

BCM

– Business Continuity

Management –

Gestão de Continuidade dos
negócios, isto existe no Brasil?

www.brasiliano.com.br

REVISTA ELETRÔNICA
BRASILIANO & ASSOCIADOS
ISSN 1678-2496N
Dezembro 2006 nº:27°

**REVISTA ELETRÔNICA
BRASILIANO & ASSOCIADOS**

SUMÁRIO

BCM

**– Business Continuity Management –
Gestão de Continuidade dos negócios, isto existe no Brasil?**

A Revista Eletrônica Brasiliano & Associados nº27 é uma publicação bimestral. Reservado todos os direitos.

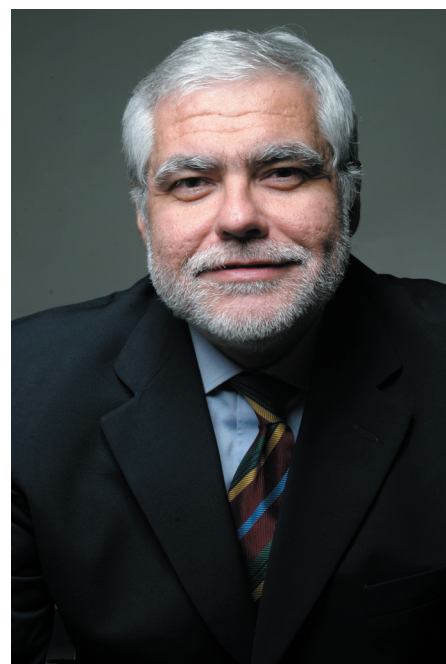
Diretor Executivo: Antonio Celso Ribeiro Brasiliano
Diretora de Treinamento: Enza Cirelli
Projeto Gráfico e Editoração: Marina Brasiliano
e-mail: mabrasiliano@yahoo.com.br



PONTO DE VISTA: A INCOMPETÊNCIA POR FALTA DE GESTÃO DE RISCOS!!

Depois de muito tempo operando com capacidade plena, o sistema de controle e tráfego aéreo do Brasil entrou em colapso após o acidente envolvendo as aeronaves da empresa Gol e um jato privado norte americano. Além da dor das vítimas deste acidente, diga-se que foi o maior acidente no Brasil nos últimos anos, ficou caracterizado que algo estava muito errado no processo brasileiro de controle de tráfego aéreo.

A deflagração da crise estourou quando houve pressão sobre os controladores de voo, tentando responsabilizá-los de alguma maneira sobre o acidente. A resposta foi imediata, com a implantação da operação padrão, fazendo com que os aeroportos brasileiros entrassem em colapso. O resultado disto tudo foi o cancelamento e atrasos dos inúmeros vôos, acarretando com isso sério desconforto aos passageiros e até uma declarada falta de respeito, aliás o que é uma atitude comum por parte de nossas autoridades. Para complicar mais a caótica situação, dando mais uma pitada no já tempero azedo, no dia 05 de dezembro houve o apagão do sistema de comunicação do tráfego aéreo, tendo como consequência direta o cancelamento de grande número de vôos. A palavra inferno é muito pouco para descrever o que os infelizes cidadãos sofreram em quase todos os aeroportos, com esperas prolongadas, noite mal dormidas e, pior, sem informações consistentes. Quem tinha compromisso teria que desmarcar, quem tinha que casar descasava, quem tinha que fazer cirurgia não fazia e assim por diante. O desrespeito foi e é muito grande. O pior dos absurdos é nossa gloriosa Força Aérea – FAB vir aos jornais pela manhã do dia 8 de dezembro afirmando que o culpado do apagão foi um sargento que durante a manutenção do sistema acabou cometendo um erro e este erro derrubou todo o sistema. O que me deixa pasmo e perplexo é a inconsistência dos nossos processos!!! Pergunto: para um processo tão crítico como esse, controlar o tráfego aéreo, não existia um plano de continuidade, um plano “b”? Se o sargento foi realmente o culpado, então todo o processo de controle e tráfego aéreo realmente está com níveis de vulnerabilidade extremamente altos, o que nos faz entender que a **IRRESPONSABILIDADE** e o **DESCASO** imperam em um processo que vidas humanas estão em jogo.



