UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

Diego Müller Cardeal de Souza

GESTÃO DE CONTINUIDADE DE NEGÓCIOS – O CASO DE UMA EMPRESA DE TELECOMUNICAÇÕES

Porto Alegre
2010

Diego Müller Cardeal de Souza

Gestão de Continuidade de Negócios – o Caso de uma Empresa de Telecomunicações

Dissertação submetida ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do título de Mestre em Engenharia de Produção, modalidade Profissional, na área de concentração em Sistemas da Qualidade.

Orientador: Professor Francisco José Kliemann Neto, Dr.

Porto Alegre

2010

Diego Müller Cardeal de Souza

Gestão de Continuidade de Negócios – o Caso de uma Empresa de Telecomunicações

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia de Produção na modalidade Profissional e aprovada em sua forma final pelo Orientador e pela Banca Examinadora designada pelo Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul.

_____

Prof. Francisco José Kliemann Neto, Dr.
Orientador PPGEP/UFRGS

_____

Prof. José Luís Duarte Ribeiro, Dr.
Coordenador PPGEP/UFRGS

Banca Examinadora:

Professor **Antônio Domingos Padula, Dr. (PPGA/UFRGS)**

Professor **Cláudio José Müller, Dr. (PPGEP/UFRGS)**

Professor **Leonardo Rocha de Oliveira, *PhD*. (PUCRS)**

Aos meus pais e à minha futura esposa,
obrigado pelo carinho e apoio.

AGRADECIMENTOS

À Deus pela oportunidade.

À Universidade Federal do Rio Grande do Sul e à Escola de Engenharia pela estrutura e competência de seus professores.

Ao Professor Francisco José Kliemann Neto pela sua compreensão e competência na orientação deste trabalho.

Aos meus parentes, amigos e colegas pela solidariedade.

RESUMO

Em um movimento iniciado principalmente nos Estados Unidos na década de 90, a governança corporativa surgiu para superar o chamado conflito de agência, decorrente da separação entre a propriedade e a gestão empresarial, criando um conjunto de instrumentos para assegurar que as decisões dos executivos estejam sempre alinhadas com os interesses dos acionistas. Dentre esses mecanismos, destaca-se com grande relevância o gerenciamento de riscos corporativos, que possibilita aos administradores tratar com eficácia as incertezas, bem como as oportunidades a elas associadas, a fim de melhorar a capacidade de agregar valor às organizações. Os esforços de prevenção e tratamento de riscos operacionais geraram boa experiência no gerenciamento de interrupções de atividades essencias das organizações, constituindo a disciplina atualmente denominada como Gestão da Continuidade de Negócios (GCN). No desenvolvimento e promoção de boas práticas de GCN, destacam-se as normas da série 25999, partes 1 e 2, do BSI (*British Standards Institution*) que tratam, respectivamente, sobre um modelo de ciclo de vida de GCN e de um Sistema de Gestão de Continuidade de Negócios (SGCN). Partindo-se de uma revisão bibliográfica sobre governança corporativa, gestão de riscos, gestão de continuidade de negócios e sistemas de gestão, além da análise do contexto de GCN em uma empresa de telecomunicações, foi desenvolvida uma proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios aplicada àquela organização e concluiu-se que essa implantação é facilitada devido ao fato de ser concebida a partir do PDCA – Plan, Do, Check, Act, modelo mundialmente conhecido e aplicável a outros sistemas de gestão. Concluiu-se também que o SGCN, além de estabelecido, precisa ser implementado, mantido e melhorado continuamente e, para isso, o patrocínio e o comprometimento da alta direção é muito importante.

Palavras-chave: gestão de continuidade de negócios, sistema de gestão, gestão de riscos, governança corporativa.

ABSTRACT

In a movement initiated primarily in the United States in the 90s, corporate governance has emerged to overcome the agency conflict resulting from the separation of ownership and management business, creating a powerful set of mechanisms in order to ensure that the behavior of executives is always aligned with the interests of stakeholders. Among these mechanisms, stands out with high importance the business risk management, enabling administrators to deal effectively with the uncertainties and opportunities associated with them in order to improve the ability to provide value to organizations. Efforts to prevent and reduce operational risks introduced good experience in management of interruptions to the critical operations of organizations developing the discipline called Business Continuity Management (BCM). In the development and promotion of best practices GCN, there are the standard series 25999, parts 1 and 2 of the BSI (British Standards Institution) dealing, respectively on a BCM model life cycle and a Business Continuity Management System (SGCN). Starting from a literature review on corporate governance, risk management, business continuity management and management systems, and form the context of GCN in a telecommunications company, has developed a proposed structure to support the implementation of a business continuity management system applied to that organization and found that this deployment is further facilitated by the fact that it is designed from the PDCA – Plan, Do, Check, Act and world-renowned model applicable to other management systems. However, it was felt that the SGCN, and deployed, must be established, improved and maintened continuously and, therefore, sponsorship and commitment from top management is very important.

Key words: business continuity management, management system, risk management, corporate governance.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. Introdução

1.1 Comentários Iniciais

A Governança Corporativa surgiu de um movimento iniciado nos Estados Unidos nos anos 90, onde os acionistas decidiram pela criação de novas regras que os protegessem de eventuais abusos da diretoria executiva de empresas, da inércia de conselhos administrativos ou da omissão de auditorias externas visando superar, assim, o chamado conflito de agência, decorrente da separação entre a propriedade e a gestão empresarial. Portanto, o foco principal da governança corporativa é estabelecer um conjunto eficiente de atividades, seja de promoção ou de monitoramento, visando garantir que o comportamento dos executivos esteja sempre alinhado com o interesse dos acionistas (IBGC, 2008). Dentre essas atividades, destaca-se com grande relevância o gerenciamento de riscos corporativos

Segundo o conceito da norma ISO/IEC Guia 73 da ABNT (2009), o risco pode ser definido como uma combinação da probabilidade de ocorrência de um evento e das suas conseqüências. Já a gestão de riscos, segundo Ferma (2003), é o processo em que as empresas buscam analisar os riscos oriundos de suas atividades, visando obter uma vantagem nessas atividades individualmente ou em conjunto.

Para Perobelli (2004), o gerenciamento de riscos é um assunto que vem ganhando destaque definitivamente no ambiente das instituições financeiras e, mais recentemente, também ganhou espaço no âmbito de instituições não-financeiras. Segundo a autora, o aumento da volatilidade dos mercados nos quais as empresas atuam, a criação de instrumentos regulatórios para minimizar perdas aos investidores e a percepção por parte destes investidores de que os mecanismos de avaliação atuais são insuficientes para identificar potenciais situações adversas em empresas, são alguns dos principais motivadores para o destaque atual desse tema.

A premissa inerente ao gerenciamento de riscos corporativos, segundo COSO (2007), é que “o gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de

melhorar a capacidade de gerar valor". O mesmo autor ressalta ainda que, caso seja estabelecido e implementado adequadamente, o gerenciamento de riscos corporativos pode ser capaz de oferecer tanto ao conselho de administração quanto à diretoria executiva de uma organização a garantia razoável do cumprimento de seus objetivos.

Nos últimos anos, diante dos escândalos financeiros protagonizados por empresas de grande porte dos Estados Unidos e com a criação da Lei Sarbanes Oxley (SOX), a preocupação com o gerenciamento de riscos aumentou, trazendo a necessidade das organizações desenvolverem uma estratégia sustentada, capaz de identificar, analisar, avaliar e tratar adequadamente os riscos inerentes ao seu negócio.

Segundo o IBGC (2007), os riscos podem ser classificados, quanto à sua natureza, em três categorias: (i) estratégicos (aqueles relacionados à estratégia e à tomada de decisão da alta administração, podendo gerar uma perda no valor econômico da organização, caso materializados); (ii) financeiros (relacionados à exposição das operações financeiras da organização ou à confiabilidade das informações transmitidas nos relatórios financeiros divulgados por esta); e (iii) operacionais (aqueles associados à possibilidade de ocorrência de perdas resultantes de falhas internas ou de eventos externos que impactem nas atividades de uma organização).

Os esforços destinados à prevenção e redução de riscos operacionais nas últimas décadas, geraram relevante experiência no âmbito do gerenciamento de impactos adversos e situações de interrupção à continuidade de negócios de organizações. O conjunto de conhecimentos, melhores práticas, habilidades e certificações profissionais constituem hoje a disciplina denominada de Gestão da Continuidade de Negócios, GCN (ou BCM, de *Business Continuity Management*), consolidando os conceitos e práticas relacionados a planos de contingência, planos de recuperação de desastres, planos de *backup*, resposta a emergências e gerenciamento de crises, entre outros (IBGC, 2007).

A cada dia ocorrem eventos externos e internos capazes de impactar não só a continuidade das atividades essenciais das empresas como também afetar a vida de milhões de pessoas. Os atentados de 11 de setembro de 2001 em Nova Iorque, o *tsunami* no Oceano Índico em 2004, a queda do vôo 3054 da TAM em 2007 e o terremoto de Sichuan na China em 2008 são alguns exemplos recentes de como pessoas e organizações são vulneráveis aos impactos devastadores causados por incidentes. Ainda em 2008, uma falha no sistema de transmissão de dados da empresa Telefônica, em São Paulo, causou uma interrupção de 36 horas no serviço de banda larga, acarretando prejuízos para milhões de usuários, bem como para a imagem da empresa. Estes acontecimentos trazem à tona a necessidade das empresas desenvolverem, cada vez mais, sua resiliência organizacional, ou seja, a capacidade de

resistirem aos efeitos de incidentes e retornarem a condições normais de funcionamento. Esta resiliência somente pode ser desenvolvida através de uma gestão de continuidade de negócios eficaz.

Nesse sentido, a ABNT (2007) conceitua a gestão da continuidade do negócio como um processo organizacional que visa estabelecer uma estrutura estratégica e operacional adequada para melhorar a resiliência de uma empresa contra possíveis interrupções e que, caso o fornecimento dos principais produtos e serviços dessa empresa sejam interrompidos, a mesma possa restabelecer o seu negócio em um nível previamente acordado e dentro de um tempo previamente determinado protegendo, assim, a sua marca e a sua reputação.

No desenvolvimento e promoção de boas práticas de GCN, destacam-se as normas da série 25999, partes 1 e 2, do BSI (*British Standards Institution*). A parte 1 da BS25999, publicada em 2006, e lançada em 2007 na versão brasileira como NBR15999-1, trata-se de um código de práticas para gestão da continuidade do negócio, ou seja, fornece uma base para o entendimento, desenvolvimento e implementação da continuidade de negócio em uma organização. A parte 2 da BS25999, publicada pelo BSI em 2007, e lançada no Brasil em 2008 como NBR15999-2, especifica os requisitos para estabelecer e gerenciar um SGCN (Sistema de Gestão de Continuidade de Negócios) eficaz definido por um programa de GCN e possui requisitos bastante semelhantes às demais normas de sistemas de gestão existentes no mundo, tais como ISO9001:2008 (Sistema de Gestão da Qualidade), ISO14001:2004 (Sistema de Gestão Ambiental), OHSAS18001:2007 (Sistema de Gestão de Segurança e Saúde) e ISO27001:2005 (Sistema de Gestão de Segurança da Informação). Como esta norma estabelece requisitos, trata-se de um padrão normativo auditável e certificável sobre GCN.

1.2 Tema e Objetivos

O tema deste trabalho envolve o gerenciamento de riscos e mais especificamente a gestão do risco da interrupção do fornecimento de produtos ou serviços, conhecida como gestão da continuidade de negócios.

Este trabalho foi motivado pelo seguinte problema: como uma empresa de telecomunicações que já possui algumas iniciativas de continuidade estabelecidas está preparada e alinhada às boas práticas internacionais para administrar o risco de interrupção do seu negócio? Ou seja, avaliar a estrutura de Gestão da Continuidade de Negócios (GCN) existente na empresa em estudo e elaborar uma proposta de estrutura de apoio para implantação de um Sistema de Gestão de Continuidade de Negócios, considerando as boas

iniciativas de GCN da empresa e as referências normativas existentes sobre o assunto. Para avançar neste problema de avaliação e estudo de caso, a seguir são apresentados o objetivo geral e os objetivos específicos.

1.2.1 Objetivo geral

O objetivo principal deste trabalho é desenvolver uma proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios numa empresa do setor de telecomunicações.

1.2.2 Objetivos específicos

Os objetivos específicos definidos para este trabalho de dissertação são:

- Caracterizar a gestão da continuidade de negócios e as boas práticas existentes sobre o tema inserida no contexto de gerenciamento de riscos e de governança corporativa;
- Caracterizar a diferenciação entre os conceitos de Gestão de Continuidade de Negócios e de Sistema de Gestão de Continuidade de Negócios;
- Analisar o contexto, os processos e a estrutura de GCN na empresa em estudo e realizar uma análise crítica desse modelo;
- Elaborar uma proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios na empresa avaliada, considerando as iniciativas de GCN já desenvolvidas pela empresa e as referências bibliográficas existentes;
- Realizar uma análise preliminar de aceitação da estrutura proposta perante usuários.

1.3 Justificativa do Tema e Objetivos

Nas últimas décadas, a gestão de riscos, vem apresentando crescente importância no contexto empresarial. Com o advento da globalização e a abertura dos mercados, a vulnerabilidade das empresas e a exposição a fatores de risco de diversas origens também aumenta, podendo afetar consideravelmente os resultados dessas organizações.

Ayres (2007) comenta que, atualmente, a gestão de riscos sofisticou-se de tal forma que sua contribuição é imprescindível para um processo de tomada de decisão. Não obstante, os frutos dessa sofisticação, dentre eles, ferramentas tecnológicas, melhor compreensão do comportamento humano e foco em processos, elevaram o *status* do gerenciamento de riscos a um patamar de destaque nas organizações.

Mas a relevância do tema gerenciamento de riscos não o põe entre os mais freqüentes em estudos e pesquisas sobre administração, com exceção à área de finanças. Nesse sentido, Padoveze e Bertolucci (2005) salientam que fica clara a ausência de trabalhos aprofundados sobre o tema do gerenciamento do risco corporativo, ainda que a área financeira ofereça muitos estudos sob uma ótica mais específica.

Atualmente, a maioria das empresas que possuem uma estrutura de gerenciamento de riscos corporativos, visando atender à lei Sarbanes-Oxley (SOX) avaliam predominantemente riscos financeiros. Por isso, é importante que seja bem estruturada também a gestão dos riscos operacionais numa organização, e mais especificamente o risco de interrupção das atividades críticas do negócio, com o objetivo prevenir os impactos causados por incidentes.

Considerando um mercado tão complexo e competitivo como é o de telecomunicações, a gestão da diversidade de riscos inerentes aos processos deste setor, bem como da continuidade de negócio, torna-se, a cada dia, um desafio mais relevante. Diante desse contexto é que acionistas, investidores e demais partes interessadas necessitam, cada vez mais, não só de um diagnóstico sobre a conformidade da estrutura de gerenciamento de riscos implementada nas suas organizações, como também precisam saber se essas organizações possuem uma estrutura para gerenciar especificamente o risco operacional de interrupção de suas atividades sendo, assim, capaz de resistir aos efeitos de um incidente e de retomar, em tempo hábil, à normalidade dessas operações.

Visando suprir esta necessidade é que surge o presente trabalho, que tem como foco principal a elaboração de uma estrutura de apoio à implantação de um sistema de gestão da continuidade de negócios numa empresa de telecomunicações.

Pelo exposto, pode-se observar que a originalidade deste trabalho encontra-se em executar a avaliação de uma empresa de telecomunicações e planejar a implantação de um SGCN, fundamentada pelo padrão normativo internacional BS25999-2, publicado em novembro de 2007 e traduzido para o português em 2008 pela ABNT, que possui aplicação recente em empresas e com escassa bibliografia a respeito.

A estrutura de apoio proposta neste trabalho considera também outras boas práticas de GCN existentes no mundo, dentre elas, principalmente, o padrão normativo BS25999-1, publicado em 2006, e o Guia de Boas Práticas de GCN publicado pelo *Business Continuity Institute* - BCI em 2008. Essas referências dão fundamento às sugestões e planejamento de ações pertinentes propostas para adequação da empresa em estudo.

A partir dessas considerações, pode-se apresentar como contribuições deste trabalho a avaliação do contexto e as sugestões para implantação de um sistema de gestão de

continuidade de negócios na organização em estudo, permitindo que se tenha uma visão mais concreta das deficiências e necessidades da empresa para gerenciar adequadamente o risco de interrupção de suas atividades. Além disso, o presente trabalho, devido à sua abrangência, fundamentação teórica e proposta de aplicação pode ser uma referência para outros estudos relacionados ao tema. Por fim, a avaliação a ser realizada pode servir não somente para o desenvolvimento de melhorias na organização, como também poderá ser usada como referência para diagnósticos futuros, sendo um ponto de partida para a melhoria contínua do sistema de gestão da continuidade de negócios da empresa.

1.4 Método de Trabalho

O desenvolvimento deste trabalho será feito a partir de quatro etapas. A primeira etapa envolve o estudo teórico sobre o tema gerenciamento de riscos e gestão da continuidade de negócios inseridos no contexto da governança corporativa. Nesta etapa, será realizada uma pesquisa bibliográfica no sentido de agregar conhecimentos referentes à origem, definição, metodologias, padrões normativos e principais benefícios da implantação desses conceitos. A pesquisa bibliográfica dar-se-á através da Internet, de periódicos e revistas especializadas, livros e teses/dissertações, utilizando como palavras-chave gestão de riscos corporativos e gestão de continuidade de negócio, abordando as questões comuns às áreas de estudo.

A segunda etapa envolve inicialmente uma abordagem conceitual sobre sistemas de gestão, incluindo aspectos como tipos, características e similaridades entre eles, com ênfase na apresentação do modelo de sistema de gestão de continuidade de negócios previsto na norma BS25999-2. Em seguida será desenvolvido um estudo comparativo teórico no sentido de apresentar as principais diferenças entre o modelo de SGCN previsto na norma BS25999-2 e o modelo de GCN da norma BS25999-1. Esta etapa será desenvolvida através de pesquisa bibliográfica em livros, teses, dissertações e Internet utilizando como palavras-chave gestão de continuidade de negócios, sistemas de gestão e sistema de gestão de continuidade de negócios.

A terceira etapa contempla o estudo de uma empresa de telecomunicações, incluindo o mercado em que atua, seus principais produtos e processos de negócio, bem como a estrutura de funcionamento de sua gestão da continuidade de negócios. Em seguida, será desenvolvida uma análise crítica da estrutura de GCN da empresa em estudo, com o objetivo de identificar as principais dificuldades observadas na implantação dessa estrutura bem como as principais não-conformidades (*GAPS*) desse modelo com relação às práticas previstas na norma internacional BS25999-1. Esta etapa será desenvolvida através de consulta à

documentação da empresa e de entrevistas com colaboradores, a ser realizada pelo autor, visando conhecer detalhadamente a empresa em estudo bem como apresentar e analisar suas práticas de GCN.

A quarta etapa envolve o desenvolvimento da proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios na empresa em estudo, considerando as informações obtidas nas etapas anteriores, sendo apresentada através de sugestões e desdobramento de ações sobre cada elemento dessa estrutura utilizando-se como auxílio a ferramenta 3W1H (*what, who, when, how*). Em seguida, será realizada uma análise preliminar da aceitação dessa proposta perante seus futuros usuários na empresa. O desenvolvimento dessa etapa será realizado com base nas boas práticas de GCN (incluindo as normas de referência), no resultado do estudo comparativo entre os modelos de SGCN e GCN, no resultado da análise crítica da estrutura de gestão de continuidade de negócios da empresa em estudo e através de entrevistas com os futuros usuários da estrutura proposta.

1.5 Delimitações do Trabalho

Em virtude da complexidade dos processos do setor de telecomunicações, bem como da diversidade de riscos inerentes ao negócio, a avaliação e proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócio terá seu foco concentrado nos riscos operacionais da organização. Riscos financeiros e estratégicos não serão tratados no presente estudo.

Este trabalho será desenvolvido no tocante a conceitos e requisitos de sistema de gestão de continuidade de negócios a partir do padrão normativo de referência BS25999-2 - Gestão de Continuidade de Negócios – Parte 2 – Requisitos, traduzida para o português como ABNT NBR15999-2. Outros sistemas de gestão de continuidade de negócios que, por ventura, existam em outros padrões internacionais não serão abordados na proposta desse trabalho.

Durante o trabalho, a empresa estudada terá seu nome original preservado e substituído por nome fictício em virtude da ausência de autorização expressa para publicação dos dados.

O estudo de caso foi desenvolvido junto a uma empresa do setor de telecomunicações. Sendo assim, as observações, sugestões e ações propostas no trabalho devem ser válidas somente para a empresa e para o setor em estudo. Outras empresas do mesmo setor ou empresas de outros setores que necessitem utilizar as informações deste trabalho deverão adaptar essas informações aos seus contextos interno e externo.

1.6 Estrutura do Trabalho

O presente trabalho de dissertação encontra-se dividido em cinco capítulos, conforme descritos a seguir.

No primeiro capítulo será feita uma abordagem introdutória sobre os temas governança corporativa, riscos, gestão de riscos corporativos e gestão de continuidade de negócios, dando ao leitor uma breve visão dos conceitos básicos e padrões normativos de referência correspondentes.

No segundo capítulo será apresentada a fundamentação teórica do trabalho, abordando os seguintes assuntos: governança corporativa, gestão de riscos corporativos, incluindo riscos e controle internos preliminarmente, gestão de continuidade de negócios, sistemas de gestão e sistema de gestão de continuidade de negócios. Esta fundamentação procura descrever a origem, definição, benefícios, métodos de implantação, padrões normativos, e as inter-relações entre esses conceitos.

No terceiro capítulo serão apresentadas informações a respeito da empresa de telecomunicações em estudo, da sua estrutura, do mercado em que ela atua, dos seus objetivos, dos seus principais produtos e processos, bem como da apresentação e análise de sua estrutura de gestão de continuidade de negócios. Essa análise inclui o levantamento das principais dificuldades observadas na implantação do modelo de GCN e a constatação dos principais *GAPS* com relação à norma BS25999-1.

