

# DISASTER RECOVERY PLAN

Eduardo Mayer Fagundes  
*e-mail:* eduardo@efagundes.com

## 1. Introdução

O principal objetivo de um plano de continuidade de negócios (BCP – *Business Continuity Plan*) é garantir a operação da empresa com o mínimo impacto aos clientes em situações de contingência. No atentado de 11 de setembro de 2001 as Torres Gêmeas do World Trade Center de Nova Iorque, as empresas que tinham BCPs bem estruturados reiniciaram suas operações poucas horas depois do atentado terrorista.

Algumas empresas subestimam os riscos de um desastre e não investem em BCPs. Os planos de continuidade de negócios podem ser classificados em dois tipos: os Planos de Continuidade das áreas de negócios e os Planos de Recuperação de Desastres (DRP – *Disaster Recovery Plan*) do Centro de Processamento de Dados.

Em muitos casos as áreas de negócios das empresas dependem fortemente do processamento de dados para suas atividades e uma paralisação do processamento pára o negócio da empresa. Um exemplo foi a paralisação do serviço de e-mail do provedor de Internet Terra por dois dias devido a um problema no subsistema de armazenamento de dados, em abril de 2003. O site Terra teve que abonar dois dias da mensalidade dos seus 800 mil assinantes com um prejuízo de mais de R\$400 mil.

Por essa razão as empresas investem em planos de recuperação de desastre (DRP) e não em planos de continuidade em suas áreas de negócios. Talvez, as exceções sejam as instituições financeiras que são mais sensíveis às paralisações de negócios motivadas por greves e blecautes de energia.

Esse estudo focará no plano de recuperação de desastre dos centros de processamento de dados – DRP.

## 2. Objetivos do DRP

O objetivo preliminar de um plano de recuperação de desastre (DRP) é permitir que uma organização sobreviva a um desastre e que possa restabelecer as operações dos negócios. A fim de sobreviver as empresas devem assegurar que as operações críticas possam recomeçar o processamento normal dentro de um espaço de tempo razoável. Para atingir esses objetivos o DRP deve atender os seguintes requisitos:

- Prover um ambiente seguro e pessoas preparadas para um desastre;
- Reduzir as perdas financeiras em casos de desastres;

- Identificar linhas de negócios críticas que requeiram suporte em situações de desastres;
- Identificar as fraquezas e executar um programa da prevenção de desastre;
- Minimizar a duração de uma paralisação das operações de negócio;
- Facilitar a coordenação eficaz de tarefas da recuperação; e,
- Reduzir a complexidade do esforço de recuperação.

### **3. Etapas de um DRP**

O desenvolvimento de um DRP envolve a criação de uma “planta de recuperação” para restaurar os recursos computacionais com as funções vitais de processamento de dados para atender as necessidades dos negócios da empresa. O plano deve procurar restabelecer o ambiente de processamento no menor tempo possível a fim de evitar um efeito catastrófico nos negócios. O desenvolvimento de uma estratégia viável de recuperação não deve ser uma iniciativa exclusiva da área de processamento de dados, mas de toda a organização para proteger os interesses da empresa.

Para atender esse objetivo deve se adotar uma metodologia que enfatize os seguintes pontos chaves:

- Fornecer a gerência uma compreensão detalhada do esforço total requerido para tornar e manter uma planta de recuperação eficaz;
- Obter o compromisso da gerência apropriada para suportar e participar no esforço de recuperação;
- Definir as exigências de recuperação na perspectiva do negócio;
- Documentar o impacto de uma perda prolongada às operações e ao negócio;
- Selecionar as equipes do DRP para testes, atualizar e assegurar uma execução eficaz do plano;
- Desenvolver uma “planta de recuperação” que seja compreensível, fácil de usar e manter;
- Definir como as premissas do DRP devem ser integradas aos processos de negócio para uma recuperação no tempo necessário para não haver ruptura nos processos de negócios

Para se atingir um planejamento eficaz é necessário que o pessoal sênior de sistemas de informação e das áreas de negócios estejam envolvidos durante todo o projeto para o benefício da organização.

