Capítulo

6

Estratégias de Contingência para Serviços de Tecnologia da Informação e Comunicação

Leonardo L. Fagundes[1], Fernando Karl[1], Luis Baptista[2] e Rafael Santos da Rosa[3]

Universidade do Vale do Rio dos Sinos – UNISINOS

[1]{llemes, fkarl}@unisinos.br; [2]luis_baptista@sicredi.com.br; [3]rsrosa@reno.unisinos.br

Abstract

The business continuity management is a process that identifies threats and their possible impacts. This process provides an appropriate structure for the organization to respond effectively in case of incidents. The purpose of this chapter is to present the theoretical and practical aspects of business continuity management with focus to the preparation disaster recovery plans.

Resumo

A gestão da continuidade de negócio é um processo de gestão que identifica ameaças e os seus possíveis impactos. Este processo fornece uma estrutura adequada para que a organização responda efetivamente em casos de incidentes. O objetivo desse curso é apresentar os aspectos teóricos e práticos da gestão da continuidade de negócio com foco para a elaboração dos planos de recuperação de desastres.

6.1. Introdução

Segundo as normas [ABNT 2008a] e [ABNT 2008b], a Gestão de Continuidade de Negócio (GCN) é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Portanto, a mesma atua de forma proativa na organização, a fim de melhorar a resiliência da organização contra ruptura ou interrupção de sua capacidade de fornecer seus produtos ou serviços.

De acordo com a [IBM Global Services 2010], a continuidade dos negócios é fundamental para o sucesso das empresas e devido à grande interdependência tecnológica atual dos processos de negócio, praticamente todos os aspectos da operação estão suscetíveis a falhas.

Conforme [Continuity Central 2010], para 32% das organizações, apenas quatro horas de tempo de inatividade podem ser fatais. Pode ser tomado, por exemplo, o incidente envolvendo a Nokia e a Ericsson. A interrupção do processo de produção da Ericsson, causada por falha de um fornecedor principal do seu processo produtivo, quase a tirou do mercado mundial de celulares. A Phillips, àquela época, era a principal fornecedora de microchips tanto para a Ericsson quanto para a Nokia, e quando ocorreu um incêndio na sua planta mexicana, houve avarias em praticamente todo o seu estoque.

Neste ponto, foi perceptível a diferença na maturidade das estratégias das duas empresas, quanto à continuidade dos seus negócios. Enquanto a Ericsson aceitou as estimativas otimistas da Phillips, que em poucos meses a produção estaria restabelecida, a Nokia foi à busca de outros fornecedores de microchips, inclusive alterando a tecnologia adotada em seus telefones, assim tornando-os compatíveis com os novos chips. Quando a Ericsson percebeu que não poderia mais ficar esperando o retorno do seu principal fornecedor, a Nokia já havia garantido a capacidade produtiva dos principais outros fabricantes mundiais. A falta de estratégia adequada para este desastre, aliada a falta de rapidez ao atuar sobre o mesmo, causou a Ericsson um grande prejuízo financeiro, como também uma grande perda de mercado, então assumido pela sua concorrente, a Nokia [Husdal 2008].

Em outros casos de desastres como aquele ocorrido no World Trade Center se observa situações ainda mais criticas, por exemplo, a empresa Cantor Fitzgerald perdeu com a queda de uma das torres 700 funcionários, talento e conhecimento referente aos seus processos, já com a queda da segunda torre essa mesma empresa perdeu todas as suas cópias de segurança e informações armazenadas, somente restando a esta empresa, a falência e a extinção.

Toda a organização está, com maior ou menor probabilidade, suscetível a interrupções das suas atividades críticas ocasionadas por ameaças tais como: falhas tecnológicas, enchentes, interrupções nos serviços públicos e atos de terrorismo. O objetivo desse capítulo é apresentar a Gestão da Continuidade como um aspecto de fundamental relevância para que uma organização possa responder de maneira eficiente aos cenários de incidentes e manter a continuidade dos serviços TI considerados críticos.

O capítulo em questão está estruturado conforme a descrição a seguir:

Seção 6.2: apresenta os diversos estágios do ciclo de vida da Gestão da Continuidade de Negócios, conforme as normas brasileiras [ABNT, 2008a] e [ABNT, 2008b];

Seção 6.3: descreve algumas das boas práticas internacionais empregadas para o desenvolvimento de estratégias de contingência em tecnologia da informação;

Seção 6.4: relata um estudo de caso, cujo objetivo é propiciar a reflexão e a aplicação dos conceitos e práticas apresentadas anteriormente no

desenvolvimento de estratégias de contingência para os serviços de tecnologia da informação e comunicação considerando uma companhia aérea fictícia;

Seção 6.5: encerra o capítulo a partir de um resgate dos objetivos propostos e da síntese dos principais aspectos apresentados ao longo do minicurso, com destaque para as questões relacionadas aos desafios da implementação e manutenção dos planos de recuperação de desastres.

6.2. Ciclo de Vida da Gestão de Continuidade de Negócios

Segundo Código de Prática para a Gestão de Continuidade de Negócios, NBR 15999 – Parte 1, o ciclo de vida da Gestão de Continuidade de Negócios segue a estrutura ilustrada Figura 6.1 [ABNT 2008a]:

Figura 6.1. Ciclo de Vida da Gestão da Continuidade de Negócios.

Este ciclo representa as etapas da Gestão de Continuidade de Negócios, em que se inicia pela Gestão do Programa de GCN, onde são designadas as responsabilidades e como será executada a gestão continua do programa. Contempla também a definição e requisitos de documentação que farão parte do programa.

Em entendendo a organização, é realizada a Análise de Impacto nos negócios (AIN/BIA) a identificação das atividades críticas, a determinação dos requisitos de continuidade, a análise de risco e definição de que ações serão tomadas quanto aos riscos identificados.

Já na etapa de determinando a estratégia de continuidade de negócios, são escolhidas as estratégias para as pessoas, instalações, tecnologia, informação e suprimentos que fazem parte do processo de negócio alvo da GCN.

Na etapa de desenvolvimento e implementação de uma resposta de GCN, é estruturada a Resposta a Incidentes e são criados os planos de Gerenciamento de Incidentes e o Plano de Continuidade de Negócios.

Em Testando, mantendo e analisando criticamente os preparativos de GCN, ocorre a validação dos testes e análises dos preparativos de GCN, Programa de Testes, a manutenção do programa, a análise crítica (auditoria interna), a Auditoria externa e o processo de auto-avaliação.

Na última etapa do ciclo de vida da GCN, Incluindo a GCN na cultura da organização, é onde são tratados os requisitos de treinamento e conscientização no que tange a GCN.

Antes de iniciar a descrição de cada um dos estágios do ciclo de vida é fundamental o entendimento de algumas definições adotadas pela ABNT NBR 15999-1 [ABNT 2008a]. A Figura 6.2 representa os principais intervalos de tempo considerados na gestão da continuidade de negócios.

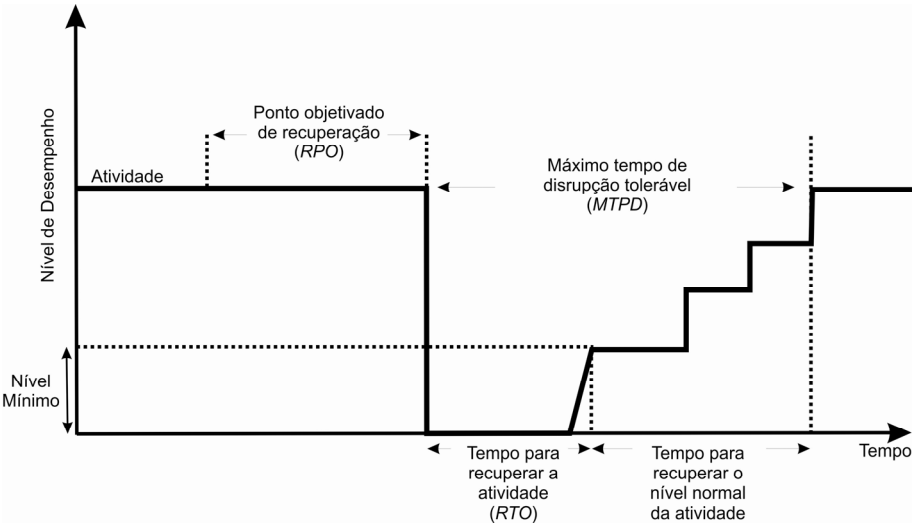

Figura 6.1. Representação dos tempos considerados em GCN.

- **Período máximo de interrupção tolerável (MTPD – maximum tolerable period of downtime)**

  Duração a partir da qual a viabilidade de uma organização será ameaçada de forma inevitável, caso a entrega de produtos e serviços não possa ser reiniciada.

- **Tempo objetivado de recuperação (RTO – recovery time objective)**

  Tempo alvo para: (a) retomada da entrega de produtos ou serviços após um incidente; ou (b) recuperação do desempenho de uma atividade após um incidente; ou ainda (c) recuperação de um sistema ou aplicação de TI após um incidente.

- **Ponto objetivado de recuperação (RPO – recovery point objective)**

  Posição (no tempo) na qual deverão estar disponíveis os dados das Aplicações recuperadas após a ocorrência de um desastre. O RPO está diretamente relacionado ao processo e freqüência de geração de cópias de segurança

6.2.1. Gestão do Programa de GCN

A gestão do programa de GCN é a estrutura principal de um processo de GCN. Na gestão do programa que é estabelecida a abordagem que a organização terá em relação à continuidade de negócios.

Importante observar a importância da participação da alta direção na introdução da GCN na cultura organizacional. Na gestão do programa, objetivando atender a Política de Gestão de Continuidade de Negócios, são desenvolvidas as seguintes etapas:

- **A atribuição de responsabilidades;**

  Nesta etapa, a direção da empresa necessita designar uma pessoa com a senioridade e autoridade necessárias para ser responsável pela política de GCN e a sua implementação.

  Também é necessário que se aponte um ou mais indivíduos para implementar e manter o programa de GCN. Assim formando a equipe de GCN da organização. Importante observar que na criação desta equipe, podem-se nomear representantes de outras áreas e/ou níveis de negócio para apoiar a implementação da GCN.

