Servidores

Anexo 5 – Inventário Hardware de Comunicações

Anexo 6 – Inventário de Aplicações

Anexo 7 – Lista de Contractos

Anexo 8 – Inventário de Licenças