# Plano de Continuidade de Negócios
# Planejamento

**Ronaldo Silva, Viviane da Cunha Moura, Euclides Deponti e Vinícius Rosa**

Universidade Católica de Brasília (UCB)
Brasília DF – Brasil
Coordenação de Pós Graduação

**Resumo.** A dependência das organizações em relação aos seus sistemas de informação cresceu assustadoramente nos últimos tempos. Os sistemas computacionais de hoje apresentam um papel extremamente importante nas atividades críticas para a sobrevivência das corporações: muitas atividades não poderiam ser executadas com eficácia – se é que poderiam ser realizadas – sem o apoio dos computadores.

Queda de energia elétrica, greves de pessoal, danos intencionais, tudo isso pode representar efeitos desastrosos nos sistemas computacionais. Casos de explosão de bombas em Londres e ataques terroristas como o do World Trade Center ilustram o fato de que organizações podem ser seriamente comprometidas se não apresentarem um plano de continuidade do serviço exeqüível e pronto para o uso.

Este artigo tem por objetivo apresentar um modelo de elaboração de um plano de continuidade de negócios, detalhando a sua estrutura, conceitos, fluxo operacional, atores e aplicabilidade.

**Palavras-Chave.** Ameaças, aplicações, backup, desastre, processo crítico e informação crítica.

**Abstract**. Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Continuilty planning supports this requirement by establishing thorough plans and procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.

This article has for objective to present a model of elaboration of a Business Continuity Planning, detailing your structure, concepts, operational flow, actors and use.

**Keywords.** Threats, applications, backup, disaster, critical process and critical information.

# 1 Introdução

Computadores e seus programas são conhecidos por automatizarem e acelerarem uma série de procedimentos enfadonhos e repetitivos, liberando seus usuários para tarefas mais criativas e gratificantes. Na prática, administradores de sistemas e usuários se vêm às voltas com atividades bastante criativas, mas nada gratificantes, de tentar recuperar dados perdidos e de enfrentar equipamento fora do ar devido às múltiplas falhas a que sistemas de computação estão sujeitos.

Falhas são inevitáveis, mas o impacto das falhas, ou seja, o colapso do sistema, a interrupção no fornecimento do serviço e a perda de dados, podem ser evitados pelo uso adequado de técnicas viáveis e de fácil compreensão.

Todavia, as técnicas que toleram falhas têm um alto custo associado. Pode ser a simples necessidade de backup dos dados, que consome espaço de armazenamento e tempo para realizar a cópia, redundância de equipamentos e espelhamento de discos,

que consome recursos de hardware sem contribuir para o aumento do desempenho, ou a terceirização da prestação dos serviços, para um Datacenter. O domínio da área de disponibilidade auxilia administradores e desenvolvedores de sistemas a avaliar a equação custo benefício para o seu caso específico e determinar qual a melhor técnica para seu orçamento.

Conhecer os problemas potencialmente provocados por falhas no sistema, as soluções que existem para evitar falhas ou recuperar o sistema após um evento, assim como o custo associado a essas soluções, torna-se imprescindível a todos que pretendem continuar usando computadores, desenvolvendo sistemas ou prestando um serviço computacional de qualidade aos seus clientes. Para desenvolvedores de software, projetistas de hardware e administradores de rede, o domínio das técnicas voltadas à disponibilidade total torna-se essencial na seleção de tecnologias, na especificação de sistemas e na incorporação de novas funcionalidades aos seus projetos.

Para a manutenção da disponibilidade total dos sistemas, é necessário que se elabore um Plano de ação, denominado PCN (Plano de Continuidade de Negócios) que é um termo relativamente novo, resultante dos Planos de Contingência e dos Planos de Recuperação de Desastres. Falando de forma genérica, o PCN é uma metodologia elaborada para garantir a recuperação de um ambiente de produção, independentemente de ocorrências que suspendam suas operações e dos danos nos componentes (softwares, hardware, infra-estrutura, etc.) por ele utilizados.