- **A implementação da continuidade de negócios na organização;**

  Na fase de implementação, é importante que contemplem o planejamento, o desenvolvimento e implementação do programa.

  Durante a implementação, deve-se prever a comunicação do programa às partes interessadas, organizar e fornecer treinamento apropriado a equipe, e realizar testes da capacidade de Continuidade de negócios da Organização.

  Para apoiar a etapa de implementação, a organização pode utilizar uma metodologia de gerenciamento de projetos reconhecida para garantir uma implementação efetiva.

- **A gestão contínua da continuidade de negócios.**

  Na etapa da gestão contínua, convém seja assegurada a incorporação da GCN na cultura da organização. Como também se prevê o mantenimento dos componentes da Continuidade de negócios, como também a análise crítica e atualização dos planos e soluções de continuidade de negócios.

  Importante observar algumas atividades que impreterivelmente fará parte da gestão contínua da GCN:
  - A definição de escopo, papéis e responsabilidades
  - A nomeação de uma pessoa ou equipe responsável pela GCN
  - Manter o programa de GCN atualizado.
  - A promoção da GCN por toda a organização
  - A administração do programa de testes.
  - Manter atualizadas as avaliações de risco e de impacto nos negócios
  - Manter atualizada a documentação do programa de GCN.
  - Monitorar o desempenho da capacidade de continuidade de negócios.
  - Gerência sobre os custos, frente à capacidade de continuidade da organização.

- Estabelecer e monitorar o gerenciamento de mudanças e o regime de sucessão.

- **A documentação da continuidade de negócios.**

  Convém para a manutenção da Gestão da Continuidade de Negócios, não se limitando a esta lista, a criação e atualização contínua da seguinte documentação:
  - A política de GCN
  - A análise de impacto nos negócios
  - A avaliação de riscos e ameaças
  - As estratégias de GCN
  - Programa de Conscientização e Treinamento
  - Plano de gerenciamento de incidentes
  - Planos de continuidade e recuperação de negócios
  - Agenda de testes
  - Contratos e acordos de níveis de serviço

6.2.2. Entendendo a organização

Para a continuidade de negócios, o entendimento da organização é provido por:

- Identificar os objetivos da organização, a obrigação das partes interessadas, deveres legais e o ambiente no qual a organização opera.
- Identificar as atividades, ativos e recursos, internos e externos, que suportam a entrega desses produtos e serviços. É importante a identificação das atividades críticas para a organização, como também a sua categorização quanto a prioridades de recuperação. Também é importante a determinação dos requisitos de continuidade que cada atividade necessitará.
- Avaliar o impacto e as conseqüências sobre o tempo de falhas sobre estas atividades, ativos e recursos. Nesta etapa, é importante definir o tempo máximo de interrupção tolerável de cada atividade, o nível mínimo no qual a atividade deve ser desempenhada após o seu reinício e o tempo máximo até a retomada dos níveis normais de operação.
- Identificar e avaliar as ameaças que possam interromper os produtos e serviços fundamentais e os ativos, atividades e recursos que os suportam.

Com o resultado da análise de impactos e da análise de riscos, cabe a organização decidir quais escolhas ela adotará para cada cenário identificado. Estas estratégias visam: ou reduzir a chance de uma interrupção, ou diminuir o tempo de uma interrupção, ou limitem o impacto de uma interrupção em produtos ou serviços na organização. Dentre as escolhas a serem adotadas, cabem:

- **Continuidade de negócios:** neste caso, serão adotadas ações que visem garantir a continuidade da atividade em caso de indisponibilidade, atendendo aos tempos levantados na análise de impacto;

- **Aceitação:** um risco identificado, pode de toda forma, ser tido como aceitável pela organização. Então, por uma decisão da direção, o mesmo pode ser tido como aceito;
- **Transferência:** ocorre, para alguns casos, que a melhor estratégia é transferi-los, sendo por meio de seguros ou acordos contratuais;
- **Mudar, suspender ou terminar:** em dadas circunstancias, devido a um risco identificado, e o beneficio adquirido com a atividade, a Direção pode decidir por terminar a atividade.

É relevante observar a importância da aprovação da direção da relação de atividades relacionadas, seus riscos, e as estratégias adotadas. Visando garantir que o trabalho realizado reflete verdadeiramente a realidade da organização.

6.2.3. Determinando a estratégia de continuidade de negócios

A seleção da estratégia de contingência mais adequada para cada situação é uma questão complexa e que exige uma análise detalhada que considere os requisitos técnicos e de negócio [Wiboonrat 2008] e [Cegiela 2006]. Convém que a abordagem da organização para determinar suas estratégias de GCN:

- Implemente medidas apropriadas, de forma a reduzir a probabilidade de ocorrência de incidentes e/ou reduzir os potenciais efeitos destes incidentes;
- Mantenha um registro das medidas de resiliência e mitigação;
- Forneça continuidade para as atividades críticas durante e após um incidente; e
- Mantenha um registro das atividades classificadas como não críticas.

Quanto à definição das opções de estratégias, convém que sejam considerados uma série de fatores, dentre os quais: (1) o período máximo de interrupção tolerável da atividade crítica, (2) os custos de implementação de uma ou mais estratégias e (3) as consequências da falta de ação. Convém que sejam elaboradas estratégias de contingência para todos os recursos da organização, o que inclui além dos aspectos tecnológicos, as pessoas, os suprimentos, as instalações, as informações e as demais partes interessadas.

Para organizações que buscam definir, implementar ou validar suas estratégias de gerenciamento de incidentes e gestão de continuidade de negócios é um fator critico de sucesso a interação com as autoridades responsáveis por responder às emergências. Estas autoridades serão fundamentais para a declaração oficial de que ocorreu uma emergência civil, além de fornecer:

- Ajuda pré ou pós-incidente;
- Procedimentos de aviso e informação; e
- Acordos de recuperação comunitária após uma emergência civil.

6.2.4. Desenvolvimento e implementação de uma resposta de GCN

Este elemento do ciclo de vida de GCN é relacionado ao desenvolvimento e implementação dos planos apropriados e dos preparativos realizados, de forma a garantir a continuidade das atividades críticas e o gerenciamento dos incidentes. Durante esta fase, convém que a organização:

- Identifique suas atividades críticas
- Avalie as ameaças a estas atividades críticas
- Escolha estratégias apropriadas que diminuam a probabilidade e os impactos dos incidentes; e
- Escolha estratégias apropriadas que permitam a continuidade ou recuperação de suas atividades críticas.

Quanto à estrutura de resposta a incidentes, convém que a organização defina uma estratégia de resposta a incidentes,com uma determinada estrutura que permita, quando da ocorrência de um incidente:

- Confirmar a natureza e extensão do incidente;
- Tomar controle da situação;
- Controlar o incidente;
- Comunicar-se com as partes interessadas

Quanto ao conteúdo dos planos, convém que todos eles, sejam de gerenciamento de incidentes, continuidade de negócios ou recuperação de negócios, sejam concisos e acessíveis àqueles que possuam responsabilidades definidas nesses planos. Quanto à estruturação dos planos, convém que contenham:

- Objetivo e escopo;
- Papéis e responsabilidades definidas
- Procedimentos de ativação dos planos;
- Detalhes de contato;

Convém que a organização nomeie o principal responsável por cada plano, e identifique e documente os responsáveis pela análise crítica, correção e atualização dos planos em intervalos regulares. Quanto aos tipos de planos, esses podem ser:

- **Plano de gerenciamento de Incidentes (PGI)**

O propósito de um PGI é permitir que a organização gerencie a fase inicial (crítica) de um incidente. Convém que o conteúdo do PGI contenha:

  - Lista de tarefas e ações
  - Contatos de emergência

- Atividade das pessoas
- Comunicação à mídia
- Gestão de partes interessadas
- Localização para o gerenciamento de incidentes
- Anexos relevantes (Plantas, mapas, planos de acesso ao local, etc.)

- **Plano de Continuidade de Negócios (PCN)**

O propósito de um PCN é permitir que a organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócio. Os PCNs são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização. Eles podem ser executados integral ou parcialmente e em qualquer etapa da resposta a um incidente. Convém que o conteúdo do PCN contenha:

- Plano de ação / Lista de tarefas
- Recursos necessários
- Responsáveis
- Formulários e anexos

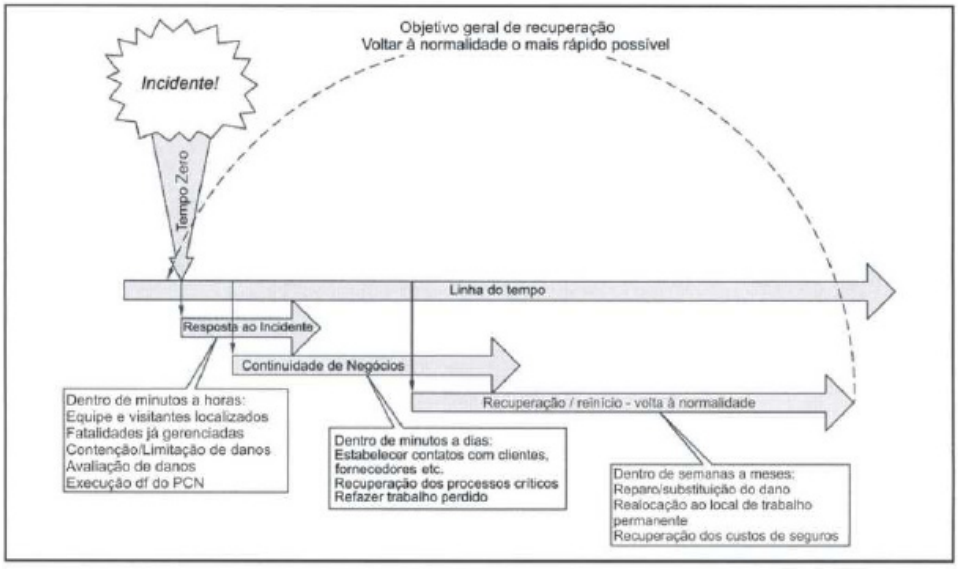

Figura 6.2. Linha do tempo do incidente, e a relação entre a ativação dos planos de gerenciamento de incidentes, continuidade de negócios e recuperação de negócios.

