Gestão da Continuidade dos Negócios

Alexandre Guindani
Pós-graduado em Segurança da Informação pela UPIS.
Profissional certificado pelo DRII -
Disaster Recovery Institute International.

Introdução

"*If anything can go wrong, it will* "[1].

A continuidade dos negócios, que num primeiro momento parece algo lógico e necessário a qualquer empresa, é domínio relativamente novo dentro do ainda jovem setor da gestão de riscos corporativos. Todos os dias, diversos sistemas sofrem interrupções, pessoas são vítimas de vírus, dados são obtidos ilegalmente e muitas empresas ficam de uma hora para outra sem poder operar normalmente devido à falta de energia elétrica.

Atualmente, a maioria das instituições tem suas atividades apoiadas por um conjunto de tecnologias que, se por um lado são responsáveis pelos expressivos níveis de eficiência, eficácia e produtividade, por outro determinam a existência de forte dependência das informações transacionadas e armazenadas em seus ambientes computacionais para a manutenção e geração de novos negócios. Nesse contexto, todos os esforços possíveis, necessários à manutenção da disponibilidade das operações precisam ser despendidos.

As empresas devem, então, dispor de planejamento e de mecanismos adequados à pronta recuperação de suas operações, no menor tempo possível, como forma de precaver-se dos efeitos desastrosos de eventos que causem interrupções significativas em parte, ou mesmo, em todos os seus processos de negócio.

Tal constatação impõe às empresas a criação e manutenção de uma estratégia de continuidade dos negócios, pronta a operar em caso de interrupção total ou parcial de suas atividades, sendo então fator fundamental para o sucesso de qualquer iniciativa de preservação ou recomposição da capacidade de realizar negócios.

Buscamos neste texto oferecer referencial teórico sobre contingência e continuidade, agentes motivadores e demais subsídios para a compreensão das práticas adotadas mundialmente para a elaboração de um programa de Continuidade dos Negócios (PCN).

1 Histórico

Em 1944, foi construído o primeiro computador eletromecânico, na Universidade de Harvard, pela equipe do professor H. Aiken e com a ajuda financeira da IBM, que investiu US$ 500.000,00 no projeto, ao qual foi dado o nome de MARK I. Tal equipamento tinha cerca de 15 metros de comprimento e 2,5 metros de altura; era envolvido por uma caixa de vidro e de aço inoxidável brilhante, composto por 760.000 peças, 800 km de fios e 420 interruptores para controle. O MARK I, apesar do tamanho, demorava de 3 a 5 segundos para realizar uma operação de multiplicação, o que atualmente uma calculadora de bolso realiza em fração de segundo.

[1] Variação da Lei de Murphy - Se alguma coisa puder dar errado, ela vai dar errado.

Outro fato relevante para a evolução da continuidade nas empresas foi o famoso *Bug* do Milênio. Tal problema, que teve origem na década de 70 quando, para minimizar o custo da memória, os fabricantes de computadores, programas e microprocessadores decidiram usar o campo para a representação do ano com apenas dois dígitos. Essa prática tornou-se comum até o final de 1997. Dessa forma, muitos computadores e utensílios interpretam 1998 como 98, 1999 como 99 e 2000 como 00. Assim, no dia 01.01.2000, às 00h01min, muitos equipamentos poderiam ter como data o ano 1900 ou simplesmente "00", desencadeando uma série de operações ilógicas e equivocadas.

O *Bug* do Milênio foi considerado uma ameaça sem precedentes na história, com data e hora marcadas para acontecer. No ano de 1999 os especialistas previam prejuízos que deveriam afetar tudo e todos, inclusive aqueles que não tivessem qualquer relacionamento com a informática. As estimativas de valor para as indenizações judiciais deveriam superar a marca de 1 trilhão de dólares. Os bancos realizaram investimentos gigantescos para a adequação de seus sistemas, por exemplo, o Citibank que investiu quantia próxima a U$ 600 milhões para realizar adequação de seus inúmeros sistemas ao redor do mundo. Os Estados Unidos, maior usuário mundial de tecnologia, preocuparam-se com o volume de processos que poderiam ser movidos por empresas afetadas pelo *bug* contra as empresas de tecnologia e, no caso dos bancos, por seus clientes. As leis em que a maioria dos processos seria baseada são a *Y2K Federal Act*, votada em julho de 1999, e a *Year 2000 Information Readiness & Disclosure Act (IRDA)*, votada em outubro de 1998. O *Y2K Federal Act* estabeleceu os direitos dos clientes de tecnologia para entrar com processos baseados em erros referentes ao *Bug* do Milênio, assim como deu à companhia um prazo para resolver o problema. O IRDA exigiu que as empresas, ao revelar os riscos potenciais do *Bug* do Milênio em seus processos de negócios, deveriam ter documentado um plano de contingência para eles. Tais planos foram considerados críticos para a compatibilidade com o ano 2000, promovendo uma evolução das metodologias de desenvolvimento de planos de contingência. Nesse evento, as empresas não mediram esforços para a criação dos planos, avaliação dos riscos e também em estratégias para minimizar os possíveis impactos.