Isto tudo nos faz pensar na real necessidade da realização constante de gestão de riscos, identificando eventos que possam causar impactos negativos. A gestão de riscos estima, através de prospectivas, a probabilidade destes eventos virem a acontecer, além de projetar os respectivos impactos. O resultado deste processo de análise de riscos é uma Matriz de Risco, que de forma estratégica orienta o decisor no tratamento de cada risco, ou seja orienta a tomada de decisão.

A importância desta triste fotografia de desamparo e desrespeito é uma só: as instituições públicas do Brasil, devem ser tratadas como no mundo privado e empresarial. Não dá resultado ou faz um péssimo serviço, o caminho é a rua. **Despedido!!!!!!**

Não há justificativa para a inexistência de um processo de gestão de riscos, onde a grande arte é pensar sempre no futuro, nunca no presente e passado. Com base nos cenários, realiza-se o planejamento de ações e medidas mitigatórias, além de elaborar um processo de gerenciamento da continuidade. O que ficou comprovado é que não existe nada em curso, e, pior, nem fala-se em implantar. As desculpas são várias e inúteis, pois sabemos que a solução neste caso é a médio prazo.

Desta forma a planificação da continuidade dos negócios é de suma importância, neste momento que o Brasil vive. O planejamento detalhado das medidas de continuidade e o estudo do impacto nas operações das empresas, são primordiais para o bom desempenho das empresas.

Espero que o artigo deste mês possa ajudar a sensibilizar a alta gestão, tanto das empresas como do nosso governo, para a importância do planejamento, treinamento e investimento nos recursos destinados a combater crises.

Gostaria de ter escrito um editorial mais alegre e menos tenso, neste último do final de 2006, mas infelizmente não foi possível. Só nos resta rezar e pedir ao todo poderoso, que sempre foi brasileiro, que continue a olhar sempre por nós, meros mortais brasileiros!!

Desejo a todos nós, apesar deste "apagão" aéreo, que possamos ter um natal cheio de felicidade e que entremos em 2007 com energia e determinação para enfrentar a incompetência dos nossos governantes.

Sorte (estamos precisando muito!!!!) e Boa leitura!

Antonio Celso Ribeiro Brasileiro
Publisher
abrasiliano@brasiliano.com.br

BCM

– Business Continuity Management – Gestão de Continuidade dos negócios, isto existe no Brasil?

1. INTRODUÇÃO

O Brasil está vivendo hoje uma das mais maiores crises de continuidade, afetando de maneira direta grande quantidade de pessoas e empresas, sob as mais diversas óticas. Estamos falando da crise dos controladores de vôo no Brasil. É uma típica crise que teve como origem um mal gerenciamento de riscos, se é que teve gestão de riscos!!

Isto demonstra a real necessidade das empresas brasileiras pensarem, de maneira prospectiva e não projetiva, quais são os tipos de eventos incontroláveis que podem impactar seus negócios. Em palestras minhas, seminários e para as empresas, tenho ressaltado aos gestores pensarem fora da caixa, pensarem de forma criativa, realizando a prospectiva dos eventos possíveis de virem a acontecer. É difícil pensar desta forma, pois geralmente a empresa sugere que os gestores de riscos são os idealizadores do mapa do inferno. Mas temos exemplos que demonstram ao contrário, o acidente da Gol com o Legacy, tinha uma chance probabilística de um para duzentos milhões. Vejam só e aconteceu!! Aconteceu por que?? Foram levados em consideração todos os fatores de risco?? A questão do fator humano? A questão da tecnologia? A questão da qualificação? A questão da infra estrutura?

Provavelmente não foram levado em consideração porque a prospectiva exige a visão antecipatória, e, esta visão para o caso da continuidade de negócios temos que construir cenários levando em consideração todas estas variáveis.

A dinamicidade do mercado e a hipercompetição exige dos gestores de risco esta visão antecipatória, ou seja não há desculpa do tipo não sabia ou tinha previsto. Infelizmente não é isto que tem acontecido, vamos pensar no caso do acidente da Gol, da crise dos controladores de vôo, do ataque do PCC em São Paulo, da pandemia de Influenza, crise energética e muitos outros eventos que poderão a vir a acontecer ou poderão a repetir a acontecer.

