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.

Já, em 1946, surgiu o ENIAC - *Eletronic Numerical Interpreter and Calculator*, ou seja, Computador e Integrador Numérico Eletrônico, projetado para fins militares, pelo Departamento de Material de Guerra do Exército dos EUA, na Universidade de Pensilvânia. Era o primeiro computador digital eletrônico de grande escala e foi concebido por John W. Mauchly e J. Presper Eckert (um gênio em engenharia, que, aos 8 anos de idade construiu um rádio a cristal e colocou-o num lápis). Só que o ENIAC apresentava um grande problema: por causa do enorme número de válvulas, operando à taxa de 100.000 pulsos por segundo, havia 1,7 bilhões de chances por segundo de que uma válvula falhasse, além da grande tendência ao superaquecimento. Isso porque as válvulas liberavam tanto calor que, mesmo com os ventiladores, a temperatura ambiente subia, às vezes, até 67°C. Então, Eckert aproveitou a idéia utilizada em órgãos eletrônicos, fazendo com que as válvulas funcionassem sob tensão menor que a necessária, reduzindo assim as falhas a uma ou duas por semana.

Em 1949, projetou-se o EDSAC - *Eletronic Delay Storage Automatic Calculator* ou Calculadora Automática com Armazenamento por Retardo Eletrônico. Isso marcou o último grande passo na série de avanços decisivos inspirados pela guerra. Começou então a Era do Computador e, com isso, a preocupação das empresas e dos responsáveis pelos sistemas computacionais, com a segurança e com mecanismos que, de alguma forma, garantissem a continuidade das operações. Naquela época, as memórias dos computadores eram construídas com o recurso a válvulas eletrônicas, lâmpadas de mercúrio e tubos de raios catódicos, dispositivos que só mantinham o seu estado quando excitados pela corrente elétrica. Assim, essas memórias eram voláteis, isto é, quando não eram excitadas pela corrente elétrica perdiam o conteúdo.

Nos primeiros computadores eram utilizados dispositivos eletromagnéticos para efetuar o *backup* do conteúdo da memória. Esse dispositivo, chamado de tambor magnético, era constituído por um cilindro de revolução metálico que rodava em torno de um eixo vertical; o movimento era assegurado por um motor elétrico. Os tambores magnéticos foram utilizados em todos os computadores construídos até meados dos anos 1960.

No início da década de 60, passou-se a utilizar, na construção dos computadores, memórias não voláteis. Já no início dos anos 1970, a concepção de computadores integrava a tecnologia de circuito monolítico na construção das memórias. A utilização dessa tecnologia provocou o regresso às memórias voláteis, passando o disco magnético a desempenhar a função de *backup* do conteúdo da memória. Por outro lado a fita perfurada foi utilizada em computadores como suporte de informação, até ao final dos anos 1970, tendo os originais teletipos sido substituídos por leitores e perfuradores de fita que permitiam atingir velocidades muito elevadas. Em 1975, a *Tandem Computers* lançou o Tandem-16, o primeiro computador com tolerância a falhas, para o processamento *on-line* de transações. O mercado financeiro adotou essa solução devido à sua capacidade de sofrer reparos e expansões em produção. Iniciou-se aqui a preocupação com disponibilidade e continuidade dos negócios, sendo sua evolução mostrada na ilustração 1:

Onda	Desastres	Recuperação de Desastres	Recuperação do Negócio	Continuidade do Negócio
Anos	1960 ➡ 1978	1978 ➡ 1990	1990 ➡ 1998	1998 ➡ Hoje
RTO[2]	Dias a Semanas	24 horas a uma semana	Horas	Minutos
Estratégia de Disponibilidade	Aquisição de equipamentos após desastre. Acordos com clientes.	Hot Site comercial. Site backup Interno. Redundância da rede WAN.	Hot Site comercial. Site backup Interno. Redundância de WAN/LAN. Centro de recuperação móvel.	Operações descentralizadas. Cluster de servidores. Implementação de SAN. Hot Site comercial.
Recuperação de dados.	Recuperação de backup. Realimentação manual de registros	Recuperação de backup incremental. Realimentação manual de registros.	Espelhamento de servidores e discos. Recuperação de backup incremental.	Cluster de servidores. Implementação de SAN. Backup diário. Replicação de dados. Espelhamento.

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.

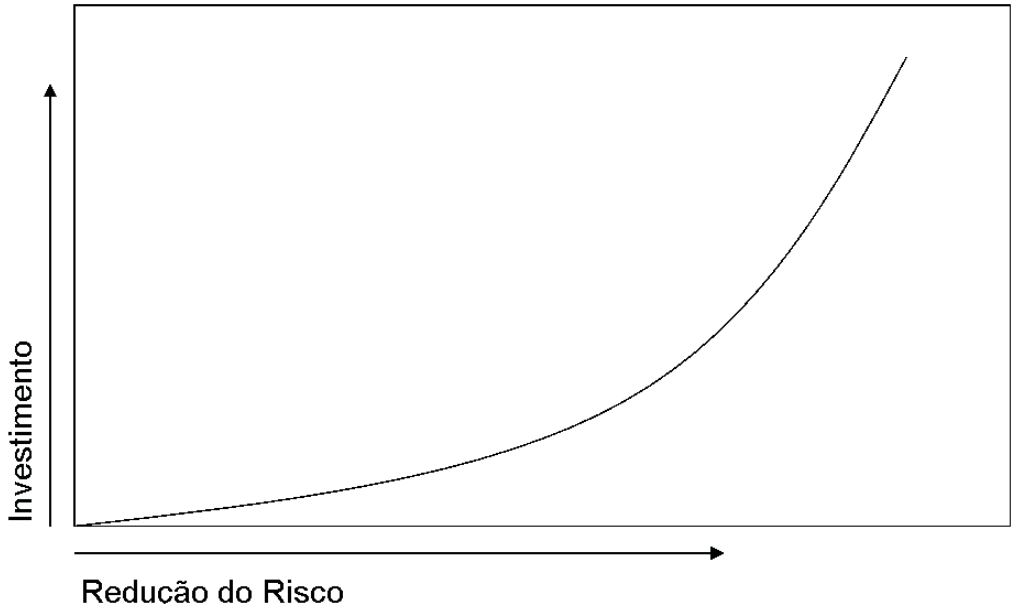
A administração de crises é um esforço contínuo, abrangente e integrado que as organizações efetivamente realizam como tentativa de, antes de tudo, entender e preveni-las. Efetivamente, administrar aquela que vier a ocorrer, considerando o interesse de seus participantes em cada etapa de suas atividades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