Mas foi o desastre de 11 de setembro de 2001 que mudou, para sempre, o conceito de continuidade de negócios. O acontecimento marcou a humanidade e quebrou paradigmas no que tange à segurança de forma geral, levando as empresas a uma reflexão sobre o impacto do inesperado sobre seus negócios. O ataque terrorista ao *World Trade Center* trouxe à tona uma série de variáveis no que diz respeito à vulnerabilidade das empresas a eventos que podem ameaçar suas operações. Observamos que a realização de uma avaliação de risco, mesmo bem executada, não é garantia de segurança e mesmo um conjunto de planos bem estruturados não pode impedir a ocorrência de catástrofes, mas, no máximo, reduzir seus impactos.

Como exemplo, citamos o acontecido com a empresa Cantor Fitzgerald, que no evento perdeu 700 funcionários, perdeu inteligência, talento e experiência, que são variáveis difíceis de substituir e de repor. Outras empresas possuíam escritório em um dos prédios e armazenavam suas cópias de segurança no outro; perderam sua memória e seus registros não sendo mais possível recriá-los; restou unicamente o caminho da extinção. Mas também existiam empresas com instalações e cópia de registros em locais remotos. Coincidência ou cautela?

2 O que é GCN?

A Gestão da Continuidade dos Negócios (GCN) é algo relativamente novo, resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, *softwares*, *hardware*, infra-estrutura etc.) por ele utilizados.

Esse conceito deve ser encarado como algo em constante mudança, ao invés de uma situação estática. Para que isso aconteça são necessárias mudanças na forma de tratar o atendimento às especificações de continuidade e preocupação com as medidas de resposta, em situações de crise, quando o ambiente corporativo sofre inúmeras ameaças com impacto efetivo nos negócios.

No Brasil, atualmente, as atividades referentes à continuidade dos negócios estão basicamente restritas às instituições em que os principais processos de negócios possuem enorme dependência de TI e àquelas cujas matrizes situam-se no exterior, onde a cultura da continuidade dos negócios é mais desenvolvida. Mas o empresariado brasileiro ainda não percebeu o enorme potencial de economia que se oculta por trás da metodologia e das melhores práticas utilizadas no desenvolvimento da GCN.

Desde o início da elaboração do BIA (*Business Impact Analysis*), quando os processos de negócios da empresa são analisados e ordenados em função do custo de uma indisponibilidade até a análise de criticidade, em que os processos são avaliados de acordo com os impactos que a empresa venha a sofrer com a sua interrupção, as informações obtidas são importantes indicadores para os executivos e responsáveis pela sua condução. As avaliações garantem a redução dos possíveis impactos, minimizando-os a níveis toleráveis para a empresa.

Atualmente, é necessário que as empresas convivam com riscos e administrem crises, normalmente provocadas pelo homem, cujo potencial, em termos de alcance e magnitude, se iguala aos desastres naturais.

De modo geral, as crises ocorrem como conseqüência das disfunções das culturas organizacionais, das crenças e valores de seus tomadores de decisões e das práticas e abordagens dadas aos processos de comunicação tanto internos quanto externos. Em estudos recentes verificou-se que a grande maioria dos desastres e catástrofes é gerada pela própria organização.

Como índice relativo e individual que pode quantificar e qualificar a probabilidade de ocorrência de eventos, o risco é outro fato presente no dia-a-dia das empresas. De forma geral, esses eventos podem abranger qualquer coisa, desde a falta de energia elétrica, contaminação da rede corporativa por um novo vírus e até mesmo a interrupção no fornecimento de água.