Podemos até dizer que vender um Plano de Continuidade nos Estados Unidos e Europa, para o Conselho e executivos tem se tornado mais fácil desde os trágicos eventos de 11 de setembro de 2001 e 11 de março de 2004, e 2006 em Londres.

O horrível ataque ao WTC colocou os holofotes integralmente sobre a continuidade. A

terrível devastação vista e revista nas telas de TV fez com que as organizações imediatamente considerassem como elas poderiam sobreviver em circunstâncias equivalentes. A catástrofe foi tão grande que a probabilidade de recuperação foi estreita, mas pôs uma porção de administradores pensando e certamente pôs o Plano de Continuidade muito mais alto nas agendas executivas.

Os desastres não precisam ser tão grandes para causar problemas para uma organização. Às vezes, o impacto pode ser terminal.

2. ANÁLISE DO CASO DO WTC – 11/09/01

Nas consequências imediatas do desastre de NY é interessante notar como as empresas lutaram e como foram eficazes e relevantes os seus planos de contingência. A análise abaixo foi retirada do livro de Michael Gallagher, "Gerenciamento para a Continuidade de Negócios, Como Proteger sua Empresa", da editora Prentice Hall, Estados Unidos, 2003.

- *Alguns planos falharam porque eles presumiram que estariam submetidos à destruição de apenas um prédio.* A ampla natureza do desastre não foi considerada. Isto é típico de muitos planos para a continuidade dos negócios.
- *Algumas organizações acharam que seus planos eram excessivamente detalhados e não se adequavam como efetivamente antecipantes.* Um fator crítico de sucesso num bom plano para a continuidade dos negócios é considerar o equilíbrio entre o muito e o pouco detalhado. Este é particularmente o caso em que o gerenciamento sênior e o operacional não estão familiarizados com o plano como deveriam estar. Obviamente, se o plano não é testado regularmente, esta familiaridade estará ausente. Também é um problema quando o plano é preparado por outros grupos que não os gerentes que estão diretamente envolvidos na organização. Uma simples lista de chamada de pessoal essencial que conhece o negócio pode ser mais eficaz do que um plano muito detalhado, que é difícil de manter atualizado e que pode estar condenado a guardar poeira na estante.
- *Alguns planos não estavam imediatamente disponíveis.* As cópias não estavam à mão das pessoas e os gerentes tiveram dificuldade em ter acesso a eles. Quantos planos estão meticulosamente preparados e com cópias guardadas em locais estratégicos no caso de surgir uma crise?
- *Viu-se que no mínimo em uma organização membros essenciais da equipe de resposta a emergências não estavam preparados para lidar com os efeitos traumáticos do pós-desastre e não estavam efetivamente em seus papéis.* A composição da equipe de resposta à emergência é crítica. Precisam ser pessoas que possam permanecer psicologicamente imunes ao impacto

de um incidente e possam efetivamente liderar durante o processo de recuperação. Não são necessariamente os mais altos executivos seniores da organização.

- *Os planos não estavam atualizados.* Um plano desatualizado é pior do que não ter plano nenhum. As corporações experimentam significativas mudanças organizacionais – expansão, contração ou mudança de foco em atividades resultando em racionalização – é muito fácil que um plano se transforme em irrelevante muito rapidamente. O ambiente mais fácil para manter um plano atualizado é aquele relativamente estagnado – o que não é muito típico no mundo de negócios atual.
- *Geralmente a recuperação de operações leva mais tempo do que aquele que estava programado nos planos.* A extensão do desastre e, em alguns casos, a perda de pessoal essencial impactaram nisso.
- *Alguns planos não foram suficientemente testados; este foi especialmente o caso relacionados com testes envolvendo pessoal outro que não do IT.* Quando o plano de contingência de sua organização foi testado pela última vez? Qual foi o tipo de teste? Todos os sistemas e interfaces foram testados? Isto pode ser crítico. O teste esteve confinado às operações de IT?
- *Algumas organizações não possuíam espaço alternativo para continuar as operações rapidamente.* Isso pode ter sido influenciado pela extensão geográfica do problema e que muitas corporações estiveram procurando por instalações ao mesmo tempo. Onde está localizada sua instalação de retaguarda? Onde seu staff trabalha? Os serviços de transporte, comunicação e outros estão disponíveis? Geralmente, os planos foram baseados mais na proteção e recuperação de ativos físicos e sistemas de computador do que em itens de pessoas.
- *Os provedores da instalação de retaguarda poderiam não ser capazes de atender eficazmente tantos pedidos de ajuda.* Você está ciente do perfil do consumidor em relação à sua instalação alternativa? Quantos desses consumidores poderiam ter sido atingidos pelo mesmo incidente? Qual medida é usada nesta adequação?
- *Em alguns casos, organizações descobriram que seus centros para gerenciamento de operações de emergência não estavam com as atividades disponíveis.* Outras instalações tiveram de ser encontradas. Houve dificuldades para ter um staff nas instalações alternativas por causa das dificuldades de transporte e da falência dos sistemas de comunicação, além do problema em si.
- *Registros vitais em papel foram perdidos.* Algumas vezes é dada insuficiente atenção à proteção de registros vitais em papel de uma organização. Se um documento está digitalizado, é provável que ele se transforme em parte do