3.4 NASD – *Rule* 3500 *Series*

A *Securities and Exchange Commission* (SEC) aprovou, em 7 de abril de 2004, a NASD *Rule* 3500 Series, a qual estabelece que os membros da *National Association of Securities Dealers* (NASD) e da Bolsa de Valores de *New York* (NYSE) estejam preparados para emergências com o desenvolvimento de planos e procedimentos. A *Rule* 3510 determina a criação e manutenção de planos de continuidade. A norma também requer que os membros mantenham atualizados todos os planos e que realizem anualmente a sua revisão.

3.5 Norma BS 25999:1

Lançada em dezembro de 2006, a BS 25999:1 é primeira norma mundial dedicada à continuidade dos negócios, sendo desenvolvida com base nas melhores práticas do mercado. A norma foi construída de forma simples e aborda claramente aquilo que uma empresa necessita em sua estrutura de continuidade de negócios, assim como um mapa de implantação e aspectos básicos para a gestão da referida continuidade. A norma traz também uma visão geral sobre gerenciamento, orienta sobre como avaliar as respostas dos sistemas e como construir a visão de continuidade corporativa, além de informar às companhias a necessidade de prever os custos decorrentes das novas práticas implantadas.

3.6 Resolução nº. 3380

Publicada em junho de 2006, pelo Conselho Monetário Nacional, essa resolução determina às instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN a implementação de estrutura de gerenciamento do risco operacional. Para efeitos desse normativo, entende-se como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

Entre os eventos de risco operacional, a resolução inclui:

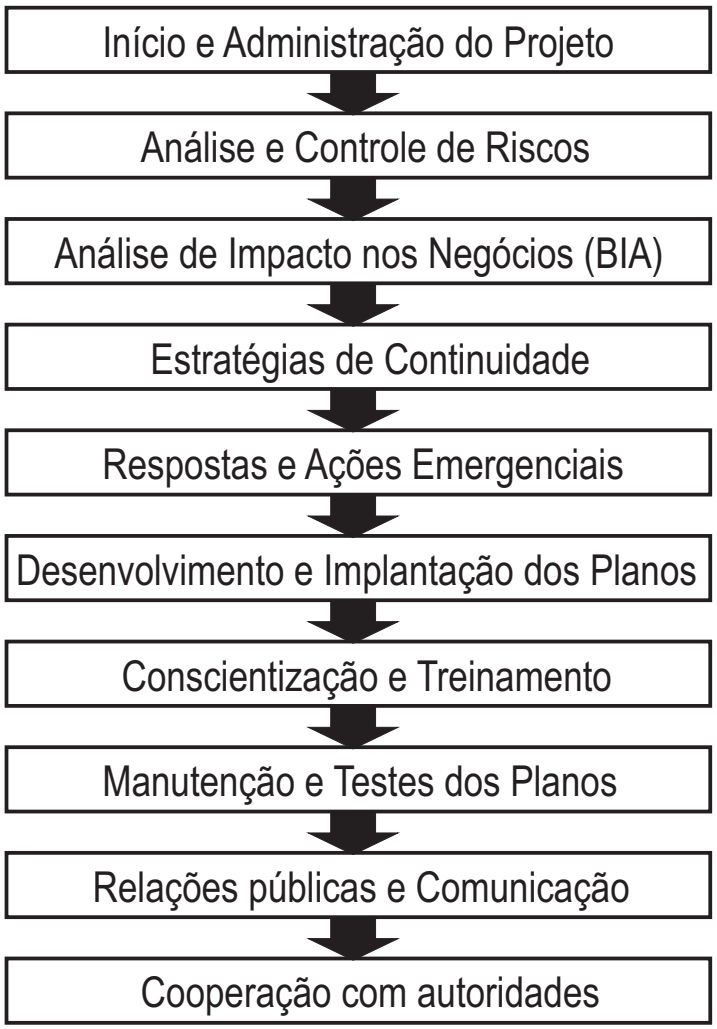
- fraudes internas e externas;
- demandas trabalhistas e segurança deficiente do local de trabalho;
- práticas inadequadas relativas a clientes, produtos e serviços;
- danos a ativos físicos próprios ou em uso pela instituição;
- aqueles que acarretem a interrupção das atividades da instituição;
- falhas em sistemas de tecnologia da informação;
- falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

Para que tais eventos sejam mitigados, as empresas devem criar uma estrutura de gerenciamento de risco operacional, a qual deve prever, dentre outras atribuições, a existência de planos de continuidade que contenham as estratégias a serem adotadas para assegurar a continuidade das atividades e para limitar graves perdas decorrentes de risco operacional.

4 Planejando e desenvolvendo a Gestão da Continuidade dos Negócios

Conforme o DRII, em seu guia profissional – *Practices for Business Continuity Planners,* as etapas para o planejamento e desenvolvimento da gestão e dos planos de continuidade de negócios são as apresentadas na ilustração 3, lembrando que tais etapas são apenas uma referência, visto não existir fórmula única ou metodologia que se aplique a todas as empresas.