Segundo pesquisa realizada pelo *Gartner Group* com empresas dos Estados Unidos, de todos os eventos que provocaram interrupção nos processos de negócio, apenas 8% foram causados por desastres naturais. Cerca de 77% das interrupções são devidas ao conjunto de falha humana (10%), falha de *software* (27%), falha de *hardware* (23%) e falha na rede de comunicações (17%).

Após o trágico evento de 11 de setembro de 2001, as corporações foram surpreendidas por algumas variáveis que até então eram propositalmente desconsideradas. Antes desse fato, não se poderia imaginar um avião de passageiros sendo utilizado como arma contra um prédio civil numa das maiores cidades do mundo e em solo americano.

Avaliar os riscos não traz em si a garantia de proteção e sim oferece uma possibilidade de se analisar vulnerabilidades e de tomar medidas que permitam reduzir as probabilidades de ocorrência e minimizar seus possíveis impactos, fazendo com que a empresa continue a trabalhar, mesmo com pequena redução no desempenho de seus processos de negócio.

Tal abordagem não condiz com o conceito popular de administração de crises, que se refere a como as organizações se comportam e respondem a incidentes catastróficos. Essa visão relega, ou mesmo ignora o leque de ações preventivas que uma organização pode adotar. Administração de crises, então, está, antes de tudo, relacionada com os aspectos preventivos, e não somente com as ações e estratégias de mitigação, remediação e controle.

Existe grande diferença entre administração de crises e gerenciamento de risco. Gerenciamento de risco envolve a avaliação do custo de um risco depois de multiplicá-lo pela probabilidade de ocorrência desse risco; a administração de crises envolve não só os incidentes mais prováveis de ocorrência, mas também os incidentes que têm o potencial de maior impacto no ambiente operacional da organização.

Na administração operacional moderna, praticamente todas as crises têm potencial para afetar os participantes de uma organização, independentemente de sua natureza. As organizações bem preparadas reconhecem que qualquer crise tem o potencial de afetar não só a própria organização e seus produtos, mas também ampla gama de participantes potenciais: consumidores, competidores, fornecedores e membros da comunidade em geral. Assim sendo, as organizações são responsáveis por muito mais que apenas seus interesses imediatos. Elas têm responsabilidades sociais para com a comunidade e o meio ambiente no qual operam.

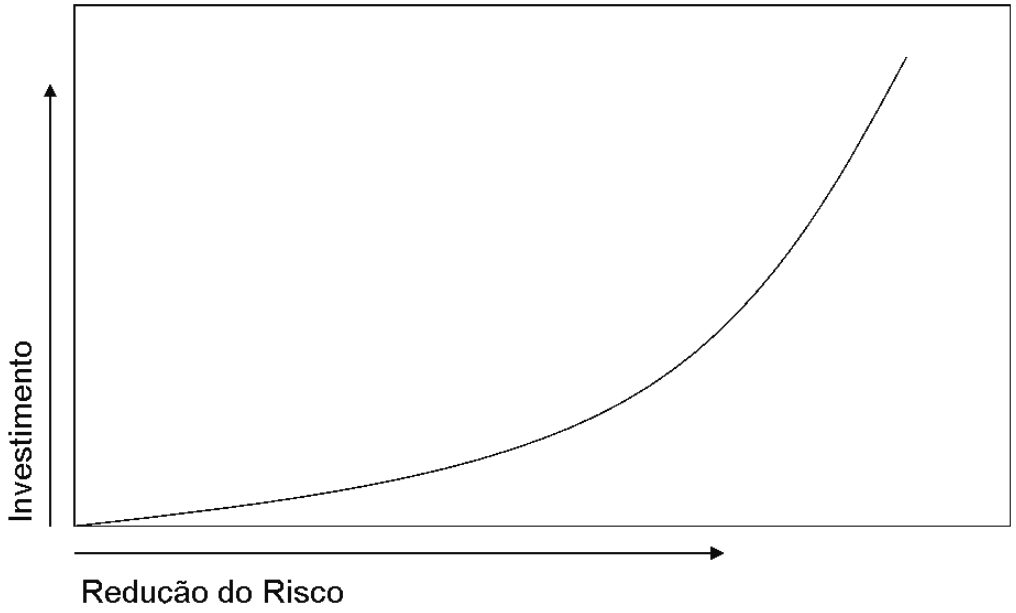
A administração de crises é um esforço contínuo, abrangente e integrado que as organizações efetivamente realizam como tentativa de, antes de tudo, entender e preveni-las. Efetivamente, administrar aquela que vier a ocorrer, considerando o interesse de seus participantes em cada etapa de suas atividades de treinamento e planejamento para crises.