No quarto capítulo será apresentada, com base nas informações obtidas nos capítulos anteriores, uma proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios na empresa em estudo. Essa proposta inclui sugestões para a implantação de elementos de SGCN e o planejamento de ações através de tabelas no formato 3W1H. Ainda nesse capítulo será desenvolvida uma análise preliminar de aceitação da estrutura proposta perante os seus futuros usuários na empresa de referência.

O trabalho é concluído no quinto capítulo, apresentando as conclusões obtidas com relação aos objetivos inicialmente propostos e esclarecendo as limitações constantes desta etapa. Neste capítulo, são também apresentadas recomendações para trabalhos futuros, no sentido de incluir a avaliação e o planejamento proposto como prática de melhoria contínua de gestão em continuidade de negócios.

2. Da Governança Corporativa ao Sistema de Gestão de Continuidade de Negócios

Neste capítulo, serão abordados cinco assuntos principais que se relacionam entre si e ao mesmo tempo fundamentam a estrutura de apoio para a implantação do SGCN desenvolvida no capítulo 4. O objetivo é apresentar uma abordagem conceitual da Gestão de Continuidade de Negócios inserida no contexto de Gestão de Riscos (pois, como será visto ela é parte integrante deste) que, por sua vez, é um dos importantes instrumentos para a prática da Governança Corporativa. Além disso, pretende-se apresentar que o conceito de GCN evolui para um sistema de gestão de continuidade de negócios e, portanto, existem algumas diferenças relevantes entre esses dois modelos.

2.1 Governança Corporativa

A lógica do mercado de capitais depende da disponibilidade dos seus investidores e do razoável conhecimento destes sobre a saúde econômica e financeira da empresa em que pretendem investir. Já os acionistas dependem de informações válidas, íntegras e precisas para monitorar o desempenho do seu negócio e suportar a tomada de decisão. Nesse sentido, ganhou força nas últimas décadas um movimento originado nos Estados Unidos e Inglaterra denominado Governança Corporativa (OLIVEIRA et al., 2004). Esse movimento estabelece regras disciplinando o relacionamento dos interesses de acionistas controladores, acionistas minoritários e administradores dentro de uma companhia (GARCIA, 2005).

A governança corporativa, segundo IBGC (2008), surgiu para superar o chamado conflito de agência ou conflito agente-principal, originado a partir do momento em que o acionista delega ao executivo o poder de decisão sobre sua propriedade e as decisões destes não convergem com os interesses daqueles. Nesse contexto, Shleyfer e Vishny (1997) afirmam que o conflito de agência está relacionado à dificuldade dos acionistas assegurarem-

se de que seus fundos não estão sendo expropriados ou desperdiçados pelos executivos em projetos pouco atraentes.

Silveira (2002) ressalta que na maior parte do mundo, inclusive no Brasil, o problema de agência fundamental não ocorre somente entre investidores externos e gestores, mas sim entre os acionistas controladores (que exercem de fato o poder de controle sobre seus gestores) e os pequenos investidores externos.

O primeiro código das práticas de Governança Corporativa, *The Cadbury Report*, citado por Lodi (2000) *apud* OLIVEIRA et al. (2004, p. 3), definiu como "o sistema pelo qual as companhias são dirigidas e controladas" e coloca os conselheiros no centro de qualquer discussão sobre Governança Corporativa.

Uma visão um pouco mais prática do conceito de governança é trazida por Rake (2004) afirmando que se trata de um mecanismo pelo qual se assegura o monitoramento de empresas que possuem uma responsabilidade pública.

No Brasil, o Instituto Brasileiro de Governança Corporativa – IBGC apresenta uma definição mais objetiva sobre o tema:

> Governança Corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua longevidade. (IBGC, 2009).

O papel da governança corporativa é de agregar valor à companhia, apesar de por si só não criá-lo, e isso só é possível se em paralelo a uma boa governança existam outros fatores como a qualidade, a lucratividade e a boa prática de gestão. Dessa forma, a boa governança é capaz de permitir uma administração ainda melhor, em benefício de todos os acionistas e demais partes interessadas no negócio (AGUIAR, 2005).

IBGC (2008) afirma que a empresa que opta pelas boas práticas de governança corporativa adota como diretrizes principais a transparência, a prestação de contas (*accountability*), a eqüidade e a responsabilidade corporativa e que, para tanto, o Conselho de Administração deve exercer seu papel, estabelecendo estratégias para a empresa, elegendo e destituindo o principal executivo, fiscalizando e avaliando o desempenho da gestão e escolhendo a auditoria independente. Além disso, o mesmo autor ressalta que a ausência de conselheiros qualificados e de bons sistemas de governança corporativa têm levado empresas a fracassos decorrentes abusos de poder, erros estratégicos ou fraudes.

2.1.1 Governança Corporativa no mundo

A prática de boa governança nas instituições, segundo Vieira e Mendes (2004), é apresentado como um instrumento capaz de proporcionar maior transparência às partes interessadas, garantir o alinhamento de informação entre administradores e proprietários e reduzir as perdas dos acionistas minoritários numa eventual venda da companhia. O mesmo autor ressalta que as recentes crises e escândalos mundiais, como os casos Enron, World Com e Parmalat, despertaram entre as empresas a necessidade de práticas corporativas fundamentadas pela transparência, ética e segregação de funções.

A lei que reformou a regulamentação do mercado de capitais norte americano (através da imposição de padrões de governança corporativa para as empresas com ações nas bolsas de valores ou com negociações na Nasdaq) foi denominada de *Sarbanes-Oxley Act* e promulgada em 2002 através de dois membros do congresso americano, Paul Sarbanes e Michael Oxley. A referida lei foi instituída em resposta à descoberta de fraudes nas demonstrações financeiras de companhias como Enron, Tyco e WorldCom e visa suprir a necessidade de maior transparência na divulgação das informações financeiras através do aumento da responsabilidade dos diretores executivos e dos níveis menores de decisão, com foco na implementação de controles internos mais rígidos sobre as operações das companhias abertas (CRUZ et al., 2006).

A adoção de melhores práticas de governança corporativa tem crescido nos últimos anos em todos os mercados, entretanto mesmo em países com mesmo idioma ou sistemas legais semelhantes, como EUA e Reino Unido, a aplicação de boas práticas de governança apresenta diferenças quanto ao estilo, estrutura e enfoque. Na realidade, não existe uma unanimidade global sobre a correta aplicação das práticas de governança nos mercados, todavia pode-se afirmar que todos se baseiam nos mesmos pilares (transparência, independência e prestação de contas) como meio para atrair investimentos (IBGC, 2008).

Com a crescente evolução do estudo e aplicação da governança corporativa, foram surgindo, inicialmente nos países com mercados mais desenvolvidos, os Códigos de Melhores Práticas de Governança Corporativa. O primeiro, denominado *The Cadbury Report*, surgiu no Reino Unido em 1992 como resultado da criação do comitê *Cadbury*, iniciativa da Bolsa de Valores de Londres (*London Stock Exchange*) com o objetivo de revisar algumas práticas de governança corporativas sobre aspectos contábeis. Em seguida, outros códigos voltados para a governança corporativa no exterior foram surgindo, dentre os quais pode-se citar os seguintes: (i) *The NACD Report*, relatório preparado pela *National Association of Corporate Directors* e publicado em novembro de 1996; (ii) *Global Share Voting Principles*, publicado pela

International Corporate Governance Network – ICGN em julho de 1998; (iii) *The OECD Report*, publicado abril de 1999; (iv) *Euroshareholders Corporate Governance Guideline* 2000, publicado pelo *European shareholders Group* em fevereiro de 2000; e (v) *Policy Statement on Corporate Governance* editado regularmente pela TIAA-CREF – *Teachers Insurance and Annuity Association – College Retirement Equities Fund*, através de seu Comitê de Governança Corporativa e Responsabilidade (GARCIA, 2005).

A criação dos códigos de governança corporativa contribuíram para mudanças culturais e históricas nos mercados mundiais. Entretanto, algumas particularidades e práticas locais permanecem fortes, pois enquanto alguns países tem como característica dominante o modelo corporativo familiar, outras têm no capital pulverizado sua referência mais marcante (IBGC, 2008).

As características acionárias e dos mercados das companhias abertas mundiais convergem para a existência de dois principais sistemas de governança corporativa (IBGC, 2008):

> *Outsider System* (acionistas pulverizados e tipicamente fora do comando diário das operações da companhia); Sistema de governança anglo-saxão (Estados Unidos e Reino Unido), caracterizado por estrutura de propriedade dispersa nas grandes empresas; papel importante do mercado de ações na economia; ativismo e grande porte dos investidores institucionais; e foco na maximização do retorno para os acionistas (*shareholder oriented*);
> *Insider System* (grandes acionistas tipicamente no comando das operações diárias, diretamente ou via pessoas de sua indicação); Sistema de governança da Europa Continental e Japão, caracterizado por estrutura de propriedade mais concentrada; presença de conglomerados industriais-financeiros; baixo ativismo e menor porte dos investidores institucionais; e reconhecimento mais explícito e sistemático de outros *stakeholders* não financeiros, principalmente funcionários (*stakeholder oriented*). (IBGC, 2008)

Lethbridge (1997) assevera que no modelo anglo-saxão as participações acionárias são relativamente pulverizadas (por exemplo, os cinco maiores acionistas dos Estados Unidos detêm, em média, menos de 10% do capital total de cada empresa investida) e o mercado de capitais desses países garantem a liquidez dessas participações. Nesse modelo, a variação no preço das ações sinaliza a aprovação ou não em relação às administrações por parte dos investidores, demandando um nível elevado de transparência e uma divulgação periódica de informações, além de rígidos controles internos sobre o uso de informações.

Já no modelo nipo-germânico, segundo Lethbridge (1997), a propriedade é mais concentrada (por exemplo, os cinco maiores acionistas alemães, detêm, em média, 40% do capital total de cada empresa investida e, no Japão, 25%), e muitas participações acionárias são de longo prazo. Por exemplo, no Japão, de 50% a 70% das ações de empresas listadas nas bolsas de valores são de propriedade de outras empresas e na Alemanha os bancos usam participações acionárias como forma de fortalecer suas relações comerciais com clientes.

Nesse modelo, os acionistas buscam as informações necessárias para a tomada de decisões junto aos seus executivos.

2.1.2 Governança Corporativa no Brasil

Segundo Silveira (2002), os modelos de governança das principais companhias abertas brasileiras variam conforme suas características de constituição (empresas privadas nacionais, estatais ou multinacionais), entretanto a análise de pesquisas realizadas por instituições e empresas de consultoria, permitem traçar um modelo comum de governança corporativa no Brasil com as seguintes características:

> a) estrutura de propriedade com forte concentração das ações com direito a voto (ordinárias) e alto índice de emissão de ações sem direito a voto (preferenciais);
> b) empresas com controle familiar ou compartilhado por alguns poucos investidores alinhados por meio de acordo de acionistas para resolução das questões relevantes;
> c) presença de acionistas minoritários pouco ativos;
> d) alta sobreposição entre propriedade e gestão, com os membros do conselho representando os interesses dos acionistas controladores;
> e) pouca clareza na divisão dos papéis entre conselho e diretoria, principalmente nas empresas familiares;
> f) escassez de conselheiros profissionais no Conselho de Administração;
> g) remuneração dos conselheiros como fator pouco relevante;
> h) estrutura informal do Conselho de Administração, com ausência de comitês para tratamento de questões específicas, como auditoria ou sucessão. (SILVEIRA, 2002, p. 31)

Diante dessas características, pode-se afirmar que o modelo de governança das companhias abertas brasileiras assemelha-se com o nipo-germânico (*insider system*). Nesse sentido, Silveira (2002) ressalta como características marcantes do modelo de governança das companhias abertas brasileiras a forte concentração das ações com direito a voto e uma ausência quase total de empresas com estruturas de propriedade pulverizadas. Essa alta concentração da propriedade e de controle das companhias faz com que o principal conflito de agência no Brasil ocorra entre acionistas controladores e minoritários, e não entre acionistas e gestores, como nos países anglo-saxões.

O desenvolvimento das práticas e dos conceitos principais de Governança Corporativa no Brasil foram impulsionados por diversos fatores, dentre eles a globalização da economia, o poder de decisão reduzido dos acionistas minoritários previstos na Lei das S.A., o movimento de fusões e aquisições internacional e as privatizações (OLIVEIRA et al., 2004).

Nesse sentido, IBGC (2008) destaca que as privatizações facilitaram as primeiras experiências de controle compartilhado no Brasil, através da formalização dos acordos de acionistas, onde os investidores integrantes do bloco de controle, formalizaram contratualmente a divisão do comando da empresa. Com essa divisão de comando nas empresas houve aumento de investimentos de estrangeiros no mercado de capitais, o que

contribuiu para a necessidade de adaptação às exigências e padrões internacionais de governança.

Dentre as principais referências ao modelo de governança corporativa no Brasil, destacam-se a reforma na Lei das S.A., a criação do Novo Mercado pela Bolsa de Valores de São Paulo – BOVESPA, a Cartilha de Governança Corporativa da Comissão de Valores Mobiliários – CVM e o Código das Melhores Práticas do Instituto Brasileiro de Governança Corporativa – IBGC (OLIVEIRA et al., 2004).

Para Aguiar (2005), a reforma da Lei das S.A., formalizada pela Lei 10.303, de 31 de outubro de 2001, teve como objetivo conferir mais transparência e credibilidade ao mercado de capitais no Brasil. Seus autores partiram da premissa de que o alinhamento de interesses gera valor e quanto maior o equilíbrio entre acionistas mais ela vale. Dentre as principais inovações da reforma, destacam-se:

> a) a proporção entre ações ordinárias e preferenciais passa a ser de 50% para as companhias constituídas a partir da nova lei;
> b) modificação das vantagens atribuídas às ações preferenciais, visando a fazer das mesmas um produto mais atraente para o investidor;
> c) explicitação das regras de atuação do conselheiro fiscal, que pode ser individual e a quem serão estendidos os mesmos deveres reservados aos conselheiros de administração;
> d) melhoria no processo de divulgação de informações para assembléias, bem como alargamento de seu prazo de convocação;
> e) a CVM passa a ter a natureza de entidade autárquica em regime especial, com personalidade jurídica e patrimônio próprios;
> f) tipificação de crimes contra o mercado de capitais como manipulação de mercado, uso indevido de informação privilegiada e exercício irregular de cargo, profissão, atividade ou função. (AGUIAR, 2005, p.20)

O Novo Mercado foi criado em 2000 pela Bovespa, inspirado no *Neuer Markt* Alemão de 1997 e teve como premissa básica o entendimento de que a redução da percepção de risco por parte dos investidores influenciaria positivamente a valorização e a liquidez das ações (SANTANA et al., 2006). Trata-se de um segmento da Bolsa de Valores de São Paulo (BOVESPA) com regras de listagem diferenciadas e destinado a empresas que se comprometem com a adoção de práticas de governança corporativa e transparência adicionais ao que é exigido pela legislação (AGUIAR, 2005).

A Comissão de Valores Mobiliários – CVM foi criada pela Lei nº 6.385 de 1976 e trata-se de entidade autárquica vinculada ao Ministério da Fazenda, mas com personalidade jurídica própria e administração independente que possui, dentre outras competências, a de fiscalizar permanentemente as atividades e os serviços do mercado de valores mobiliários, assim como a veiculação de informações relativas ao mercado, às pessoas que dele participem, e aos valores nele negociados (CVM, 2008). Em junho de 2002, a CVM publicou uma cartilha de governança corporativa com o objetivo de estimular o desenvolvimento do mercado de capitais brasileiro por meio da divulgação de práticas de boa governança. Trata-se

de um documento baseado em práticas internacionais e adaptado à realidade brasileira com informações sobre questões influentes sobre a relação entre administradores, conselheiros, auditores independentes, acionistas controladores e acionistas minoritários (CVM, 2002).

Em 1995 foi criado o IBCA – Instituto Brasileiro de Conselheiros de Administração que passou a chamar-se em 1999 de IBGC – Instituto Brasileiro de Governança Corporativa. Trata-se de uma sociedade civil sem fins lucrativos de referência nacional no desenvolvimento de conceitos e disseminação da governança corporativa (IBGC, 2008).

Dentre os trabalhos desenvolvidos por esse instituto, destaca-se o Código Brasileiro de Melhores Práticas de Governança Corporativa, lançado em maio de 1999, época em que o assunto era praticamente desconhecido no Brasil e que influenciou os debates sobre os principais modelos e práticas de governança, contribuindo para a evolução do ambiente institucional e empresarial brasileiro (OLIVEIRA et al., 2004).

Os princípios básicos que norteiam este Código, que encontra-se atualmente na quarta edição, são:

> a) transparência: mais que a obrigação de informar é o desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. A adequada transparência resulta um clima de confiança, tanto internamente, quanto nas relações da empresa com terceiros. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à criação de valor;
> b) equidade: caracteriza-se pelo tratamento justo de todos os sócios e demais partes interessadas (*stakeholders*). Atitudes ou políticas discriminatórias, sob qualquer pretexto, são totalmente inaceitáveis;
> c) prestação de contas *(accountability):* os agentes de governança devem prestar contas de sua atuação, assumindo integralmente as conseqüências de seus atos e omissões;
> d) responsabilidade: os agentes de governança devem zelar pela sustentabilidade das organizações, visando à sua longevidade, incorporando considerações de ordem social e ambiental na definição dos negócios e operações. (IBGC, 2009)

O Código Brasileiro de Melhores Práticas de Governança Corporativa divide-se em seis capítulos, a saber: 1) Propriedade; 2) Conselho de Administração; 3) Gestão; 4) Auditoria Independente; 5) Conselho Fiscal e 6) Conduta e Conflito de Interesses. Nos capítulos 2 e 3 do Código do IBGC de 2009 destaca-se a preocupação com os temas Gerenciamento de Riscos e Controles Internos, que serão vistos com mais detalhes na próxima seção. Sobre estes assuntos o Código estabelece:

> a) Gerenciamento de riscos: o Conselho de Administração deve assegurar-se de que a Diretoria identifique preventivamente – por meio de sistema de informações adequado – e liste os principais riscos aos quais a sociedade está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização;
> b) Controles internos: o principal executivo é responsável pela criação de sistemas de controle internos que organizem e monitorem um fluxo de informações corretas, reais e completas sobre a sociedade, como as de natureza financeira, operacional, de obediência às leis e outras que apresentem fatores de risco importantes. A efetividade de tais sistemas deve ser revista no mínimo anualmente. (IBGC, 2009)

Verifica-se, portanto, através do Código de Melhores Práticas de Governança Corporativa, a responsabilidade do Conselho da Administração e da Diretoria em garantir a identificação, avaliação e tratamento dos riscos a que suas companhias estão expostas, bem como garantir uma estrutura de controles internos adequada. Esse exemplo demonstra a relação intrínseca entre os temas gestão de riscos e governança corporativa. Na próxima seção, serão apresentados mais detalhes sobre como a gestão de risco se estabelece e se desenvolve no contexto corporativo.

2.2. Riscos, Controles Internos e Gestão de Riscos Corporativos

Como se viu na seção anterior, o gerenciamento de riscos é um dos instrumentos para a aplicabilidade da Governança Corporativa nas organizações. Nesta seção, serão abordados com mais detalhes o significado da Gestão de Riscos (GR), a sua importância e como este conceito é aplicado nas Organizações. Todavia, antes que este tema seja desenvolvido, é importante que se faça uma abordagem histórica e conceitual sobre dois temas que precedem a GR historicamente e ao mesmo tempo a fundamentam. São eles: riscos e controles internos.

2.2.1 Riscos

Antever o futuro, para as antigas civilizações, era um dom destinado apenas aos oráculos e adivinhos, que realizavam previsões sobre possíveis eventos futuros e detinham certo monopólio sobre o conhecimento humano. Todavia, a capacidade de desenvolvimento do ser humano em pensar, analisar e tomar suas próprias decisões e responsabilidades definiu a fronteira entre o passado e os tempos modernos e transformou o futuro da humanidade em algo mais previsível e não fruto da vontade dos deuses (ARAÚJO, 2006).

Segundo Bernstein (1997) *apud* Ayres (2007), a palavra risco vem do italiano *risicare* que significa ousar. Ayres (2007) comenta que o autor, no livro Desafio aos deuses, apresenta a história do risco ao longo dos séculos desde a época em que o homem julgava não ter inferência sobre fatos e procurava sacerdotes ou oráculos para entender o que as forças superiores lhe haviam reservado, transitando pela Renascença, onde matemáticos começaram a refletir questões sobre probabilidade e criaram problemas a partir de jogos de azar. Nesse sentido, o mesmo autor comenta que Cardano, Pascal e Fermat deram contribuições importantes ao desenvolver um método para cálculo do risco de cada arremesso dos dados, contribuindo decisivamente para a teoria das probabilidades.

Ainda sobre a evolução do risco, Ayres (2007) comenta que:

> [...] numa das passagens do livro, Bernstein (1997) cita Daniel Bernoulli, matemático suíço do século XVII, o qual associava risco com utilidade e dizia que a utilidade resultante de qualquer pequeno aumento da riqueza será inversamente proporcional à quantidade de bens anteriormente possuídos, ou seja, ao valor do patrimônio anteriormente conquistado. Bernoulli quebra um paradigma, pois sustenta em sua obra (Nova Teoria) que - ao contrário de Pascal e Fermat, os quais forneceram métodos para calcular riscos de maneira probabilística - são as motivações pessoais que contam numa opção pelo risco. Em sua obra, Bernoulli tenta explicar porque poucas pessoas se dispõem a pagar preços proporcionalmente elevados por uma promessa ou perspectiva de lucros, mesmo que ela seja enorme. Ou seja, dada a probabilidade de um determinado cenário, quanto uma pessoa estaria disposta a apostar (investir)? Nesse período a base científica da gestão de risco começa a tomar forma, pois Bernoulli não se concentrou nos eventos em si, mas nos seres humanos que, em maior ou menor grau, temem certos resultados. (AYRES, 2007, p.3)

A atitude de enfrentar riscos mostrou ao mundo como identificar, medir e avaliar suas conseqüências, sendo um dos principais motivadores do desenvolvimento. A partir da sociedade feudal gradativamente as sociedades adotaram essa atitude influenciando as empresas atuais a se exporem a determinados riscos e administrá-los (ARAÚJO, 2006).