A recente BS 7799 e a brasileira NBR ISO/IEC 17799 consideram dez itens para definir um ambiente seguro. Um destes itens é a recomendação de desenvolvimento de um PCN. Quando se fala em segurança, a área de TI imediatamente pensa em firewalls, proxys, antivírus, senhas, política de segurança, deixando de lado as questões referentes aos PROCESSOS que dependem de TI e da velocidade de substituição de um hardware danificado.

O conceito de segurança deveria ser encarado como algo em constante mudança, ao invés de uma situação estática, alcançada com a aplicação de um "simples procedimento passo-a-passo”.

Dentre estas mudanças, existem duas frentes de atuação: o atendimento às especificações padronizadas de segurança exigidas pelo ambiente corporativo convencional e a preocupação com as medidas de resposta, em situações de crise e de eventos, quando o ambiente corporativo sofre inúmeras ameaças de impacto.

Basicamente, um PCN é um conjunto de três outros planos: o Plano de Gerenciamento de Crises (PGC), o Plano de Continuidade Operacional (PCO) e o Plano de Recuperação de Desastres (PRD). Cada um destes planos é focado em uma determinada variável de risco, numa situação de ameaça ao negócio da empresa (ou ambiente): O PGC, nas atividades que envolvem as respostas aos eventos; O PCO, voltado para as atividades que garantam a realização dos processos e o PRD, voltado para a substituição ou reposição de componentes que venham a ser danificados.

Desde a etapa de avaliação BIA (Business Impact Analysis), onde os processos de negócios da empresa são ordenados em função do seu custo de parada, até a etapa de Análise de Criticidade, onde os mesmos são avaliados de acordo com os impactos que a organização venha a sofrer com a sua interrupção, as informações apresentadas agregam importantes indicadores para os gestores e responsáveis pela direção da empresa.

Utilizando-se o PCN, garantimos a redução dos possíveis impactos, minimizando-os a níveis toleráveis para a empresa ou para o ambiente que nos interessa proteger.

# 2 Definições

- Plano de Continuidade de Negócios – Um plano para a resposta de emergência, operações backup e recuperação de ativos atingidos por uma falha ou desastre. Tem como objetivo o de assegurar a disponibilidade de recursos de sistema críticos, recuperar um ambiente avariado e promover o retorno à sua normalidade.

- Planejamento da continuidade do negócio - diz respeito ao planejamento da recuperação de processos organizacionais críticos em seguida a um desastre.

- Desastres - não se resumem somente a fogo, inundação e outras causas de dano à propriedade; eles também podem resultar de problemas corriqueiros como greves ou mau funcionamento de hardware ou software. E ainda que a restauração do processamento computacional seja um passo importante do processo de recuperação, outros problemas igualmente importantes freqüentemente precisam ser resolvidos.

- Disponibilidade – A propriedade que um sistema ou um dos seus recursos de estarem acessíveis e utilizáveis sob demanda por uma entidade autorizada, de acordo com especificações de desempenho projetadas; isto é, um sistema que está disponível para fornecer serviços de acordo com o seu projeto, sempre que uma solicitação for realizada.

- Confiabilidade – A habilidade de um sistema de executar uma função requerida sob condições indicadas por um período de tempo especificado.

- Integridade – A propriedade de manutenção dos dados da forma como foram gerados, não sofrendo alteração durante a sua manipulação.

- Sobrevivência - A habilidade de um sistema de continuar em operação ou existindo apesar das condições adversas, inclui as ocorrências naturais, ações acidentais, e ataques ao sistema.

# 3 Justificando um PCN

Mesmo sem ter planos formais de continuidade, através dos questionamentos abaixo a alta gerência poderá saber se a sua organização está preparada para uma fatalidade operacional:

- Quais são os principais negócios da minha organização?
- Quais são os fatores de risco operacionais que podem afetar seriamente os negócios da organização?
- Qual seria o impacto nas receitas geradas pelos negócios da empresa se um ou mais fatores de risco acontecesse?
- Como a empresa está preparada para lidar com o inevitável ou uma ameaça?