O planejamento do DRP deve prever as seguintes etapas:

- Fase 1 – Pré-planejamento das atividades
- Fase 2 – Avaliação da vulnerabilidade e definição das exigências do projeto
- Fase 3 – Avaliação de impacto no negócio
- Fase 4 – Definição detalhada das exigências
- Fase 5 – Desenvolvimento do plano
- Fase 6 – Plano de teste/simulação

- Fase 7 – Programa de manutenção
- Fase 8 – Testes iniciais e implementação

1) *Fase 1 – Pré-planejamento das atividades*

Essa fase determina as necessidades iniciais do projeto com base em informações sobre os requerimentos de processamento de dados para as funções críticas da empresa. Isso permite a equipe refinar o escopo de trabalho e identificar os aspectos críticos para o sucesso do projeto.

Durante esta fase o comitê executivo do projeto (*Steering Committee*) deve ser estabelecido. O comitê tem a responsabilidade total para fornecer o sentido e a orientação à equipe do projeto. O comitê deve também tomar todas as decisões relacionadas ao esforço de planejamento do DRP. O gerente de projeto deve trabalhar com o comitê para finalizar o planejamento detalhado e desenvolver entrevistas para avaliar a segurança e elaborar a análise de impacto no negócio.

Outros dois aspectos chaves desta fase são: o desenvolvimento de uma política para suportar os programas da recuperação; e um programa para educar a gerência e as pessoas-chave do projeto nas atividades que lhes serão atribuídas.

2) *Fase 2 – Avaliação da vulnerabilidade e definição das exigências do projeto*

Como diz o ditado é melhor evitar que remediar. Essa fase analisa as vulnerabilidades do ambiente de processamento e avalia as possibilidades de ocorrência de um desastre. Essa análise deve conduzir medidas para reduzir a probabilidade de desastre.

Esta fase incluirá as seguintes tarefas chaves:

- Uma avaliação completa da segurança do ambiente de processamento de dados e do ambiente das comunicações, incluindo:
  - Pessoal;
  - Segurança física;
  - Procedimentos operacionais;
  - Planejamento de apoio e de contingência;
  - Desenvolvimento e manutenção dos sistemas;
  - Segurança das bases de dados;
  - Segurança de comunicações dos dados e voz;
  - Sistemas e segurança do software de controle do acesso;
  - Apólices de seguro;
  - Planejamento e administração da segurança;
  - Controles da aplicação;
  - Computadores pessoais.
- A avaliação da segurança permitirá a equipe de projeto melhorar os procedimentos de emergência existentes e medidas de prevenção de desastres.

- Recomendações de atividades sobre a segurança devem ser encaminhadas ao comitê executivo de modo que as ações corretivas possam ser iniciadas em um momento oportuno.
- Definição do esforço do planejamento.
- Análise, recomendação e compra de um software para a manutenção e controle permanente do DRP.
- Desenvolvimento da estrutura da “planta de recuperação”.
- Montagem da equipe do projeto.

3) *Fase 3 – Avaliação de Impacto no Negócio*

Nessa fase é realizada uma avaliação de impacto nos negócios de todas as unidades da empresa para identificar os sistemas, processos e funções críticas. Essa análise de impacto econômico deve avaliar a negação de acesso aos serviços de sistemas e outros serviços e facilidades. Deve-se definir também qual o máximo tempo de sobrevivência do negócio sem acesso aos sistemas.

O relatório de avaliação de impacto deve ser apresentado ao comitê executivo. Esse relatório identifica as funções críticas dos serviços e os tempos que devem ser recuperados os sistemas em caso de desastre. As informações são usadas como base para definir os recursos necessários para suportar os serviços críticos.