back-up tradicional do IT e do plano de recuperação. De outra forma, a menos que haja uma política e procedimentos definidos para garantir que cópias de documentos importantes sejam feitas e armazenadas nas instalações alternativas, documentos vitais estão em risco.

- *Do lado positivo, houve algumas histórias muito boas.* Serviços terceirizados de recuperação funcionaram bem. Organizações com bons planos administraram bem.

Geralmente, as corporações com acordos de serviço da recuperação estavam razoavelmente bem distribuídas em relação aos principais fornecedores de serviços e todas as chamadas de clientes foram aparentemente facilitadas - mesmo se algumas das instalações de recuperação não eram as originalmente contratadas e com as quais o staff de recuperação não estivesse familiarizado. Todavia, isto justifica os grandes investimentos das organizações em contratar esse tipo de serviço.

CONCENTRAÇÃO GEOGRÁFICA

A concentração de tantas organizações, incluindo seus sistemas operacionais de retaguarda, dentro da relativamente concentrada área do WTC encorajou muitas organizações e corporações a reconsiderar o aumento de risco atribuível à concentração geográfica.

Em muitas cidades, os serviços de empresas financeiras tendem a ser concentrados em certas partes da cidade. Londres é um bom exemplo, onde tantas empresas financeiras e em alguns casos, suas instalações de retaguarda, estão concentradas na City e em Canary Wharf. No caso de um incidente afetando ambas as localizações, incluindo áreas não-afetadas, mas estreitamente relacionadas, muitas empresas estarão com sérios problemas. Elas poderão estar inaptas a operar unidades críticas de negócios uma vez que tanto unidades primárias como as de retaguarda estarão inutilizáveis ou inacessíveis.

A despeito da forma com a qual o desenvolvimento de IT possa facilitar a descentralização de funções de negócios e atividades, tem havido uma relutância em descentralizar. Os aparentes benefícios da concentração, em termos de custos – por exemplo a economia em transporte, pagamentos de subsistência e na minimização de duplas funções – tem sido o motivo.

Desde 11 de Setembro algumas grandes organizações têm revisto favoravelmente o processo de descentralização e de redução da concentração do staff em locações individuais. Tecnologias como a vídeo-conferência que facilitam a dispersão do staff têm sido estimulantes. O e-work (trabalho à distância) também está nesta categoria. A provisão de acesso remoto eficaz para sistemas de IT é agora vista como prioridade por algumas organizações. Com um razoável nível de investimento, a capacidade para habilitar o staff a trabalhar em casa e a estar capacitado a acessar rapidamente a instalação de IT numa locação alternativa no evento de uma crise é altamente desejável. Um subproduto de prover tais instalações é a facilidade com que funcionários podem ser mantidos

plenamente informados de como a crise está sendo trabalhada através de um website exclusivo.

3. CONCEITO DE BUSSINES CONTINUITY MANAGEMENT - BCM

“Gerenciamento para a continuidade dos negócios é o ato de antecipar incidentes que afetarão os processos e funções críticas de missão da organização e garantir que ela responda a qualquer incidente de maneira planejada e ensaiada.”