De maneira simplista, a empresa envolve-se na prevenção, mitigação e recuperação de incidentes que podem atingir negativamente os ativos tangíveis e/ou intangíveis da organização.

A administração de crises começa e termina com o planejamento. As atividades relacionadas à administração de crises são abrangentes e integradoras, iniciando-se muito antes da ocorrência de um processo de interrupções. Dentre essas atividades encontram-se o desenvolvimento de cenários que possam macular a reputação da organização, sua marca, seu bem-estar financeiro, sua participação no mercado, e possíveis efeitos de uma ocorrência aos participantes da organização. Devem ocorrer, ainda, simulações, desenvolvimento de tipologia de crises, planejamento efetivo para as distintas fases de uma crise etc.

É possível estar preparado para enfrentar todos os riscos existentes? A resposta à pergunta está diretamente relacionada ao tamanho do investimento que a empresa esteja disposta a realizar. Na ilustração 2, podemos verificar que o investimento é diretamente proporcional ao quão protegidos desejamos estar contra os possíveis riscos.

Ilustração 1



Conclui-se que, para estarmos 100% protegidos e/ou seguros, o investimento seria tão alto que se tornaria inviável. Daí, a necessidade de se realizar uma avaliação dos riscos, para definir os possíveis e prováveis cenários que fazem parte do ambiente corporativo e que podem afetar a organização, seja com interrupções não previstas, quanto com desastres. A avaliação permitirá direcionar os investimentos, buscando o desenvolvimento de uma estrutura de alta disponibilidade para os processos de negócio críticos. As interrupções que por desventura ocorrerem nesses processos, sejam elas curtas ou prolongadas, sempre afetam a organização, causando impactos que muitas vezes são irreversíveis.

Segundo o DRII – *Disaster Recovery Institute International*, de cada cinco empresas que possuem interrupção nas suas operações, por uma semana, duas fecham as portas em menos de três anos. O dado justifica-se porque no mercado mundial um dos maiores desafios dos executivos é garantir a continuidade de seus negócios, independentemente do tipo de evento que possa ocorrer.

Existem vários tipos de eventos causadores de falhas e interrupções, para os quais as empresas geralmente não estão preparadas. Muitas vezes, a ocorrência de um evento pode causar impactos desastrosos. No Brasil, eventos como incêndios, enchentes, roubos, atos de vandalismo, sabotagens, blecautes, invasão de sistemas, interrupção de comunicação de dados e voz podem ser considerados como os principais tipos.

É sabido que toda instituição tem dependência das informações armazenadas dentro de seu ambiente computacional. A possibilidade de ocorrer perda de dados e os conseqüentes prejuízos tangíveis (faturamento, clientes) e intangíveis (imagem, aceitação no mercado) em algumas instituições é da ordem de milhões de reais, podendo causar até a extinção total de uma organização em curto espaço de tempo, em caso de desastre. Num mercado tão competitivo como o de hoje, ter acesso direto à informação pode representar a diferença entre lucro e prejuízo, assegurando a viabilidade de uma companhia.

Normalmente, é necessário ter acesso às informações na base 24 x 7, ou seja, ininterruptamente. Os fornecedores e os distribuidores, os empregados e clientes devem ter acesso às informações sempre que necessitem. Possibilitar esse nível de disponibilidade da informação é tarefa árdua e deve ser provido mesmo em circunstâncias adversas e imprevisíveis ou até mesmo em desastres catastróficos.

É durante esses acontecimentos imprevisíveis que os negócios podem sofrer prejuízos, arriscando-se muitas vezes as vantagens competitivas da empresa. Examinar as medidas apropriadas para impedir a indisponibilidade da informação e mitigar os riscos, envolve perseguir uma estratégia da continuidade do negócio, o que era chamado tradicionalmente como recuperação de desastres.

A garantia de continuidade permite a redução de perdas financeiras, uma vez que a empresa não deixa de atender ao cliente. Consequentemente, existem outras vantagens financeiras, decorrentes de possíveis reflexos acarretados pela parada da empresa (multas, sanções legais, perda de mercado) que não se concretizam devido a GCN.