**Para cada questão não respondida ou respondida insatisfatoriamente, aumenta a vulnerabilidade da empresa frente a fatos cuja ocorrência esteja fora de seu controle.**

# 4 Relação dos planos de um PCN

Planos distintos são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. Estes planos são:

- Plano de Gerenciamento de Crises PGC – Este documento tem o propósito de definir as responsabilidades de cada membro das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

- Plano de Continuidade Operacional PCO – Tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, conseqüentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet, exemplificam os desafios organizados pelo plano.

- Plano de Recuperação de Desastres PRD – Tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação, no menor tempo possível.

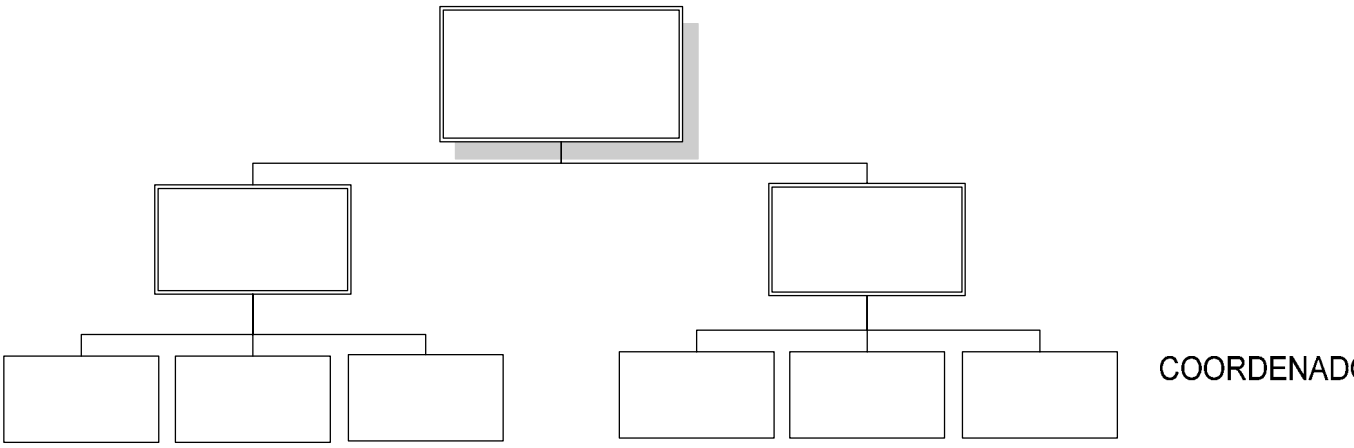
Para obtenção de sucesso nas ações dos planos, é necessário estabelecer adequadamente os gatilhos de acionamento para cada plano de continuidade. Estes gatilhos são parâmetros de tolerância usados para sinalizar o início da operacionalização da contingência, evitando acionamentos prematuros ou tardios.

Após o retorno à normalidade, relatórios deverão ser entregues pelas equipes que operacionalizaram o plano, ao Gestor do plano, com informações sobre o evento, apontando, por exemplo, características do objeto da contingência, percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros, etc.

# 5 Atores e suas Responsabilidades no Grupo de Gerência de Crise

A estrutura organizacional para o plano de continuidade de negócios, está descrita abaixo, onde se apresentam a definição, as atribuições e os responsáveis nomeados. O organograma terá validade enquanto durar as ações de emergência, até ser resolvida, cancelada ou paralisada.

Modelo de organograma, com sua estrutura hierárquica, definições e descrições de atribuições:




Participantes do Grupo de Gerência de Crise – organograma

| Posição | Atribuições |
|---|---|
| Coordenador do plano / Substituto | ▪ Nomear os participantes do plano.<br>▪ Garantir a documentação atualizada dos sistemas.<br>▪ Garantir cópias redundantes das informações e dados da organização.<br>▪ Disponibilizar recursos para ação de resposta.<br>▪ Promover treinamento dos colaboradores.<br>▪ Promover exercícios simulados.<br>▪ Garantir a revisão periódica do plano.<br>▪ Enviar relatório final de situação para o Comitê de Segurança da Informação. |
| Grupo de atuação direta | ▪ Planejamento das ações de resposta relacionadas à sua área.<br>▪ Determinar as orientações para as equipes de atuação.<br>▪ Seguir os procedimentos descritos para o cenário.<br>▪ Auxiliar, no que for necessário, nas ações de combate.<br>▪ Avaliar a participação do grupo após um incidente.<br>▪ Elaborar relatório final de situação. |
| Grupo de apoio | ▪ Planejamento das ações de resposta relacionadas à sua área.<br>▪ Seguir as orientações do coordenador do plano.<br>▪ Executar as atividades de infra-estrutura de engenharia e manutenção.<br>▪ Executar as atividades de provimento de recursos.<br>▪ Elaborar relatório final de situação. |