Fonte: BCI – Business

Continuity Institute

Esta é a definição usada pelo Instituto para a Continuidade de Negócios – Business Continuity Institute (BCI). Há outras definições de BCM. Algumas delas enfatizam a combinação de disciplinas de gerenciamento e atividades que ajudam a garantir a operação contínua das funções essenciais de negócios sob quaisquer circunstâncias.

A definição do BCI enfatiza três elementos essenciais:

É o ato de antecipar incidentes ... A organização precisa examinar os riscos e ameaças a que ela está exposta e considerar como é melhor lidar com eles se um incidente ocorrer. A escolha da palavra “incidente” ao invés de “desastre” é importante. O termo “desastre” imediatamente invoca imagens de uma explosão, incêndio ou inundação séria. “Incidente” inclui essas ocorrências, mas também abarca falha de energia, fraude, contaminação de produtos, poluição do meio ambiente, falência de fornecedores essenciais e outros eventos que não estão considerados confortavelmente como o termo “desastre” comumente é empregado. O termo “incidente” pode até incluir comentários inapropriados de executivos seniores indiscretos em funções públicas!

‘... que afetam os processos e funções críticas de missão ...’ BCM não é feito para planos e procedimentos para as coisas do dia-a-dia que caminham erradamente. Ele se relaciona com incidentes significativos que têm um considerável impacto sobre as atividades de núcleo da organização. Está longe de desviar qualquer esforço para documentar procedimentos para as falhas de processos operacionais cotidianos. Ainda que esses processos precisem existir, o BCM enfatiza a grande imagem, BCM enfatiza a sobrevivência da organização.

‘...garantir que ela responda a qualquer incidente de maneira planejada e ensaiada.’ Este elemento da definição abrange o planejamento,

o envolvimento significativo do pessoal apropriado, a aceitação, o domínio do plano, testes completos que são requisitos essenciais para uma resposta adequaram bem. Organizações com bons planos administraram bem.

Algumas vezes, quando descrevendo o BCM para um grupo de gerentes é melhor tentar relacioná-lo aos seus negócios de uma maneira pessoal. Algo como o que segue pode ter um maior impacto. BCM é sobre garantir que, se sua organização experimenta um desastre ou outro incidente sério, você já considerou essa possibilidade. Você terá tomado medidas para reduzir o risco de isso acontecer e para minimizar o impacto, caso realmente ocorra. Você terá um plano à mão com o qual todos os gerentes essenciais estarão familiarizados, que terá sido testado e que habilitará sua organização a continuar funcionando tão perto do normal quanto possível, com a mínima interrupção possível.

Isto também enfatiza que BCM não é simplesmente uma questão de ter um plano. Um aspecto pró ativo do BCM é garantir que medidas sejam introduzidas para reduzir a probabilidade de problemas surgindo e injetar elementos de resiliência e contingência nas operações – o que é parte de estabelecer a apropriada cultura de BCM.

Em vendendo e ganhando a aceitação por parte da gerência da necessidade de BCM, pode ser muito eficaz colocar perguntas relacionadas ao impacto de um incidente sério sobre as áreas pelas quais cada um dos gerentes é responsável.

4. FASES DO BCM

O ciclo de vida do gerenciamento para a continuidade dos negócios, segundo o guia do BCI – Business Continuity Institute, são cinco estágios. É uma sugestão para que o gestor possa controlar e identificar falhas em seu planejamento. O progresso do processo de continuidade deve sempre ser medido comparando-se com o total do ciclo de vida do gerenciamento e através de toda a organização. Não podemos esquecer que a continuidade de negócios é um processo, portanto não deve ser estanque.

O CICLO DE BUSINESS CONTINUITY



Programa de Gerenciamento para a Continuidade dos Negócios:

- Estratégia de BCM e Política de BCM para a Organização (Corporativa).
- Gerenciamento para a Continuidade dos Negócios
- Prontidão para incidentes e resposta

Estágio No.1: Entender o seu negócio:

- Estratégia organizacional
- Análise do impacto sobre o negócio
- Avaliação dos riscos e controle

Estágio No.2: Estratégias de Gerenciamento para a Continuidade dos Negócios:

- Estratégia de BCM para a Organização (Corporativa)
- Estratégia de BCM em Nível de Processo
- Estratégia de BCM de recursos para recuperação