Em pesquisa realizada no ano de 2004 pela revista *Continuity Insights* e KPMG, com a participação de 410 empresas, foram apontadas as sete maiores causas de interrupção. São ocorrências normais e que podem afetar os negócios de grandes corporações:

- 81% das empresas afetadas por falta de energia.
- 65% por desastres naturais.
- 62% por falhas na rede de telecomunicação.
- 61% por falhas de *hardware*.
- 58% por vazamento de informações.
- 57% por erro humano.
- 56% por falha de *software*.

Para 64% das empresas entrevistadas, as paralisações ocorridas nos 12 meses anteriores ao período da pesquisa causaram prejuízo médio da ordem de U$ 100,000 e, para 24% delas, de até U$ 500,000.

Sabe-se que qualquer empresa pode ser vítima de tragédias e estar sujeita aos inúmeros riscos existentes, faz-se então necessário definir o direcionamento que será tomado, visando minimizar os impactos no negócio, caso alguma dessas ameaças venha a se concretizar. Essa avaliação deve considerar que nível de risco estamos dispostos a correr e qual o volume de investimentos necessário para a sua mitigação.

3 Regulamentação e legislação

Existe hoje uma série de leis e regulamentos sobre continuidade dos negócios, principalmente com relação ao mercado financeiro, o setor mais sensível a interrupções e que, historicamente, tem maior nível de controle.

3.1 Norma ISO/IEC 17799

Em dezembro de 2000, a ISO divulgou a norma internacional ISO/IEC 17799, cópia da BS 7799-1 do *British Standard*. A ABNT, responsável por assuntos pertinentes à segurança da informação, adotou essa norma, tendo sido publicada, em 2001, visando estabelecer referencial para as organizações desenvolverem, implementarem e avaliarem a gestão da segurança da informação. Essa documentação aborda dez tópicos para definir um ambiente seguro. Um dos tópicos faz referência à necessidade do desenvolvimento de ações que garantam a continuidade dos negócios.

3.2 Acordo de Basiléia II

O acordo de Basiléia II trata basicamente da gestão de riscos operacionais em instituições financeiras, as quais, segundo o Comitê de Basiléia, deverão demonstrar práticas eficazes de gerenciar e supervisionar seus riscos operacionais.

Esse mesmo Comitê, no documento *Sound Practices for the Management and Supervision of Operational Risk,* publicado em fevereiro de 2003, em seu princípio nº 7 diz que: "Bancos deverão ter planos de contingência e de continuidade dos negócios para assegurar sua capacidade de operar de maneira contínua e com perdas limitadas na eventualidade de interrupção significativa nas suas operações de negócio".

Um evento extremo pode resultar no impedimento do banco, de cumprir algumas ou todas as obrigações do negócio, particularmente quando a infra-estrutura de telecomunicações ou de tecnologia de informação estiverem danificadas ou inacessíveis. Isso certamente resultará em perdas financeiras significativas para o banco. Paralisações prolongadas de algum sistema que dá suporte às transações financeiras, como por exemplo, o sistema de pagamentos brasileiro, expõe o banco a sanções.

O risco potencial requer que os bancos desenvolvam planos de continuidade do negócio e recuperação de desastre, examinem os diferentes cenários possíveis de vulnerabilidade, proporcionais ao tamanho e à complexidade das operações.

Os bancos devem identificar processos críticos de negócio, incluindo a dependência de fornecedores ou de terceiros, para os quais a solução rápida do problema é essencial. Os bancos devem identificar mecanismos alternativos para recuperar a capacidade produtiva em caso de interrupção. Atenção particular deve ser dada à capacidade de restaurar registros eletrônicos ou físicos que são necessários para a recuperação dos negócios.

Os bancos periodicamente devem revisar seus planos de continuidade, de modo que estejam coerentes com as operações e atuais estratégias do banco. Além do mais, esse plano deve ser testado constantemente, assegurando que o banco seja capaz de executá-lo diante do acontecimento de ocorrência nos processos de negócio.