Ilustração 2



Detalharemos a seguir as etapas propostas pelo DRII para o planejamento e desenvolvimento da Gestão da Continuidade dos Negócios Corporativa.

5 Início e administração

Nessa etapa, será estabelecido o escopo para o desenvolvimento dos planos de continuidade, incluindo as questões de obtenção de apoio da alta direção, abrangência, orçamento, estrutura organizacional, organização e gerenciamento do programa.

É importante para o responsável ter em mente algumas premissas básicas, as quais devem estar compreendidas pelos patrocinadores. A primeira delas, e a mais importante, é saber que a gestão da continuidade dos negócios não é um projeto e sim um programa evolutivo contínuo, pois não é uma atividade feita apenas uma vez. Também é bom lembrar que continuidade dos negócios não é burocracia para atender aos órgãos reguladores e, principalmente, não é despesa; é investimento.

Os executivos também devem ter a percepção das suas responsabilidades tanto civis quanto criminais, diante das legislações nacionais e internacionais e das determinações dos órgãos reguladores. Como a GCN deve ser encarada como um programa de magnitude, devemos lembrar que não existem fórmulas nem receitas prontas; não existe um produto de prateleira que nos auxilie nesse desenvolvimento. Cada empresa requer solução diferente; o que é bom para uma pode não ser bom para outra.

As boas práticas indicam que deva existir uma estrutura responsável pelo programa. Ela pode estar vinculada ao gestor de riscos corporativos ou à área de Tecnologia da Informação ou, ainda, a alguma

outra estrutura similar capaz de conduzir as atividades relativas ao Programa de Continuidade dos Negócios (PCN).

Deverá ser criada a figura do *Business Continuity Coordinator* – BCC o qual constitui um grupo permanentemente ativo, responsável por todas as ações relativas ao PCN, sendo elo entre as equipes e a alta direção.

Ao BCC compete buscar o comprometimento da diretoria executiva, gerências operacionais e de todos os funcionários, envolvidos direta ou indiretamente nos processos de negócio da empresa.

Deverá também, nessa etapa, ser desenvolvida uma política corporativa de continuidade de negócios em que deverão estar definidos os seguintes itens:

Responsáveis pelo programa.
Motivos para elaboração do PCN.
Objetivos e expectativas.
Premissas assumidas.
Papel do BCC.

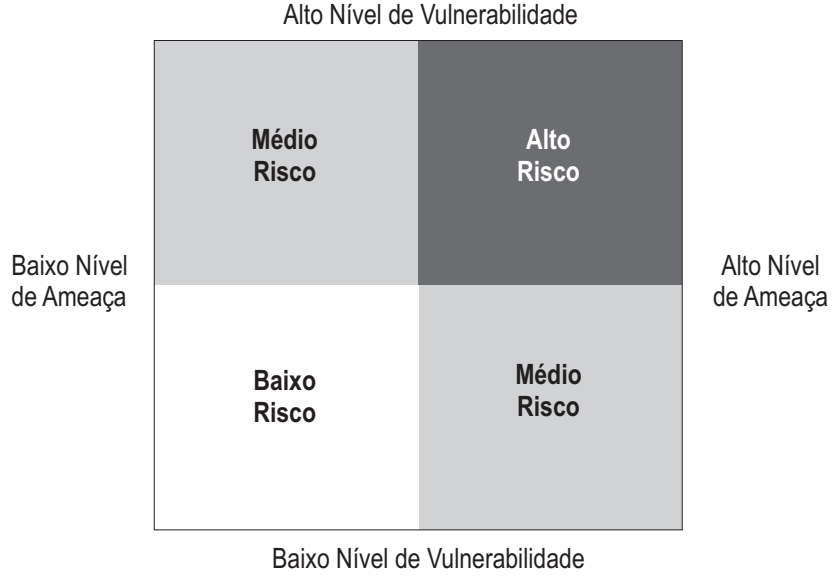
Nesse ponto do programa, podem surgir os primeiros obstáculos ao PCN, ou seja, resistência da corporação à mudança. Caberá então aos responsáveis a realização de um trabalho de convencimento com os empregados, o qual deverá ter o apoio do setor de recursos humanos e/ou marketing.

6 Análise e controle de riscos

Define os prováveis eventos e riscos que possam provocar uma interrupção significativa nos processos de negócio e as instalações físicas. Elenca os possíveis danos acarretados de cada evento e quais as medidas necessárias para prevenir e/ou reduzir os efeitos de perda potencial. Oferece a possibilidade de ser realizada análise de retorno do investimento (ROI) para justificar os custos no controle de redução de riscos.

A análise de riscos é fundamental para orientar a abrangência das atividades de planejamento do PCN e deve ser baseada na vivência e experiência dos gestores dos processos de negócio. Os riscos são inerentes a processos, pessoas e lugares e sempre serão particulares a cada caso; por isso não podem ser generalizados.

Na ilustração 3, a seguir, observa-se o relacionamento entre risco, ameaça e vulnerabilidade. Definiremos risco como a probabilidade da ocorrência de perdas decorrentes de alguma ameaça. Ameaça como evento que pode ser interno ou externo, e provocar perdas explorando alguma vulnerabilidade. Vulnerabilidade, como a existência de, pelo menos, um ponto de falha num recurso, processo ou local que, associado a uma ameaça, possa provocar perdas.



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.