De acordo com Cocurullo (2004) risco é qualquer situação que pode afetar a capacidade de atingir objetivos, sendo inerente a qualquer atividade, decisão ou até mesmo à vida.

Santos (2002) *apud* Oliveira et al. (2006, p.2) define risco como “o grau de incerteza em relação à possibilidade de ocorrência de um determinado evento, o que, se realizado, redunda em prejuízos”, onde perda para a empresa pode significar prejuízo, lucro menor, ou redução de ativos.

Segundo a ABNT (2009), que publicou a nova versão do ISO Guia 73 (guia internacional de referência no vocabulário sobre Gestão de Riscos) o risco é o efeito da incerteza nos objetivos, o que, muitas vezes, é caracterizado pela referência aos eventos potenciais e às conseqüências, ou uma combinação destes, ou também sendo expresso em termos de uma combinação de conseqüências de um evento e a probabilidade de ocorrência associada.

Para Padoveze e Bertolucci (2005, p.1), risco corporativo é “o conjunto de riscos identificáveis que podem afetar uma organização, cada um com sua probabilidade de ocorrência e nível de impacto econômico”.

Já Baraldi (2005) apresenta um conceito menos técnico e mais prático, afirmando que os riscos empresariais tratam-se de eventos que impedem a empresa e as pessoas de ganharem dinheiro e respeito.

Conforme Linsmeier e Pearson (1996) *apud* OLIVEIRA et al. (2006) o risco do negócio pode surgir de várias formas, podendo estar ligado tanto à tomada de decisões sobre

investimentos como no lançamento de determinado produto ou nas estratégias de marketing e vendas.

Os eventos podem gerar tanto impacto negativo quanto positivo e, em alguns casos, ambos. Os eventos de impacto negativo podem impedir a criação de valor ou até mesmo destruir o valor existente numa organização. Em contrapartida, os eventos de impacto positivo podem representar oportunidades, influenciando favoravelmente na realização dos objetivos da organização criando ou preservando valor. Nesse sentido, a direção da organização possui papel fundamental no sentido de canalizar as oportunidades na elaboração de estratégias ou objetivos (COSO, 2007).

Segundo o Guia de Orientação para o Gerenciamento de Riscos Corporativos, desenvolvido por IBGC (2007) é importante determinar a origem dos eventos (riscos externos ou internos), pois auxilia na definição da abordagem a ser empregada por parte da organização. O Guia define a origem dos eventos através dos seguintes conceitos:

> a) Riscos externos: são ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a organização opera. Exemplos: nível de expansão do crédito, grau de liquidez do mercado, nível das taxas de juros, tecnologias emergentes, ações da concorrência, mudança no cenário político, conflitos sociais, aquecimento global, catástrofes ambientais, atos terroristas, problemas de saúde pública, etc. A organização, em geral, não consegue intervir diretamente sobre estes eventos e terá, portanto, uma ação predominantemente reativa. Isto não significa que os riscos externos não possam ser "gerenciados"; pelo contrário, é fundamental que a organização esteja bem preparada para essa ação reativa;
> b) Riscos internos: são eventos originados na própria estrutura da organização, pelos seus processos, seu quadro de pessoal ou de seu ambiente de tecnologia. A organização pode e deve, em geral, interagir diretamente com uma ação pró-ativa. (IBGC, 2007, p. 18).

No tocante à natureza dos riscos, IBGC (2007) destaca a importância de se classificar os riscos, o que permite sua agregação de uma forma organizada e de acordo com a sua natureza. Os riscos podem pertencer a categorias diferentes e em alguns casos poderão se encaixar em duas ou mais categorias simultaneamente. Segundo o autor, em alguns segmentos de negócio mais regulados, como no setor bancário, o órgão regulador estabelece como esses riscos devem ser classificados.

Portanto, segundo o entendimento do IBGC (2007), os riscos podem ser classificados em três naturezas diferentes:

> a) Riscos estratégicos: estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização. Os riscos decorrentes da má gestão empresarial muitas vezes resultam em fraudes relevantes nas demonstrações financeiras. Exemplos: falhas na antecipação ou reação ao movimento dos concorrentes causadas por fusões e aquisições; diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência em função de desenvolvimento de novas tecnologias/produtos pelos concorrentes.
> b) Riscos operacionais: estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos

> externos como catástrofes naturais, fraudes, greves e atos terroristas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impacto regulatório negativo na reputação da sociedade, além da potencial geração de passivos contratuais, e ambientais;
> c) Riscos Financeiros (mercado, crédito e liquidez): são aqueles associados à exposição das operações financeiras da organização. São os riscos de que os fluxos de caixa não sejam administrados efetivamente para maximizar a geração de caixa operacional, gerenciar os riscos e retornos específicos das transações financeiras e captar e aplicar recursos financeiros de acordo com as políticas estabelecidas. São ocorrências tais como a administração financeira inadequada, que conduz a endividamento elevado, podendo causar prejuízo frente à exposição cambial ou aumentos nas taxas de juros, etc. Incluem-se neste grupo operações no mercado de derivativos de *commodities*. Ainda no contexto de riscos financeiros é comum que se destaque o risco associado à confiabilidade das informações transmitidas nos relatórios financeiros divulgados pelas organizações - principalmente na literatura dedicada ao cumprimento da Lei Sarbanes-Oxley. (IBGC, 2007, p.18-19).

Além da classificação quanto à natureza e origem dos eventos, os riscos também são usualmente classificados conforme o tipo. Essa classificação por tipo de risco, conforme COSO (2007), está relacionada ao tipo de evento associado. A Figura 1, desenvolvida por Deloitte (2003) ilustra esquematicamente os tipos de riscos mais utilizados nas organizações, de acordo com a natureza e origem dos eventos. Nela pode-se observar as categorias de riscos externos e internos, as categorias de riscos operacional, estratégico e financeiro (representada como mercado e crédito) e diversos tipos de riscos, tais como competição, disponibilidade de capital, regulamentação, fraudes, práticas comerciais, relações trabalhistas, execução e gestão de processos, recursos humanos, liquidez, inadimplência, etc. Além desses tipos de riscos, destaca-se o risco de interrupção de negócio, a ser estudado em 2.3 e que, segundo Deloitte (2003), pode ter origem externa ou interna.

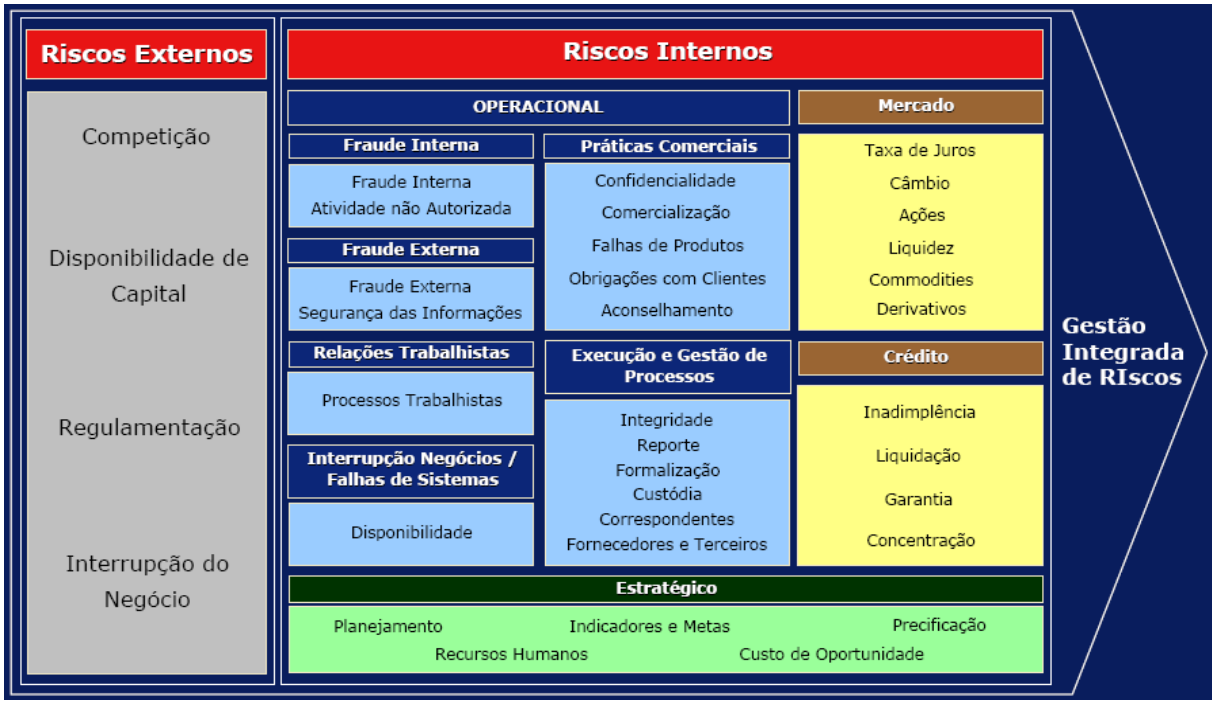

Figura 1 – Classificação de Riscos

Fonte: Deloitte (2003)

Araújo (2006) comenta que muitos riscos dentro das organizações podem decorrer de processos inadequados ou da ineficiência dos controles internos. Nesses casos, em geral, o risco se materializa através de fraudes ou erros praticados por empregados, do inadequado desenho de processos corporativos, da falta de planejamento e monitoração, na delegação inadequada de competências e na falta de procedimentos padronizados, repercutindo em uma área específica ou em toda a companhia.

2.2.2 Controles Internos

Os riscos, segundo Araújo (2006), fazem parte da vida empresarial e gerenciá-los é medida essencial para o desenvolvimento da organização que visa obter lucros e agregar valor para seus proprietários. A classificação dos riscos pode variar de acordo com as características das empresas e do setor em que elas atuam o que demanda a utilização de controles internos diferenciados. O mesmo autor ressalta que na medida em que as atividades empresariais envolvem riscos, o empresário deve avaliar e mensurar os riscos envolvidos em suas decisões, devendo administrá-los com base nos controles internos existentes.

Bergamini Junior (2005) comenta que, em trabalhos recentes, alguns autores vêm aumentando o nível de abrangência dos controles internos ao afirmarem que estes constituem um processo implementado pela alta administração da empresa e que envolve todos os colaboradores, visando prover razoável garantia quanto à realização dos objetivos específicos da companhia. Essa razoável garantia a ser obtida através de controles internos deve prover, dentre outros, o alinhamento das ações ao direcionamento estratégico, conceder efetividade e eficiência às operações, obter confiabilidade no processo de comunicação (em especial a divulgação de relatórios financeiros) e assegurar a conformidade com as leis e regulamentos aplicáveis.

Gherman (2005) *apud* Rego et al. (2007) afirma que grandes, médias e até mesmo pequenas instituições utilizam controles internos para atender diferentes propósitos, como, por exemplo, obter conformidade legal, implantar projetos de Governança Corporativa e buscar certificação por órgão acreditador. O mesmo autor comenta que o grande desafio das instituições seria a busca da solução ideal para o processo de gestão de riscos, sendo este um dos importantes pilares para o processo de Governança Corporativa.

Na mesma linha, Araújo (2006) afirma que a prática de um controle interno eficiente contribui para um Gerenciamento de Riscos mais eficaz e que o direcionamento dos controles internos possibilita à Alta Administração supervisionar o processo de gerenciamento dos

riscos conduzido pelos administradores, facilitando o aumento do valor da empresa e o seu desenvolvimento.

Escândalos recentes no cenário corporativo mundial trouxeram à tona declarações de executivos que afirmavam desconhecer as atividades fraudulentas praticadas por suas companhias como, por exemplo, as participações não registradas nos livros caixa e os reconhecimentos impróprios de receitas. Para prevenir essas atividades, foi criada a Lei americana Sarbanes-Oxley que regulamentou várias medidas no sentido de intensificar a avaliação de controles internos e aumentar a responsabilidade civil e criminal dos executivos. Portanto, pode-se afirmar que a Lei Sarbanes-Oxley privilegia o papel crítico do controle interno, sendo um processo executado pela Diretoria, pelo Conselho de Administração ou por outras pessoas da companhia que visa garantir o sucesso dos negócios sob três aspectos: eficácia e eficiência das operações, confiabilidade dos relatórios financeiros e cumprimento de leis e regulamentos aplicáveis (DELOITTE, 2003).

De acordo com Cocurullo (2003), as necessidades de controle interno das organizações são diferentes, pois estas podem depender tanto do tamanho da instituição como da filosofia da gerência, do setor em que ela atua ou da cultura e, dessa forma, não existem sistemas de controle interno idênticos.

Segundo Gherman (2005) *apud* Araújo (2006), muitas empresas possuem dificuldades para elaborar uma estrutura de controles internos adequada às suas necessidades, fato que ocasionou uma grande procura das empresas por estruturas prontas e flexíveis, denominadas *frameworks*, cuja funcionalidade engloba normalmente o foco nos objetivos de negócio e missão da instituição, a gestão de riscos corporativos (em especial os riscos operacionais e a conformidade com a legislação aplicável.

Segundo Deloitte (2003), várias estruturas (*frameworks*) para a avaliação dos controles internos estão disponíveis. Dentre as mais importantes, destacam-se:

> a) COSO – Estrutura Integrada de Controles Internos: desenvolvida pelo *Committee of Sponsoring Organizations of the Treadway Commission* e patrocinada pela AICPA, FEI e IIA entre outros, o COSO é a estrutura dominante nos Estados Unidos. As diretrizes foram publicadas em 1991, com revisões antecipadas e atualizações posteriores. É a estrutura escolhida pela grande maioria das companhias de capital aberto sediada nos EUA;
> b) CoCo – Modelo de Controles: desenvolvido pelo *Criteria of Control Committee of Canadian Institute of Chartered Accountants*, o CoCo concentra-se nos valores comportamentais como a base fundamental para os controles internos de uma companhia, e não na estrutura e nos procedimentos de controle;
> c) *Turnbull Report* – Controles Internos: Diretrizes para Diretores sobre o Código Combinado: desenvolvido pelo *Committee on Corporate Governance of the Institute of Chartered Accountants in England & Wales*, em parceria com a *London Stock Exchange*, o guia foi publicado em 1999. O Turnbull exige que as companhias identifiquem, avaliem e administrem seus riscos significativos e avaliem a eficácia do sistema de controles internos relacionado;

> d) ACC – *Australian Criteria of Control*: emitido em 1998 pelo *Institute of Internal Auditors* – Austrália, o ACC enfatiza a competência da administração e dos funcionários para desenvolver e operar a estrutura de controles internos. Trata-se de um controle independente, que inclui atributos como atitudes, comportamentos e competência, e é promovido como o enfoque mais compensador em termos de custo para os controles internos;
> e) *King Report* – expedido pelo *King Committee on Corporate Governance* em 1994, promove padrões gerais para governança corporativa na África do Sul. O King Report ultrapassa os aspectos financeiros e reguladores usuais da governança corporativa, direcionando questões sociais, éticas e ambientais. (DELOITTE, 2003, p. 14)

Segundo Deloitte (2003) muitas companhias elaboram a sua estrutura de controles internos baseadas no *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, entretanto o *framework* de COSO (1992), apesar de ser o mais reconhecido e aplicado mundialmente, representa apenas uma das muitas estruturas de controles internos existentes. A estrutura de COSO (1992) divide os controles internos eficazes em cinco componentes inter-relacionados (visando simplificar o gerenciamento e supervisão das atividades que fazem parte de uma estrutura de controles internos bem-sucedida), os quais são descritos a seguir:

> a) Ambiente de Controle: abrange toda a estrutura de controles internos – é o universo no qual todos os outros elementos existem. O Ambiente de Controle inclui conceitos como conduta, atitude, consciência, competência e estilo. Grande parte de sua força é extraída da conduta estabelecida pelo Conselho de Administração e pelos executivos da companhia;
> b) Avaliação de Riscos: envolve a identificação e a análise pela Administração dos riscos mais relevantes para a obtenção dos objetivos do negócio. No decorrer de uma avaliação de riscos, cada objetivo operacional, do nível mais alto (como "dirigir uma companhia lucrativa") ao mais baixo (como "salvaguardar caixa"), é documentado e então cada risco que possa prejudicar ou impedir o alcance do objetivo é identificado e priorizado;
> c) Atividades de Controle: são desenvolvidas para direcionar especificamente cada objetivo de controle, visando atenuar os riscos identificados anteriormente. As atividades de controle são políticas, procedimentos e práticas adotados para assegurar que os objetivos operacionais sejam atingidos e as estratégias para atenuar riscos sejam executadas;
> d) Informação e Comunicação: fornecem suporte aos controles internos, transmitindo diretrizes do nível da administração para os funcionários, em um formato e uma estrutura de tempo que lhes permitem executar suas atividades de controle com eficácia. O processo também poderia percorrer o caminho inverso, partindo dos níveis mais baixos da companhia para a administração e para o Conselho de Administração, transmitindo as informações sobre os resultados, as deficiências e as questões geradas;
> e) Monitoramento: é o processo para estimar e avaliar a qualidade dos controles internos durante avaliações contínuas e especiais. O Monitoramento pode incluir tanto a supervisão interna quanto externa dos controles internos pela administração, pelos funcionários, ou pelas partes externas (COSO, 1992 *apud* DELOITTE, 2003, p. 14)

2.2.3 Gestão de Riscos Corporativos

A gestão de riscos, segundo FERMA (2003), trata-se de um elemento fundamental na gestão estratégica de qualquer empresa, sendo definido como o processo através do qual as

organizações analisam os riscos inerentes às suas atividades com o objetivo de atingirem uma vantagem sustentada em suas atividades individuais ou em conjunto. Segundo o autor, o ponto principal de uma boa gestão de riscos é a oportunidade de identificação e tratamento dos mesmos, buscando acrescentar valor à organização, interpretar os potenciais aspectos positivos e negativos dos eventos capazes de impactar a organização e aumentar a probabilidade de êxito no alcance dos objetivos globais da organização.

Dessa forma, FERMA (2003) afirma que a gestão de riscos deve:

> (i) ser um processo contínuo e em constante desenvolvimento aplicado à estratégia da organização e à implementação dessa mesma estratégia; (ii) analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e, em especial, futuras de uma organização; (iii) ser integrada na cultura da organização com uma política eficaz e um programa conduzido pela direção de topo; (iv) traduzir a estratégia em objetivos tácticos e operacionais, atribuindo responsabilidades na gestão dos riscos por toda a organização, como parte integrante da respectiva descrição de funções. Esta prática sustenta a responsabilização, a avaliação do desempenho e respectiva recompensa, promovendo desta forma a eficiência operacional em todos os níveis da organização. (FERMA, 2003, p.3)

A gestão de riscos ou o gerenciamento de riscos corporativos, como também é chamado, segundo COSO (2007) é:

> o processo conduzido em uma organização pelo Conselho de Administração, pela diretoria executiva e pelos demais funcionários, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetar a referida organização, e administrar os riscos para mantê-los compatíveis com o seu apetite a risco e possibilitar garantia razoável de cumprimento dos objetivos da entidade. (COSO, 2007, p.4)

A gestão de riscos tornou-se atualmente uma ferramenta empresarial necessária para um processo de tomada de decisão. Nesse sentido, Buchanan e O´Connell (2006) comentam que ao longo dos anos foram desenvolvidas diversas ferramentas visando a melhor compreensão e previsibilidade do comportamento humano e dos eventos.

Segundo Ministério da Previdência Social (2003) - que desenvolveu uma cartilha sobre gerenciamento de riscos operacionais de previdência social - o gerenciamento de riscos propicia diversos benefícios para a organização, dentre os quais:

> a) gerenciamento mais efetivo de recursos, eventos, programas e atividades;
> b) visão clara dos objetivos e resultados do negócio;
> c) benefícios decorrentes da identificação sistemática das deficiências organizacionais;
> d) maior habilidade na identificação das necessidades de todos os envolvidos;
> e) maior segurança para os servidores e para o cliente-cidadão;
> f) aperfeiçoamento da comunicação, tanto interna quanto externa;
> g) aprimoramento da conformidade legal, aderência aos regulamentos ou outras exigências formais;
> h) custos menores e previsões orçamentárias mais precisas;
> i) melhora da imagem e da reputação da organização;
> j) maior participação e interesse da sociedade no negócio e na organização;
> k) maior suporte financeiro;
> l) maior compromisso e responsabilidade dos gestores (*accountability*); e
> m) uma organização melhor gerenciada, capaz de sustentar os objetivos governamentais. (MPS, 2003, p.10)

Na visão do IBGC (2007), o gerenciamento de riscos é uma prática antiga que faz parte da rotina de qualquer empresário e historicamente têm sido elaborada uma ampla literatura sobre o assunto para a área de seguros. Atualmente, segundo o autor, esse tema tem se desenvolvido como uma metodologia estruturada a partir de vertentes como finanças, auditoria e tecnologia da informação.

As principais referências que historicamente vêm consolidando os conceitos e ferramentas da gestão de riscos são segmentadas, segundo Macieira (2008), em dois grupos:

> a) regulações que definem o conjunto de requisitos mínimos a ser atendido visando a assegurar o bem estar de uma determinada indústria (BACEN, SUSEP) ou segmento empresarial (CVM, SOX); e
> b) modelos de referências que consolidam as principais boas práticas de gestão de riscos, controles internos e auditoria interna. (MACIEIRA, 2008, p.3)

Segundo Macieira (2008), tanto os modelos de referência como as regulações são comumente desenvolvidos por áreas usuárias, consultorias, auditorias, órgãos reguladores ou normatizadores de gestão de risco. Segundo o autor, tais referências possuem o importante papel de difundir amplamente um conjunto de práticas de gestão de riscos. O Quadro 1 apresenta de forma sistematizada, a evolução histórica das legislações de referência em gestão de riscos.