A Figura 6.3 ilustra a sequência em que as ações (planos) são executadas após a ocorrência de um incidente que compromete a continuidade de uma operação e/ou serviço crítico. É importante salientar que devem existir regras bem definidas para a a avaliação do incidente e a ativação dos planos.

6.2.5. Testando, mantendo e analisando criticamente os preparativos de GCN

Os preparativos de continuidade de negócios e de gerenciamento de incidentes da organização não podem ser considerados confiáveis até serem testados e apenas se estiverem atualizados. Portanto, convém que os preparativos sejam verificados por meio de testes, auditoria e processos de auto-avaliação, de forma a garantir que estejam adequados. Para garantir a obtenção destes objetivos, convém que:

- Seja instituído um programa de testes, partindo dos testes de mesa, até testes completos da solução de continuidade de negócios;
- Seja instituído um programa de manutenção do GCN, visando garantir que, quaisquer mudanças, internas ou externas, que causem um impacto à organização, sejam analisadas criticamente quanto a GCN;
- A alta direção, nos intervalos que considerar apropriados, analise criticamente a capacidade de GCN da organização, de forma a garantir sua aplicabilidade, adequação e funcionalidade;
- A organização providencie uma auditoria independente para avaliar a sua competência de GCN e a sua capacidade de identificar falhas reais e potenciais;
- Um processo de auto-avaliação seja instituído objetivando garantir que a organização tenha competência e capacidade de GCN sólidas, eficazes e adequadas.

A Tabela 6.1 representa os métodos de testes aplicáveis a fim de avaliar e identificar oportunidades de melhorias das estratégias de contingência.

Tabela 6.1. Tipos e métodos de teste de estratégias de GCN.

Complexidade	Teste	Processo	Variações	Freqüência recomendada [a]
Simples	Testes-de-mesa	Análise crítica/correção Questionar conteúdo do PCN	Atualização/Validação Auditoria/Verificação	Ao menos anualmente Anualmente
	"Walk-through" (repassar os passos) do plano	Questionar o conteúdo do PCN	Incluir interação e validar papéis dos participantes	Anualmente
Médio	Simulação	Usar situação "artificial" para validar se os PCN possuem as informações necessárias e suficientes, de forma a permitir uma recuperação com sucesso	Incorporar planos associados	Anualmente ou duas vezes ao ano
	Testar atividades críticas	Execução em ambiente controlado que não prejudique o andamento normal dos negócios	Executar algumas operações a partir de um local alternativo por um tempo determinado	Anualmente ou menos
Complexo	Testar todo o PCN, incluindo o gerenciamento de incidentes	Teste que envolve todo o prédio/campus/zona de exclusão		Anualmente

[a] Convém que a freqüência dos testes dependa das necessidades da organização, do ambiente no qual ela opera e das necessidades das partes interessadas. Porém, convém que o programa de testes seja flexível, levando em conta a freqüência de ocorrência de mudanças na organização e o resultado dos testes anteriores. Os métodos de teste acima podem ser empregados para cada componente de um plano ou para um ou mais planos.

6.2.6. Incluindo a GCN na cultura da organização

Para obter sucesso, a continuidade de negócios precisa se tornar parte da gestão da organização, independente de seu tamanho ou setor. O desenvolvimento, promoção e incorporação da cultura de GCN na organização garantem que a GCN se tornará parte dos valores básicos e da gestão da organização.

Convém que a organização possua um processo para identificar e implementar os requisitos de treinamento de GCN e para avaliar a eficácia desta implementação.

6.2.6.1 Conscientização

Convém que a organização crie, aumente e mantenha uma consciência por meio da educação permanente em GCN e de um programa de informações para toda a equipe. Este programa deve incluir:

- Um processo de consulta junto a toda equipe sobre a implementação do programa de GCN;
- Discussão de GCN nos informativos, apresentações, programas ou relatórios diários da organização;
- Inclusão da GCN nas paginas pertinentes da web ou da intranet;
- Aprendizado por meio de incidentes internos e externos;

- GCN como um tópico nas reuniões de equipe;
- Testes de planos de continuidade em locais alternativos, por exemplo, um local de recuperação; e
- Visita a esses locais alternativos.

A organização deve estender seu programa de conscientização de GCN para seus fornecedores e outras partes interessadas.

6.2.6.2 Treinamento

Convém que a organização treine a equipe de GCN para tarefas como:

- Gestão do programa de GCN
- Execução de uma análise de impacto nos negócios
- Desenvolvimento e implementação de PCN
- Execução de um programa de testes de PCN
- Avaliação de riscos e ameaças
- Comunicação com a mídia

Além da equipe de GCN o pessoal não relacionado diretamente a GCN, mas que tenha algum papel definido no processo de GCN também deve ser treinado, pois isso pode representar o sucesso ou fracasso no momento da execução dos planos [Wei 2009].

6.3. Boas Práticas

Essa seção apresenta um conjunto de boas práticas relacionadas com a gestão da continuidade de negócios e de maneira mais especifica com as estratégias de contingência de TI, também denominados de planos de recuperação de desastres.

6.3.1. Disaster Recovery International Institute (DRII)

As práticas profissionais recomendadas pelo DRII – Disaster Recovery International Institute, ilustradas da Figura 6.4, para atuação em Gestão de Continuidade de negócios são distribuídas em dez aspectos [DRII 2010]:

Figura 6.4. As 10 Práticas Profissionais do Disaster Recovery Internacional Institute (DRII)

Inicio e Gestão do Programa

São definidos os requisitos de continuidade, obtidos apoio da alta direção quanto ao programa e definição de papéis e responsabilidades.

Avaliação de riscos e controles

Nesta etapa, são identificados os riscos levantados junto às pessoas, instalações e tecnologias do escopo, identificação de perdas potenciais e definição de controles a serem aplicados.

Análise de Impacto nos Negócios (AIN / BIA)

Identificação dos impactos resultantes de interrupções de negócio, e técnicas que podem ser usadas para quantificar e qualificar esses impactos. Definição também de tempos críticos, prioridades de recuperação e interdependências.

Estratégias de continuidade de negócios

Apoiado pelos resultados da AIN/BIA e da análise de riscos e controles, recomendar estratégias de continuidade de negócios.

Preparação e Resposta a emergência

Preparar um estado de prontidão para a organização para responder a uma emergência de forma coordenada e eficaz.

Planos de continuidade de negócios

Projetar, desenvolver e implementar Planos de Continuidade de Negócios.

Programas de sensibilização e formação

Preparar um programa para criar a consciência referente à GCN.

Exercício, auditoria e Manutenção dos Planos de Continuidade de Negócios

Estabelece o plano de exercícios e testes dos PCN's, e estabelece também os procedimentos de auditoria do programa e planos de continuidade de negócios.

Comunicação de Crises

Desenvolve os planos de ação para comunicação com as partes interessadas para garantir a clareza das informações na comunicação das crises.

Coordenação com Agências Externas

Estabelecer procedimentos e políticas para a coordenação e continuidade das atividades de restauração com agências externas.

6.3.2. Business Continuity Institute (BCI)

A Figura 6.5 ilustra o ciclo de vida da gestão de continuidade de negócios segundo o *Business Continuity Institute* [BCI 2010].

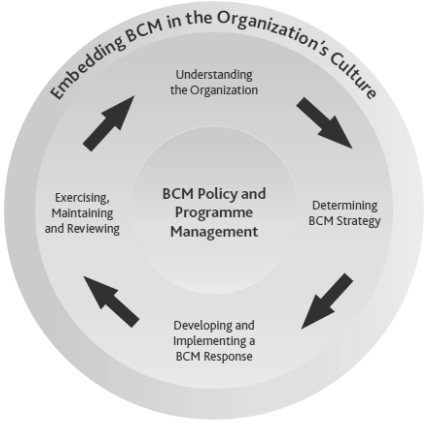

Figura 6.5. Ciclo de Vida da Gestão de Continuidade de Negócios

Gestão da Política e do Programa

A política de GCN é o documento chave que define o escopo e a governança do programa de GCN, e reflete os motivos pelos quais a GCN está sendo implementada. Ela fornece o contexto em que os recursos solicitados serão implementados, e identifica os princípios aos quais a organização aspira e contra os quais seu desempenho pode ser auditado.

Incorporando a GCN na Cultura da Organização

A criação bem sucedida da cultura de GCN da organização depende da sua integração com o planejamento estratégico da organização, bem como o seu alinhamento com as prioridades de negócios.

Entendendo a Organização

Prática profissional dentro do Ciclo de Vida da GCN que analisa a organização em termos de quais seus objetivos, como estrutura funcional e os obstáculos do ambiente em que opera. As informações coletadas tornam possível determinar a melhor forma de preparar uma organização para ser capaz de gerenciar as suas interrupções.

Determinando a Estratégia de Continuidade de Negócios

Prática profissional dentro do ciclo de vida do BCM que determina quais as estratégias que vão ao encontro da política de GCN e exigências organizacionais e seleciona respostas tácticas dentre as opções disponíveis.

Desenvolvimento e Implementando uma Resposta de GCN

Essa é a prática profissional que implementa estratégias de acordo com o processo de desenvolvimento de um conjunto de planos de continuidade de negócios.

Exercitando, mantendo e revisando a GCN

"Exercitando, mantendo e revisando a GCN" é a prática profissional no âmbito do Ciclo de Vida da GCN, que visa assegurar que a melhoria contínua é alcançada através das ações em curso. As atividades realizadas nesta seção serão apoiadas pela política de BCM.