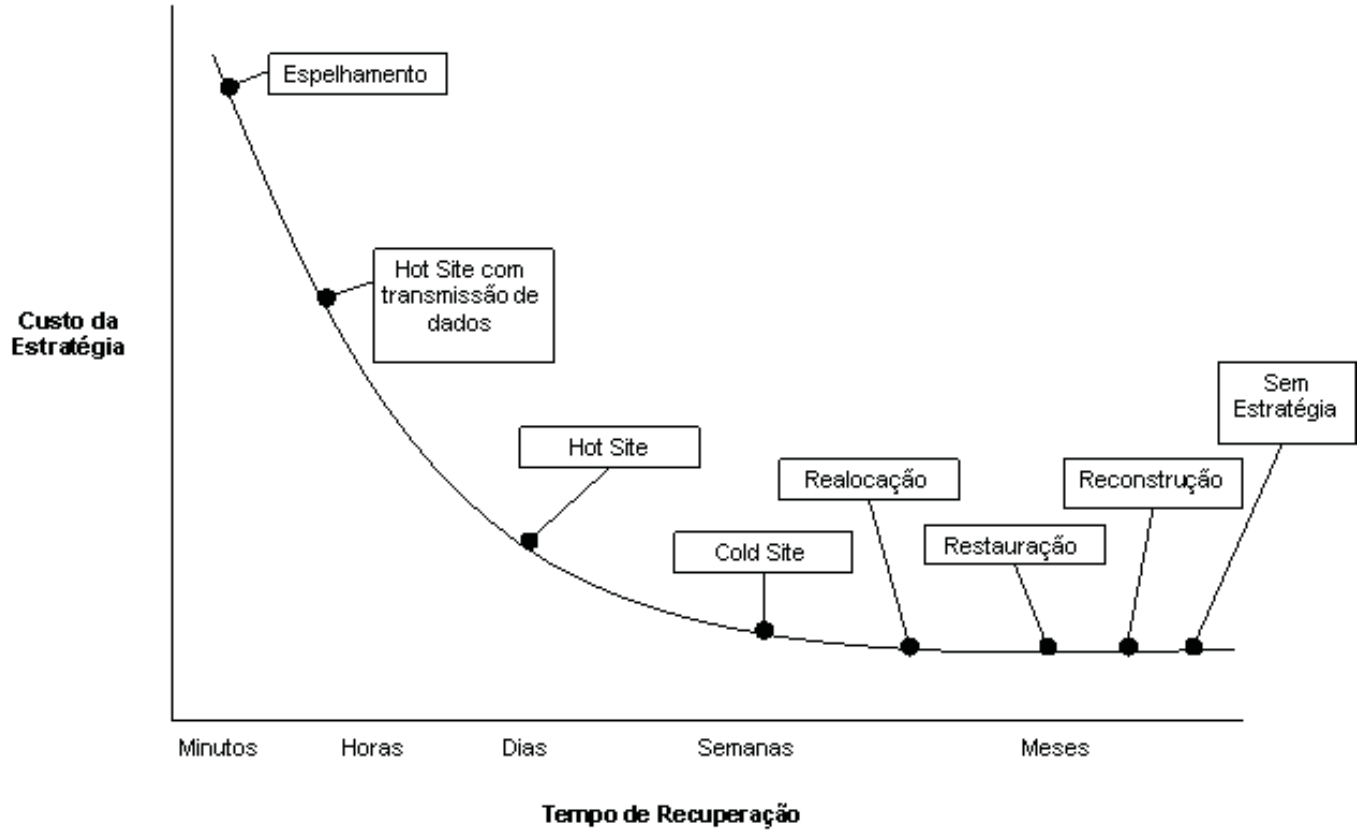
Essa é provavelmente a etapa mais desafiadora do programa, pois vai requerer experiência técnica e conhecimento dos negócios. Visto serem possíveis múltiplas combinações, cada uma com suas vantagens e desvantagens, é praticamente impossível agradar todos os gestores, ou seja, não existindo solução correta 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:

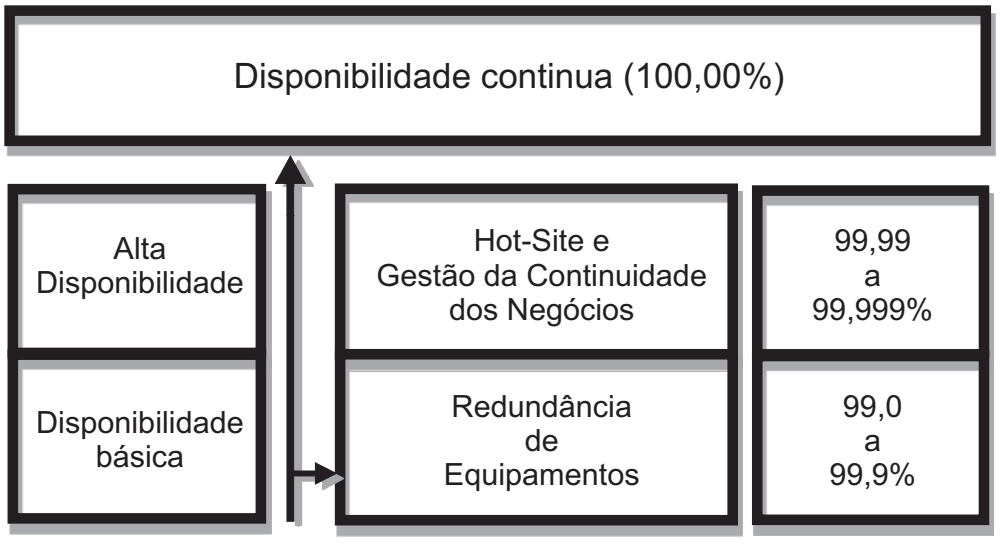
Disponibilidade básica.

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.

As atividades devem ser escritas como ordens de comando, curtas e simples, com maior detalhamento para as atividades diferentes do dia-a-dia. Se necessário, inserir comentários e/ou informações adicionais.

Listas de acionamento com nome, telefone de contato, endereços etc. dos colaboradores envolvidos no processo de negócio.

Lista de acionamento de fornecedores e terceiros.

Inventário de recursos necessários para recuperação.

Os planos também devem estar armazenados em local único, que possa ser acessados mesmo no pior cenário; o acesso às informações deve ser controlado, garantindo a sua confidencialidade.