Quadro 1 – Legislação de Referência em Gestão de Riscos

Legislação	Ano	Descrição Geral	Autor
Basiléia II	2004	Publicação desenvolvida por diversas empresas e instituições do setor financeiro com a intenção de se criar um padrão internacional para a formulação de leis e regulamentações relacionadas à gestão de riscos em bancos. O documento é dividido em três pilares: Requerimento mínimo de capital, processo de revisão para supervisão e disciplina de mercado. Trata-se de um conteúdo bastante detalhado que propõe o uso de ferramentas matemáticas não triviais.	*Basel Committee on Banking Supervision*
Sarbanes-Oxley Act	2002	Lei federal que determina práticas de controles internos sobre relatórios financeiros para todas as empresas com ações negociadas na bolsa de Nova York. Além disso, a lei responsabiliza, civil e criminalmente os principais executivos destas empresas pela confiabilidade das informações financeiros e contábeis publicada. Esta lei também exige que as organizações realizem avaliações dos seus sistemas de controle e que tais avaliações sejam objeto de uma auditoria independente.	SEC - *Security Exchange Comission*
JSox (*Financial Instruments and Exchange Act*)	2006	Considerada a versão japonesa da SOX.	Parlamento Japonês
Combined Code of Corporate Governance (*Turnbull Cadbury Report*)	1992 (1a versão) 2003 (última revisão)	Código de práticas de Governança corporativa e controles internos sobre relatórios financeiros com o qual todas as empresas com ações negociadas na bolsa de Londres devem estar em conformidade e demonstrá-las através da publicação de relatórios públicos. O código consiste da combinação de dois documentos: o Cadbury Report, que trata de governança corporativa e o Turnbull Report que aborda controles internos sobre relatórios financeiros.	FRC - Financial Reporting Council

BSA (*Bank Secrecy Act*)	1970 (publicação versão do BSA) 2001 (Patriot Act)	Determina a colaboração de todas as instituições financeiras norte americanas com o Governo objetivando a prevenção da lavagem de dinheiro. Para tanto, as instituições financeiras devem submeter ao governo relatórios específicos sobre determinadas transações financeiras. Outros atos foram promulgados atualizando o *Banks Secrecy Act*, o último dos quais foi o *Patriot Act*.	Governo Federal dos Estados Unidos
Resoluções do Banco Central No 2554, 3056, 3380 e 3490	2554 - 1998; 3056 - 2001; 3380 - 2006; 3490 -2007	Determina a implementação de práticas de gestão de riscos por parte de instituições financeiras no Brasil, dentre algumas: 2554 – implementação de um sistema de controles internos; 3056 – dispõe sobre a auditoria interna; 3380 – implementação de uma área de riscos operacionais; 3490 – trata da apuração do Patrimônio de Referência Exigido (capital econômico).	Banco Central do Brasil
Circular SUSEP 249, 280, 327	249 – 2004 280 - 2004 327 - 2006	Determina a implementação de práticas de controles internos em seguradoras. Alguns exemplos destas circulares são: circular 249 que dispões sobre a criação de uma estrutura de controle internos em uma seguradora; circular 280 que estabelece os procedimentos mínimos associados aos controles internos e sobre o descumprimento de dispositivos legais e regulamentares; circular 327 que dispõe sobre os controles internos específicos para o tratamento de situações relacionadas a crimes como lavagem de dinheiro, etc.	SUSEP - Superintendência de Seguros Privados

Fonte: Macieira (2008, p.3)

Dentre a legislação aplicável à Gestão de Riscos destaca-se com maior relevância em relação às demais a Lei Sarbanes Oxley, promulgada em 2002 em resposta aos escândalos de fraudes nas demonstrações financeiras de grandes companhias norte americanas e que obrigou as empresas com ações negociados em bolsas americanas a desenvolverem adequadamente a sua estrutura de governança, gestão de riscos e controles internos. Nesse sentido, o IBGC (2007) comenta que essa lei serviu de base para regulamentações locais internacionais e contribuiu para a aplicação metodologia que a área de auditoria vinha desenvolvendo sobre controles internos. Segundo o autor, a SOX recomenda que o *framework* de controles internos a ser utilizado pelas empresas seja baseado no COSO – *The Committee of Sponsoring Organizations of the Tradeway Commission*).

Sobre os modelos de referência em gestão de riscos, o Quadro 2 apresenta, de forma sistematizada, a evolução histórica dos principais frameworks existentes no mundo.

Quadro 2 – Modelos de Referência em Gestão de Riscos

Modelo	Ano	Descrição Geral	Autor
COSO Internal Control – *Integrated Framewok*	1992	Principal *framework* existente até hoje para implantação de uma estrutura de controles internos a partir de cinco componentes centrais: ambiente de controle; risk assessment; atividades de controle; informação e comunicação; monitoração.	COSO – *Committee of Sponsoring Organizations of the Treadway Commission*
FSA *Handbook*	2001	*Handbook online* completo com orientações e boas práticas bem detalhadas para instituições financeiras. O site da FSA permite ainda a construção de *handbooks* com conteúdos personalizados de acordo com a organização.	FSA - *Financial Services Authority*. Órgão regulador de instituições financeiras no Reino Unido
FERMA	2002	Cartilha para difusão da disciplina de gestão de riscos na Europa a partir de uma visão objetiva do processo de gestão de riscos. Este manual também apresenta um conjunto de *templates* para descrição e análise de riscos.	FERMA – *Federation of European Risk Managers Association*
AS/NZS 4360	1995 (1a versão) 2004 (última revisão)	Uma das principais referências utilizadas para processos de gestão de riscos no mundo. Este modelo apresenta um conjunto interessante de *templates* e práticas que se propõe ser aplicáveis para gerir riscos no contexto de um processo, de uma empresa, ou até mesmo no projeto de vida de um indivíduo.	*Standards Australia e Standards New Zealand*
COSO *Enterprise Risk Management – Integrated Framewok*	2004	Este *Framework* se propõe a ampliar o conceito de COSO Internal Control, de forma a maximizar o valor gerado pela gestão de riscos alinhando-o a estratégia da organização. Este manual introduz os conceitos de apetite de riscos e visão integrado de riscos (ERM).	COSO – *Committee of Sponsoring Organizations of the Treadway Commission*
Orange Book	2004	Visão inicial da abordagem de gestão de riscos e como esta disciplina se desdobra nos vários níveis de uma organização, desde o planejamento estratégico, até suas operações específicas.	*Her Majesty's Treasury* - Ministério econômico e financeiro do Reino Unido
Best practicies in qualitative operational risk management	2006	Handbook prático para a gestão de riscos operacionais baseado em experiências reais em instituições financeiras e na estrutura do COSO *Enterprise Risk Management – Integrated Framewok*. Este manual apresenta diversos insights práticos sobre o uso gestão de riscos operacionais.	*TransConstelation* - Associação de empresas da área de processamento de transações financeiras
Red Book	2007	Apresenta um Framework constituído de 9 componentes para a implantação de um programa que integre as diversas iniciativas organizacionais de Governança, Riscos e *Compliance* (GRC). Cada componente é dividido em sub-componentes e em diretrizes.	OCEG – *Open Compliance and Ethics Group*
BS 31100	2008	Manual desenvolvido pela BSI para orientar a gestão de riscos. Apresenta 10 princípios-chave para gestão de riscos, um modelo de gestão de riscos, um framework de gestão de riscos, um processo de gestão de riscos e um capítulo dedicado à implantação da gestão de riscos.	BSI – *British Standard Institution*
ISO 31000	2009	Principal norma de gestão de riscos do mundo. Apresenta os 11 princípios da gestão de riscos, uma orientação sobre como construir e monitorar um *framework* para gestão de riscos e um processo genérico de gestão de riscos.	ISO – *International organization for standardization*

Fonte: Adaptado de Macieira (2008, p.3)

Dentre os modelos de referência em Gestão de Riscos Corporativos destacam-se com maior relevância o COSO, a Norma AS/NZS4360 e a ISO31000. Segundo o IBGC (2007), o COSO é uma entidade internacional sem fins lucrativos com o propósito de desenvolver a melhoria dos relatórios financeiros através de promoção da ética, efetividade dos controles internos e da governança corporativa. Seu primeiro trabalho foi publicado em 1992, denominado Controles Internos – Estrutura Integrada, ou COSO I, visando orientar as organizações a avaliar e aprimorar seus sistemas de controles internos através da aplicação de cinco componentes. Em setembro de 2004, foi publicado o documento denominado Gerenciamento de Riscos Corporativos – Estrutura Integrada, também conhecido como COSO II, que trouxe uma abordagem mais sólida ao tema de gerenciamento de riscos corporativos, incluindo 3 componentes a mais ao modelo COSO I. Essa obra foi traduzida para o português e lançada no Brasil em 2007.

Segundo COSO (2007), o gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados, através dos quais a alta administração gerencia a organização de maneira integrada. Esses componentes são:

> a) Ambiente Interno: o ambiente interno compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados pelo seu pessoal, inclusive a filosofia de gerenciamento de riscos, o apetite a risco, a integridade e os valores éticos, além do ambiente em que estes estão;
> b) Fixação de Objetivos: os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização. O gerenciamento de riscos corporativos assegura que a administração disponha de um processo implementado para
> estabelecer os objetivos que propiciem suporte e estejam alinhados com a missão da organização e sejam compatíveis com o seu apetite a riscos;
> c) Identificação de Eventos: os eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização devem ser identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos;
> d) Avaliação de Riscos: os riscos devem ser analisados considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto à sua condição de inerentes e residuais;
> e) Resposta a Risco: a administração escolhe as respostas aos riscos - evitando, aceitando, reduzindo ou compartilhando - desenvolvendo uma série de medidas para alinhar os riscos com a tolerância e com o apetite a risco;
> f) Atividades de Controle: políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos sejam executadas com eficácia;
> g) Informações e Comunicações: as informações relevantes são identificadas, colhidas e comunicadas de forma e no prazo que permitam que cumpram suas responsabilidades. A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos os níveis da organização.
> h) Monitoramento: a integridade da gestão de riscos corporativos é monitorada e são feitas as modificações necessárias. O monitoramento é realizado através de atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas. (COSO 2007, p.6)

Já a norma AS/NZS 4360 trata-se de um modelo internacional de referência para o estabelecimento do processo de Gestão de Riscos nas Organizações. Tendo sua primeira versão em 1999 e a mais recente em 2004, a norma AS/NZS 4360:2004 estabelece um *framework* com algumas etapas que devem ser seguidas para o alcance do melhor resultado na implantação do processo de gerenciamento de riscos corporativos. Este *framework*, que é apresentado na Figura 2, serviu, inclusive, como referência para o desenvolvimento da norma ISO31000:

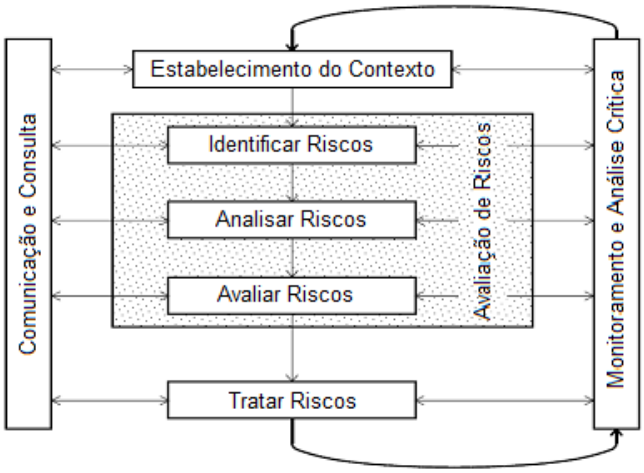

Figura 2 – Etapas de implantação do processo de gerenciamento de riscos corporativos

Fonte: Adaptado de AS/NZS (2004)

MPS (2003) apresenta uma breve definição de cada uma das etapas da versão publicada em 1999 desse *framework:*

> a) Estabelecimento do Contexto: significa definir o que é feito e como mensurar se este está sendo bem sucedido, a quem se pode causar impacto com este trabalho e quais as categorias ou grupos de atividades que compõem este trabalho.
> b) Identificar Riscos: é o processo que define aqueles eventos ou resultados que possam ter impacto no atingimento do sucesso de uma organização.
> c) Analisar Riscos: é o processo que determina o impacto que um risco pode ter (conseqüência) e a probabilidade de sua ocorrência.
> d) Avaliar Riscos: determina a prioridade no gerenciamento dos riscos através da comparação do nível destes riscos no contexto dos objetivos da organização. A comparação deve ser feita entre o nível estimado do risco determinado na análise e critérios pré-estabelecidos (os dois numa mesma base).
> e) Tratar Riscos: é a ação empreendida após a identificação e a avaliação de riscos considerados inaceitáveis para a organização. Nessa etapa a organização deve decidir qual a estratégia de mitigação de risco mais adequada: tratar, tolerar, transferir ou terminar;
> f) Monitoramento e Análise Crítica: é o processo que tem como objetivo verificar, supervisionar, observar criteriosamente ou registrar a melhoria de uma atividade, ação ou sistema a fim de identificar mudanças. Análise Crítica é o processo de avaliação do realizado em relação ao planejado;
> g) Comunicação e Consulta: consiste em um meio adequado de diálogo entre os *stakeholders*, com ênfase em consulta, além de um meio de informação dos tomadores de decisão para os demais stakeholders. (MPS, 2003, p.13)

Ainda no tocante a modelos de referência, foi publicada em 2009 pela ISO e traduzida para o português pela ABNT naquele mesmo ano a mais recente e relevante norma

de Gestão de Riscos existente no mundo. Trata-se da ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes, que é baseada na AS/NZS 4360. Segundo o IBGC (2007), o desenvolvimento da ISO 31000 foi realizado por um comitê especial, denominado *ISO Technical Management Board on Risk Management*, composto por integrantes de 35 países oriundos dos mais diversos setores: financeiro, indústria, governança corporativa, segurança, agronegócios, qualidade, meio ambiente, tecnologia, projetos, saúde, seguros, dentre outros.

Segundo ABNT (2009), a Norma ISO31000 estabelece princípios e diretrizes sobre gestão de riscos, recomendando que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cuja finalidade é integrar o processo para gerenciar riscos em toda a organização, seja do ponto de vista de governança, estratégia, planejamento, gestão, comunicação, políticas, valores ou cultura.

Desse modo, conforme apresenta-se na Figura 3 de ABNT (2009), o modelo (*framework*) de Gestão de Riscos proposto pela Norma ISO31000 possui três dimensões principais (apresentadas na Norma através de seções) que se relacionam entre si no sentido do mais abrangente ao mais específico: (i) os princípios de gestão de riscos – seção 3 da norma; (ii) a estrutura de gestão de riscos – seção 4 da norma; e (iii) o processo de gestão de riscos – seção 5 da norma.

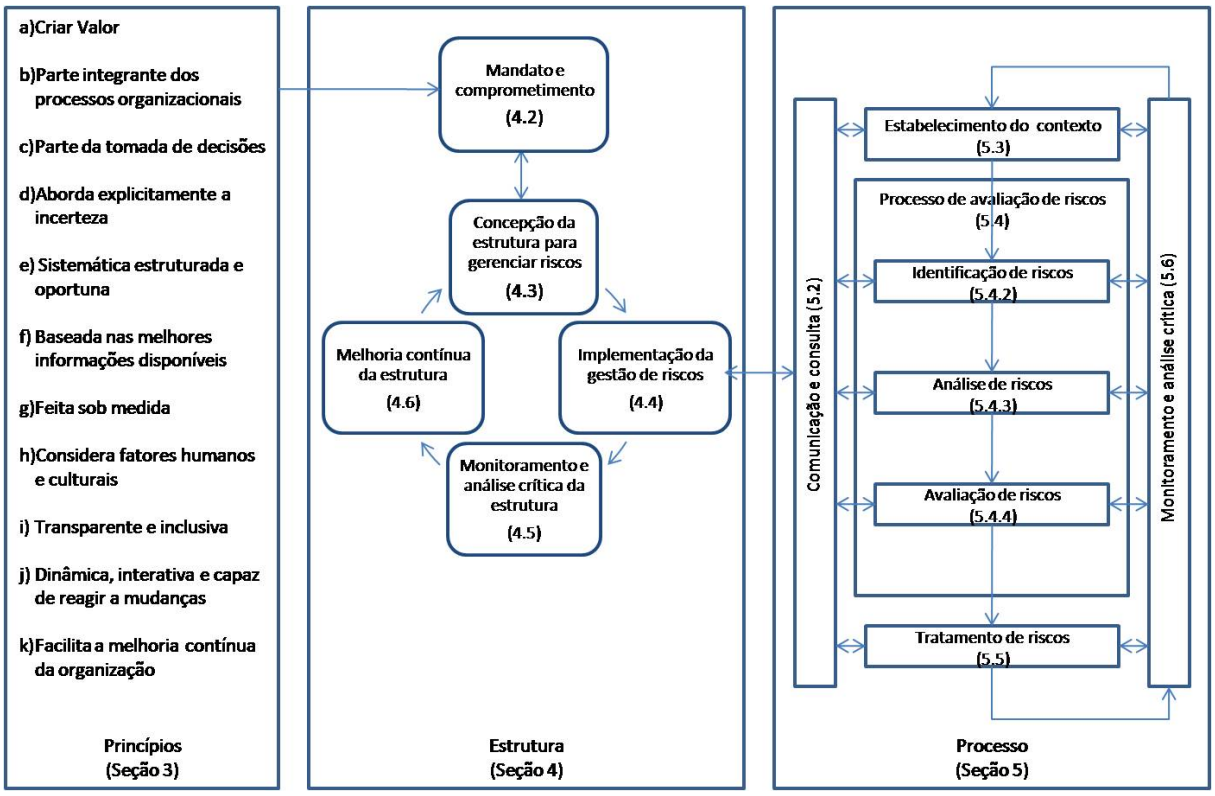

Figura 3 – Relacionamentos entre os princípios da gestão de riscos, estrutura e processo

Fonte: ABNT (2009)

Conforme ABNT (2009), os princípios de gestão de riscos são as diretrizes a serem atendidas em todos os níveis de uma organização para uma gestão de riscos eficaz. Segundo esses princípios:

> (i) a gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho referente, por exemplo, à segurança e saúde das pessoas, à segurança, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação; (ii) a gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças; (iii) a gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação; (iv) a gestão de riscos explicitamente leva em consideração a incerteza, a natureza dessa incerteza, e como ela pode ser tratada; (v) uma abordagem sistemática, oportuna e estruturada para a gestão de riscos contribui para a eficiência e para os resultados consistentes, comparáveis e confiáveis; (vi) as entradas para o processo de gerenciar riscos são baseadas em fontes de informação, tais como dados históricos, experiências, retroalimentação das partes interessadas, observações, previsões, e opiniões de especialistas; (vii) a gestão de riscos está alinhada com o contexto interno e externo da organização e com o perfil do risco; (viii) a gestão de riscos reconhece as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização; (ix) o envolvimento apropriado e oportuno de partes interessadas e, em particular, dos tomadores de decisão em todos os níveis da organização assegura que a gestão de riscos permaneça pertinente e atualizada; (x) a gestão de riscos continuamente percebe e reage às mudanças; e (xi) convém que as organizações desenvolvam e implementem estratégias para melhorar a sua maturidade na gestão de riscos juntamente com todos os demais aspectos da sua organização. (ABNT, 2009, p.7-8)

A estrutura de gestão de riscos, segundo definição de ABNT (2009, p.1) no ISO Guia 73, é um “conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise critica e melhoria contínua da gestão de riscos através da toda a organização”.

A estrutura de gestão de riscos proposta pela Norma ISO31000 é consistente com o modelo PDCA (*Plan, Do, Check, Act*), que é mundialmente reconhecido como referência para implantação de sistemas de gestão. Segundo ABNT (2009) pode-se descrever brevemente essas 4 etapas como:

a) *Plan* (planejar): envolve o mandato e o comprometimento da organização para gerenciar riscos (item 4.2 da norma) e a concepção da estrutura para gerenciar riscos (item 4.3 da norma). Essa concepção abrange diretrizes como: (i) entendimento da organização e seu contexto; (ii) estabelecimento da política de gestão de riscos; (iii) responsabilização; (iv) integração nos processos organizacionais; (v) recursos; (vi) estabelecimento de mecanismos de comunicação de reporte internos e externos.
b) *Do* (executar): envolve a implementação da gestão de riscos propriamente dita (item 4.4 da norma). Essa implementação abrange diretrizes para a implementação da estrutura de gestão de riscos e também do processo de gestão de riscos;

c) *Check* (verificar): envolve o monitoramento e a análise crítica da estrutura de gestão de riscos (item 4.5 da norma);
d) *Act* (agir): envolve as ações de melhoria contínua da estrutura de gestão de riscos (item 4.6 da norma).

Já o processo de gestão de riscos, segundo definição de ABNT (2009, p.2) no ISO Guia 73, trata-se de uma "aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos". Envolve diretrizes sobre: (i) comunicação e consulta às partes interessadas durante o processo de gestão de riscos; (ii) estabelecimento do contexto interno e externo do processo de gestão de riscos; (iii) processo de avaliação de riscos; (iv) tratamento de riscos; (v) monitoramento e análise crítica do processo de gestão de riscos; (vi) registros do processo de gestão de riscos.

Dentre os principais modelos de referência em Gestão de Riscos citados (COSO, AS/NZS4360 e ISO31000) faz-se presente a diferença de estrutura (*framework*) entre o modelo do COSO (2004) com os modelos AS/NZS4360 e ISO31000, assim como a grande semelhança entre os dois últimos. Dentre os modelos da AS/NZS4360 e da ISO31000, pode-se afirmar que o primeiro modelo fundamentou o desenvolvimento do segundo, tanto que os processos de Gestão de Riscos apresentados nesses dois modelos são idênticos. Portanto, a ISO31000 trata-se de uma evolução natural do conceito de Gestão de Riscos proposto pela AS/NZS4360. Nesse sentido, Erben (2008) afirma que o desenvolvimento da ISO 31000 foi predominantemente baseado na AS/NZS4360 e que uma análise comparativa mais aprofundada entre essas duas normas lhe parece pouco relevante.