3.3 Lei Sarbanes-Oxley

O Congresso e o governo dos Estados Unidos editaram em 2002, o Sarbanes-Oxley *Act*, que aumenta as responsabilidades sobre presidentes e diretorias e as exigências dirigidas a auditorias e advogados responsáveis pela fiscalização dos relatórios contábeis das empresas. A medida, que faz referência aos dois membros do Congresso responsáveis por sua elaboração, Paul S. Sarbanes e Michael Oxley, introduz regras severas de governança corporativa para assegurar maior transparência aos resultados das organizações; institui punições contra fraudes empresariais e garante maior independência aos órgãos de auditoria. Válida, até o momento, para as empresas americanas e empresas estrangeiras que operam no mercado americano, a lei responsabiliza os gestores da empresa pela manutenção de controles internos e publicação de seus resultados da empresa. A Seção 404 dessa lei trata da continuidade das operações como uma das formas de reduzir os riscos do negócio. O descumprimento da Sarbanes-Oxley prevê penas de até 20 anos de cadeia e multas de US$ 15 milhões de dólares para os responsáveis.

Conclui-se, então, que o risco é proporcional à existência de vulnerabilidades e ameaças, que uma interrupção, geralmente, não acontece devido a um único risco e, definitivamente, que nada é 100% seguro.

7 Análise de Impacto nos Negócios (BIA)

Estima os impactos financeiros e operacionais resultantes da interrupção e de cenários de desastres que podem afetar a instituição, bem como as técnicas para quantificar e qualificar esses impactos. Define a criticidade dos processos de negócio, suas prioridades de recuperação e interdependências para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos, de acordo com o RTO[1] acordado.

A realização do BIA busca entre outras coisas aumentar a conscientização da corporação com relação aos riscos existentes, dependência dos processos de negócio da estrutura de TI e a confiança dos executivos quanto à continuidade das operações. O BIA também servirá como justificativa para investimentos em prevenção e contenção, estratégias de continuidade e no próprio desenvolvimento do PCN.

O BIA é realizado mediante coleta de informações sobre os processos de negócio sendo que tais questionamentos devem ser feitos aos gerentes de nível intermediário, ou seja, quem realmente conhece o processo. As informações serão coletadas pelo preenchimento de um questionário cujo foco é o negócio e não a tecnologia. Com esse questionário devemos obter as seguintes informações:

- Impactos e exposições financeiras.
- Impactos e exposições operacionais.
- Interdependências entre os processos de negócios.
- Grau de dependência de TI.
- Tempo máximo para retorno à operação.
- Recursos necessários à recuperação do processo de negócio.

Após a análise das respostas, teremos um relatório gerencial detalhado contendo os impactos financeiros e operacionais quantificados, processos prioritários para recuperação, interdependências existentes, recursos mínimos para recuperação e definição do tempo máximo de recuperação.

8 Estratégias de continuidade

Define e orienta a seleção de estratégias operacionais alternativas para a recuperação dos processos e componentes de negócio, dentro dos prazos de recuperação desejados, enquanto os processos corporativos críticos são mantidos em atividade.