4) *Fase 4 – Definição detalhada das exigências*

Durante essa fase o perfil das exigências do plano de recuperação é desenvolvido usando como base o relatório de impacto no negócio. Devem ser desenvolvidas estratégias alternativas de recuperação com o auxílio de uma ferramenta para estruturar as informações, como a técnica da matriz de alternativas. O planejamento deve contemplar:

- Hardware (*mainframe*, servidores, comunicação de dados e voz, computadores pessoais, impressoras, etc.)
- Software (pacotes, desenvolvimentos *in-house* e desenvolvimento externo)
- Documentação (processamento de dados, sistemas e usuários)
- Provedores de serviços externos (telecomunicações, telefonia, *web hosting*, etc.)
- Facilidades (energia, escritórios, equipamentos de escritórios, etc.)
- Pessoal.

As estratégias de recuperação devem completar planos de curto, médio e longo prazo.

5) *Fase 5 – Desenvolvimento do Plano*

Nesta fase, os componentes das plantas de recuperação são definidos e as plantas são documentadas. Esta fase inclui também a execução das mudanças nos procedimentos dos usuários e a implementação de processos

para suportar as estratégias selecionadas para a recuperação e as alternativas identificadas.

Devem ser formalizados os acordos contratuais com os fornecedores de hardware, software e serviços para suportar o plano de recuperação. As equipes de apoio ao plano de recuperação devem ser formadas e definidas suas responsabilidades no plano. Os padrões de recuperação devem ser consolidados nessa fase.

6) *Fase 6 – Plano de Teste/Simulação*

O programa de teste/simulação do DRP deve ser desenvolvido nessa fase. O objetivo dos testes/simulações é validar o plano de recuperação e fazer os ajustes necessários. Lembrando que os ambientes de negócios e processamento de dados são dinâmicos, os planos de recuperação devem ser constantemente revistos, atualizados e testados.

7) *Fase 7 – Programa de Manutenção*

A manutenção das plantas é fator crítico de sucesso de uma recuperação real. As plantas de recuperação devem refletir as mudanças nos ambientes reais. É crítico que os processos existentes sejam revisados para fazer a manutenção da planta de recuperação do cliente através do processo de gerência de mudanças. Nas áreas onde a gerência de mudanças não existe, esse procedimento deve ser implementado. Muitos produtos de software de recuperação possuem a facilidade de gerência de mudanças.

8) *Fase 8 – Testes Iniciais e Implementação*

Uma vez os planos desenvolvidos, inicia-se a fase de implementação e testes. Essa fase deve ser repetida no mínimo duas vezes por ano ou quando ocorrer uma mudança significativa no ambiente de processamento de dados ou de negócios.

As seguintes atividades devem ser realizadas:

- Definição do escopo do teste;
- Identificação das equipes de teste;
- Estruturação do teste;
- Condução do teste;
- Análise dos resultados do teste; e,
- Modificação dos planos de recuperação, se necessário.

O escopo do teste depende da estratégia de recuperação selecionada, o que reflete os requerimentos de negócio da empresa. O plano de recuperação desenvolvido deve ser escrito de forma que seja compreensível e fiel a realidade da organização.

#### 4. Estrutura Organizacional do DRP

A organização da equipe do projeto de recuperação deve ser flexível para atender os requisitos desse tipo de atividade. A implementação, manutenção e execução de um plano de recuperação exige dedicação do pessoal e trabalho sob pressão. Um fator crítico de sucesso é a criação de uma organização dedicada para essa finalidade.

Os planos de recuperação devem ser tratados como documentos vivos. As informações estão em constante processo de mudança e a cada dia tornam-se mais integradas e complexas. Os planos de recuperação devem acompanhar essas mudanças. Os planos de testes/simulações devem assegurar a capacidade de recuperação do ambiente considerando as constantes mudanças dos processos. A organização deve assegurar que a equipe do DRP esteja sempre atualizada sobre as mudanças nos negócios.

A seguir é apresentado um modelo de organização para conduzir o plano de recuperação:

##### 1) *Comitê Executivo*

O comitê executivo deve incluir representantes das áreas chaves da organização:

- Sistemas de Informação;
- Infra-estrutura de tecnologia da informação;
- Desenvolvimento de Sistemas;
- Redes de Comunicações de Dados;
- Comunicação de Voz;
- Unidades de Negócios.