Já se forem comparados o modelo COSO com a ISO31000, as diferenças são mais marcantes. Segundo Carvalho (2009), apesar de existirem semelhanças entre as normas ISO 31000 e COSO (como a identificação de riscos x identificação de eventos, análise de riscos x avaliação de riscos, monitoramento e comunicação) o foco de cada uma é diferente. A norma 31000 tem um processo com foco principal no risco que afeta a empresa, com o objetivo de mitigá-los, assumi-los ou evitá-los. Já a norma COSO tem um processo com foco principal no controle, para garantir a eficiência e eficácia do monitoramento das atividades que irão tratar os riscos.

Como visto, independente do modelo a ser utilizado, o tema Gestão de Riscos está associado tanto à forma com que os riscos são identificados, analisados e avaliados, como também ao modo como eles são tratados ou mitigados; e nesta última destaca-se a implementação de controles internos. Viu-se também que um dos tipos de riscos que merece destaque dentre os riscos operacionais é o risco de interrupção das atividades críticas da

organização, ou o risco de descontinuidade do negócio, cuja origem dos eventos associados pode ser externa ou interna. Na próxima seção, será visto com mais detalhes como esse risco deve ser gerenciado nas organizações através da chamada Gestão de Continuidade de Negócios.

2.3 Gestão da Continuidade de Negócios (GCN)

Segundo Macedo (2003), a falta de um planejamento prévio para enfrentar situações de emergência em empresas pode causar perdas irreparáveis aos seus recursos mais importantes, como prédios, instalações e pessoas ou impactar a continuidade de suas atividades. Por essa razão, a vida de pessoas e a integridade do patrimônio das organizações dependem de uma resposta rápida e eficaz em uma situação de emergência. Além disso, a empresa precisa ainda garantir seus compromissos com o mercado, parceiros e colaboradores. Portanto, em uma crise ou desastre, dependendo do nível de planejamento e preparação da organização para responder a incidentes, as funções da empresa podem ser gravemente afetadas, tornando-se críticas, e impactarem diretamente os seus principais negócios.

FEBRABAN (2008) relata que, em 1920, a empresa americana John B. Eichleay mudou de lugar um prédio de oito andares com cinco mil toneladas no centro de Pittsburg, Arkansas (EUA), sem interromper os negócios e sua infra-estrutura como água, eletricidade e gás. Segundo o autor, a mudança foi para permitir o alargamento de uma avenida e o prédio foi arrastado em 12 metros ao custo de US$ 80 mil. Já em 1930, a mesma empresa realizou o mesmo tipo de operação em outro prédio de oito andares e 12 mil toneladas da Companhia Telefônica Bell, em Indiana, Indianápolis (EUA) e também sem interromper os serviços de telefonia de 650 funcionários que lá trabalhavam, atendendo 60 mil clientes. Segundo o autor, sem dúvida, essas foram algumas das primeiras iniciativas de Gestão de Continuidade de Negócios no mundo.

Gutierrez (2008) afirma que o tema ganhou força a partir dos atentados terroristas de 11 de setembro nos Estados Unidos, mas que a preocupação já existia alguns anos antes, por exemplo, quando o assunto era o *bug* do milênio. Segundo o autor, foram notadas várias ações típicas de Gestão de Continuidade de Negócios, como treinamento, planos alternativos, análises de riscos, análises de impacto nos negócios, comunicação com a mídia e clientes.

Teixeira (2007) afirma que a Marsh, maior corretora de seguros do mundo, costuma chamar de *anti-cases* de seguro os desastres recentes ocorridos no Brasil, como o megaderramamento de lama de uma planta da mineradora Rio Pomba Cataguases ou o

colapso da obra de expansão do metrô de São Paulo. Segundo o autor, nessas situações que envolvem responsabilidade civil e danos ambientais ficou bastante evidente o despreparo das companhias para enfrentar situações de crise e que a maioria das empresas brasileiras está atrasada em relação aos padrões internacionais de controle de grandes riscos. Além disso, o autor afirma que grande parte desses desastres é provocada por falhas operacionais e não por causas naturais, podendo gerar impacto significativo no desempenho das companhias e, conseqüentemente, no retorno para os seus acionistas.

Segundo IBGC (2007), o conjunto de conhecimentos, boas práticas, e habilidades no campo no campo do gerenciamento de impactos adversos e situações de interrupção às operações das organizações, constituem a disciplina denominada de Gestão da Continuidade de Negócios (GCN) - ou BCM, de *Business Continuity Management.* Para o autor, essa disciplina é bastante ampla e engloba todos os conceitos e práticas anteriores sobre o assunto, tais como planos de contingência, planos de continuidade, planos de recuperação de desastres, planos de backup, resposta a emergências e gerenciamento de crises.

BUSINESS CONTINUITY INSTITUTE *apud* Brasiliano (2006, p.9) conceitua o GCN como "o ato de antecipar incidentes que afetarão os processos e funções críticas de missão da organização e garantir que ela responda a qualquer incidente de maneira planejada e ensaiada".

A ABNT (2007), através da norma NBR 15999:2007 apresenta o seguinte conceito de GCN:

> Gestão da continuidade de negócios (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. Este processo fornece uma estrutura para que se desenvolva uma resiliência (capacidade de uma organização de resistir aos efeitos de um incidente) organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado. (ABNT, 2007, p.3)

O gerenciamento da continuidade de negócios, segundo o IBGC (2007), é implementado através da elaboração de Planos de Continuidade de Negócios, os PCN's (ou BCP's, de *Business Continuity Plans*) para os diversos eventos de risco identificados nas organizações. Esses planos baseiam-se na análise dos impactos para a organização, na avaliação de estratégias de continuidade e nas respectivas análises de custos e benefícios de implementação.

A GCN, segundo ABNT (2007) é um processo complementar a uma estrutura de gestão de riscos. Enquanto a gestão de riscos visa administrar o risco relacionado aos produtos e serviços fundamentais que uma organização fornece, a GCN identifica o que é necessário para que a organização continue cumprindo suas obrigações e planejando o que precisa ser

realizado antes da ocorrência de um incidente, visando proteger seus principais recursos (pessoas, instalações, tecnologia, informações, cadeia de fornecimento, partes interessadas e reputação). Essa atividade permite que a organização tenha uma visão clara das respostas necessárias quando e se ocorrer uma interrupção, mantendo a confiança de que conseguirá administrar eventuais conseqüências sem atrasos na entrega de seus produtos ou interrupção nos seus serviços.

Para FEBRABAN (2008), quem implanta um programa desse tipo atualmente, procura definir precisamente as vulnerabilidades operacionais de sua empresa e estruturar planos de continuidade de negócios para enfrentar com eficácia situações adversas, de modo a evitar qualquer tipo de interrupção do negócio. O objetivo principal dessas atividades é garantir a sobrevivência da companhia.

Segundo a ABNT (2007), a GCN é um elemento importante da boa gestão de negócios, fornecimento de serviços e prudência empresarial. Dentre os principais benefícios de um programa eficaz de GCN, destacam-se que a organização:

> a) é capaz de identificar proativamente os impactos de uma interrupção operacional;
> b) tem uma resposta eficiente às interrupções o que minimiza o impacto à organização;
> c) mantém uma capacidade de gerenciar os riscos que não podem ser segurados;
> d) promove o trabalho entre equipes;
> e) é capaz de demonstrar uma resposta possível por meio de um processo de testes;
> f) pode melhorar sua reputação; e
> g) pode ganhar uma vantagem competitiva por meio da capacidade demonstrada de manter a entrega de seus produtos e serviços. (ABNT, 2007, p.7)

2.3.1 Práticas de referência em GCN

Segundo IBGC (2007), no desenvolvimento e promoção de boas práticas de GCN destacam-se, nos Estados Unidos, e com ampla aceitação internacional, o BCI, *Business Continuity Institute* e o DRII, *Disaster Recovery Institute International*.

Com versão mais recente publicada em 2008, o Guia de Melhores Práticas de Gestão da Continuidade de Negócios, elaborado pelo BCI (organismo britânico de referência sobre GCN), é reconhecidamente um dos mais importantes guias de orientação sobre GCN, pois está totalmente alinhado aos requisitos e definições das normas BS25999. O guia apresenta recomendações detalhadas para implementação da GCN nas organizações, sendo dividido em 6 seções: 1) Introdução, Política e Programa de Gestão de GCN; 2) Entendendo a Organização; 3) Determinando a estratégia de GCN; 4) Desenvolvendo e implementando a GCN - plano de resposta; 5) Exercitando, mantendo e revisando a estrutura de GCN; 6) Incluindo a GCN na cultura da organização (BCI, 2008).

Já o DRII – *Disaster Recovery Institute International*, trata-se de um organismo especializado na elaboração de recomendações, treinamentos e certificação de profissionais da área de GCN. Este instituto elaborou o Guia de Práticas Profissionais de GCN com versão mais recente publicada em 2008, que é dividido em 10 capítulos, apresentando recomendações para o desenvolvimento técnico e qualificação de profissionais que atuam na área de GCN (DRII, 2008).

Ainda no tocante a guias de referência em GCN, pode-se destacar os seguintes:

a) *Handbooks* HB 221:2004, HB292:2006 e HB293:2006: tratam-se de manuais (*handbooks*) de referência sobre gestão da continuidade de negócios elaborados e publicados pelo organismo normatizador australiano *Standards Australia*. O manual HB 221 foi publicado em 2004 e apresenta um *framework* sobre GCN a ser implementado nas organizações. O manual está alinhado à norma AS/NZ4360:2004 (norma de referência sobre gerenciamento de riscos) e foi elaborado pelo mesmo comitê criador desta (STANDARDS AUSTRALIA, 2004). O manual HB 292 foi publicado em 2006 e apresenta um guia detalhado de melhores práticas para implementação da GCN nas organizações. O manual está alinhado ao HB221 e aos documentos Spring TR19:2005, NFPA 1600 e BCI Guideline (SA, 2006). Já o manual HB 293, também publicado em 2006, trata-se de um guia executivo sobre GCN, orientado à alta administração, que apresenta um resumo dos conceitos e processos-chave requeridos para a implementação e manutenção de um programa de gestão da continuidade de negócios (SA, 2006);

b) Guia FSA de Práticas de Gestão da Continuidade de Negócios: publicado em 2006, o guia prático de gestão da continuidade de negócios foi elaborado pela FSA – *Financial Services Authority*, organismo britânico não governamental com influência na regulação de serviços financeiros do Reino Unido. O guia apresenta uma lista de melhores práticas sobre GCN sendo mais direcionado a empresas financeiras. É dividido em 5 tópicos principais: 1) Continuidade Corporativa; 2) Gerenciamento de Crises; 3) Sistemas; 4) Facilidades; e 5) Pessoas (FSA, 2006);

c) Guia ASIS de Continuidade de Negócios: com versão mais recente publicada em 2005, este guia de continuidade de negócios foi elaborado pela ASIS - *American Society for Industrial Security*, organismo americano de referência na área de Segurança. O guia apresenta recomendações sobre a criação, teste e manutenção do plano de continuidade de negócio em organizações. É dividido em duas partes: Parte 1) Desenvolvimento do plano; Parte 2) Implementação e manutenção do plano (ASIS, 2005);

d) Guia FEMA de Gerenciamento de Emergências para Indústria e Negócios: publicado em 1993, este guia para gerenciamento de emergências foi elaborado pela FEMA – *Federal*

Emergency Management Agency, agência do governo americano especializada no gerenciamento de emergências. Dividido em 4 capítulos, o Guia de Gerenciamento de Emergência para Indústria e Negócios apresenta recomendações para desenvolvimento e implementação de planos de emergência, incluindo procedimentos de resposta a emergência e recuperação de negócios (FEMA, 1993).

Segundo Macedo (2003), na elaboração de processos e planos de continuidade de TI (Tecnologia da Informação), destaca-se a norma britânica BS7799, com o objetivo principal de assegurar a continuidade e diminuir o dano empresarial, prevenindo e minimizando o impacto de incidentes relacionados à segurança da informação (baseada nos princípios de integridade, disponibilidade e confiabilidade dos recursos incorporados). Em 2000 essa norma foi homologada como ISO/IEC (*International Electrotechnical Commission*) 17799:2000 e tornou-se conhecida internacionalmente.

Em 2005, a 17799:2000 passou a pertencer à família de normas da série 27000, mudando de nome para ISO/IEC27001 e ISO/IEC27002. A primeira, ISO27001, foi traduzida e publicada pela ABNT em 2006, e apresenta os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação. Esta norma é um padrão certificável e foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) (ABNT, 2006). Já a segunda, ISO 27002, trata-se de um código de práticas para a gestão da segurança da informação. Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Ambas as normas contém um item específico sobre gestão da continuidade de negócios (item 14). Nesse item são abordados aspectos da gestão da continuidade do negócio aplicados à segurança da informação (ABNT, 2005).

No campo da continuidade de serviços de TI, destacam-se as normas da série ISO20000. A primeira parte, ISO20000-1, denominada Tecnologia da Informação – Gerenciamento de serviços – Especificação, foi publicada pela ABNT em 2008, e define os requisitos para o provedor de serviços entregar serviços gerenciados com qualidade aceitável para seus clientes. Trata-se de um padrão certificável. A segunda parte, ISO20000-2, denominada Tecnologia da Informação – Gerenciamento de serviços – Código de Práticas, também foi publicada pela ABNT em 2008. A norma descreve as melhores práticas para processos de gerenciamento de serviços de TI. Ambas as normas contém um item específico sobre gestão da continuidade de serviços (item 6.3). Nesse item são apresentadas recomendações para garantia da continuidade dos serviços de TI acordados com os clientes (ABNT, 2008).

Na Europa, o BSI (*British Standards Institution*) elaborou as duas normas internacionais mais relevantes atualmente sobre Gestão de Continuidade de Negócios, a BS 25999 - 1 e BS 25999-2. A primeira, publicada em 2006, trata-se de um código de práticas para gestão da continuidade do negócio. A segunda, publicada em 2007, apresenta a especificação para a gestão da continuidade do negócio.

A BS 25999-1:2006 ganhou uma versão brasileira em 2007, na forma da norma NBR 15999-1:2007. Esta norma possui as mesmas diretrizes da norma britânica estabelecendo o processo, os princípios e a terminologia da Gestão da Continuidade de Negócios (GCN), fornecendo uma base para entendimento, desenvolvimento e implementação da continuidade de negócios em uma organização e permitindo uma avaliação da capacidade de GCN de maneira consistente e reconhecida (ABNT, 2007). Os principais elementos da norma NBR15999-1:2007 serão vistos na subseção 2.3.2.

Existem, ainda, outras normas internacionais com influência na implementação de boas práticas de GCN. Dentre elas, pode-se destacar:

a) Norma ISO22399:2007: publicada pela ISO em 2007, trata-se da primeira norma desta instituição relacionada a gestão de continuidade de negócios. A Especificação Pública ISO/PAS 22399:2007, *Societal security – Guideline for incident preparedness and operational continuity management* é baseada nas melhores práticas de normas da Austrália, Israel, Japão, Reino Unido e Estados Unidos. Trata-se de um guia de preparação para incidentes e continuidade operacional que estabelece o processo, princípios e terminologia de resposta a incidentes e gestão da continuidade de negócios com foco na segurança pública e defesa civil (ISO, 2007);

b) Norma NFPA 1600: publicada em 2007 pelo NFPA (*National Fire Protection Association*) dos Estados Unidos, esta norma estabelece diretrizes para o gerenciamento de desastres/emergências, bem como para a implantação de um programa de continuidade de negócios. A Norma estabelece um conjunto de critérios para a gestão de emergências e programas de continuidade do negócio com vistas a implementar, manter, avaliar e desenvolver programas para mitigar, preparar, responder e recuperar de emergências (NFPA, 2007);

c) Norma Spring TR 19:2005: publicada em 2005 pelo organismo *Spring Singapore* (de Singapura), esta norma especifica requisitos às organizações interessadas em construir competência, capacidade, resiliência e preparação para responder e recuperar-se de eventos que causem descontinuidade às atividades e operações de seus negócios. Batizada de Referência Técnica para a Gestão da Continuidade de Negócios (*Technical Reference for Business Continuity Management*) a norma, dentre outros requisitos, apresenta um framework

sobre GCN, além de definições e recomendações sobre estratégia, BIA (*business impact analysis*), programa de gestão e plano de continuidade de negócios (SPRING SINGAPORE, 2005)

No tocante à regulamentação brasileira, em junho de 2006 o Banco Central publicou a Resolução 3.380, que obriga os bancos a terem sua estrutura de Gestão de Riscos e Planos de Continuidade de Negócios, incluindo seus fornecedores. Em seu artigo 3º, inciso VI, a resolução prevê que a estrutura de gerenciamento do risco operacional deve prever a existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional. Isso fez com que os bancos, principalmente os grandes, se conscientizassem da real necessidade desses planos (FEBRABAN, 2008).

2.3.2 A Norma Internacional de referência em GCN (BS25999-1 ou NBR 15999-1)

A NBR 15999-1:2007, segundo ABNT (2007), estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios (GCN) e tem como objetivo fornecer uma base conceitual para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização. Além disso, segundo o autor, a aplicação dessa norma visa garantir à empresa que a implementa a confiança nos seus negócios perante clientes e outras empresas e também uma avaliação contínua da sua capacidade de GCN de modo consistente.

Conforme ABNT (2007) *apud* Alves (2009), o ciclo de vida da GCN é composto por seis elementos, que podem ser visualizados na Figura 4.

Figura 4 – Ciclo de Vida da Gestão da Continuidade de Negócios

Fonte: ABNT (2007) *apud* Alves (2009)

O ciclo de vida de GCN pode ser implementado em organizações de todos os tamanhos e de todos os setores: público, privado, sem fins lucrativos, educacional, manufatura etc. O escopo e a estrutura do programa de GCN podem variar e o esforço gasto será adaptado às necessidades de cada organização, mas esses elementos fundamentais serão sempre obrigatórios. A seguir, conforme ABNT (2007), são descritos cada um dos elementos do ciclo de GCN:

> a) Gestão do programa de GCN: a gestão do programa possibilita que a capacidade de continuidade de negócios seja estabelecida (se necessário) e mantida de forma apropriada ao tamanho e complexidade da organização;
> b) Entendendo a organização: as atividades associadas a este elemento fornecem informações que permitem 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;
> c) Determinando a estratégia de continuidade de negócios: permite que uma série de estratégias seja avaliada. Isso facilita que uma resposta apropriada seja escolhida para cada produto ou serviço, de modo que a organização possa continuar fornecendo esses produtos e serviços em um nível de operações e em uma quantidade de tempo aceitáveis durante e logo após uma interrupção. As escolhas feitas devem levar em conta a resiliência e as opções de contramedidas já presentes na organização;
> d) Desenvolvendo e implementando uma resposta de GCN: resulta na criação de uma estrutura de gestão e numa estrutura de gerenciamento de incidentes, continuidade de negócios e planos de recuperação de negócios que detalhem os passos a serem tomados durante e após um incidente, para manter ou restaurar as operações. O termo incidente é usado de forma a refletir a escalabilidade dos eventos, de pequeno, médio ou grande portes, que podem afetar a organização. Um único incidente ou uma série de incidentes pode resultar em sérias interrupções na capacidade da organização de cumprir suas obrigações. Se um incidente for bem gerenciado, ele pode não resultar em uma crise. Porém, alguns eventos podem causar uma interrupção tão profunda aos objetivos da organização, a ponto de serem considerados crise imediatamente. Um incidente pode exceder o nível de preparação da organização, mesmo que ela tenha cuidadosamente avaliado medidas de respostas para um determinado nível de dano esperado. É, então, imperativo que a direção e as estruturas que a suportam não sigam o plano existente à risca, independentemente da situação, mas o adaptem às circunstancias atuais. Um plano de continuidade de negócios nunca irá substituir a tomada de decisões competente e bem-informada por parte da direção.
> e) Testando, mantendo e analisando criticamente os preparativos de GCN: testar, manter, analisar criticamente e auditar o GCN faz com que a organização seja capaz de demonstrar a que ponto suas estratégias e planos estão completos, atualizados e precisos; e identificar oportunidades de melhoria;
> f) Incluindo a GCN na cultura da organização: a inclusão da GCN na cultura da organização permite que ela se tome parte dos valores da organização, dando confiança às partes interessadas quanto à capacidade da organização de sobreviver a interrupções. (ABNT, 2007, p.9)

Nas seções anteriores viu-se que o conceito de GCN está incluído no contexto da gestão de riscos corporativos e este, por sua vez, está inserido num contexto mais abrangente de gestão, denominada governança corporativa. Na próxima seção, será visto que o modelo de GCN, ou ciclo de vida de GCN, evolui para um modelo sistêmico de gestão, denominado Sistema de Gestão de Continuidade de Negócios, que é consistente com outros sistemas de gestão consagrados mundialmente.

2.4 Sistema de Gestão de Continuidade de Negócios (SGCN)

Afinal, o que é um sistema? Deming (1990) *apud* Management Wisdom define sistema como uma série de funções ou atividades (que podem ser subprocessos, etapas ou componentes) que trabalham em conjunto dentro de uma organização e para alcançar os seus objetivos. O autor exemplifica a questão afirmando que as peças mecânicas e elétricas de um automóvel ou até mesmo as de um aspirador de pó, trabalhando em conjunto para o funcionamento destes, são uma forma de sistema.

Deming (1990) *apud* Management Wisdom afirma que o objetivo do sistema deve ser indicado por sua gestão, pois a existência de um sistema depende de um ou mais objetivos. Ou seja, os componentes de um sistema precisam ser gerenciados, pois isoladamente não são suficientes para cumprir os objetivos propostos.

Mello et al. (2002) *apud* Turrioni e Barbedo (2003, p.65) define sistema de gestão como "tudo o que a organização faz para gerenciar seus processos ou atividades" e que em pequenas organizações é comum não existir um sistema propriamente dito, mas sim uma forma de fazer as coisas e que normalmente está na cabeça do gestor ou proprietário e não em procedimentos documentados. Já em organizações maiores, onde existem processos e pessoas, é mais comum a existência de procedimentos, instruções, formulários ou registros documentados. Mas independente da documentação ou não de procedimentos, organização precisa gerenciar suas atividades de modo sistêmico para ser realmente eficiente e eficaz.