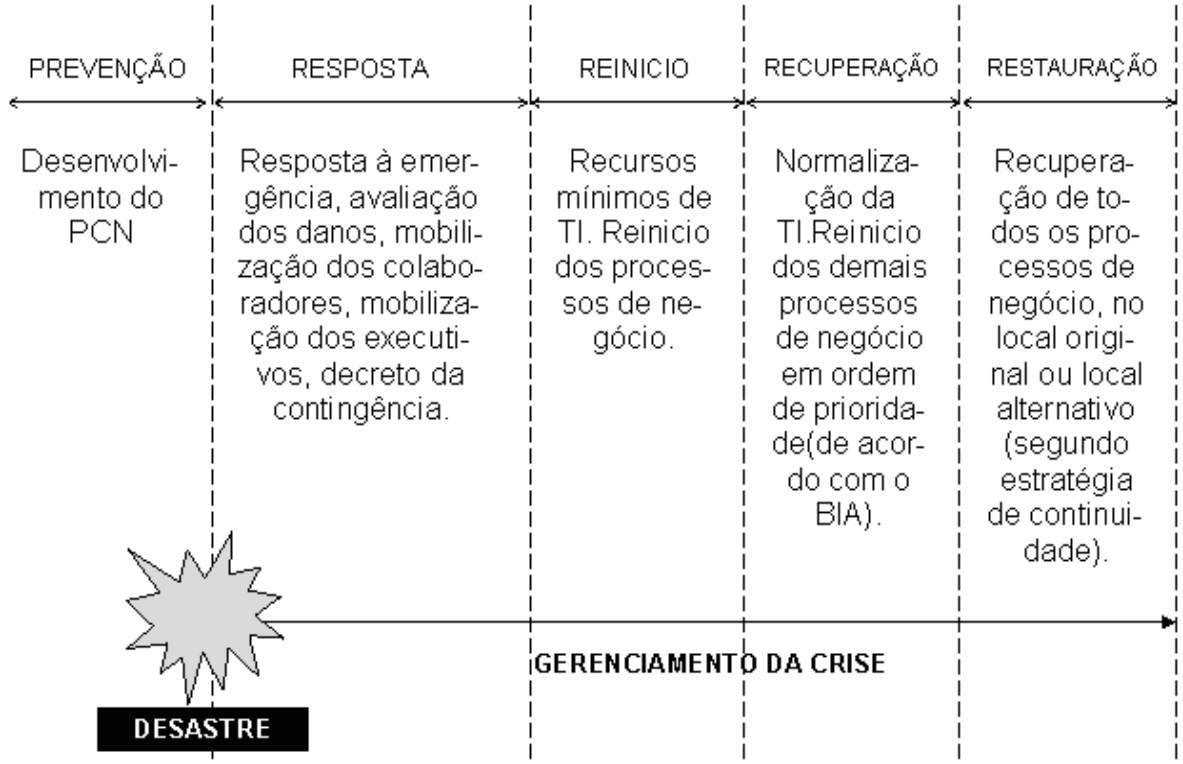
Devido ao grande volume de planos que serão desenvolvidos e gerenciados, principalmente no ambiente das grandes corporações, o uso de ferramentas de gestão especialistas em continuidade dos negócios deve ser considerado.

13 Respostas e ações emergenciais

É conveniente desenvolver e implementar os procedimentos de resposta a situações de desastre, incluindo a criação e a especificação de normas para o gerenciamento de um centro operacional de emergência (COE), utilizado como central de comando durante uma crise.

Antes de verificar as ações dessa etapa, será interessante decompor as fases de uma interrupção, conforme ilustração 6

Ilustração 6



De acordo com dados da Strohl Systems[1], 80% das interrupções acontecem fora do horário normal de trabalho, quando normalmente há menor número de funcionários, menos preparados e geralmente desatentos. Daí a necessidade de existirem políticas, procedimentos e planos que instruam todos os colaboradores em como proceder adequadamente numa crise.

Para que o PCN seja realmente eficiente, as atividades referentes à recuperação devem estar estruturadas e distribuídas por equipes com atribuições específicas que, em caso de emergência, são prioritárias a quaisquer outras que estejam fora dos procedimentos de continuidade.

As equipes são constituídas por colaboradores com adequado nível de qualificação técnico profissional e conhecimento do negócio da empresa.

Internamente, em cada equipe, os respectivos integrantes são subordinados hierarquicamente a uma liderança nomeada.

Não se diferencia nível hierárquico de qualquer colaborador, para que detenha esse poder em tempos de crise. Os colaboradores são escolhidos por sua característica técnica e gerencial. Não se dá, em virtude desse nível, qualquer diferencial executivo, funcional ou de remuneração especial.

Os líderes das equipes têm as seguintes responsabilidades: coordenar e assegurar a execução de todas as atividades sob sua responsabilidade, solucionando conflitos, dúvidas e problemas não previstos; elaborar relatórios de avaliação sobre a execução das atividades e estabelecer ações corretivas que forem necessárias; interagir com os líderes das demais equipes, com o objetivo de coordenar as ações conjuntas em estrita observância ao estabelecido nos Planos; e reportar em nome do grupo que representam a equipe de Gestão e Decisão ou Administração, Organização e Informação quando necessário ou solicitado.

Além da hierarquia das equipes, é adotado o estabelecimento de poderes, que deverão ser respeitados com o objetivo do restabelecimento da ordem normal dos processos. É adotado, para a designação dos perfis, o conceito no menor privilégio: "Tudo o que não é explicitamente permitido é proibido!"

É responsabilidade de cada membro da Equipe fornecer informações quando ocorrerem alterações zelando para que os planos mantenham-se sempre com os dados atualizados.