6.3.3. Gerenciamento dos Serviços de TI

A norma denominada ISO 20000 [ABNT 2008c] descreve, entre outros aspectos, a importância do gerenciamento da continuidade e da disponibilidade dos serviços de TI que oferecem suporte ao negócio. Por ser focada em tecnologia, essa norma agrega conceitos práticos refere a TI que devem ser considerados ao elaborar os planos de recuperação de desastres, tais como:

- Avaliação do acordo de nível de serviço quando da definição dos Planos de continuidade;
- A importância de uma série de testes dos planos, após grandes mudanças no ambiente de TI;
- A análise de impacto que qualquer mudança no ambiente de TI pode acarretar na disponibilidade dos serviços prestados;

A Figura 6.6 ilustra a estrutura do processo de gerenciamento dos serviços de TI. A norma em questão destaca que eventos inesperados que tenham impactado na disponibilidade dos serviços devem ser investigados, e ações adequadas devem ser tomadas. Com isto, busca-se a excelência operacional de serviços, mantendo-os disponíveis aos clientes com a qualidade requerida.

A norma ISO 20000 ressalta que os planos de continuidade de serviço, lista de contatos e a base de dados de gerenciamento devem estar disponíveis quando da ocorrência de uma indisponibilidade para que os planos de ação possam ser colocados em execução.

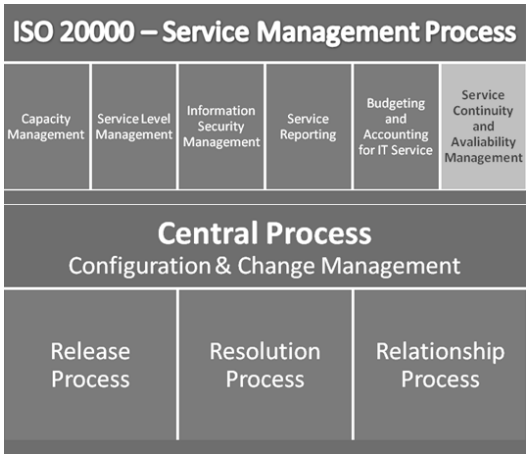

Figura 6.6. Processos e serviços representados pela ISO 20000.

6.3.4. Código de Prática para a Gestão da Segurança da Informação

A norma denominada ABNT NBR ISO/IEC 27002, cujo objetivo é estabelecer diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão da segurança da informação em uma organização define o seguinte objetivo de controle no que tange a gestão da continuidade do negócio: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra defeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso [ABNT 2005].

Para tal, são definidos controles para (1) incluir a segurança da informação no processo de gestão da continuidade de negócio, (2) identificar eventos de risco que possam causar interrupções aos processos de negócio, (3) desenvolver e implementar planos de continuidade relativos à segurança da informação, (4) garantir a consistência dos planos e (5) para testar e analisar criticamente os planos de continuidade do negócio.

6.3.5. COBIT

O *Control Objectives for Information and related Technology* (COBIT) é um conjunto de boas práticas para o gerenciamento da tecnologia da informação criado pela *Information Systems Audit and Control Association* (ISACA) e pelo IT Governance Institute (ITGI) em 1996 [IT Governance Institute 2008a].

O COBIT está organizado em quatro domínios, sendo que conforme a Figura 6.7 um desses domínios possui objetivos de controle voltados para assegurar a continuidade dos serviços.

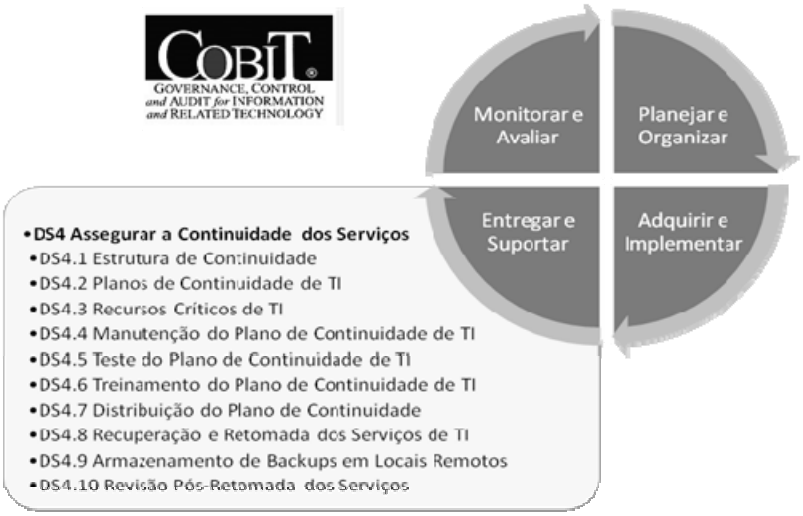

Figura 1.7. COBIT – Controles e Objetivos em Tecnologia da Informação

A seguir a descrição de cada um dos objetivos de controle que possuem relação com a continuidade dos serviços de TI.

Estrutura de Continuidade

Desenvolver um modelo para continuidade de TI a fim de apoiar o gerenciamento da continuidade do negócio de toda a empresa através de um processo consistente orientado a estrutura organizacional quanto ao gerenciamento da continuidade, contemplando papéis, tarefas e responsabilidades dos provedores de serviço internos e externos, seus gerenciamentos, clientes e as regras e estruturas para documentar, testar e executar planos de recuperação de desastres e continuidade de TI

Planos de Continuidade de TI

Desenvolver planos de continuidade de TI com base na estrutura e projetados para reduzir o impacto de uma grande interrupção de funções e processos de negócio fundamentais.

Recursos Críticos de TI

Dar atenção especial aos itens mais críticos no plano de continuidade de TI para assegurar a capacidade de restabelecimento e definir prioridades em situações de recuperação. Prevenir o desvio de atenção para os itens de recuperação menos críticos e assegurar resposta e recuperação em alinhamento com as necessidades de negócio de maior importância; ao mesmo tempo, assegurar que os custos sejam mantidos em um nível aceitável e em conformidade com os requisitos contratuais e regulamentares.

Manutenção do Plano de Continuidade de TI

Encorajar o gerenciamento de TI a definir e executar procedimentos de controle de mudança para assegurar que o plano de continuidade de TI seja mantido atualizado e reflita sempre os requisitos de negócios atuais.

Teste do Plano de Continuidade de TI

Testar o plano de continuidade de TI regularmente para assegurar que os sistemas de TI possam ser efetivamente recuperados, que desvios sejam tratados e que o plano se mantenha relevante. Para tanto, são necessários preparação cuidadosa, documentação, registro dos resultados dos testes e implementação de planos de ação de acordo com os resultados.

Treinamento do Plano de Continuidade de TI

Assegurar que todas as partes envolvidas recebam treinamento regular sobre os procedimentos, papéis e respectivas responsabilidades no caso de um incidente ou desastre. Verificar e intensificar o treinamento de acordo com os resultados dos teste de continuidade.

Distribuição do Plano de Continuidade

Definir e gerenciar uma estratégia de distribuição para assegurar que os planos sejam seguramente distribuídos e que estejam apropriadamente disponíveis às partes interessadas e autorizados quando e onde necessário. Toda atenção deve ser dispensada para tornar o plano acessível em todos os cenários de desastre.

Recuperação e Retomada dos Serviços de TI

Planejar as ações a serem executadas nos momentos de recuperação e retomada dos serviços de TI. Isto pode incluir ativação de backup sites, iniciação de processamento alternativo, comunicação para as partes interessadas e os clientes, procedimentos de retorno à produção etc. Assegurar que o negócio entenda o tempo de recuperação de TI e os investimentos tecnológicos necessários para sustentar as necessidades de recuperação e retorno à produção.

Armazenamento de Backups em Locais Remotos

Armazenar remotamente todas as mídias de cópias de segurança críticas, documentação e outros recursos de TI necessários para a recuperação da TI e os planos de continuidade de negócio. O conteúdo armazenado nas cópias de segurança precisa ser determinado em colaboração entre os proprietários dos processos de negócio e o pessoal de TI. Assegurar a compatibilidade de hardware e software para restaurar os dados arquivados e testar e atualizar periodicamente os dados arquivados

Revisão Pós-Retomada dos Serviços

Após a retomada bem-sucedida da função de TI depois de um desastre, determinar se o gerenciamento de TI tem procedimentos para avaliar a adequação do plano atual e realizar sua atualização, se necessário.

Importante observar que o COBIT, além das recomendações alinhadas com as demais boas práticas, apresenta recursos de governança até então não adotadas pelas demais. Dentre elas, podemos citar a proposta de matriz de responsabilidade (Figura 6.8) incluída na versão 4.1 do COBIT.

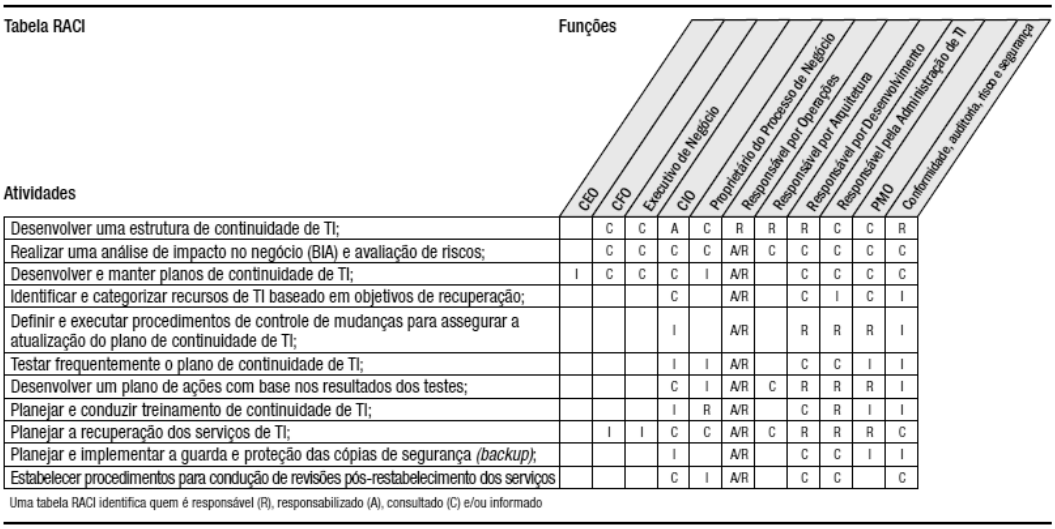

Tabela RACI

Atividades \ Funções	CEO	CFO	Executivo de Negócio	CIO	Proprietário do Processo de Negócio	Responsável por Operações	Responsável por Arquitetura	Responsável por Desenvolvimento	Responsável pela Administração de TI	PMO	Conformidade, auditoria, risco e segurança
Desenvolver uma estrutura de continuidade de TI;		C	C	A	C	R	R	R	C	C	R
Realizar uma análise de impacto no negócio (BIA) e avaliação de riscos;		C	C	C	C	A/R	C	C	C	C	C
Desenvolver e manter planos de continuidade de TI;	I	C	C	C	I	A/R		C	C	C	C
Identificar e categorizar recursos de TI baseado em objetivos de recuperação;				C		A/R		C	I	C	I
Definir e executar procedimentos de controle de mudanças para assegurar a atualização do plano de continuidade de TI;				I		A/R		R	R	R	I
Testar frequentemente o plano de continuidade de TI;				I	I	A/R		C	C	I	I
Desenvolver um plano de ações com base nos resultados dos testes;				C	I	A/R	C	R	R	R	I
Planejar e conduzir treinamento de continuidade de TI;				I	R	A/R		C	R	I	I
Planejar a recuperação dos serviços de TI;		I	I	C	C	A/R	C	R	R	R	C
Planejar e implementar a guarda e proteção das cópias de segurança *(backup)*;				I		A/R		C	C	I	I
Estabelecer procedimentos para condução de revisões pós-restabelecimento dos serviços				C	I	A/R		C	C		C