##### 2) *Equipe do Projeto*

A composição da equipe do projeto varia de acordo com o ambiente tecnológico e de negócios onde os planos foram desenvolvidos. É importante notar que os gerentes dos ambientes tecnológicos e das unidades de negócios são responsáveis pela manutenção e teste de seus respectivos planos. Entretanto, o pessoal responsável pelo planejamento da estratégia de recuperação deve ser o coordenador das atividades de teste, revisão dos planos e manutenção do plano principal.

A Auditoria Interna deve ser convidada a fazer parte de todas as equipes. Os gerentes representados nas diversas equipes devem recomendar pessoas seniores para representá-los ou eles próprios participarem das equipes contribuindo com sua experiência no desenvolvimento dos planos de recuperação.

##### (1) Equipe Principal

- Gerente do Projeto;
- Especialista em operação de computadores e redes de dados;
- Especialista em suporte de sistemas;

- Especialista em suporte de voz, redes e telecomunicações.
- (2) Equipe Técnica
- Analista de redes;
  - Analista de infra-estrutura física;
  - Analista de banco de dados;
  - Analista de segurança;
  - Analista de operação;
  - Analista de suporte de rede;
- (3) Equipe de Negócios
- Membros das diversas áreas de negócios que fazem parte do plano de recuperação.

## **5. Recursos Necessários para o DRP**

As empresas devem evitar implementar planos de recuperação sem uma equipe e recursos dedicados para essa finalidade sob o risco de falharem após altos investimentos. Uma das razões do fracasso de alguns planos é a falta de comprometimento das equipes na manutenção e testes do plano de forma contínua, o que resulta na perda da compatibilidade do plano de recuperação com a realidade da empresa.

Para garantir o sucesso do plano de recuperação deve se investir em três categorias:

1) *Pessoal*

Os gerentes devem alocar profissionais experientes e competentes para participar das equipes de recuperação.

2) *Investimento inicial*

A empresa deve investir na compra de equipamentos redundantes nas áreas de voz e comunicação de dados, processamento de dados (incluindo servidores e subsistemas de armazenamento de dados), equipamentos redundantes de geração de energia (UPS, geradores a diesel, etc.) e equipamentos de apoio (fax, PCs, scanner, copiadoras, etc.).

3) *Despesas recorrentes.*

As despesas recorrentes incluem o aluguel de espaço para instalar os computadores e outros equipamentos, contratos de serviços e manutenção. Uma alternativa eficaz e que exige menos investimentos é a contratação de uma empresa especializada em DRP, onde é possível contratar todos os serviços de recuperação, desde o planejamento, manutenção e equipamentos.

## DADOS DO AUTOR



Eduardo Mayer Fagundes estuda os impactos da tecnologia da informação e modelos de gestão de TI nas organizações, focando em tecnologia, técnicas e gestão de pessoas. Seu livro "Como Ingressar nos Negócios Digitais" foi publicado em parceria com o SEBRAE Nacional com o objetivo de ampliar a visão empresarial no comércio eletrônico.

Eduardo é graduado em engenharia elétrica, possui especialização em telecomunicações e é mestre em ciência da computação. Foi professor por mais de 20 anos em conceituadas instituições de ensino. Palestrante em vários seminários e congressos. Foi gerente de infra-estrutura e sistemas da Ford Brasil, responsável pelo desenho da infra-estrutura de TI da moderna fábrica da montadora em Camaçari-Bahia.

Atualmente é diretor de TI (CIO) das empresas do grupo americano AES no Brasil. A AES atua nos mercados de geração e distribuição de energia e na área de telecomunicações. A AES Eletropaulo, maior distribuidora de energia da América do Sul, é uma das empresas do grupo.

Escreve artigos no site [www.efagundes.com](http://www.efagundes.com).