É obrigação comum a todos os membros desses grupos apresentarem-se ao COE ou outro local determinado, trazendo cópia dos Procedimentos de Continuidade e Recuperação e identificação pessoal, tão logo seja notificado de problema ocorrido.

14 Conscientização e treinamento

Aqui, o responsável pelo programa deve desenvolver ações para incrementar a cultura corporativa no que se refere à manutenção, implementação e execução do PCN.

A melhor forma de conscientizar os colaboradores é por meio do seu envolvimento e comprometimento com o programa. Para tal, o responsável deve contar com as áreas de Recursos Humanos e *Marketing*. É aconselhável criar um espaço na *Intranet* corporativa para a divulgação de notícias, textos etc. sobre o programa. Importante também realizar campanhas internas com a distribuição de vídeos, pôsteres, brindes, organizar palestras que divulguem as razões do PCN, quais etapas já foram cumpridas, os responsáveis pelo programa etc.

A disseminação do conhecimento sobre o programa aumenta a segurança nas ações de recuperação numa situação real, diminui as dúvidas, reduz os tempos de recuperação e os impactos previstos no BIA diante de um desastre real.

[1] Strohl Systems Inc. Empresa americana especialista em continuidade dos negócios.

15 Testes e manutenção dos planos

Nesta fase, é definida a estratégia para a realização dos testes/simulações e os mecanismos de manutenção dos planos.

Os testes/simulações realizados irão gerar as evidências, possibilitando aprimorar e/ou corrigir os planos, validando a eficácia das estratégias de recuperação adotadas e os planos desenvolvidos.

A instituição ao realizar um teste verificará a real capacidade da recuperação dos processos de negócio críticos, garantindo aos clientes, acionistas, colaboradores e fornecedores que a instituição é capaz de operar após um desastre.

É recomendável que os testes sigam um modelo evolutivo, iniciando com escopos menores, controlados e com objetivos menos desafiadores, mas sempre envolvendo tanto a área de TI quanto a de negócio. O teste sempre deve considerar um cenário válido, ou seja, possível de acontecer.

Os testes podem ser realizados da seguinte forma:

Teste de Mesa: em que os participantes ensaiam a execução do plano, geralmente na mesa de reunião.

Teste Modular: focado em um único processo de negócio ou recurso.

Teste Funcional: integrado de vários processos de negócio, esse teste é mais realista por envolver vários grupos, múltiplas interfaces e considerar as interdependências existentes.

A freqüência com que os testes serão realizados varia de acordo com a instituição, tipo de teste, quantidade de alterações sofridas nos planos ou alterações significativas nos processos de negócio. É boa prática que os testes sejam feitos no mínimo uma vez ao ano ou a cada alteração significativa nos planos. Os bancos, por força do acordo de Basiléia, deverão comprovar a consistência dos resultados dos testes realizados.

Após a realização do teste, o responsável deverá apresentar um relatório contendo:

Escopo do teste.

Responsáveis pelo teste.

Tempo de recuperação – Previsto X Realizado.

Melhorias propostas no plano.

Evidências da destruição das informações utilizadas.

Esse relatório deverá ser armazenado juntamente com os planos, onde poderá ser consultado caso necessário.

A manutenção dos planos deverá ser periódica de acordo com o definido na política do PCN. Essa atividade é tão importante quanto a própria confecção do plano. As informações devem estar atualizadas, completas e integras assegurando a disponibilidade dos recursos necessários para a realização das tarefas previstas.

A manutenção pode ser realizada das seguintes formas:

Eventual: antes de cada teste.

Periódica: conforme definido pela política ou órgão regulador.

Integrada: automatizada, como a utilização de *softwares* que integram os inventários corporativos ou a gerência de mudanças.

Devido ao grande volume de informações, é recomendável a utilização de uma ferramenta de gestão, pois a prática mostra que as alterações, principalmente dos dados cadastrais dos colaboradores e recursos de TI, é freqüente. Estima-se que em um ano, 50% desses dados estarão inconsistentes, se não for realizada manutenção periódica.

16 Relações públicas e comunicação

É importante desenvolver, coordenar, avaliar e exercitar o manuseio de mídias e documentos durante as situações de crise, bem como os possíveis meios de comunicação que minimizem os impactos traumáticos entre a instituição, seus funcionários e suas famílias, clientes, fornecedores, investidores e gestores corporativos. Assegura o fornecimento de informações por meio de uma fonte única e constantemente atualizada.

Provavelmente, no caso de desastre, a mídia deverá chegar ao local antes dos responsáveis pela instituição. Deverá existir a figura do porta-voz, pessoa capacitada e designada para interagir com a mídia. Em momento algum, os colaboradores devem dar declarações à imprensa.

As informações somente serão repassadas pelo porta-voz em horários pré-definidos e deverão ser classificadas; ou seja, a instituição deve verificar o que pode e o que não pode ser divulgado. Caso necessário, poderão ser omitidos alguns dados, mas nunca deverão ser divulgadas informações inverídicas.

As autoridades, órgãos reguladores, sindicatos e empregados devem ter um canal alternativo de informação funcionando 24 X 7, mas com as mesmas informações que serão repassadas à imprensa.

17 Cooperação com autoridades

Estabelece os procedimentos necessários e as políticas de coordenação de resposta, atividades de continuidade e restauração do negócio, com o auxílio de autoridades públicas ou privadas para o atendimento de normas e leis.

Deverão ser revistos periodicamente os planos, no que diz respeito à observância das leis e normas públicas relacionadas aos procedimentos de emergência. Isso assegura que a execução dos planos esteja coordenada com as autoridades públicas, quando necessário ou exigido por lei; por exemplo, quando há a obrigatoriedade de intervenção policial ou de bombeiros.