Uma tabela RACI identifica quem é responsável (R), responsabilizado (A), consultado (C) e/ou informado

Figura 6.8. Matriz de Responsabilidade (RACI)

Outra abordagem trazida pelo COBIT é apresentação de um modelo de maturidade, em que o processo de continuidade de serviço de TI pode ser comparado e avaliado, conforme os níveis de maturidade descritos na Tabela 6.2.

Tabela 6.2. Modelo de Maturidade para Continuidade de serviços conforme o COBIT.

Nível	Descrição
Inexistente	Não há entendimento dos riscos, vulnerabilidades e ameaças às operações de TI ou do impacto da perda dos serviços de TI nos negócios. Não é considerado que a continuidade dos serviços deve ter atenção da Direção.
Inicial /*Ad hoc*	As responsabilidades pela continuidade dos serviços são informais e a autoridade para exercer essas responsabilidades é limitada. O gerenciamento está se tornando consciente dos riscos relacionados e da necessidade da continuidade dos serviços. O foco da Direção quanto à continuidade dos serviços está relacionado aos recursos de infra-estrutura e não aos serviços de TI. Os usuários implementam paliativos em resposta a interrupções nos serviços. A resposta da TI para a maioria das interrupções é reativa e despreparada. Paralisações dos sistemas são agendadas para atender às necessidades da TI, porém não consideram os requisitos do negócio.
Repetível, porém Intuitivo	A responsabilidade de assegurar a continuidade do serviço é estabelecida. As abordagens para assegurar a continuidade do serviço são fragmentadas. Relatórios de disponibilidade de sistema são esporádicos, podem ser incompletos e não levam em consideração o impacto nos negócios. Não existe um plano de continuidade de TI documentado, embora haja comprometimento da continuidade da disponibilidade de serviços e seus maiores princípios sejam conhecidos.

	Existe um inventário de sistemas e componentes críticos, mas ele pode não ser confiável. Práticas de serviços contínuos estão surgindo, contudo o sucesso depende das pessoas.
Processo Definido	A responsabilidade solidária pelo gerenciamento da continuidade dos serviços está clara. A responsabilidade pelo planejamento e pelos testes da continuidade dos serviços é claramente definida e atribuída. O plano de continuidade de TI é documentado e baseia-se na importância do sistema e no impacto nos negócios. Há relatos periódicos dos testes de continuidade de serviços. As pessoas tomam a iniciativa de seguir padrões e recebem treinamento para lidar com a maioria dos incidentes ou desastres. A Direção comunica consistentemente a necessidade do plano de assegurar a continuidade de serviço. Componentes de alta disponibilidade e redundância de sistema estão sendo aplicados. É mantido um inventário sobre os componentes e sistemas críticos.
Gerenciado e Mensurável	As responsabilidades e os padrões para a continuidade dos serviços são impostos. A responsabilidade por manter o plano de continuidade de serviço é atribuída. As atividades de manutenção são baseadas nos testes de continuidade de serviço, em boas práticas internas, e na mudança do ambiente de negócio e de TI. Dados estruturados sobre a continuidade dos serviços estão sendo coletados, analisados, relatados e gerando ações. É dado treinamento obrigatório e formal sobre os processos de continuidade de serviço. Boas práticas de disponibilidade de sistemas estão sendo consistentemente implementadas. As práticas de disponibilidade e planejamento de continuidade de serviços influenciam um ao outro. Os incidentes de descontinuidade são classificados e os procedimentos de encaminhamento de cada incidente é bem conhecido por todos os envolvidos. Objetivos e métricas de continuidade dos serviços foram desenvolvidos e acordados, mas podem ser inconsistentemente medidos.
Otimizado	Processos integrados de continuidade de serviços consideram a comparação com o mercado *(benchmarking)* e as melhores práticas externas. O plano de continuidade de TI é integrado ao plano de continuidade de negócio e é rotineiramente mantido. A necessidade de assegurar a continuidade de serviços é garantida pelos fornecedores e principais prestadores de serviço. Ocorrem testes formais do plano de continuidade de TI, e seus resultados são a base da atualização do plano. Coleta e análise dos dados são utilizados para melhoria contínua do processo. O planejamento de continuidade de serviço e as práticas de disponibilidade

	estão completamente alinhados. A Direção assegura que um desastre ou incidente importante não ocorrerá devido a um único ponto de falha. Práticas de encaminhamento são entendidas e rigorosamente impostas. Os objetivos e métricas sobre o alcance da continuidade de serviços são mensurados de forma sistemática. A Direção ajusta o planejamento à continuidade do serviço em resposta às medições

6.3.6. Alinhamento entre Boas Práticas

As organizações adotam diferentes modelos, padrões e normas para orientar o seu processo de gestão de segurança e de tecnologia da informação. As boas práticas discutidas na seção anterior representam o que convém que seja implementado (COBIT e ISO 27002) e os processos que oferecem suporte e orientação para a definição de como pode se dar a aplicação dos objetivos de controles.

Tabela 6.3. Consolidação das boas práticas na Gestão de Continuidade de Negócios.

CobiT 4.1	ITIL V3	ISO/IEC 27002:2005
DS4.1 IT continuity framework	SD 4.5 IT service continuity management	6.1.6 Contact with authorities
	SD 4.5.5.1 Stage 1—Initiation	6.1.7 Contact with special interest groups
	CSI 5.6.3 IT Service continuity management	14.1.1 Including information security in the business continuity management process
		14.1.2 Business continuity and risk assessment
		14.1.4 Business continuity planning framework
DS4.2 IT continuity plans	SD 4.5.5.2 Stage 2—Requirements and strategy	6.1.6 Contact with authorities
	SD 4.5.5.3 Stage 3—Implementation	6.1.7 Contact with special interest groups
	SD App K The typical contents of a recovery plan	14.1.3 Developing and implementing continuity plans including information security
DS4.3 Critical IT resources	SD 4.4.5.2 The proactive activities of availability management	14.1.1 Including information security in the business continuity management process
	SD 4.5.5.4 Stage 4—Ongoing operation	14.1.2 Business continuity and risk assessment
DS4.4 Maintenance of the IT continuity plan	SD 4.5.5.4 Stage 4—Ongoing operation	14.1.5 Testing, maintaining and reassessing business continuity plans
DS4.5 Testing of the IT continuity plan	SD 4.5.5.3 Stage 3—Implementation	14.1.5 Testing, maintaining and reassessing business continuity plans
	SD 4.5.5.4 Stage 4—Ongoing operation	
DS4.6 IT continuity plan training	SD 4.5.5.3 Stage 3—Implementation	14.1.5 Testing, maintaining and reassessing business continuity plans
	SD 4.5.5.4 Stage 4—Ongoing operation	

DS4.7 Distribution of the IT continuity plan	SD 4.5.5.3 Stage 3—Implementation	14.1.5 Testing, maintaining and reassessing business continuity plans
	SD 4.5.5.4 Stage 4—Ongoing operation	
DS4.8 IT services recovery and resumption	SD 4.4.5.2 The proactive activities of availability management	14.1.1 Including information security in the business continuity management process
	SD 4.5.5.4 Stage 4—Ongoing operation	14.1.3 Maintain or restore operations and ensure availability of information
DS4.9 Offsite backup storage	SD 4.5.5.2 Stage 2—Requirements and strategy	10.5.1 Information backup
	SO 5.2.3 Backup and restore	
DS4.10 Post-resumption review	SD 4.5.5.3 Stage 3—Implementation	14.1.5 Testing, maintaining and reassessing business continuity plans
	SD 4.5.5.4 Stage 4— Ongoing operation	

A Tabela 6.3 representa o mapeamento entre os objetivos de controle do COBIT, os processos do ITIL e os controles previstos no Código de Prática para Gestão da Segurança da Informação [IT Governance Institute 2008b]. Através do alinhamento entre as boas práticas é possível realizar tanto a análise de aderência das práticas implementadas em cada organização, como aprofundar o entendimentos dos controles e processos referentes à continuidade dos serviços de TI.

6.4. Estudo de Caso

O estudo de caso proposto demonstra a aplicação dos conceitos abordados nas seções anteriores na produção de planos para companhia aérea Voe Sempre. As fases a serem descritas são: (a) entendendo a organização, (b) determinando a estratégia de Continuidade de Negócios, (c) desenvolvendo e implementando uma resposta de GCN e (d) testando, Mantendo e Analisando Criticamente os preparativos de GCN.

A organização fictícia deste estudo situa-se no segmento aéreo tendo como diferencial das demais sua utilização de tecnologia da informação voltada à redução de custos e alta confiabilidade.