Para a implementação e desenvolvimento de sistemas de gestão, o ciclo de PDCA (*Plan-Do-Check-Act*) tem se mostrado como a ferramenta de maior referência. Segundo Quinquiolo (2002) *apud* Pacheco et al. (2007, p.3), o Ciclo PDCA, também conhecido como Ciclo de Shewhart, Ciclo da Qualidade ou Ciclo de Deming, é "uma metodologia que tem como função básica o auxílio no diagnóstico, análise e prognóstico de problemas organizacionais, sendo extremamente útil para a solução de problemas". Segundo o autor, poucos instrumentos têm se apresentado tão efetivos quanto este método de melhoria contínua para a busca do aperfeiçoamento de um processo ou atividade, devido às suas ações sistemáticas que agilizam a obtenção de melhores resultados e facilitam o crescimento das organizações.

2.4.1 Normas de referência em Sistemas de Gestão

Nas últimas duas décadas, organismos internacionais normatizadores como o BSI (*British Standards Institution*), ISO (*International Organization for Standardization*) e IEC

(*International Electrotechnical Commission*), visando padronizar as melhores práticas de gestão nas organizações, iniciaram um movimento pela elaboração de requisitos sobre sistemas de gestão nos mais variados campos: qualidade, saúde e segurança, meio ambiente, segurança da informação e, mais recentemente, continuidade de negócios. O resultado foi a criação de normas internacionais de referência em sistemas de gestão.

Dentre os sistemas de gestão mais utilizados e reconhecidos mundialmente, pode-se destacar os seguintes:

a) Sistema de Gestão da Qualidade: segundo ABNT (2008), representa um sistema de gestão para dirigir e controlar uma organização no que se refere à qualidade. Com versão mais recente publicada em 2008, a Norma NBR ISO 9001 especifica os requisitos para um sistema de gestão da qualidade, onde uma organização precisa demonstrar sua capacidade para fornecer produtos que atendam os requisitos do cliente e os requisitos regulamentares aplicáveis, e objetiva aumentar a satisfação do cliente. De acordo com a definição dessa norma, processo é o resultado de um conjunto de atividades inter-relacionadas ou interativas que transforma insumos (entradas) em produtos (saídas). Em resumo, essa norma é usada para avaliar a capacidade da organização de atender aos requisitos do cliente, os regulamentares e os da própria organização.
b) Sistema de Gestão Ambiental: segundo a ISO 14000, é definido como “a parte do sistema de gestão global que inclui a estrutura organizacional, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos para desenvolver, implementar, atingir, analisar criticamente e manter a política ambiental” (ABNT, 2004, p.2). Tendo sua última versão publicada em 2004, a NBR ISO 14001 especifica requisitos relativos a um sistema de gestão ambiental, permitindo que a organização possa elaborar uma política e objetivos que considerem as obrigações legais e os impactos ambientais significativos. Esses conceitos são aplicáveis a qualquer organização que deseje: (i) implementar, manter e aprimorar um sistema de gestão ambiental; (ii) assegurar sua conformidade com a política ambiental definida; (iii) demonstrar sua conformidade a terceiros; (iv) buscar certificação/registro do seu SGA por uma organização externa; e (v) realizar uma auto avaliação e emitir autodeclaração de conformidade com a norma (ABNT, 2004).
c) Sistema de Gestão de Saúde e Segurança Ocupacional: de acordo com BSI (2007) é definido como aquela parte do sistema de gestão global que facilita o gerenciamento dos riscos de SST associados aos negócios da organização. Isto inclui a estrutura organizacional, as atividades de planejamento, as responsabilidades, práticas,

procedimentos, processos e recursos para desenvolver, implementar, atingir, analisar criticamente e manter a política de SST da organização. Tendo sua versão mais recente publicada em 2007, a OHSAS 18001, cuja sigla significa *Occupational Health and Safety Assessment Series*, foi elaborada pelo *British Standards Institution* (BSI) e é a norma de especificação de referência para esse tipo de sistema. Como complemento, a BSI publicou a OHSAS 18002, que explica com mais detalhes sobre a implementação dos requisitos previstos na OHSAS 18001 (BSI, 2007).

d) Sistema de Gestão de Segurança da Informação: segundo Santos e Nascimento (2008, p.2), um Sistema de Gestão de Segurança da Informação (SGSI) é "um conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos tecnológicos". A norma de referência mundial em SGSI é a ISO/IEC27001, antiga BS7799, que foi publicada em versão brasileira pela ABNT em 2006 e apresenta os requisitos para a implementação de um Sistema de Gestão de Segurança da Informação. Esta norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação. A norma ISO/IEC27001 contém um item específico sobre gestão da continuidade de negócios (item A.14). Nesse item são abordados aspectos da gestão da continuidade do negócio aplicados à segurança da informação, visando prevenir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil (ABNT, 2006).

Já no campo da Continuidade de Negócios, vêm ganhando destaque internacionalmente o Sistema de Gestão de Continuidade de Negócios, ou SGCN, que será visto com mais detalhes em 2.4.2. Desenvolvido pelo BSI e apresentado ao mundo em 2006 através da norma BS25999-2, esse modelo apresenta uma abordagem sistêmica sobre continuidade de negócios, fundamentada no conceito de melhoria contínua, através do Ciclo PDCA.

Como todos os sistemas de gestão propostos pelos padrões normativos de referência são baseados no ciclo PDCA, existem diversas similaridades entre seus requisitos facilitando, assim, a integração entre os mesmos. Nesse sentido, Labodová (2004) apresentou um modelo de integração de sistemas de gestão de qualidade, meio ambiente, saúde e segurança do trabalho e comenta que a integração de sistemas separados é possível pela estruturação do planejamento caracterizado pelo clássico ciclo PDCA e um sistema de análise de risco apropriado.

Um sistema de gestão integrado pode ser definido, segundo Cicco (2004) *apud* Chaib (2005, p.25), como “a combinação de processos, procedimentos e práticas utilizados em uma organização para implementar suas políticas de gestão”. Segundo o autor, essa prática integrada de sistemas de gestão pode ser mais eficiente na consecução dos objetivos da organização do que quando há diversos sistemas individuais se sobrepondo.

2.4.2 Sistema de Gestão de Continuidade de Negócios e a Norma BS25999-2

ABNT (2008, p.2) conceitua sistema de gestão de continuidade de negócios (SGCN) como “a parte de um sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantém e aprimora a continuidade de negócio”.

A norma internacional de referência sobre SGCN é a BS 25999-2:2007, que especifica os requisitos para estabelecer e gerenciar um SGCN eficaz definido por um programa de GCN. Esta norma ganhou uma versão brasileira em 2008, a NBR15999-2.

Segundo ABNT (2008), o sistema de gerenciamento de continuidade de negócios apresentado pela BS25999-2 possui os seguintes componentes-chave:

> a) Uma política;
> b) Pessoas com responsabilidades definidas;
> c) Processos de gerenciamento relativos a: política; planejamento; implementação e operação; análise de performance; análise crítica do gerenciamento; melhorias;
> d) Conjunto de documentação fornecendo evidências auditáveis; e
> e) Processos de tópicos específicos relativos ao tema, no caso, continuidade de negócios, tais como Análise de Impacto nos Negócios (BIA) e desenvolvimento de plano de continuidade de negócios. (ABNT, 2008, p. v)

Baseada no modelo PDCA, o sistema de gestão proposto pela BS25999-2 admite como entrada as necessidades da continuidade de negócios das partes interessadas e, por meio de ações necessárias e processos, resulta em saídas de continuidade de negócios (por exemplo, continuidade de negócios gerenciada) que atendem aqueles requisitos e expectativas, conforme a Figura 5.

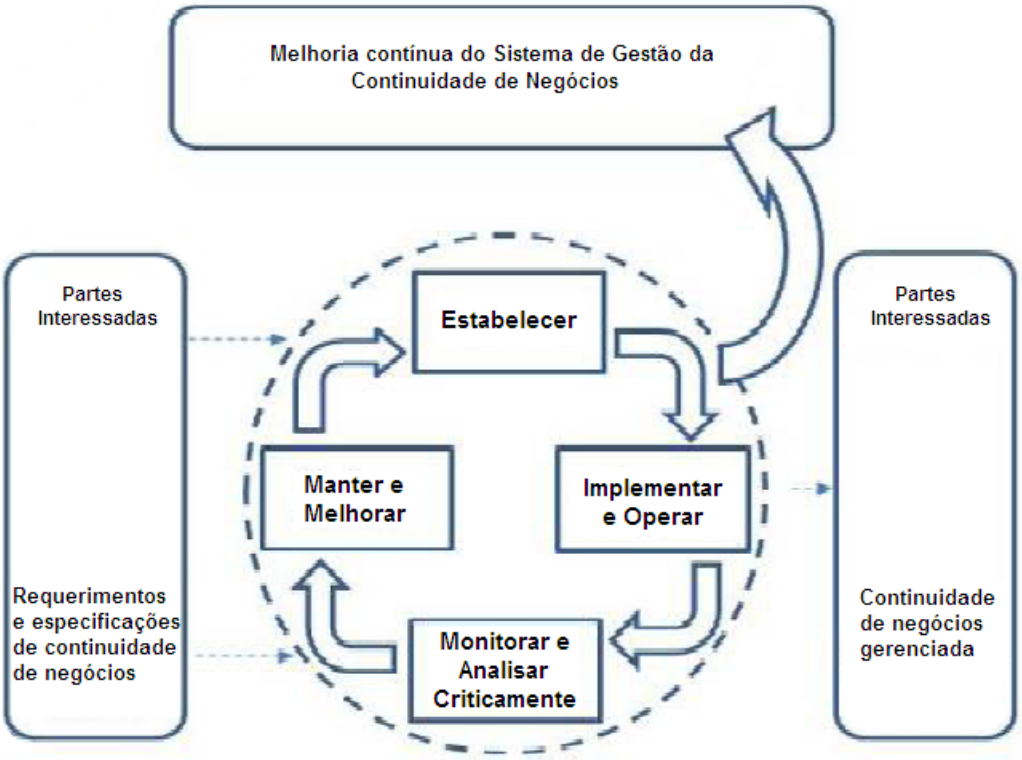

Figura 5 – Modelo PDCA aplicado aos processos do SGCN

Fonte: ABNT (2008)

O ciclo de PDCA do SGCN, conforme ABNT (2008), compreende as seguintes etapas:

> a) *Plan* (Planejar): estabelecer uma política de continuidade do negócios, objetivos, metas controles, processos e procedimentos pertinentes a gestão de risco e melhorar a continuidade do negócios para ter resultados conforme os objetivos e políticas de toda a organização;
> b) *Do* (Fazer): implementar e operar a política de continuidade de negócios, controles, processos e procedimentos;
> c) *Check* (Verificar): monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para uma análise critica, e definir a autorizar ações de melhorias e correções;
> d) *Act* (Agir): manter e melhorar a SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise critica do gestor e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade do negócios. (ABNT, 2008, p. vi)

Dessa forma, observa-se que o sistema de gestão de continuidade de negócios proposto pela BS25999-2 possui consistência com outras normas de sistemas de gestão tais como ISO9001 (sistemas de gestão da qualidade), ISO14001 (sistemas de gestão ambiental), ISO27001 (sistemas de gestão de segurança da informação), e OHSAS18001 (Sistema de Gestão de Saúde e Segurança) possuindo, inclusive, requisitos comuns, que facilitam a operação consistente e integrada com esses sistemas. A Figura 6 apresenta o relacionamento entre os requisitos desses sistemas:

BS 25999-2:2007	ISO27001:2006	ISO14001:2004	OHSAS18001:2007	ISO9001:2008
Introdução	Introdução	Introdução	Introdução	Introdução
1 Objetivo	1 Objetivo	1 Objetivo	1 Objetivo	1 Objetivo
2 Referências Normativas	2 Referências Normativas	2 Referências Normativas	2 Referências Normativas	2 Referências Normativas
3 Termos e Definições	3 Termos e Definições	3 Termos e Definições	3 Termos e Definições	3 Termos e Definições
4 Sistema de GCN	4 Sistema de GSI	4 Requisitos do SGA	4 Elementos do SGSST	4 Sistema de Gestão da Qualidade
5 Implementando e operando o SGCN	4.2.2 Implementar e operar o SGSI 5 Responsabilidades da direção	4.4 Implementação e operação 4.4.1 Estrutura e Responsabilidade	4.4 Implementação e operação 4.4.1 Recursos, funções, responsabilidades	5 Responsabilidades da direção 6 Recursos 7 Realização do Produto
6 Monitoramento e Análise crítica do SGCN	6 Auditorias Internas 7 Análise crítica do SGSI pela direção	4.5.5 Auditoria interna 4.6 Análise crítica pela administração	4.5.5 Auditoria Interna 4.6 Análise crítica pela administração	8 Medição, análise e melhoria
7 Manutenção e melhoria do SGCN	8 Melhoria do SGSI	4.5.3 Não conformidade, ação corretiva e preventiva	4.5.3.2 Não conformidade, ação corretiva e preventiva	

Figura 6 – Relacionamento entre requisitos de Sistemas de Gestão

Fonte: adaptado de ABNT (2008)

2.4.3 Diferenças entre o modelo de SGCN e o GCN

Conforme apresentado nas subseções anteriores, a gestão da continuidade de negócios possui como principal referência a série normativa BS25999, elaborada pelo BSI, que é segmentada em duas normas: a BS25999-1 (Código de Prática de Gestão de Continuidade de Negócio) e a BS25999-2 (Requisitos de Gestão de Continuidade de Negócio). A primeira norma apresenta um modelo de implantação da gestão de continuidade de negócios, denominado ciclo de vida de GCN. Já a segunda apresenta requisitos para a implantação de um sistema de gestão de continuidade de negócios, baseado no ciclo de melhoria contínua PDCA.

Após a análise sobre as características de cada um desses modelos, bem como das suas principais etapas, pode-se perceber a grande similaridade de conceitos entre os dois, bem como dos elementos que os compõem. Essa semelhança entre os modelos remete a uma necessária apresentação das suas principais diferenças, de modo a fornecer subsídios para responder-se à seguinte pergunta: qual dos dois modelos é o mais indicado para implantação da gestão de continuidade de negócios numa organização?

ABNT (2008, p.vii), no conteúdo da norma NBR 15999-2 (tradução da BS25999-2), dá uma pista sobre a diferença entre os dois modelos, afirmando que o ciclo de vida de GCN "representa a operação contínua do programa de continuidade de negócios dentro da organização", ao passo que o modelo PDCA de SGCN "é o meio de garantir que a continuidade de negócios esteja gerenciada e aprimorada eficazmente numa organização e se

aplica a todas as partes do ciclo de vida de GCN". Pelo exposto, entende-se que o modelo de SGCN trata-se de um instrumento para a melhoria do ciclo de vida de GCN.

No entanto, essa explicação ainda é insuficiente para responder ao questionamento proposto, sendo necessária uma análise comparativa mais aprofundada sobre os dois modelos. Para facilitar essa análise, com base nas normas NBR15999-1 e NBR15999-2, foi elaborado um quadro comparativo com as características mais marcantes de cada um dos modelos, apresentado no Quadro 3, através dos seguintes critérios: conceito, foco, aplicação e elementos estruturantes.

Quadro 3 – Comparativo entre modelos de GCN e SGCN

Critério	GCN (NBR 15999-1)	SGCN (NBR 15999-2)
Conceito	Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.	Parte de um sistema global de gestão que estabelece, implementa, opera, monitora, analisa criticamente, mantém e aprimora a continuidade de negócio.
Foco	Programa de GCN (Ciclo de Vida)	Sistema de GCN (PDCA)
Apresentação	Recomendações conforme boas práticas	Requisitos certificáveis
Elementos Estruturantes (números dos elementos conforme os itens das normas que fundamentam cada modelo)	-	3 Planejamento do SGCN
	-	3.2 Estabelecendo e Gerenciando o SGCN
	-	3.2.1 Escopo e Objetivos do SGCN
	4 Política de Gestão de Continuidade de Negócios	3.2.2 Política de GCN
	5 Gestão do Programa de GCN	-
	5.2 Designando Responsabilidades	3.2.3 Provisão de Recursos
	10.3 Treinamento	3.2.4 Competência do Pessoal de GCN
	10 Incluindo a GCN na Cultura da Organização	3.3 Incorporando a GCN na Cultura da Organização
	10.2 Conscientização	
	5.5 Documentação de GCN	3.4 Registros e Documentação do SGCN
	-	3.4.2 Controle dos Registros do SGCN
	-	3.4.3 Controle da Documentação do SGCN
	5.3 Implementando a Continuidade de Negócios na Organização	4 Implementação e Operação do SGCN
	6 Entendendo a Organização	4.1 Entendendo a Organização
	6.2 Análise de Impacto de Negócios (BIA)	4.1.1 Análise de Impacto de Negócios (BIA)
	6.3 Identificação de Atividades Críticas	-
	6.4 Determinando Requisitos de Continuidade	-
	6.5 Avaliando Ameaças a Atividades Críticas	4.1.2 Avaliação de Riscos
	6.6 Determinando Escolhas	4.1.3 Determinando Escolhas
	7 Determinando a Estratégia de Continuidade de Negócios	4.2 Determinando a Estratégia de Continuidade de Negócios
	8 Desenvolvendo e Implementando uma Resposta de GCN	4.3 Desenvolvendo e Implementando uma Resposta de GCN
	8.2 Estrutura de Resposta a Incidentes	4.3.2 Estrutura de Resposta a Incidente
	8.4 Plano de Gerenciamento de Incidentes	4.3.3 Plano de Gestão de Continuidade de Negócios e Gestão de Incidentes
	8.6 Plano de Continuidade de Negócios	
	9 Testando, Mantendo e Analisando Criticamente Providências de GCN	4.4 Exercitando, Mantendo e Analisando Criticamente Providências de GCN
	9.2 Programa de Testes	4.4.2 Exercitando a GCN
	9.3 Testando os Preparativos de GCN	

	9.4 Manutenção dos Preparativos de GCN	4.4.3 Mantendo e Analisando Criticamente as Providências de GCN
	9.5 Análise Crítica dos Preparativos de GCN	
	5.4 Gestão Contínua	5 Monitoração e Análise Crítica do SGCN
	9.6 Auditoria	5.1 Auditoria Interna
	9.7 Auto-Avaliação	
	-	5.2 Análise Crítica do SGCN pela Alta Direção
	-	5.2.2 Entrada para Análise Crítica
	-	5.2.3 Saída da Análise Crítica
	5.5 Manutenção Contínua	6 Manutenção e Melhoria do SGCN
	-	6.1 Ações Corretivas e Preventivas
	-	6.1.2 Ação Preventiva
	-	6.1.3 Ação Corretiva
	-	6.2 Melhoria Contínua

Fonte: adaptado de ABNT (2007) e ABNT (2008)

Com base no quadro comparativo apresentado, pode-se chegar a algumas observações importantes sobre os dois modelos de acordo com cada critério utilizado. No tocante ao conceito, nota-se na terminologia utilizada pela ABNT a primeira diferença marcante entre os dois modelos. O SGCN, segundo ABNT (2008), trata-se de parte de um sistema global de gestão, ou seja, um sistema específico. Já o GCN, consoante ABNT (2007), trata-se de um processo de gestão. Portanto, se um é sistema (SGCN) e o outro um processo (GCN), pode-se afirmar que o modelo de SGCN é mais abrangente que o de GCN.

A avaliação dos dois modelos conforme o foco de atuação reafirma essa observação. Segundo o comparativo, enquanto o SGCN tem seu foco em um sistema de gestão, portanto, mais abrangente, o GCN tem seu foco concentrado num programa de gestão, que é algo mais específico. Além disso, o programa de gestão de GCN remete à implantação tão somente de um conjunto de atividades predeterminadas, mas sem a mesma garantia de melhoria contínua estruturada preconizada pelo SGCN.

No tocante à apresentação das informações de referência de cada um dos modelos, outra diferença marcante foi observada. Enquanto o modelo de SGCN é apresentado através de requisitos, ou seja, apresenta o que se deve fazer para estabelecer o SGCN, o modelo de GCN apresenta o que é recomendável fazer para implantá-lo, portanto sugerindo (e não obrigando). Essa diferença remete à observação de que o modelo de SGCN é mais rígido (e conceitualmente pronto) do que o GCN, que é mais flexível quanto à implantação de suas recomendações.

Por fim, quanto à análise dos elementos estruturantes que compõem cada um dos modelos, outra grande diferença foi percebida. Enquanto o SGCN possui seus elementos bem distribuídos conforme cada uma das etapas do PDCA (Planejamento, Implementação, Verificação e Manutenção), nota-se no modelo de GCN uma concentração bastante acentuada na etapa de implementação e bastante discreta nas demais. Isso remete à observação de que o

GCN trata-se de um modelo para facilitar a etapa de implementação do SGCN, reafirmando novamente a característica de abrangência e de especificidade entre o SGCN e o GCN respectivamente.

Com base nas diferenças apresentadas entre os dois modelos, pode-se chegar um pouco mais próximo de uma resposta sobre o questionamento inicial. Pelo exposto, pode-se afirmar que o SGCN é mais abrangente e estruturado (por apresentar requisitos e consistência com o PDCA) do que o GCN, fato que pode influenciar na escolha pelo primeiro. No entanto, considerando o nível de detalhamento do GCN na etapa de implementação do PDCA, a solução mais segura de aplicação seria a combinação dos dois modelos. Considerando, ainda, a ausência de uma avaliação prática da implantação de cada um desses modelos isoladamente, a solução conjunta parece ainda mais indicada.

Conforme apresentado neste capítulo, o tema Gestão de Continuidade de Negócios surgiu com o intuito de administrar um tipo de risco: a interrupção da entrega dos produtos e serviços fundamentais de uma organização e, portanto, trata-se de uma estrutura complementar à Gestão de Riscos Corporativos. Este, por sua vez, foi apresentado como um dos importantes instrumentos para a prática da Governança Corporativa numa organização.