18 Recomendações

As etapas apresentadas ao longo deste trabalho, baseadas nas recomendações do DRII, abordam praticamente todas as variáveis que devem ser consideradas para o planejamento e desenvolvimento de um PCN. O guia do DRII, respeitado mundialmente, devido a seu pioneirismo e consistência, é indicando aos profissionais responsáveis pela árdua tarefa de inserir na cultura corporativa os preceitos da continuidade dos negócios como a direção a ser seguida.

No intuito de auxiliar os que, por ventura, venham a utilizar este trabalho como fonte de pesquisa, a seguir são apresentados alguns itens que merecem maior atenção, os quais são repetidamente apontados na literatura e pelos especialistas na área, como críticos no desenvolvimento de um bom Programa de Continuidade dos Negócios.

19 Relevância do tema

Devido à necessidade de cumprimento das determinações do BACEN, COBIT, *Sarbanes-Oxley* e Basiléia II, as instituições devem, no futuro próximo, priorizar o desenvolvimento de um PCN. Mas o atendimento às leis e às regulamentações não deve ser o foco, nem o principal motivador da realização de tal projeto. É necessário que a alta direção das instituições entenda o PCN como algo maior e que certamente não será feito apenas uma única vez. O maior bem das empresas, sem dúvida, é sua marca e credibilidade e o PCN vai contribuir para o fortalecimento dessa imagem, criando condições para o atendimento aos clientes com qualidade e alta disponibilidade.

Ao percorrer as etapas de desenvolvimento do programa, será possível realizar uma revisão nos processos de negócio, verificar os relacionamentos existentes no emaranhado de sistemas de TI, descobrir a duplicidade de informações e até encontrar processos de negócio em que um simples arquivo texto seja crítico para sua continuidade. Deixaremos de "achar" que algo é importante e que pode ter impacto nos processos; após o desenvolvimento do PCN, teremos certeza do que é importante e vital para a continuidade dos negócios.

20 Investimento

Os executivos tendem a encarar o PCN como despesa. Esse é um problema para a realização do projeto e cabe aos responsáveis por seu desenvolvimento modificar tal percepção. Fazendo um paralelo com nossa vida pessoal, podemos comparar o PCN ao seguro do carro, ou seja, uma pequena quantia investida para preservar o bem maior. No caso dos bancos, o investimento não deve ser pequeno, devido à complexidade dos processos, controles, dependência tecnológica e grande número de sistemas que integram a infra-estrutura de TI.

Devem ser previstos investimentos no desenvolvimento dos responsáveis pelo PCN, já que não existe "produto de prateleira" para esse projeto. É preciso adquirir ferramentas para a gestão do programa, pois em grandes empresas o número de planos pode ultrapassar os dois mil, os quais dificilmente serão administrados e atualizados com processadores de texto ou planilhas. Deve também ser considerada a contratação de uma empresa especializada no assunto, para auxiliar os responsáveis pelo PCN, bem como para promover a transferência de conhecimento. É necessário o desenvolvimento de inteligência interna com referência ao tema, garantindo às empresas independência em relação às consultorias, visto o PCN ser evolutivo e contínuo.

21 Estrutura

Não existe local próprio para a equipe responsável pela gestão do PCN na organização; algumas empresas têm a equipe vinculada à TI; outras, à área de Segurança da Informação; outras, à auditoria. As boas práticas recomendam a criação do BCC - *Business Continuity Coordinator,* que não será apenas uma pessoa e sim a equipe responsável pelo desenvolvimento do PCN. A equipe deverá ter patrocínio da alta direção, possuir conhecimento sobre os negócios da empresa, estar capacitada em continuidade dos negócios e ter trânsito fácil nas várias áreas da instituição.

Recomenda-se que essa equipe esteja vinculada ao conselho diretor ou ao gestor de riscos corporativos, visando garantir maior independência nas ações e maior poder de mando. Como as atividades do PCN irão provocar alterações no dia a dia da empresa, a resistência do corpo funcional a essas mudanças poderá ser obstáculo para o desenvolvimento do PCN; daí a necessidade do posicionamento estratégico do BCC.

A criação do centro operacional de emergência (COE) deve considerar também, que o local terá infra-estrutura básica, como microcomputadores, telefones, fax, etc. e será utilizado em situações de emergência. No restante do tempo, a estrutura pode ser utilizada para cursos, palestras ou grupos de trabalho.

22 Treinamento

O treinamento é item fundamental para o sucesso do PCN. O BCC deverá receber treinamento aprofundado no tema, bem como os conhecimentos básicos deverão ser disseminados na corporação. Hoje, no Brasil, existem poucos cursos disponíveis; pode ser necessário realizar um curso *in-company* ou então aguardar as oportunidades oferecidas pelo mercado. O DRII ministra vários cursos sobre o assunto, normalmente realizados nos Estados Unidos, preparatórios para os exames de certificação existentes.

23 Manutenção e testes

A atualização e testes dos planos são essenciais para preservar a eficácia. O dinamismo verificado nos processos de negócio propicia o aparecimento contínuo de novos riscos, os quais devem ser contemplados nos planos. Informação desatualizada no momento de crise não terá valor nenhum.

Conclusão

A continuidade dos negócios que, na maioria das instituições, não tinha muita projeção até meados de 2001, quando ocorreu o atentado às torres do World Trade Center, passa hoje a ser tratada de forma mais séria e está presente na agenda da maioria das grandes corporações.

Os diversos eventos catastróficos que ocorreram ao longo desses anos, como as explosões no metrô de Londres ou o *Tsunami,* que atingiu a costa da Ásia, fizeram com que a continuidade dos negócios deixasse de ser meramente assunto para técnicos, passando a ser abordado também pelo nível estratégico das empresas.

Lembramos que desastres acontecem raramente, mas incidentes menores podem interromper os processos de negócio de uma empresa por longos períodos. A continuidade hoje deve ser tratada como atividade indispensável para a manutenção dos negócios, sendo discutida no nível de diretoria e suas diretrizes disseminadas por toda a empresa.