6.4.1. Entendendo a organização

A organização conta com dois datacenters de Tier 2[1] conforme ANSI/TIA-942, o primeiro de construção própria e o segundo locado através de modalidade *colocation* com uma empresa especializada. Alguns sistemas já possuem contingências, porém não existe uma análise formal dos processos críticos para a organização, sendo assim também não sabemos se as contingências existentes são suficientes e se os sistemas que não tem contingência deveriam ter.

Então, o primeiro passo a ser executado é uma análise de impacto no negócio através de um formulário que terá como produto final os processos críticos da

[1] Datacenter com componentes redundantes.

organização, os RTOs e RPOs exigidos para os sistemas críticos e uma visão ampla sobre MTPD e impactos financeiros.

6.4.1.1. Análise de Impacto no Negócio

Conforme definido anteriormente a Análise de Impacto no Negócio é o processo que envolve a análise das funções de negócio e os efeitos que uma interrupção possa causar nelas. Neste ponto é essencial a participação de todas as áreas de negócios da empresa, pois os dados e informações aqui coletadas trarão a luz todos os requisitos de organização para montagem de estratégias de recuperação de desastres em tecnologia da informação.

Ao fim desta etapa, a área de Tecnologia da Informação poderá entender quais as premissas deverá utilizar para montagem da infraestrutura, contratação de serviços, definição de acordos de níveis de serviço, impacto financeiro por processo de negócio e aplicação e, de priorizações entre sistemas para recuperação após desastres.

O envolvimento principal da área de Tecnologia da Informação neste momento é fornecer uma lista de sistemas utilizados pelo negócio que seja de fácil entendimento e compreensão pelos usuários de negócio. Neste sentido é necessário compreender que as áreas de negócio podem enxergar um conjunto de aplicações como um sistema único, requerendo que a área de Tecnologia da Informação trate este conjunto como uma entidade inseparável para o planejamento de planos de recuperação de desastres em tecnologia da informação.

Para o entendimento da organização, deve-se organizar uma análise de impacto do negócio, atividade na qual são realizadas entrevistas com as pessoas chaves de cada processo de negócio visando identificar a criticidade de cada processo de negócio e sua relação com sistemas da informação.

Um trabalho prévio deve ser realizado na análise de impacto do negócio buscando preparar dados iniciais requeridos durante todo trabalho:

- Identificação de todos os processos de negócio;
- Identificação de todos os sistemas da informação da companhia;
- Estabelecer critérios para cada nível de criticidade (alto, médio e baixo);
- Identificar as pessoas que serão entrevistadas.

Após a identificação de todos os processos de negócio, sistemas, o estabelecimento de critérios e identificação das pessoas que serão entrevistadas, então é organizado uma agenda de entrevistas. No formulário proposto para a análise de impacto no negócio, foram inseridas apenas as informações relevantes para a criação de estratégias e planos de recuperação de desastres de TI, porém cabe registrar que outras informações sobre o negócio que auxiliem na construção de estratégias e planos de continuidade de operacional, planos de resposta a emergências e planos de gerenciamento de crises podem ser incluídas.

Para este estudo de caso se utilizou o formulário da Tabela 6.4. Vale destacar que a variável de criticidade está vinculada diretamente com o RTO e o MTPD, que são

dependentes dos impactos legais, financeiros e de imagem em caso de indisponibilidade do processo de negócio em questão.

Tabela 6.4. Formulário de Análise de Impacto do Negócio.

PROCESSO DE NEGÓCIO:			
RTO:			
RPO:			
PERÍODO CRÍTICO:			
MTPD:			
CRITICIDADE:	□ Alto	□ Médio	□ Baixo
SISTEMAS DE INFORMAÇÃO:			

Para o desenvolvimento da análise de impacto dos negócios, aconselha-se a utilizar um roteiro de entrevista informal, de forma a poder entender o processo de negócio e o entrevistado entender o significado daquela atividade. Abaixo segue o roteiro utilizado para a companhia aérea em estudo:

(1) O processo de negócio em questão é mais crítico em qual período do mês? Por quê?
(2) Quais sistemas você utiliza para executar as atividades deste processo de negócio?
(3) Se o sistema não está disponível existe alguma atividade alternativa que você realiza?
(4) Quanto tempo é necessário para executar esta atividade alternativa sem o sistema estar disponível?
(5) Os dados no sistema precisam estar sempre atualizados e disponíveis para consulta? Se os mesmos estivessem alguns dias atrasados causariam algum problema operacional?
(6) Qual o período máximo de atraso dos dados aceitável para a execução das atividades críticas desse processo de negócio?
(7) Na área de Tecnologia da Informação temos um segundo Datacenter, o mesmo provê 50% da capacidade para este processo de negócio. Logo, se você tiver que trabalhar usando um sistema com a metade da velocidade do atual, quanto tempo você conseguiria trabalhar assim?

(8) Em caso de indisponibilidade desse processo de negócio existe algum impacto legal, tais como: multas, advertências ou outro tipo de sanção pelo órgão regulador?
(9) Com o processo de negócio indisponível o impacto recairia sobre os clientes?
(10) Qual o percentual de receita direta que esse processo de negócio gera para a organização?

Com base nas respostas para as questões supracitadas se obtêm as informações para o modelo representado na Tabela 6.5.

Tabela 6.5. Modelo de Informações Gerais de um Plano de Continuidade.

PROCESSO DE NEGÓCIO:	**[Nome do Processo de Negócio]**
RTO:	**[Resposta3 e Resposta 4]**
RPO:	**[Resposta 5 e Resposta 6]**
PERÍODO CRÍTICO:	**[Resposta 1]**
MTPD:	**[Resposta 7]**
CRITICIDADE:	**[Resposta 8, Resposta 9, Resposta 10 e uma análise sobre o RTO e MTPD]**
SISTEMAS DE INFORMAÇÃO:	**[Resposta 2]**

Para a organização deste estudo de caso, a Tabela 6.6 apresenta os resultados obtidos através da análise de impacto de negócio:

Tabela 6.6. Resultado de Análise de Impacto do Negócio.

PROCESSO DE NEGÓCIO:	Vendas		
RTO:	1h		
RPO:	0h		
PERÍODO CRÍTICO:	24h durante os 7 dias da semana		
MTPD:	3h		
CRITICIDADE:	■ Alto	□ Médio	□ Baixo
SISTEMAS DE INFORMAÇÃO:	ERP – Módulo de Vendas ERP – Módulo de Relatórios		

		Telecomunicações (WAN) Navegação Web	
PROCESSO DE NEGÓCIO:		Check-In	
RTO:		30min	
RPO:		0h	
PERÍODO CRÍTICO:		24h durante os 7 dias da semana	
MTPD:		1h	
CRITICIDADE:	■ Alto	□ Médio	□ Baixo
SISTEMAS DE INFORMAÇÃO:		ERP – Módulo de Check-In ERP – Módulo de Vendas ERP – Módulo de Relatórios Telecomunicações (WAN) Navegação Web	
PROCESSO DE NEGÓCIO:		Back Office (Administrativo, Pessoal, Contabilidade, etc..)	
RTO:		72 h	
RPO:		Encerramento do Mês	
PERÍODO CRÍTICO:		Todo 5º. útil de cada mês	
MTPD:		3 meses	
CRITICIDADE:	□ Alto	■ Médio	□ Baixo
SISTEMAS DE INFORMAÇÃO:		ERP – Módulo Administrativo Sistema de Contabilidade e Tributos Sistema de Talentos Telecomunicações (LAN) Navegação Web E-mail	
PROCESSO DE NEGÓCIO:		Manutenção e Compras	
RTO:		720h	
RPO:		Encerramento do Mês	
PERÍODO CRÍTICO:		Dias 15 e 30 de cada mês.	
MTPD:		6 meses	
CRITICIDADE:	□ Alto	□ Médio	■ Baixo

SISTEMAS DE INFORMAÇÃO:		Sistema de Manutenção ERP – Módulo de Compras Telecomunicações (LAN) E-mail	
PROCESSO DE NEGÓCIO:		Call Center	
RTO:		1h	
RPO:		Última Transação Efetuada	
PERÍODO CRÍTICO:		8h às 20h de segunda a sábado	
MTPD:		1 dia	
CRITICIDADE:	■ Alto	□ Médio	□ Baixo
SISTEMAS DE INFORMAÇÃO:		Sistema de Atendimento Telefonia Telecomunicações (LAN) E-mail	

Um resumo do resultado da análise de impacto de negócio pode ser observado na Tabela 6.7:

Tabela 6.7. Resumo do Resultado da Análise de Impacto de Negócio.

Processo de Negócio	RTO	RPO	MTPD	Criticidade
Vendas	1h	0h	3h	Alta
Call Center	1h	0h	24h	Alta
Check-in	3h	24h	48h	Média
Back Office	72h	744h	2232h	Média
Manutenção e Compras	720h	744h	4464h	Baixa

6.4.2 Determinando a estratégia de Continuidade de Negócios

Agora a organização já conhece seus processos de negócio críticos, ou seja, com alta criticidade e de baixo RTO. Nessa etapa o mais importante é reunir a equipe de infraestrutura de TI e pensar nas estratégias para recuperação de desastres de TI.

Cada estratégia pensada deve ser precificada, além de observar a viabilidade técnica e esforço de implementação. Uma lista para avaliar o custo benefício deve ser entregue a alta administração para a escolha da estratégia a ser implementada.

6.4.2.1 Tipos de Estratégias

As estratégias de recuperação de desastres serão definidas dentro de três categorias:

- ***Hot site*:** os aplicativos podem ser balanceados e trabalhar com servidores ativos nos dois datacenters, ou seja, em caso de indisponibilidade do datacenter principal o usuário do sistema não percebe a queda;
- ***Warm site*:** os aplicativos trabalham com um dos dois datacenter estiver em modo de espera e são necessárias algumas configurações;
- ***Cold site*:** para restaurar os aplicativos é necessário reinstalar todo o sistema, pois no datacenter secundário existe apenas a infraestrutura de comunicação.