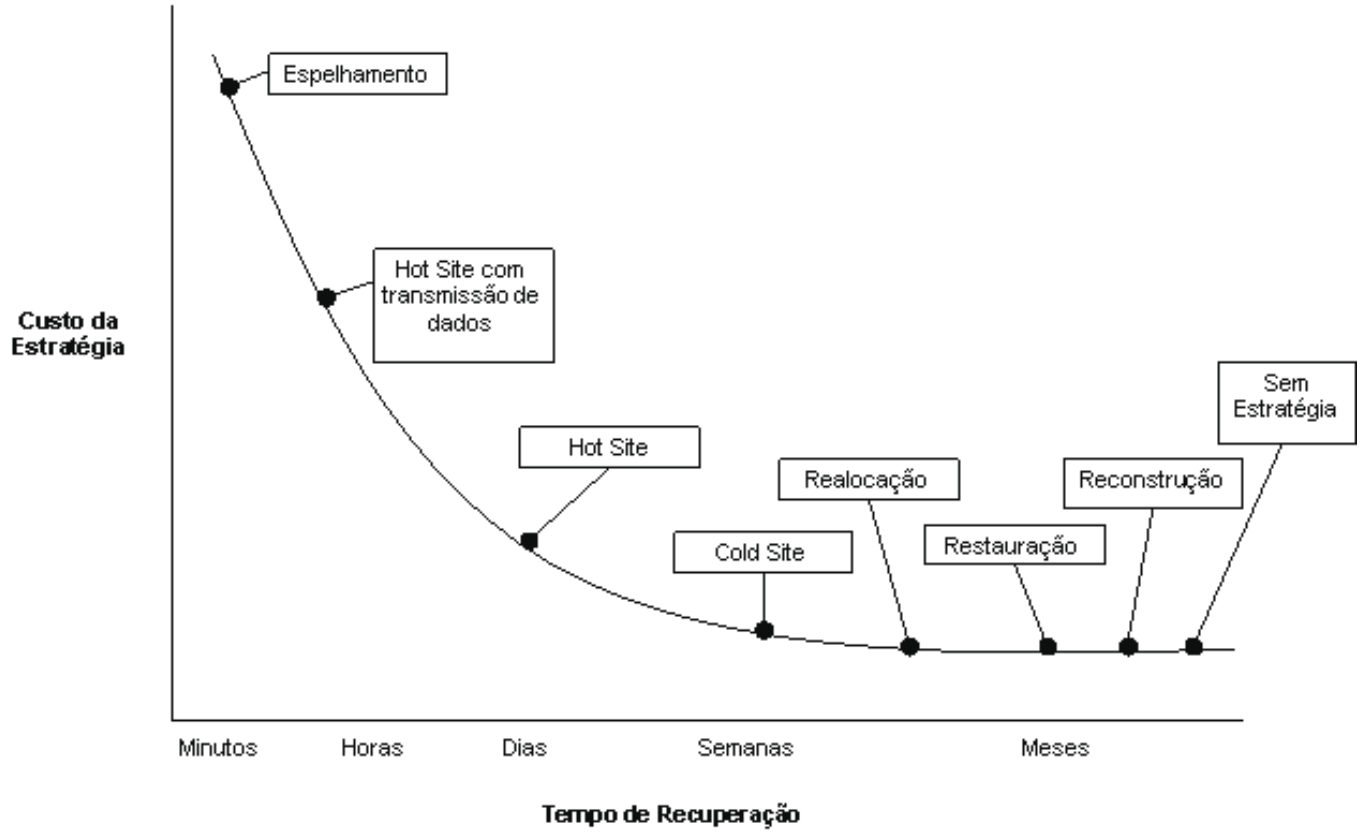
Essa é provavelmente a etapa mais desafiadora do programa, pois vai requerer experiência técnica e conhecimento dos negócios. Visto serem possíveis múltiplas combinações, cada uma com suas vantagens e desvantagens, é praticamente impossível agradar todos os gestores, ou seja, não existindo solução correta nem errada, o responsável pelo PCN deverá pesar as variáveis existentes, juntamente com o nível de risco que a instituição está disposta a correr.

As melhores estratégias são aquelas que têm a melhor relação custo X benefício, as que reduzem os riscos e as exposições e que atendem às necessidades do negócio e não só de TI.

No gráfico abaixo, apresentamos algumas das estratégias de continuidade possíveis, comparadas ao tempo de recuperação. Lembramos que as estratégias podem ser combinadas de acordo com as necessidades do negócio.

[1] *Recovery time objective* vem a ser o tempo pré-definido no qual um processo deverá estar disponível após a decretação do regime de contingência.

Ilustração 4



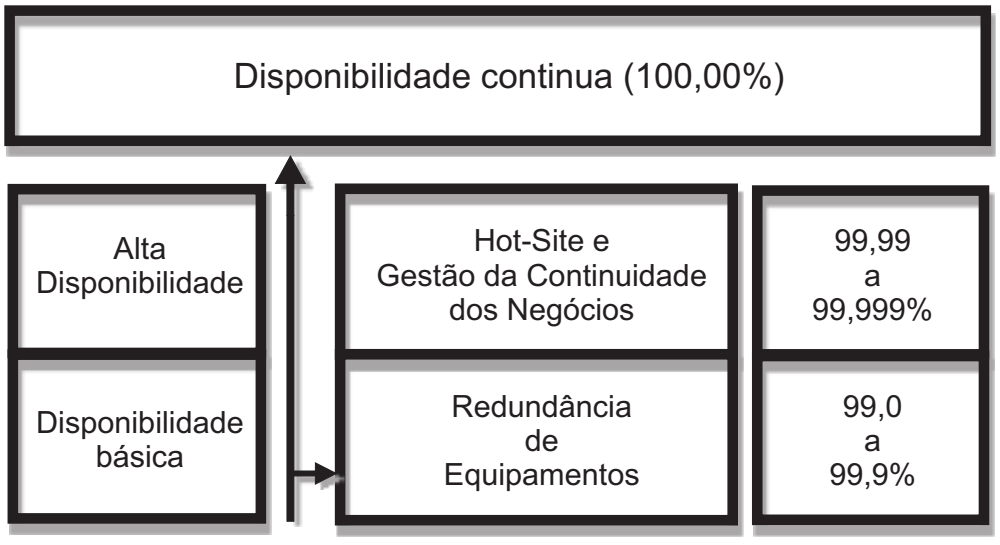
Outro fator que deverá ser considerado é a disponibilidade requerida pelo processo de negócio. Podemos definir disponibilidade como a probabilidade de que o sistema esteja funcionando e pronto para uso em certo instante.