Viu-se, também, através da norma internacional de referência BS25999-1, que a Gestão de Continuidade de Negócios depende de um ciclo de vida composto por seis elementos principais para ser implantado numa organização. No entanto, o conceito de GCN não parou por aí. Também foi apresentado que o conceito de GCN evolui para um SGCN (Sistema de Gestão de Continuidade de Negócios), proposto pelo padrão normativo BS25999-2, e que é baseado no ciclo de melhoria contínua. Esse último modelo remete ao entendimento de que o ciclo de vida de gestão de continuidade de negócios não é um processo estático; precisa ser planejado, implementado, monitorado, analisado criticamente e melhorado continuamente dentro de uma organização.

É dessa evolução de conceitos que surge a referência para o desenvolvimento da estrutura de apoio à implantação de um SGCN numa empresa de telecomunicações, objeto do presente trabalho.

3. Gestão de Continuidade de Negócios – Contextualização e Estudo de Caso de uma Empresa de Telecomunicações

No capítulo 2 viu-se que a Gestão de Continuidade de Negócios (GCN) está inserida na Estrutura de Gestão de Riscos que, por sua vez, está inserida no contexto de Governança Corporativa de uma organização.

Viu-se também que a Gestão de Continuidade de Negócios possui como referência para implantação em uma organização um processo denominado ciclo de vida de GCN, que possui seis elementos principais.

Foi visto, ainda, que o GCN evolui para um modelo mais estruturado (certificável) que é consistente com o conceito de melhoria contínua do modelo PDCA (*Plan-Do-Check-Act*), sendo denominado de Sistema de Gestão de Continuidade de Negócios, e que a aplicação deste numa organização pode ser facilitada se ocorrida em combinação com o ciclo de GCN.

Após a revisão conceitual sobre GCN e dos temas que o fundamentam ocorrida capítulo 2, pode-se afirmar que o capítulo 3 possui dois objetivos principais. Em primeiro lugar, pretende-se apresentar o contexto de GCN da empresa de telecomunicações objeto desse trabalho, incluindo informações sobre o setor em que atua, principais produtos, serviços, processos e elementos de GCN implementados.

Em segundo lugar, pretende-se realizar uma análise crítica da estrutura de GCN da empresa em estudo, denominado de pré-teste, visando avaliar a consistência do modelo de GCN implementado nessa organização. O resultado dessa análise será um dos principais direcionadores para a elaboração da estrutura de apoio de SGCN prevista no Capítulo 4.

3.1 Estudo do Contexto de uma Empresa de Telecomunicações

Esta seção apresenta o cenário da empresa onde foi realizado o estudo de caso. O cenário da empresa estudada será apresentado através do setor em que atua, aspectos gerais, estrutura organizacional, principais processos e uma breve análise sobre a estrutura de SGCN existente na empresa, que atualmente encontra-se em fase inicial de implantação.

Por questões de confidencialidade de informações, a empresa de telecomunicações estudada será apresentada com o nome fictício de XY Telecom.

3.1.1 Setor de Telecomunicações

O setor de telecomunicações é um dos instrumentos de promoção do desenvolvimento econômico e social de um país, pois uma plataforma de telecomunicações moderna e eficiente é capaz de aumentar a produtividade de outros setores da economia, assim como facilitar o acesso das pessoas à informação (XY TELECOM, 2008).

No Brasil, a reestruturação do setor de telecomunicações conduzida na segunda metade dos anos 90 propiciou a universalização do serviço telefônico fixo, aumentando muito sua abrangência geográfica e inclusão em todas as camadas da população, principalmente entre os domicílios das classes C, D e E. Com relação à telefonia móvel, a expansão no Brasil foi bastante acelerada, demonstrando que o modelo adotado obteve sucesso (XY TELECOM, 2008).

Essa reestruturação fez com que as empresas de telecomunicações realizassem o maior plano de investimento da história desse setor no país, através da expansão, modernização e melhoria na qualidade da prestação de serviços. Entre 2001 e 2006, por exemplo, a penetração da telefonia fixa e móvel, como percentual dos domicílios, evoluiu de 58,9% para 74,5%. Atualmente, 34 mil localidades brasileiras dispõem do serviço telefônico (XY TELECOM, 2008).

Em 2007, a riqueza produzida pelo setor representou cerca de 6,5% do PIB brasileiro, apesar do elevado o volume de tributos recolhidos - cerca de 40,3% da receita operacional líquida das empresas do setor. Os investimentos realizados em 2007 totalizaram R$ 11,8 bilhões com uma força de trabalho de mais de 312 mil pessoas (XY TELECOM, 2008).

Após o ciclo de desenvolvimento desse setor no Brasil, orientado pela a universalização do segmento de telefonia fixa, as operadoras de telecomunicações atualmente focam em serviços que ofereçam maior valor agregado. É o caso da banda larga, que é um

suporte capaz de oferecer uma gama de serviços relacionados com conteúdos, entre os quais o IPTV (*Internet Protocol Television*, que significa a conectividade da televisão com a Internet).

Em decorrência desse desenvolvimento, houve também uma importante expansão da internet no Brasil, onde o número de microcomputadores em relação ao número de domicílios saltou de apenas 12,6%, em 2001, para 22,1% em 2006 (XY TELECOM, 2008).

Já o microcomputador com acesso à internet, em igual período, evoluiu de 8,6%, para 16,9%. De acordo com estudos especializados, o Brasil tem o terceiro maior mercado de internet das Américas, ficando atrás apenas dos EUA e do Canadá (XY TELECOM, 2008).

Nos últimos anos, a Lei Geral de Telecomunicações (LGT), a regulamentação setorial e a atuação da Agência Nacional de Telecomunicações (ANATEL) proporcionaram não só disciplina e fiscalização para o setor de telecomunicações como também seu desenvolvimento e a diversificação dos serviços prestados pelas operadoras no país (XY TELECOM, 2008).

3.1.2 Aspectos Gerais da XY Telecom

O Grupo XY Telecom é composto por empresas que atuam na cadeia de valor do setor de telecomunicações brasileiro, estando presente nos segmentos de telefonia fixa local e longa distância, telefonia móvel, transmissão de dados, *data center* e Internet.

Constituída a partir da cisão do Sistema Telebrás, em 1998, a XY Telecom foi adquirida em leilão de privatização. A empresa conta com uma infra-estrutura de rede ampla e orientada pela eficiência operacional que utiliza recursos tecnológicos modernos para garantir maior flexibilidade e qualidade na oferta dos serviços.

A empresa está listada na Bolsa de Valores de São Paulo (Bovespa) e na *New York Stock Exchange* (NYSE). Em 2008, a XY TELECOM também passou a fazer parte do Índice de Sustentabilidade Empresarial (ISE) da Bovespa, refletindo o seu comprometimento com a responsabilidade social e a adoção de práticas gerenciais sustentáveis.

As iniciativas das empresas que compõem a XY TELECOM visam obter a liderança do mercado e gerar valor para os seus acionistas. O estilo de gestão da XY TELECOM é caracterizado pelo foco em serviços e por um conjunto de atitudes que serve de orientação e apoio na busca pelos resultados da companhia. Todas as iniciativas refletem o posicionamento de sua gestão, que é pautado pelos princípios de agilidade, simplicidade e objetividade.

Para manter a liderança do mercado, aumentar a competitividade e melhorar o desempenho financeiro do grupo, criando valor para os acionistas e demais *stakeholders*, a estratégia geral da XY TELECOM inclui:

a) Foco na convergência: através dela, a XY TELECOM consolida a diferenciação que possui no mercado, por meio da oferta de pacotes integrados de telefonia fixa, móvel, banda larga e TV por assinatura. A convergência é forte instrumento para aumentar a fidelização de clientes e alavancar vendas, além de garantir sinergias importantes, que reduzirão custos operacionais da companhia;
b) Expansão da base de clientes de banda larga: por ser uma alavanca de crescimento e elemento essencial na oferta de serviços integrados, o serviço de acesso à internet em banda larga é um dos focos principais da empresa. Para potencializar esse crescimento, a XY TELECOM continua investindo na expansão das suas redes, fixa, móvel e de banda larga, além de ampliar a oferta de velocidade e a evolução para novas tecnologias;
c) Atuação em novos negócios e expansão para outros mercados: expandir a atuação para novos negócios a partir de suas plataformas e atuar em segmentos que completem a oferta de serviços para os clientes é um ponto-chave para garantir o crescimento da organização. A empresa analisa continuamente oportunidades de expansão e consolidação em outros mercados, seja no Brasil ou no exterior, de modo a ampliar seu porte e alavancar novas fontes de receita, para tornar-se um dos grandes *players* mundiais do mercado de telecomunicações;
d) Explorar as oportunidades de crescimento como operadora móvel nacional, com foco em rentabilidade: a diferenciação por meio de ofertas inovadoras continua sendo a principal estratégia para consolidar a liderança de mercado e a rentabilidade nesse segmento. A empresa continuará explorando a oferta de serviços de valor adicionado, e novos produtos através da sua base de clientes, potencializando ainda mais a expansão de sua receita e rentabilidade;
e) Ampliar a eficiência e o controle de custos: as iniciativas para melhoria dos processos internos, com a conseqüente otimização dos custos e da alocação de recursos, continuarão a fazer parte da estratégia de aumento da eficiência operacional e ganhos de escala.

A XY TELECOM possui cerca de 55,9 milhões de clientes, sendo 22 milhões em telefonia fixa, 30 milhões em telefonia móvel, 3,8 milhões em banda larga e 61 mil em TV por assinatura. Essa carteira de clientes representou no Brasil em 2007 cerca de 47% do

mercado de telefonia fixa, 19,2% do mercado de telefonia móvel e 16,4% do mercado de banda larga.

A XY TELECOM possui aproximadamente 25 mil colaboradores alocados em todo o território nacional. Sua estrutura organizacional principal é composta pela Presidência e 14 diretorias, distribuídas conforme o organograma apresentado na Figura 7.

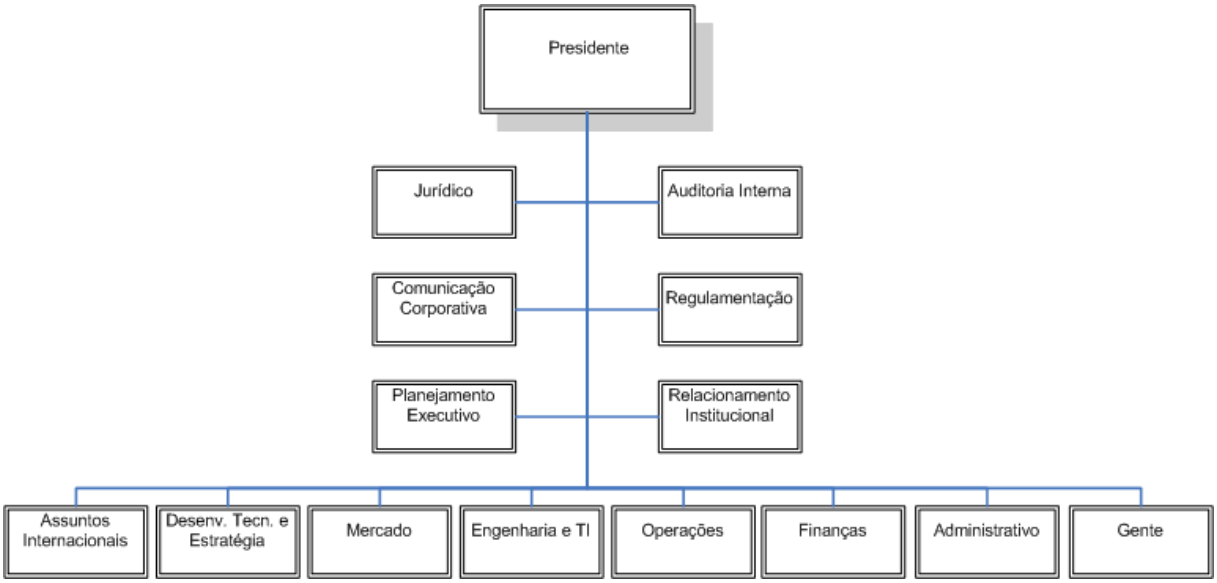

Figura 7 – Organograma da XY TELECOM
Fonte: XY TELECOM (2009)

3.1.3 Principais Serviços e Canais de Distribuição da XY Telecom

Conforme descrito anteriormente, a XY Telecom possui diversificação de produtos/serviços em toda a cadeia de valor do setor de telecomunicações brasileiro. Seus produtos/serviços de telecomunicações consistem em:

- serviços de telefonia fixa local, incluindo instalação, assinatura mensal, serviço de medição, chamadas a cobrar e serviços locais complementares;
- serviços de longa distância nacional e internacional, realizadas por telefones fixos e celulares usando o Código de Seleção de Operadora de longa distância, e serviços de longa distância inter-regional;
- uso de rede para (i) completar chamadas iniciadas por clientes de outros provedores de serviços de telecomunicações (serviços de interconexão), ou (ii) para provedores que não tenham a rede necessária;
- serviços de telefonia móvel;
- serviços de telefonia pública (Terminais de Uso Público, ou TUP);

- serviços de transmissão de dados, englobando serviços ADSL (*Assymmetric Digital Subscriber Line*), aluguel de linhas digitais e analógicas dedicadas para clientes corporativos, provedores de serviços de telecomunicações e ISPs (*Internet Service Providers*), IP (*Internet Protocol*), além de outros serviços de transmissão de dados;
- serviços de valor adicionado, que incluem correio de voz, identificador de chamadas, auxílio às listas, entre outros serviços;
- serviços de voz avançado para clientes corporativos, como serviços de 0800 (chamada gratuita); e
- televisão por assinatura.

Quanto aos canais de marketing, a estratégia da XY TELECOM é ter o produto adequado ao canal mais apropriado, o que pode ocorrer através da disponibilidade de produtos diferentes em canais diferentes, bem como através da utilização de diferentes níveis de comissões para um determinado produto dependendo do canal.

No segmento varejo, os principais canais de distribuição da empresa são:

- Franquias: lojas diferenciadas focadas em vendas para o segmento de alta renda;
- Tele-vendas: foco em uma visão *multi-skill* (multi-habilidades) dos atendentes;
- Canal direto: venda de produtos diretamente nos prédios de grandes organizações;
- Agentes exclusivos e lojas multi-marcas;
- Lojas do grande e pequeno varejo;
- Outros canais focados em consumidores de baixo valor, tais como *call centers* e agentes porta-a-porta;

No segmento corporativo, a XY TELECOM vende seus produtos e serviços através de:

- força de vendas direta, que se concentra principalmente sobre grandes clientes corporativos;
- rede da XY TELECOM, composta de agentes comissionados não-exclusivos dedicados a negócios de portes pequeno e médio.

Os serviços de telecomunicações móveis são vendidos através de uma grande rede de vendas, inclusive pontos de venda de varejo de terceiros e lojas próprias, bem como através de centrais de contato e internet.

3.1.4 Principais Processos da XY Telecom

A XY TELECOM trabalha com o modelo de gestão por processos e possui quase a totalidade dos seus processos internos mapeados. O modelo utilizado pela empresa é chamado de MAP – Modelo de Arquitetura de Processos, e o projeto é gerenciado pela Gerência de Arquitetura de Processos, que é ligada à Diretoria de Gente da XY TELECOM.

O MAP implantado na XY TELECOM foi desenvolvido com base no modelo eTOM. O eTOM (*Enhanced Telecom Operations Map*), publicado pela TM Forum (associação de aproximadamente 700 companhias de 75 países nos segmentos de comunicação, informação e entretenimento), é um modelo mundialmente conhecido e muito utilizado para processos de negócio do setor de telecomunicações (TELECO, 2009). Segundo o autor, o modelo eTOM descreve todo o âmbito de processos de negócio exigido por um prestador de serviços e define elementos fundamentais e como eles interagem. É decomposto num conjunto de processos que provê níveis de detalhe.

O eTOM, conforme Teleco (2009), está dividido em 3 seções de processos: (i) operacional; (ii) estratégicos, infraestrutura e produtos; e (iii) gestão empresarial. As duas primeiras seções, segundo o autor, podem ser vistas sob duas perspectivas:

- Agrupamento vertical dos processos: representam uma visão dos processos fim-a-fim dentro de um negócio, como por exemplo tudo que estiver envolvido num fluxo de faturamento para um cliente;
- Agrupamento horizontal dos processos: representam uma visão funcional dentro de um negócio como, por exemplo, a gestão de canais de fornecimento.

A Figura 8, adaptada de Teleco (2009), detalha a estrutura do quadro geral de processos da XY Telecom, de acordo com o modelo eTOM.

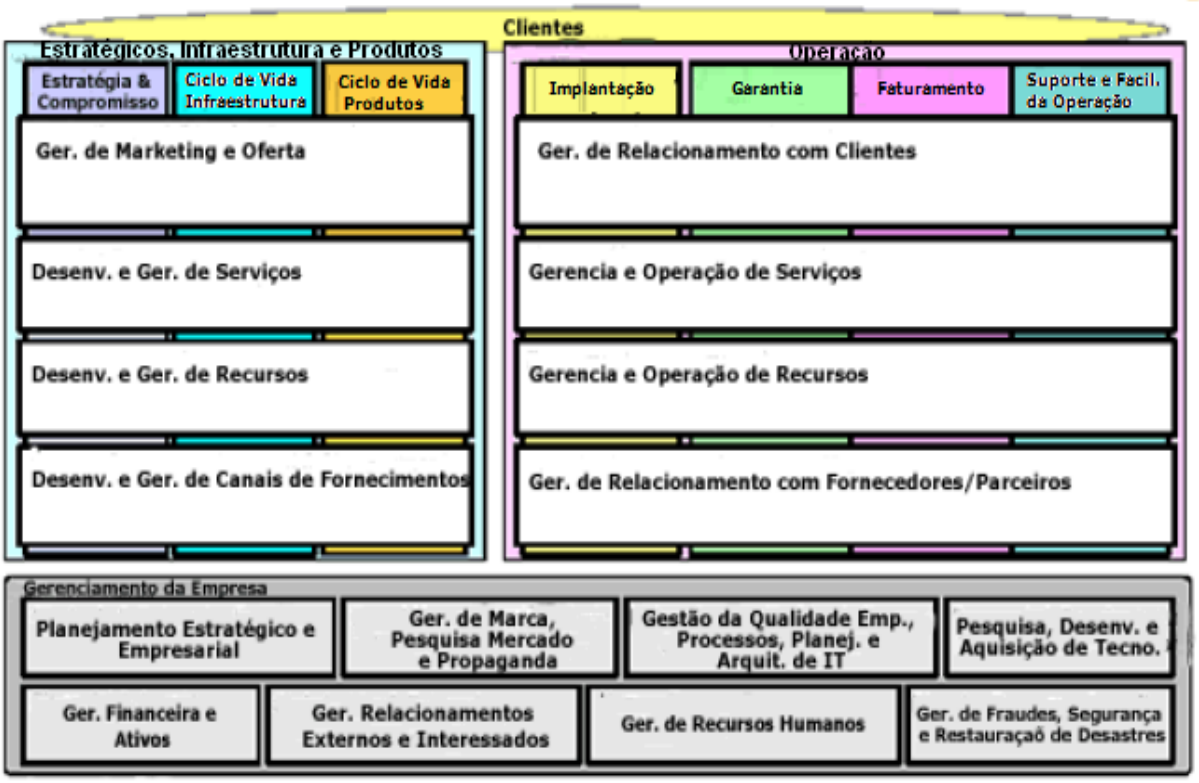

Figura 8 – Quadro Geral de Processos da XY Telecom conforme Modelo eTOM
Fonte: Adaptado de Teleco (2009)

A seguir, conforme o modelo eTOM de Teleco (2009), serão apresentados brevemente os grupos de processos que fazem parte de cada seção do eTOM da XY Telecom.

a) Processos Estratégicos, Infraestrutura e Produtos - SIP

a.1) Agrupamentos Verticais

- Estratégia e Compromissos: grupo responsável pela geração de estratégias de suporte aos processos do ciclo de vida das infraestruturas e produtos da empresa. É também responsável pelo acompanhamento do sucesso dessas estratégias e pela realização das ações corretivas que, por ventura, sejam necessárias;
- Ciclo de Vida das Infraestruturas: grupo responsável pela definição, planejamento e implementação das ações necessárias relativas à infraestrutura (aplicações, computadores e redes), assim como ao suporte de outras infraestruturas e facilidades (centros de operação, etc.);
- Ciclo de Vida dos Produtos: grupo responsável pela definição, projeto e implementação de todos os produtos do *portfolio* da empresa. Esse grupo de processos gerencia os produtos em operação de forma a garantir o lucro, a satisfação do cliente e o atendimento aos requisitos de qualidade.

a.2) Agrupamentos Horizontais

- Gerenciamento de Marketing e Oferta: grupo responsável pelas funcionalidades necessárias para definir estratégias, desenvolvimento de novos produtos, gerenciando os produtos existentes e implementação de estratégias de marketing e ofertas, especialmente adequadas para informação e divulgação de produtos e serviços;
- Desenvolvimento e Gerenciamento de Serviços: grupo responsável pelo planejamento, desenvolvimento e entrega de serviços no domínio da operação;
- Desenvolvimento e Gerenciamento de Recursos: grupo responsável pelo planejamento, desenvolvimento e entrega de recursos necessários para dar suporte aos produtos e serviços sob domínio da operação;
- Desenvolvimento e Gerenciamento de Canais de Fornecimento: grupo responsável pela interação requerida à empresa para relacionar-se com os seus fornecedores e parceiros, que estejam envolvidos na manutenção de seus canais de fornecimento. O canal de fornecimento é uma rede complexa de relacionamentos que o provedor de serviços gerencia de maneira a fornecer e entregar seus produtos.

b) Processos de Operação - OPS

b.1) Agrupamentos Verticais

- Implantação: grupo responsável pela entrega dos produtos desejados pelo cliente, informando ao mesmo o *status* de seu pedido, garantindo a sua execução dentro do prazo e atendendo à sua satisfação;
- Garantia: grupo responsável pela execução de atividades de manutenção preventiva e corretiva, de forma que os serviços estejam continuamente disponíveis e nos níveis de performance estabelecidos pelo acordo de nível de serviço ou pela qualidade do serviço;
- Faturamento: grupo responsável pela produção de faturas precisas e no tempo correto;
- Suporte e Facilidades da Operação: grupo responsável pelo suporte aos três outros processos do grupo IGF (Implantação, Garantia e Faturamento), e por garantir as facilidades operacionais das áreas de implantação, garantia e faturamento.

b.2) Agrupamentos Horizontais

- Gerenciamento do Relacionamento com Clientes (CRM): grupo responsável pelo conhecimento das necessidades dos clientes e inclui todas as funcionalidades necessárias para a aquisição, ganho e retenção do relacionamento com um cliente.