A área de Tecnologia da Informação deverá analisar os resultados obtidos e comparar com a situação atual dos seguintes aspectos:

- **Infraestrutura Tecnológica:**
  - Capacidade de o serviço funcionar em dois sites simultaneamente;
  - Tempo para ativação da contingência para serviços que não forem ativos nos dois *datacenters*;
  - Capacidade de atender o RPO com a estrutura de backups e replicações;
  - Custo para atender os RTOs e RPOs solicitados;
- **Contratos com fornecedores**
  - Validar a possibilidade de fazer atualizações dos sistemas de forma parcial, ou seja, por datacenter;
  - Realizar contratos para priorização de entrega de insumos em momentos de crise;
- **Acordos de Nível de Serviço**
  - Verificar o tempo de atendimento em caso de indisponibilidades;
  - Verificar a capacidade de processamento necessária no ambiente de contingência;

Nesse estudo de caso, os resultados demonstraram que havia aderência parcial dos aspectos analisados, requerendo que acordos de níveis de serviço tivessem sido revistos para adequação, devido a escalabilidade da execução dos processos de negócios relacionados a vendas e check-in. Os serviços obedecerão às estratégias de recuperação de desastres em TI conforme a Tabela 6.8

Tabela 6.8. Estratégias de Recuperação.

Sistema	Estratégia de Recuperação	Processos de Negócio	Custo de Implantação

ERP – Módulo de Vendas	*Hot Site*	Vendas, Check-In	Já existe a estrutura.
ERP – Módulo de Relatórios	*Warm Site*	Vendas, Check-In	Já existe a estrutura.
Telecomunicações (LAN / WAN)	*Hot Site*	Vendas, Check-In, Back Office, Manutenção e Compras, Call Center	Já existe a estrutura.
Navegação Web	*Hot Site*	Vendas, *Check-In*, *Back Office*, Manutenção e Compras	Já existe a estrutura.
ERP – Módulo de Check-In	*Hot Site*	Check-In	Já existe a estrutura.
ERP – Módulo Administrativo	*Cold Site*	*Back Office*	Já existe a estrutura.
Sistema de Contabilidade e Tributos	*Cold Site*	*Back Office*	*R$ 100.000,00*
Sistema de Talentos	*Cold Site*	*Back Office*	*R$ 150.000,00*
E-mail	*Hot Site*	*Back Office*, Manutenção e Compras, *Call Center*	*R$ 350.000,00*
Sistema de Manutenção	*Cold Site*	Manutenção e Compras	R$ 20.000,00
ERP – Módulo de Compras	*Cold Site*	Manutenção e Compras	Já existe a estrutura.
Sistema de Atendimento	*Warm Site*	*Call Center*	*R$ 1.000.000,00*
Telefonia	*Warm Site*	*Call Center*	Já existe a estrutura.

Conforme dito anteriormente o RTO e o MTPD guiam o impacto financeiro, de imagem ou legal gerado através de uma parada dos serviços de TI que suportem processos de negócios críticos, mas cabe salientar que a análise custo/beneficio é fator determinante na escolha de uma estratégia de recuperação de desastres em TI. As estratégias *hot site* e *warm site*, têm uma estrutura duplicada, ou seja, custos duplicados com a infraestrutura de TI.

Além da conotação de estrutura, há uma implicação nas tecnologias a serem utilizadas para implementar esta estratégia. Não há possibilidade de implementar uma tecnologia de alta redundância com uma tecnologia de *software* e *hardware* que não suporte tal configuração. Um exemplo que pode ser estabelecido foi do sistema de e-mail da Voe Sempre, que utilizava uma plataforma baseada no *software sendmail* em um ambiente Unix que não suportava uma configuração de cluster. Logo, foi necessário um investimento em uma nova plataforma de e-mail corporativo baseado em Postfix com dois servidores em cluster ativo/ativo localizados um em cada datacenter.

Deve-se salientar que não necessariamente o uso de uma estratégia de Hot Site acarreta na necessidade de suporte da aplicação à alta disponibilidade, pois se pode

considerar um período de ativação pequeno ainda como Hot Site. Nestes casos, sempre se deve analisar qual a necessidade de negócio e o custo necessário para implementação da alta disponibilidade requerida.

6.4.3 Desenvolvendo e Implementando uma Resposta de GCN

A organização decidiu apenas criar os planos da estrutura existente e irá avaliar para o próximo ciclo do programa de continuidade de negócios o investimento para a infraestrutura de telefonia.

6.4.3.1 Plano de Recuperação de Desastres em TI

Na etapa de desenvolvimento dos planos é o momento em que é necessário o maior esforço por parte das áreas de Tecnologia da Informação e demais áreas de negócio, pois é aqui que os planos são desenvolvidos baseados nas necessidades definidas na etapa anterior e no ambiente corporativo.

Um plano de recuperação de desastres em TI pode ser documentado utilizando como base o modelo 5W2H[2]. A Tabela 6.9 mostra o modelo utilizado para documentação de cada passo dos procedimentos:

Tabela 6.9. Modelo para Documentação de Procedimentos.

ORDEM	
O QUE:	*Ação a ser realizada*
QUEM:	*Cargo do responsável pela ação*
QUANDO:	*Momento de execução*
COMO:	*Passo a passo das ações para ativação*
DURAÇÃO:	*Tempo de duração da ação*

Em virtude das constantes mudanças ao qual o ambiente de TI está sujeito, é aconselhável documentar os procedimentos até a um nível tático, não incluindo informações de procedimentos como instalação de sistemas operacionais, bancos de dados, etc. Estes procedimentos inclusive devem estar documentados separadamente em outros locais como manuais e guias de sistemas da informação. Devendo a configuração dos ambientes estar armazenada em cópias de segurança que serão restauradas no caso da ocorrência de incidentes. A Tabela 6.10 descreve os procedimentos definidos para o processo de Vendas.

[2] Modelo de plano de ação que define: responsabilidades, o que deve ser feito, quando, como, onde porque e os custos e prazos.

Tabela 6.10. Registro de Procedimentos por Processo.

PLANO	Vendas
RTO:	1h
RPO:	0h
CENÁRIO:	*Indisponibilidade do Data Centre Alpha*
RESPONSÁVEL:	*Leonardo Silva - +55 55 555-5678*
SUBSTITUTO:	*Rafael Alves - +55 55 555-8765*
ORDEM	1
O QUE:	Comunicar a indisponibilidade do Datacenter Alpha para o Gerente de TI
QUEM:	Equipe de Monitoramento de TI da Voe Sempre
QUANDO:	Após a detecção da indisponibilidade do Data Center
COMO:	Através de uma ligação telefônica, utilizando a árvore de chamadas pré-estabelecida.
DURAÇÃO:	10 minutos
ORDEM	2
O QUE:	Reunir o time de gestão de crises
QUEM:	Gerente de TI
QUANDO:	Após receber a comunicação da indisponibilidade do Data Center Alpha
COMO:	Através de uma conferência via telefone
DURAÇÃO:	10 minutos
ORDEM	3
O QUE:	Decidir Ativar o Data Center Beta
QUEM:	Time de Gestão de Crises
QUANDO:	Durante a reunião via conferência
COMO:	Através da análise das possibilidades
DURAÇÃO:	10min
ORDEM	3

O QUE:	Ativar equipe de TI
QUEM:	Equipe de Monitoramento de TI
QUANDO:	Após comunicar o gerente de TI
COMO:	Através dos telefones celulares, contidos na árvore de chamadas
DURAÇÃO:	15 minutos
ORDEM	4
O QUE:	Comunicar equipe para ativação do Datacenter Beta
QUEM:	Gerente de TI
QUANDO:	Após decisão de ativar o Datacenter Beta
COMO:	Através de uma ligação para equipe de Monitoramento de TI
DURAÇÃO:	15 minutos
ORDEM	5
O QUE:	Ativar o Datacenter Beta
QUEM:	Equipe de TI
QUANDO:	Após comunicação da equipe de monitoramento
COMO:	Utilizando os procedimentos de ativação
DURAÇÃO:	2h
ORDEM	6
O QUE:	Reunir equipe de Gestão de Crises
QUEM:	Equipe de Gestão de Crises
QUANDO:	Após reunião via telefone do time de Gestão de Crises
COMO:	Reunindo-se em um ponto de encontro a ser definido na reunião
DURAÇÃO:	30 minutos
ORDEM	7
O QUE:	Preparar comunicados internos e externos
QUEM:	Equipe de Gestão de Crises
QUANDO:	Após reunir-se

COMO:	Em conjunto
DURAÇÃO:	1h
ORDEM	8
O QUE:	Identificar a extensão dos danos e passos necessários para recuperar o Datacenter Alpha
QUEM:	Equipe de Gestão de Crises
QUANDO:	Após reunião do time de Gestão de Crises
COMO:	Através da análise de dados obtidos de diversas áreas, incluindo: - Monitoramento de TI - Segurança Corporativa - Engenharia
DURAÇÃO:	45 minutos

Os serviços relacionados ao ERP de vendas e *check-in* adotam a estratégia denominada *hot site* e mesmo com a queda do datacenter Alpha continuaram em operação. A equipe de infraestrutura foi ativada para recuperar os serviços que adotam as estratégias *warm site* e *cold site* da infraestrutura existente no datacenter Beta.

6.4.4 Testando, Mantendo e Analisando Criticamente os preparativos de GCN

A organização passou por um incidente crítico que foi o Black-out do seu datacenter Alpha, esse evento serviu como um teste para seus planos de recuperação de desastres em TI.

Os processos de manutenção e de analise crítica também são ativados no caso do uso dos planos por motivos de incidente, porém sem os testes periódicos nenhum outro processo dessa etapa é possível.

6.4.4.1 Testes Periódicos

Após implementar um plano de recuperação de desastres em TI, deve-se testar a solução a fim de verificar se a mesma está adequadamente implantada ou requer melhorias a fim de atingir as necessidades do negócio. Para isto, a organização definiu:

- Planos de Sistemas Críticos - devem ser testados anualmente via simulação real com uma revisão a cada seis meses via teste de mesa
- Testes de Árvore de Chamadas – devem ser realizados sem aviso prévio.

Para os testes de mesa é essencial a definição dos papéis e responsabilidades, conforme a Tabela 6.11.