# 6 Fases da Elaboração do PCN

Um Plano de Continuidade ao ser desenvolvido deverá resultar num conjunto de documentos onde estarão registradas as ações do Plano propriamente dito e num conjunto de ações relativas às adequações da infra-estrutura e relativas às alterações dos procedimentos do dia a dia da Organização. Porém, antes de desenvolvido e implementado, ele passará por todas as fases abaixo:

## 6.1 Anteprojeto do PCN

O Anteprojeto abrange a parte dos Planos de Continuidade mais controvertida e discutida no momento. Esta discussão é em parte decorrente da importância desta etapa do trabalho, mas também devido aos diferentes entendimentos sobre ela. Apesar da sua importância observamos que a pressão exercida sob os responsáveis pela estruturação do Plano tem feito com que esta etapa seja ignorada, ou sub-valorizada

optando-se por se iniciar de imediato as etapas subseqüentes. Como resultado desta postura encontramos inúmeros Planos de Continuidade pouco confiáveis por não atenderem às reais necessidades da Organização para a qual eles foram desenvolvidos. Não há como se estruturar um Plano de Continuidade, sem a realização de um anteprojeto que possibilite a identificação das reais necessidades da Organização e de cada processo crítico. Perguntas como estas deverão ser respondidas nesta fase:

- O que proteger (Quais processos?);
- Do que proteger (Quais desastres?);
- Com o que proteger (Que Processos e recursos adotar?);
- Grau de exposição (Quanto o(s) processo(s) está(ão) exposto(s) a um desastre?);
- Estimativa de Impacto de um Desastre (Qual a conseqüência de um desastre?);
- Estratégia de Continuidade (Como manter a capacidade produtiva no caso de um desastre?).

## 6.2 Elaboração do Plano de Continuidade

Neste ponto devemos construir os Planos propriamente ditos, conforme as definições do item 2 deste documento.

- Plano de Gerenciamento de Crises PGC;
- Plano de Continuidade Operacional PCO;
- Plano de Recuperação de Desastres.

## 6.3 Implementação

Ao final desta fase, poderá parecer que o trabalho está concluído. Mas não está. Falta ainda:

- Treinamento;
- Teste;
- Revisão dos procedimentos (manutenção do Plano de Continuidade).