Estágio No.3: Desenvolver e implementar uma resposta de BCM

- Gerenciamento da crise, Relações Públicas e a Mídia
- Planos para a continuidade dos negócios
- Planos para unidades de negócios, resposta a incidentes

Estágio No.4: Desenvolver uma cultura de gerenciamento para a continuidade dos negócios

- Avaliar
- Projetar e produzir
- Mensurar os resultados

Estágio No.5: Exercitar, manter e auditar

- Exercitar os planos de BCM
- Manutenção do BCM
- Auditar o BCM

5. CONCLUSÃO

O BCM não pode ser uma atividade isolada e ou secundária. A cultura de BCM precisa influenciar as estratégias e decisões de negócios.

A função de continuidade dos negócios deve também ter algum envolvimento no processo de desenvolver planos corporativos e de negócios – embora se a cultura de continuidade dos negócios estiver suficientemente desenvolvida dentro da empresa, as considerações de continuidade serão uma parte natural do desenvolvimento de planos.

BCM é um projeto contínuo, enquanto a maior parte do trabalho na empresa pode ter voltado a estar envolvida em “erguê-la das cinzas” introduzindo medidas de redução de risco, decidindo estratégias de recuperação e criando planos iniciais, o trabalho de BCM continuará – talvez menos intensamente.

O gestor não pode descansar uma vez que os planos iniciais tenham sido produzidos. Tem de haver comprometimento e envolvimento contínuos no processo. Deve-se insistir em relatórios regulares e recomendações devem ser direcionadas. O grupo de trabalho montado no início do processo precisa continuar a funcionar.

Podemos finalizar este pequeno artigo enfatizando a real necessidade do BCM ser um processo contínuo, de tal forma que a sua atualização seja constante.

ANTONIO CELSO RIBEIRO BRASILIANO

Master Degree - Diplome D'Etudes Approfondies (DEA) en Information Scientifique et Technique Veille Technologique (Inteligência Competitiva) pela UNIVERSITE TOULON - França; Especializado em: Inteligência Competitiva pela Universidade Federal do Rio de Janeiro - UFRJ; Gestión da Seguridad Empresarial Internacional – Universidad Comillas – Espanha; Management of Information Systems and Information Technology pela University of California Berkley - EUA; Business Intelligence pela Dominican College of San Rafael – EUA; Segurança Empresarial pela Universidad Pontificia Comillas de Madrid – Espanha; Planejamento Empresarial, pela Fundação Getúlio Vargas - SP; Elaboração de Currículos pelo Centro de Estudos de Pessoal do Exército - CEP, Bacharel em Ciências Militares, graduado pela Academia Militar das Agulhas Negras; Bacharel em Administração de Empresas; Autor dos livros: "Análise de Risco Corporativo – Método Brasileiro"; "Manual de Análise de Risco Para a Segurança Empresarial"; "Manual de Planejamento: Gestão de Riscos Corporativos"; "A (IN)Segurança nas Redes Empresarias: A Inteligência Competitiva e a Fuga Involuntária das Informações"; "Planejamento da Segurança Empresarial: Metodologia e Implantação"; Co-Autor dos Livros: "Manual de Planejamento Tático e Técnico em Segurança Empresarial"; "Segurança de Executivos" - Noções Anti-Seguestro e Seguestro: Como se Defender; Atual Coordenador Técnico e Professor dos Cursos: Curso de Especialização (MBA) Gestão em Segurança Empresarial e do Curso Avançado em Segurança Empresarial, ambos da Fundação Escola de Comércio Álvares Penteado – FECAP - SP; Membro do Instituto Brasileiro de Governança Corporativa – IBGC; Membro do Institute of Internal Auditors IIA; do Instituto dos Auditores Internos do Brasil – AUDIBRA; Membro e Diretor de Planejamento Estratégico da Associação Brasileira dos Profissionais de Segurança Orgânica – ABSO, da Associação Brasileira dos Analistas de Inteligência Competitiva – ABRAIC; Coordenou a 1ª Pesquisa de Vitimização Empresarial 2003 – Contrato pela PENUD/ONU/SENASP; Editor da Revista Proteger e Diretor Executivo da **BRASILIANO & ASSOCIADOS**.