Tabela 6.11. Papéis e Responsabilidades.

Pessoa/Cargo	**Papel no Teste**
Gestor de Continuidade de Negócio	Coordenador
Gestor da área de Tecnologia da Informação	Participante / Patrocinador
Dono do plano de continuidade de negócios	Responsável
Usuários da área de negócio	Participantes
Observadores	Observadores

Os observadores são pessoas elencadas pelo Gestor de Continuidade de Negócios para estarem atentos durante o andamento dos testes, já que cabe ao gestor coordenar todas as atividades e desenvolver novas situações durante a leitura dos planos.

Na definição do escopo do teste é essencial avaliar os seguintes aspectos:

- Escopo e a maturidade dos participantes e do plano
- Tempo e orçamento requerido
- Definir objetivos e indicadores a serem medidos durante o teste
- O cenário e duração do teste de maneira a atingir seus objetivos
- Entendimento de todos envolvidos dos planos
- Encaminhar a todos participantes os objetivos e limitações do teste

A Tabela 6.12 apresenta um registro de teste de mesa executado na organização Voe Sempre.

Tabela 6.12. Registro de Teste

Informação Inicial	
Data:	23/08/2008
Hora de Início:	22 h
Localização:	Unidade São Sebastião
Patrocinador:	João Humberto Gonzaga
Responsável:	Luis Garcia
Coordenador:	Manoel Elias
Processos de Negócio:	Vendas
Sistemas Envolvidos:	ERP – Módulo de Vendas
Cenário:	Cenário 3 – Falha de comunicação com a base de dados
RTO:	1h
RPO:	0h
Pressupostos:	- Os demais sistemas devem continuar ativos - O teste ocorrerá com participação via telefone para contato com técnicos - A sincronia deverá indisponibilizar somente a base de dados

	central para área de vendas

Neste caso, o cenário a ser testado apresenta uma falha de sincronia entre bases de dados e, como se pode ver nos pressupostos, o teste ocorrerá somente com a área de Vendas, principal usuária deste sistema. Ou seja, não é necessário envolver todas as áreas que acessam determinado sistema se o mesmo será testado, mas sim as áreas que dependem essencialmente deste sistema ou processo de negócio.

O teste de mesa é executado percorrendo os procedimentos vigentes do plano de continuidade em conjunto com as pessoas que constam como participantes no mesmo. Cabe ao coordenador da atividade, o Gestor de Continuidade de Negócios, conduzir o andamento passo-a-passo, cabendo então aos observadores da atividade identificar: se o passo é passível de ser executado, se não são necessários passos adicionais ou se existem oportunidades para racionalizar o plano. Um relatório final de um teste de mesa aplicado a uma aplicação deve obter como resultado:

- Tempo requerido para restaurar a aplicação
- Problemas encontrados
- Aderência ao plano documentado
- Lições aprendidas
- Plano de ação para resolução dos problemas

A Tabela 6.13 reúne os resultados obtidos após a realização do teste descrito anteriormente.

Tabela 6.13. Resultado de um Teste de Mesa.

Resultados	
Resultado Geral:	Completado com falhas.
Aderência ao plano:	Durante a execução do passo 3, houve a necessidade de comunicação de mais uma pessoa
Tempo:	01:15:20
Problemas:	Demonstrou-se que o plano não prevê situações como horário de almoço e de saída, onde pode ocorrer que as pessoas estejam em locais sem acesso a telefone, Internet ou que requeiram mais de 30 minutos de deslocamento.
Lições Aprendidas:	O tempo requerido para o passo 7, que deveria ser de 15 minutos, tomou cerca de 20 minutos devido à indisponibilidade do contato principal. Logo, indicou-se um terceiro substituto que deve constar no plano.

No caso acima, pode-se notar que há uma falha no tempo estimado do plano e que o mesmo pode falhar no caso de uma situação real ocorrer em horários específicos. Então será necessário rever todo o plano para adequação do mesmo aos requisitos do negócio.

6.5. Conclusão

A proteção dos ativos e a continuidade do negócio são alguns dos principais objetivos da segurança da informação. Para garantir a continuidade das operações mesmo mediante cenários de desastres é fundamental que as organizações, independente do segmento e/ou porte, coloquem em prática um programa de gestão da continuidade de negócio.

Esse programa, conforme discutido na seção 6.2, é composto por planos que têm como objetivo: gerenciar incidentes, garantir o estado de contingência e a recuperação da organização. Nesse capítulo foram apresentados conceitos, práticas e um estudo de caso com foco na elaboração das estratégicas de contingência para os recursos de tecnologia da informação, normalmente denominado de plano de recuperação de desastres.

A elaboração de planos de recuperação de desastres precisa ser cuidadosamente planejada, definida e testada para assegurar que: (a) as estratégias de contingência escolhidas estão de acordo com o nível de serviço vigente e (b) que as pessoas estejam devidamente capacitadas e cientes sobre como proceder mediante eventos que comprometam a continuidade dos serviços de TI.

O processo de construção desses planos compreende um conjunto coordenado de atividades interdependentes que inicia com o entendimento das necessidades da organização. Nessa etapa é necessário obter informações que permitam definir a priorização dos produtos e serviços da organização e a urgência das atividades que são necessárias para fornecê-los. Isso estabelece os requisitos que irão definir a seleção das estratégias de GCN apropriadas.

A definição da estratégia de continuidade permite que uma série de estratégias seja avaliada a fim de que uma resposta apropriada seja escolhida de modo que a organização possa continuar fornecendo esses produtos e serviços em um nível de operações aceitável pelo tempo necessário. Essas escolhas levarão em consideração muitas variáveis, entre elas a resiliência e as opções de contramedidas já presentes na organização.

Em seguida, é chegado o momento de desenvolver e aplicar uma resposta de gestão de continuidade de negócios para cada produto e/ou serviço critico. No caso especifico dos ativos de TI, conforme apresentado na seção 6.3, existe um conjunto de boas práticas amplamente divulgadas e que servem de apoio no momento do desenvolvimento das estratégias de contingência. Essa resposta deve ser regularmente testada, revista e auditada para que a organização esteja ciente a que ponto as suas estratégias e planos estão completos, atualizados.

Ao longo do desenvolvimento das atividades dos autores como profissionais da área de gestão de continuidade de negócio e das pesquisas realizadas para elaboração deste capítulo foram identificados os seguintes aspectos que podem vir a fomentar questões de pesquisa: (a) a grande parte das ferramentas de apoio e suporte ao processo de GCN realizam apenas a gestão da documentação, (b) inexistência de sistema especialista que possa contribuir para definição / estimativa de grandezas como RPO, RTO e MTPD e (c) da mesma forma não foram identificados muitos trabalhos científicos focados no desenvolvimento de ambientes para simulação das estratégias de

contingência como, por exemplo, no trabalho proposto em [Bartolini, Stefanelli and Tortonesi 2009] e [Tjoa and Jakoubi 2008].

Referências

[ABNT 2005] ABNT (2005). Tecnologia da Informação – Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação. ABNT NBR ISO/IEC 27002:2005.

[ABNT 2008a] ABNT (2008). Gestão de Continuidade de Negócios Parte 1: Código de Prática. ABNT NBR 15991-1:2008.

[ABNT 2008b] ABNT (2008). Gestão de Continuidade de Negócios Parte 2: Requisitos. ABNT NBR 15991-2:2008.

[ABNT 2008c] ABNT (2008). Gerenciamento de Serviços de TI Parte 1: Especificação. ABNT NBR ISO/IEC 2000-1:2008.

[Bartolini, Stefanelli and Tortonesi 2009] Bartolini, C., Stefanelli, C., Tortonesi, M. (2009). Business-impact analysis and simulation of critical incidents in IT service management. University of Ferrara, Ferrara, Italy.

[BCI 2010] BCI (2010). The Business Continuity Institute Good Practice Guidelines. Disponível em: http://www.thebcicertificate.org/bci_gpgdownload.html. Acessado em 21 de mar. de 2010.

[Cegiela 2006] Cegiela, R. (2006). Selecting Technology for Disaster Recovery. Warsaw University of Technology, Institute of Control and Computation Engineering, Warsaw, Poland.

[Continuity Central 2006] Continuity Central (2006). Business Continuity Unwrapped, Disponível em: http://www.continuitycentral.com/feature0358.htm (em inglês), acessado em 21 de mar. de 2010.

[DRII 2010] DRII (2010). Disaster Recovery International Institute: Professional Practices. Disponível em: https://www.drii.org/docs/profprac_details.pdf. Acessado em 21 de mar. de 2010.

[Husdal 2008]. Husdal (2008). Ericsson versus Nokia – the now classic case of supply chain disruption. Disponível em: http://www.husdal.com/2008/10/18/ericsson-versus-nokia-the-now-classic-case-of-supply-chain-disruption/print/. Acessado em 21 de mar. de 2010.

[IBM Global Services 2007]. IBM Global Services (2007). Continuidade de negócios e resiliência" Disponível em: http://www.ibm.com/br/services/bcr/. Acessado em 21 de mar. de 2010.

[IT Governance Institute 2008a]. IT Governance Institute (2008). IT Governance Institute (2007). COBIT - Control Objectives for Information and related Technology. Disponível em http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx. Acessado em 20/06/2010.

[IT Governance Institute 2008b]. IT Governance Institute (2008). Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. Disponível em http://www.isaca.org/knowledge-

center/Research/ResearchDeliverables/Pages/Aligning-COBIT-4-1-ITIL-V3-and-ISO-IEC-27002-for-BusinessBenefit.aspx. Acessado em 20/08/2010.

[Tjoa and Jakoubi 2008] Tjoa, S., Jakoubi, S. (2008). Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology. The Third International Conference on Availability, Reliability and Security, EUA.

[Wei 2009] Wei, N.Z.W. (2009). The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. Journal of Business Continuity & Emergency Planning Vol. 4 No. 1, pp. 62–68. United Kingdom.

[Wiboonrat 2008] Wiboonrat, M. (2008). An Empirical IT Contingency Planning Model for Disaster Recovery Strategy Selection. Graduate School of Information Technology, Assumption University. Bangkok, Thailand.