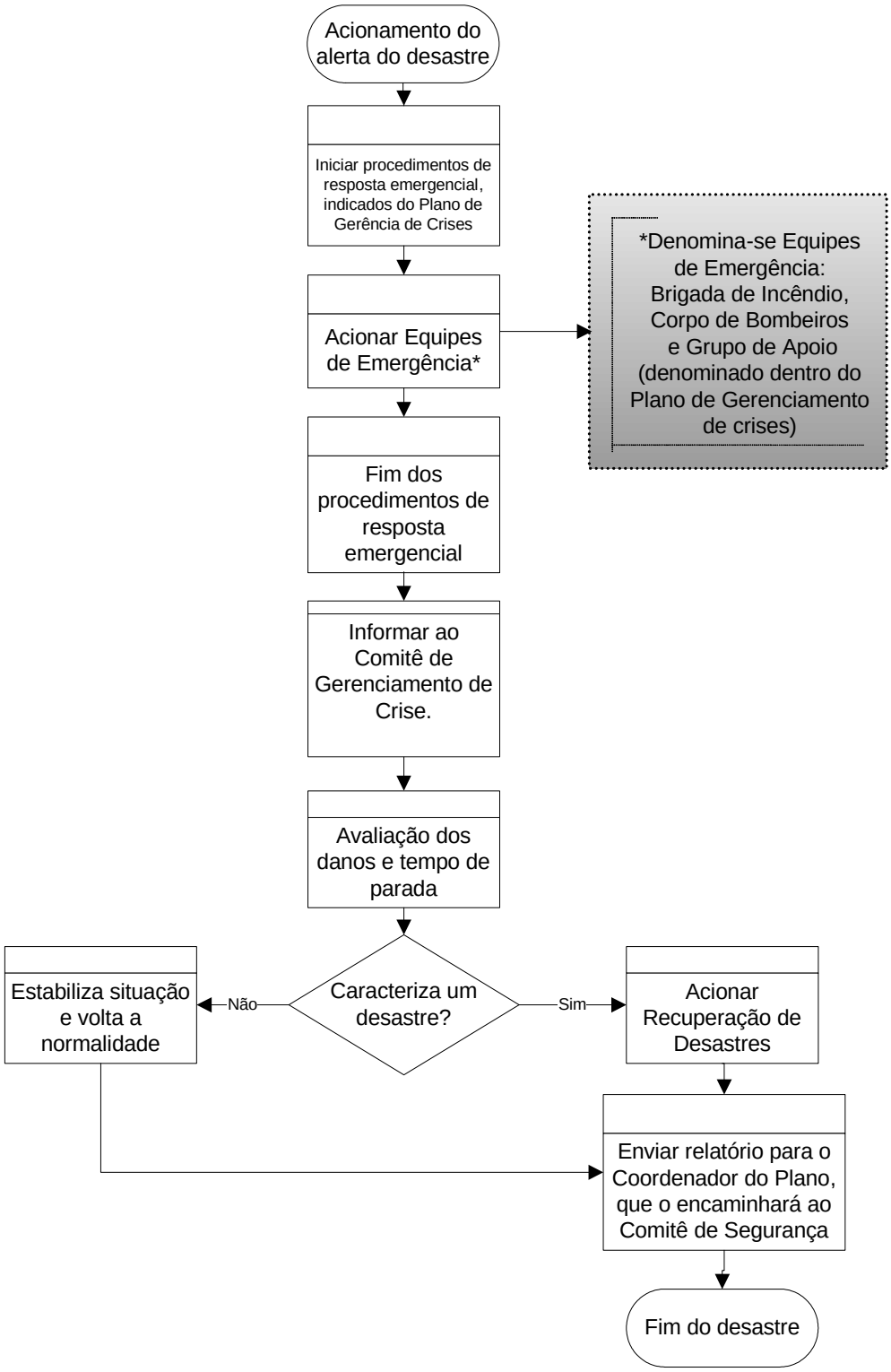
O Treinamento pode e deve ser feito utilizando-se todos os meios já disponíveis na organização. O envolvimento da área de treinamento da Organização e fundamental para que todos os funcionários, de alguma forma, sejam alcançados por esta etapa e assim venham a possuir informação sobre o Plano de Continuidade.

Uma vez que a equipe está treinada, é chegada a hora do Teste dos Planos, em especial dos Planos de Continuidade Operacional e Recuperação de Desastres onde os fatores tempo e recursos são sempre críticos. Temos vários tipos de testes possíveis. Estes testes podem ir desde a leitura em conjunto dos procedimentos (teste de mesa) de um grupo/equipe, até uma simulação completa envolvendo todos os funcionários.

Dos resultados dos testes e do treinamento obteremos dados para realizar uma atualização do PCN. Esta revisão deverá ser a primeira de uma série de atualizações que devem ser feitas enquanto a Organização existir. Um Plano de Continuidade sem atualização não será eficaz na hora de um evento de indisponibilidade. Esta atualização

poderá ser feita tanto para descrever um novo cenário instalado ou, simplesmente, para modificar, para melhor, um procedimento descrito.

# 7 Fluxograma de Acionamento do PCN



# 8 A Mais Importante Estratégia do PCN

"Sem uma solução de backup eficaz, não teremos continuidade de serviços"

O Plano de Continuidade tem sua sustentação básica composta pelos procedimentos de cópias de base de dados e a respectiva guarda destas cópias em local seguro.