A disponibilidade pode ser enquadrada em três classes, de acordo com a faixa de valores da probabilidade, conforme segue:

- Disponibilidade básica.
- Alta disponibilidade.
- Disponibilidade contínua.

A ilustração 5 mostra as três classes mencionadas.

Ilustração 5



9 Disponibilidade básica

A disponibilidade básica é aquela encontrada em máquinas comuns, sem nenhum mecanismo especial, em *software* ou *hardware*, que vise de alguma forma mascarar as eventuais falhas dessas máquinas. Costuma-se pensar que máquinas nessa classe apresentam disponibilidade de 99% a 99,9%. Isso equivale a dizer que, em um ano de operação, a máquina pode ficar indisponível por período de nove horas a quatro dias. Esses dados são empíricos e os tempos não consideram a possibilidade de paradas planejadas; porém são aceitas como o senso comum na literatura especializada.

10 Alta disponibilidade

Adicionando-se mecanismos especializados de detecção, recuperação e mascaramento de falhas, pode-se aumentar a disponibilidade do sistema, de forma que ele venha a se enquadrar na classe de alta disponibilidade. Nessa classe, as máquinas normalmente apresentam disponibilidade na faixa de 99,99% a 99,999%, podendo ficar indisponíveis por período de pouco mais de cinco minutos até uma hora em um ano de operação. Aqui se encaixam grande parte das aplicações comerciais de alta disponibilidade, como centrais telefônicas.

11 Disponibilidade contínua

Com a "adição de noves" após a vírgula, ao fator de disponibilidade, será obtida uma disponibilidade cada vez mais próxima de 100%, com a diminuição do tempo de inoperância do sistema de forma que ele possa se tornar desprezível ou mesmo inexistente. Chega-se então à disponibilidade contínua, o que significa dizer que todas as paradas planejadas e não planejadas são mascaradas e o sistema está sempre disponível, ou *non-stop*.

Com isso, percebe-se que a alta disponibilidade é toda a base para se obter a disponibilidade contínua e é implementada, geralmente, pela utilização de componentes redundantes entre si. Quanto maior o número de componentes e mais efetiva sua ação, mais elevado o nível da disponibilidade obtida.

No mercado financeiro, o que se busca é implementar mecanismos altamente disponíveis, que garantam níveis excelentes de qualidade operacional.

12 Desenvolvimento e implantação dos planos

Nesse ponto, julgamos pertinente uma inversão na seqüência proposta pelo DRII, devendo ser tratados os assuntos relacionados ao desenvolvimento dos planos, deixando o item, Respostas e Ações Emergenciais, para a próxima etapa. Dando continuidade ao programa, nesse momento serão planejados e elaborados os planos componentes, visando o atendimento às janelas de recuperação dos processos de negócio da instituição. Portanto, não teremos apenas um plano e sim vários planos componentes que, em conjunto, comporão um grande programa corporativo.

Tais planos devem cobrir todo o ciclo de uma interrupção significativa, contendo as ações e procedimentos necessários à recuperação dos processos de negócio, inventário dos recursos críticos, listas de contato dos responsáveis e demais informações vitais.

É sugerido sempre planejar para o pior cenário possível, o que os americanos chamam *worst case scenario* e lembrar que a recuperação somente poderá contar com os recursos e suprimentos que foram armazenados fora do local afetado.

Os planos deverão ter um formato padrão definido pela instituição e deverão conter no mínimo:

- Todos os passos a serem executados pelos colaboradores durante a recuperação de um processo de negócio, de suporte ou recurso crítico.