O pequeno percentual de empresas que possuem internalizados os conceitos de continuidade dos negócios, apesar de não ser surpreendente, é muito preocupante. Em outras palavras, mais de 75% delas estão correndo sérios riscos de terem perdas de recursos financeiros, humanos e materiais, estando até mesmo sujeitas à falência.

Verifica-se que a maioria está preocupada com a segurança de seus negócios, mas a conscientização dos riscos que as ameaçam ainda não é suficiente para que destinem todos os recursos necessários para tal.

Para as instituições que não possuem ainda alto grau de maturidade em continuidade de negócios, recomenda-se avaliação criteriosa da sua atual exposição aos riscos e a observação da quantidade e intensidade de incidentes que ocorrem no dia-a-dia. A visão da maioria dos executivos, de que todos os investimentos devem gerar retorno financeiro, tem contribuído para essa restrição orçamentária. A criação de um PCN deve ser tratada como um seguro, sendo que cada empresa deve estudar suas necessidades, a fim de estabelecer o nível mais adequado de segurança para seu caso.

Um fato positivo é que a grande maioria das empresas que possui um PCN treina sua equipe em continuidade de negócios. No entanto, elas ainda não estão certas de que estejam bem preparadas para agir nos casos de incidentes. Por conseguinte, recomenda-se às instituições aumentar e melhorar o treinamento de seus funcionários.

Por fim, fica aqui a recomendação para todas as empresas de todos os portes, dos diversos setores, para que apurem corretamente os riscos a que estão sujeitas e as conseqüências que os incidentes podem causar. Os impactos podem certamente justificar o investimento em um programa de continuidade de negócios.

Busco aqui o ponto de partida para outras pesquisas na área, em particular no Brasil, onde existem poucas semelhantes. Ainda há muito a ser explorado.

Referências

ABNT. **Tecnologia da informação** – Código de prática para a gestão da segurança da informação (NBR ISO/IEC 17799). Rio de Janeiro, RJ: 2001.

BARNES, JAMES C. **A Guide to Business Continuity Planning**. Chichester, UK: Wiley, 2001.

BASEL COMMITTEE ON BANKING SUPERVISION. **Risk Management Principles for Electronic Banking**. Julho 2003.

_____. **Sound Practices for the Management and Supervision of Operational Risk**. Fevereiro 2003.

_____. **The New Basel Capital Accord**. Abril 2003.

COMPUTER HISTORY MUSEUM. Disponível em <http://www.computerhistory.org>. Acesso em 12 de maio de 2005.

DELOITTE TOUCHE TOHMATSU. **Lei Sarbanes-Oxley** – Guia para melhorar a governança corporativa através de eficazes controles internos. Maio de 2003.

DISASTER RECOVERY INSTITUTE INTERNATIONAL. **Professional Practices for Business Continuity Planners.** 2003.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL. **Business Continuity Planning Booklet**. Março 2003.

GARTNER GROUP. CLAUNCH, C. **Best Practices in Business Continuity and Disaster Recovery.** 2004.

_____. NOAKES-FRY, KRISTEN., DIAMOND, TRUDE. **Business Continuity and Disaster Recovery Planning and management***:* technology overview. 2003.

_____. NOAKES-FRY, KRISTEN., DIAMOND, TRUDE. **Business Continuity Planning Software:** technology overview. 2003.

_____. WITTY, R. **A Business Continuity Management Program is Critical**. 2003.

ISAAC, A., ZAWADA, B. Basel II and Business Continuity. **Continuity Insights**. Janeiro/Fevereiro 2005.

MARINHO, Fernando. **Como proteger e manter seus negócios**: um guia básico para contingência e continuidade nas empresas. Rio de Janeiro: Elsevier, 2003.

NIST. **Contingency Planning Guide for Information Technology Systems** (SP 800-34). 2002.

STROHL SYSTEMS DO BRASIL. **Imersão no Gerenciamento da Continuidade dos Negócios.** São Paulo. 2005.

SUNGARD. **Sarbanes-Oxley Act Section 404***:* Ensuring Data Integrity and Availability for Compliance and Attestation. 2004.

SUNGARD WORLD. **The evolution of contingency planning**. Vol. 2, pp. 16-20.

Resumo

Este trabalho apresenta a metodologia mais utilizada atualmente e os requisitos necessários para o desenvolvimento da gestão da continuidade dos negócios. Serão abordadas as ações necessárias para a elaboração, manutenção e testes dos planos de continuidade de negócios, as justificativas para o investimento e os fatos motivadores para a elaboração destes planos, sejam eles, exigências dos órgãos reguladores ou necessários à manutenção dos negócios, bem como os fatores humanos associados à mudança de comportamento.

Palavras-chave: gestão da continuidade dos negócios; contingência; recuperação de desastres; gestão de riscos corporativos.

Abstract

This paper presents the most actually used methodology and the necessaries requests to build a Business Continuity Plan. Actions needed to build, to maintain and to test the BCP are being considered, as well as costs investment justifies and the main motivated facts to develop the BCP. No matter if those facts are motivated by external controlling or real demands to keep business running, or even concerned to human being behaviors changes.

Key-words: Business continuity management; contingency; disaster recovery; corporative risks.

Resumen

Este artículo presenta la medodología más utilizada actualmente y los requisitos necesarios para el desarrollo de la gestión de continuidad en los negocios. Se abordarán las acciones necesarias para la elaboración, manutención y testes de los planes de continuidad en los negocios, las justificantes para inversión en ese sector y los elementos motivadores para la elaboración de dichos planes, sea motivados por las exigencias de las entidades reguladoras, ó bien por necesidades internas de manutención del negocio, ó aún en lo que atañe al cambio de los comportamientos humanos.

Palabras-clave: plan de continuidad de negocios; contingencia; recuperación de desastres; gestión de riesgos corporativos.