Cada tipo de arquivo irá exigir um tipo de cópia. Entretanto, numa primeira abordagem, podemos distinguir entre dois tipos de arquivos: os arquivos de uso Corporativo e os arquivos de uso pessoal. Independente do tipo de arquivo, sua cópia e a respectiva armazenagem desta cópia é uma exigência do Plano de Continuidade, claro de acordo com a política de segurança estabelecida.

As cópias (backup's) de todas as bases de dados corporativas devem ser feitas com a freqüência que suas atualizações demandarem pela área gestora dos Recursos de Tecnologia de Informação.

A guarda deve ser feita em local seguro, com uma distância geográfica mínima que evite que problemas nas instalações tenham repercussão no local de guarda das cópias (ou vice-versa).

Baseado na importância dos backup's, pois guardam uma cópia fiel dos dados minutos, ou até segundos, antes de um desastre, foram criadas diversas estratégias para o seu armazenamento, que são:

- Estratégia de Contingência Hot-site – Recebe este nome por ser uma estratégia pronta para entrar em operação assim que uma situação de risco ocorrer. O tempo de operacionalização desta estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamento tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milessegundos de tolerância para garantir a disponibilidade do serviço mantido pelo equipamento.

- Estratégia de Contingência Warm-site – Esta se aplica a objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade, como exemplo, o serviço de e-mail dependente de uma conexão. Vemos que o processo de envio e recebimento de mensagens é mais tolerante que o exemplo usado na estratégia anterior, pois poderia ficar indisponível por minutos, sem, no entanto, comprometer o serviço ou gerar impactos significativos.

- Estratégia de Contingência Cold-site – Dentro da classificação nas estratégias anteriores, esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto, aplicável à situação com tolerância de indisponibilidade ainda maior, claro que esta estratégia foi analisada e aprovada pelos gestores.

- Estratégia de Contingência Datacenter – Considera a probabilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado; portanto, fora dos domínios da empresa. Por sua própria natureza, em que requer um tempo de indisponibilidade menor em função do tempo de reativação

operacional da atividade, torna-se restrita a poucas organizações, devido ao seu alto custo. O fato de ter suas informações manuseadas por terceiros e em um ambiente fora de seu controle, requer atenção na adoção de procedimentos, critérios e mecanismos de controle que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.

# 9 Conclusão

O Plano de Continuidade deve ser estruturado para responder a determinados desastres. Um Plano de Continuidade não é um Plano genérico para qualquer tipo de desastre. Antes de sua estruturação devem ser selecionados os que serão contemplados no Plano (A existência de um Plano de Continuidade para um determinado tipo de desastre, poderá vir a ser útil na resposta a um desastre cuja ocorrência não tenha sido considerada quando da estruturação do Plano. A existência de procedimentos previamente planejados e disseminados aumentará a capacidade de resposta da Organização a qualquer tipo de desastre).

Muito embora um dos produtos importantes da elaboração de um Plano de Continuidade de Negócios seja a sua documentação, ela por si só é ineficiente. A documentação visa registrar as premissas, os procedimentos e deverá somente servir de base para os treinamentos e orientações dos envolvidos, capacitando-os a operacionalizá-lo quando for necessário.

Lembrem-se “Plano de Continuidade de Negócios não é papel”.

# 10 Referências Bibliográficas


- Norma brasileira NBR ISO/IEC 17799-1:2001 – Código de Práticas para a Gestão da Segurança da Informação, tradução da norma internacional ISO/IEC 17799-1:2000;
- Norma britânica BS 7799-2:1999 – Specification for Information Security Management Systems;
- Norma internacional ISO/IEC 13554 “Code of Pratice for Information Security Management”;
- O Common Body of Knowledge e Professional Practices for Business Continuity Planners, do Disaster Recovery Institute International – DRI International (www.drii.org);
- Jon William Toigo, Disaster Recovery Planning: Strategies for Protecting Critical Information;
- James C. Barnes , A Guide to Business Continuity Planning;
- Documentos Microsoft Technet;