- Gerência e Operação de Serviços: grupo responsável pelas funcionalidades necessárias para o gerenciamento e operação dos serviços de comunicações e informações que atendam aos propósitos dos clientes;
- Gerência a Operação de Recursos: grupo responsável pelos recursos da empresa (aplicações, sistemas computacionais e infraestrutura de rede), e também pelo gerenciamento de todos os recursos utilizados para entregar os serviços assim como dar o suporte requerido pelo cliente;
- Gerenciamento do Relacionamento com Fornecedores/Parceiros: grupo responsável pelo suporte dos processos operacionais, nos dois sentidos: da área do IGF (vertical) e da área funcional de operação (horizontal). Inclui solicitações de compra e o acompanhamento desde a entrega, resolução de problemas, validação da fatura e autorização para o pagamento, assim como o gerenciamento da qualidade dos fornecedores e parceiros.

c) Processos de Gestão

Esta seção de processos do eTOM envolve o conhecimento de ações e necessidades no nível da empresa, envolvendo todos os processos de gerenciamento do negócio necessários para dar o devido suporte às demais partes da empresa. A seção de processos de gestão da empresa são representados pelos seguintes grupos:

- Planejamento Estratégico e Empresarial;
- Gerenciamento de Marca, Pesquisa Mercado e Propaganda;
- Gestão da Qualidade, Processos, Planejamento e Arquitetura de TI;
- Pesquisa, Desenvolvimento e Aquisição de Tecnologia;
- Gestão Financeira e de Ativos;
- Gerenciamento de Relacionamentos Externos e Outros Interessados;
- Gestão de Recursos Humanos;
- Gestão de Fraudes, Segurança e Restauração de Desastres.

3.2 Apresentação da Estrutura de GCN da XY Telecom

No ano de 2008 iniciou-se o projeto de implantação da gestão de continuidade de negócios na companhia XY TELECOM. Liderado pela área de Segurança de Informação, o projeto teve como objetivos, além da redução de perdas com a mitigação do risco de interrupção do negócio, também um cunho estratégico pelo fato de que concorrentes da XY

TELECOM ainda não haviam estruturado e implantado um modelo de GCN em suas companhias.

O projeto de GCN da XY Telecom foi planejado para cumprir, ainda em 2008, as etapas do ciclo de vida de GCN de entendimento da organização e de determinação das estratégias de continuidade. Portanto, o modelo de GCN utilizado no projeto foi o ciclo de vida previsto pela norma BS25999-1.

As etapas previstas no projeto foram implementadas ao final do prazo estabelecido e contaram com o apoio de uma consultoria especializada em GCN.

Após a realização de inventário da documentação e de entrevistas com colaboradores participantes do projeto de GCN da XY TELECOM, pôde-se observar com mais detalhes as principais atividades desenvolvidas e que caracterizam a estrutura de GCN existente nessa companhia. Dessa forma, constatou-se que a referida estrutura foi implementada através das seguintes fases:

- Fase I – Definição do Escopo e Planejamento;
- Fase II – Documentação da Gestão de Continuidade de Negócios;
- Fase III – Análise de Riscos e Análise de Impacto no Negócio (BIA);
- Fase IV – Estratégias de Continuidade.

A seguir, serão brevemente descritas as atividades desenvolvidas em cada uma dessas fases da estrutura de GCN da XY Telecom.

3.2.1 Fase I - Definição do Escopo e Planejamento

Esta fase compreendeu as atividades de definição do escopo inicial do projeto e do planejamento das principais ações a serem implementadas para estruturação do GCN na XY Telecom e foi desenvolvida pela equipe interna do projeto com o apoio de uma consultoria externa.

Na definição do escopo foram inicialmente inventariados todos os processos mapeados pela companhia. Essa atividade foi facilitada pela boa abordagem por processos existente na XY Telecom, vista na subseção 3.1.4. O inventário contabilizou o universo de aproximadamente 300 processos. A seguir, um a um dos processos elencados foram analisados pela equipe do projeto e avaliados quanto à significância com relação aos seguintes critérios:

- O processo deve possuir tempo reduzido nos controles de suas atividades e entrega de seus produtos;
- O processo deve estar envolvido com questões de obrigações Legais e/ou Regulamentares;
- O processo deve estar envolvido com questões de segurança (Fraudes);
- O processo deve ser estratégico para a companhia (Atendimento ao cliente – cuida da qualidade do serviço prestado e da imagem da companhia no mercado);
- O processo deve ser fundamental para a companhia (independentemente do segmento de atuação). (XY TELECOM, 2008)

Essa atividade de avaliação dos processos contou com o apoio também das áreas de negócio da XY Telecom, conhecedoras do universo de processos da companhia, como a área de Processos e a de Governança Corporativa. Após entrevistas com os colaboradores dessas áreas e a classificação dos processos conforme os critérios determinados, foi selecionado um universo de 50 processos para o escopo inicial do projeto. Os processos selecionados pertencem a diversos agrupamentos do modelo de processos (MAP) da XY Telecom, sendo mais concentrados nos agrupamentos referentes ao relacionamento com clientes e gestão de serviços. Desses 50 processos do escopo, foram também selecionados os 25 principais sistemas que os suportam, visando delimitar a abrangência da infra-estrutura de tecnologia de informação incluída no projeto GCN.

No tocante ao planejamento, foram realizadas reuniões entre os membros da equipe do projeto e a consultoria contratada com o objetivo de programar as principais ações de implantação do projeto GCN. Esse planejamento, assim como a definição do escopo inicial do projeto, foram documentados em um relatório executivo e comunicado aos principais gestores envolvidos.

3.2.2 Fase II - Documentação da Gestão de Continuidade de Negócios;

Nesta fase, foi desenvolvida a proposta de documentação de referência da Estrutura de Gestão de Continuidade de Negócios da XY Telecom. Para a realização dessa atividade, a equipe de coordenação do projeto, em conjunto com a consultoria, realizaram um roteiro de entrevistas com os principais gestores da companhia em busca de informações de subsídio para a elaboração de documentos de GCN aplicáveis à realidade da XY Telecom.

Os principais documentos propostos foram a Política, o Regulamento e o Procedimento de GCN. Estes documentos foram desenvolvidos visando caracterizar o processo de Gestão da Continuidade de Negócios na XY Telecom incluindo informações sobre conceitos, equipes, responsabilidades, manutenção de planos, etc.

O documento da Política de GCN da XY Telecom foi desenvolvido para servir como instrumento direcionador para a implementação da estrutura de GCN e documentação de suporte naquela organização. Dentre as principais informações contidas no documento, destacam-se as diretrizes de continuidade e as responsabilidades. Segundo a política, as diretrizes de continuidade da XY Telecom são:

> - A Continuidade de Negócios é fator preponderante para XY Telecom, devendo estar alinhada com o Planejamento Estratégico e com todas as mudanças na organização;
> - As ações de Continuidade de Negócios devem estar baseadas no resultado de avaliações de riscos e de análises de impacto nos negócios, além de garantir a conformidade com a legislação vigente e com a regulamentação da Anatel;
> - Todo processo de Continuidade de Negócios deverá ser documentado e formalizado através de regulamentos e procedimentos corporativos;
> - Os recursos humanos, físicos e financeiros devem ser disponibilizados de acordo com as estratégias de continuidade definidas e observando as orientações da XY Telecom. (XY TELECOM, 2008)

No tocante a responsabilidades, a política estabelece que: (i) a Diretoria Executiva é responsável por promulgar e fazer cumprir a Política, garantindo o respaldo necessário às áreas responsáveis; (ii) a equipe de Coordenação do Projeto é responsável pela Gestão de Continuidade de Negócios, incluindo sua manutenção e a melhoria contínua; (iii) o Comitê Executivo é responsável por avaliar e implementar o GCN na XY Telecom, tendo, dentre as diversas atividades, a responsabilidade de mantê-lo alinhado ao negócio; e (iv) os colaboradores são responsáveis por conhecer os planos e procedimentos de continuidade existentes e as situações em que serão utilizados.

Já o documento denominado Regulamento de GCN, apresenta informações mais detalhadas sobre as responsabilidades dos envolvidos em cada uma das etapas da estrutura de GCN da XY Telecom. Segundo o documento, a equipe de coordenação possui, dentre outras responsabilidades: (i) avaliar riscos e impactos ao negócio; (ii) propor estratégias de continuidade; (iii) administrar os planos de continuidade; (iv) definir um plano de testes dos planos desenvolvidos; e (v) definir os grupos funcionais de continuidade de negócio. Além disso, o documento define a responsabilidade dos gestores da XY Telecom em manter sempre treinados e atualizados os colaboradores envolvidos na estrutura de GCN sob sua gestão.

Por fim, o documento denominado Procedimento de GCN, estabelece as principais características e dá alguns detalhes sobre as atividades da estrutura de GCN da XY Telecom.

Segundo o documento, a estrutura de GCN da XY Telecom é caracterizada através de um ciclo de vida de GCN (o mesmo modelo previsto na norma BS25999-1) e, portanto, composto pelos elementos: (i) gestão do programa de GCN; (ii) entendo a organização; (iii) determinando a estratégia de continuidade de negócios; (iv) desenvolvendo e implementando uma resposta de GCN; (v) testando, mantendo e analisando criticamente os preparativos de

GCN; e (vi) incluindo a GCN na cultura da organização. Dessa forma, o documento dá alguns detalhes sobre as características de cada uma dessas etapas, à luz da norma de referência.

Além disso, o documento estabelece alguns detalhes importantes sobre os Grupos Funcionais, que são as equipes com responsabilidade para atuar em resposta aos diferentes tipos e níveis de eventos que possam ocorrer na companhia. Segundo o procedimento, a XY Telecom previu em sua estrutura de GCN os seguintes grupos funcionais: (i) Grupo Executivo (formado por integrantes da Diretoria Executiva e responsável pela tomada de decisões estratégicas em caso de grandes crises ou desastres); (ii) Grupo de Gestão/Decisão (responsável por assegurar recursos para operacionalização dos planos e atendimento das necessidades básicas ao pessoal de GCN); (iii) Grupo de Execução (responsável pela operacionalização dos planos de resposta).

Outra informação importante prevista no Procedimento de GCN é a definição dos níveis de acionamento, ou seja, a classificação dos níveis de impactos dos eventos capazes de afetar a XY Telecom e a descrição da medida cabível para cada caso. Os níveis de acionamento da XY Telecom são apresentados no Quadro 4.

Quadro 4 – Níveis de Acionamento da XY Telecom

Nível de Acionamento	Descrição do Evento	Medida de Acionamento
A	Situação em que o problema pode ou não ser resolvido rapidamente, mas que não impede a efetivação de uma operação.	Respeitando-se os procedimentos usuais de cada unidade, caberá ao próprio funcionário acionar a medida de contingência, bem como as providências para a solução do problema pelas unidades competentes.
B	Situação em que o problema afeta significativamente o ambiente de trabalho da unidade, impedindo que suas atividades normais sejam realizadas.	O superior hierárquico (Gerente Superior) deve ser avisado prontamente, cabendo a este avaliar a situação e se não houver tempo hábil para aguardar a solução do problema deve estabelecer contato com a área de Contingência para acionamento / participação nos Procedimentos de Contingência.
C	Situação em que o problema afeta o processo critico, fazendo com que todos os usuários estejam sem condições de realizar suas operações normalmente.	Os superiores hierárquicos (Gerente superior e chefe imediato) devem ser avisados prontamente, cabendo a estes avaliarem a situação e se não houver tempo hábil para aguardar a solução do problema devem estabelecer contato com a área de Contingência, para acionamento e participação nos Procedimentos de Contingência.
D	Situação em que o problema é em entidade externa, ou seja, o fator que impede o procedimento normal e independe de ação da XY Telecom para superá-lo.	Caberá a estas entidades comunicarem a XY Telecom o procedimento de contingência a ser adotado. Em caso de dúvidas poderá ser realizado contato direto com estas no sentido de se obter as devidas orientações. Caso seja necessário a área de Contingência estará enviando orientações específicas.

Fonte: XY Telecom (2008)

O Procedimento de GCN da XY Telecom apresenta, ainda, informações sobre os Centros de Comando, ou salas-de-guerra, que são os locais protegidos de onde os esforços de recuperação dos ambientes da empresa, afetados pela crise ou desastre deverão ser direcionados. Segundo o documento, cada Centro de Comando deve ser munido de equipamentos necessários para controlar uma situação de desastre, incluindo-se:

> - Duas linhas telefônicas: uma para acesso com provedor de Internet (linha discada) e outra para demais fins (com recursos de áudio conferência). Uma linha telefônica especial deve ser implementada para os funcionários da empresa como ponto central de contato para solicitar ajuda, relatar a situação, e compartilhamento de informações durante um desastre de grande proporção, e deverá ser divulgada tão logo existam condições de fazê-lo.
> - Desktop ou notebook com placa fax-modem;
> - Pontos de rede;
> - Impressora;
> - Fax;
> - Copiadora;
> - Outros sistemas portáteis de comunicação (celulares, rádios, etc.), devem ser verificadas a duração das baterias;
> - Quadro/*Flip Chart*;
> - Mobiliários (mesas de trabalho, armários, mesas de reunião, mesas de café, cadeiras, etc.);
> - Material de escritório em geral. (XY TELECOM, 2008)

3.2.3 Fase III – Análise de Riscos e Análise de Impacto no Negócio (BIA);

Nessa fase, foram desenvolvidas pela XY Telecom as atividades de Análise de Impacto no Negócio (ou BIA – *Business Impact Analysis*) e a Análise de Riscos. O objetivo foi o levantamento dos impactos que uma interrupção nos processos críticos da organização pode causar à companhia e quais são as ameaças e vulnerabilidades existentes nos ativos que suportam esses processos.

A atividade de Análise de Riscos contemplou os ambientes e/ou escritórios onde se encontram os ativos físicos que suportam os processos críticos para o negócio da XY Telecom e foi apresentada através do Relatório de Análise de Risco. Essa atividade iniciou-se através do mapeamento das interdependências entre os 50 processos definidos no escopo e dos ativos existentes para cada um deles e foi executada através de entrevistas com os gestores desses processos. Em seguida, foi executada a identificação e análise dos riscos para os ativos de TI e para a infra-estrutura predial dos processos críticos.

A análise de riscos de TI foi desenvolvida através de amostragem e contou com o auxílio de uma ferramenta informatizada fornecida pela consultoria. Nessa ferramenta, foram cadastrados os ativos de TI selecionados em cada processo, incluindo as informações sobre características, criticidade e relacionamento. Em seguida o *software*, com base nessas informações, avaliou a vulnerabilidade de cada ativo (através de sua base de conhecimento) e

calculou os riscos existentes, com base nos componentes de probabilidade, severidade e relevância chegando-se a um resultado (valor numérico) por ativo. A descrição de cada componente para cálculo dos riscos foi apresentada no Quadro 5.

Quadro 5 – Descrição dos Componentes para Cálculo de Riscos em Ativos da XY Telecom

PROBABILIDADE	SEVERIDADE	RELEVÂNCIA
É a possibilidade da vulnerabilidade (na falta do controle) ser explorada pelas ameaças.	É a conseqüência na segurança da informação caso as ameaças explorem a vulnerabilidade nos aspectos de Confidencialidade, Integridade e Disponibilidade.	É o grau de importância do Ativo para o negócio da empresa considerando os componentes de negócio que ele apóia.

Fonte: XY Telecom (2008)

Por fim, foram listados os ativos de TI avaliados de acordo com os níveis de riscos identificados e definida a estratégia de priorização para tratamento desses ativos. Essa estratégia de priorização obedeceu a escala apresentada no Quadro 6.

Quadro 6 – Escala de Níveis de Riscos em Ativos da XY Telecom

Níveis de Risco	Interpretação
Muito Alto	São riscos inaceitáveis, e os gestores dos ativos devem ser orientados que os eliminem imediatamente.
Alto	São riscos inaceitáveis e os gestores dos ativos devem ser orientados para pelo menos controlá-los.
Médio	São riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos, contudo a aceitação do risco deve ser feita por meios formais.
Baixo	São riscos que podem ser aceitáveis após revisão e confirmação dos gestores dos ativos.
Muito Baixo	São riscos aceitáveis e devem ser informados para os Gestores dos ativos.

Fonte: XY Telecom (2008)

Já a análise de risco dos ativos de infra-estrutura predial também foi desenvolvida através de amostragem e contou com auxílio de ferramenta informatizada, mas teve como principal característica a realização de inspeções *in loco* nos principais ambientes onde operam os processos críticos da XY Telecom. Para essa tarefa, inicialmente foram levantados os prédios e instalações relacionados aos 50 processos do escopo. Em seguida, foi selecionada uma amostra de 11 prédios a serem inspecionados fisicamente, onde foram avaliadas e documentadas informações sobre as características ambientais de cada prédio, incluindo: (i) energia (instalações elétricas); (ii) climatização; (iii) comunicação de dados e voz; (iv) detecção e combate a incêndio; (v) perímetro de segurança física; (vi) controle de entrada física; (vii) segurança de escritórios, salas e instalações; (viii) proteção da localização de equipamentos; etc. As principais informações levantadas foram cadastradas no *software* fornecido pela consultoria que calculou os riscos existentes (através de sua base de conhecimento) em cada ativo. Por fim, a exemplo dos ativos de TI, foram listados os prédios mais críticos, conforme nível de risco, para definição da priorização no tratamento dos riscos.

Após a atividade de análise de riscos, foi desenvolvida a atividade de análise de impacto de negócios ou BIA (*business impact analysis*). Essa atividade foi desenvolvida através de entrevistas com os gestores de cada um dos 50 processos definidos no escopo do projeto com o objetivo de determinar quais desses processos devem ser priorizados através de estratégias de continuidade. Para essa tarefa, inicialmente foram planejados os questionários de entrevista com os gestores de negócio e agendadas as reuniões. Em seguida, os questionários foram aplicados, onde foram obtidas, para cada processo do escopo, as seguintes informações: (i) período máximo de interrupção tolerável; (ii) tempo objetivado de recuperação (ou RTO – r*ecovery time objective*); e (iii) estimativa do impacto financeiro imediatamente após a violação do período máximo de interrupção. Por fim, os processos analisados foram listados em ordem crescente, de acordo com o tempo objetivado de recuperação.

3.2.4 Fase IV – Estratégias de Continuidade

Nessa fase foi desenvolvida a atividade de definição das estratégias de continuidade de negócios da XY Telecom. O objetivo foi o desenvolvimento das estratégias para o restabelecimento dos serviços críticos, em uma recuperação compatível com o tempo objetivado de recuperação dos processos críticos do negócio da companhia.

Essa atividade iniciou-se através da consolidação da macro-estratégia de continuidade, que foi definida através da seqüência de retomada dos processos e sistemas da companhia. Para esse seqüenciamento, foi utilizado como critério a informação sobre o tempo objetivado de recuperação de cada processo e de cada sistema. Em seguida, os 50 processos do escopo foram classificados e agrupados conforme o tipo de estratégia de infra-estrutura predial a ser aplicada:

- *Cold Site*: processos com RTO maior que 30 dias. Consiste no espaço adequado e na infra-estrutura disponível (energia elétrica, distribuidor geral de telecomunicações e climatização) para suportar as operações e o ambiente deve possuir necessariamente a infra-estrutura capaz de receber os equipamentos para uma operação entrar em funcionamento (TI e não TI);
- *Warm Site*: processos com RTO entre 7 e 30 dias. Consiste em ambientes parcialmente preparados contendo alguns ou todos os elementos da infra-estrutura disponíveis (energia elétrica, climatização, linhas e links de comunicações, equipamentos de TI, equipamentos de escritório, softwares, e outros.) para suportar as operações;

- *Hot Site*: processos com RTO entre 1 e 6 dias. Consiste no espaço dimensionado e adequado para suportar os requerimentos de cada ativo e configurados com hardware, infra-estrutura de suporte (energia elétrica, climatização, linhas e links de comunicações, equipamentos de TI, equipamentos de escritório, softwares, e outros.) e equipe de apoio necessária. O *Hot Site* é tipicamente projetado para funcionar em regime 24 horas por dia, 7 dias por semana;
- *Mirrored Site*: processos com RTO menor que 1 dia. Consiste no espelhamento total dos componentes (redundância e atualização de informações em tempo real) necessários para o funcionamento de cada Ativo. O *Mirrored Site* é idêntico ao site principal em todos os aspectos técnicos.

Após esse agrupamento, foi realizada uma estimativa de investimento para cada tipo de estratégia de infra-estrutura predial a ser adotada.

A próxima tarefa dessa etapa foi identificar os sites críticos para os processos considerados como *Mirrored Site*, os recursos humanos desses sites e a infra-estrutura necessária para essas pessoas trabalharem. Após essa identificação, foram elaboradas as alternativas de contingência para esses sites. Essas alternativas foram apresentadas através de 3 opções:

- Opção 1 – Site de Contingência de Terceiro: o site de contingência estará instalado em local físico de um prestador de serviço, a ser contratado mediante contrato específico firmado para este fim;
- Opção 2 – Site de Contingência Próprio: consta de um site de contingência próprio às instalações da XY Telecom e suficientemente distante, de forma a não sofrer transtornos conseqüentes de um desastre;
- Opção 3 – Site de Contingência Misto (Terceiro e Próprio): abrange simultaneamente as opções 1 e 2, onde tem-se um site de contingência de terceiros e próprio (novo ou remanejado).

Por fim, cada uma dessas opções foi avaliada qualitativamente pela equipe de coordenação do projeto, conforme os seguintes critérios: (i) isolamento; (ii) agilidade operacional; (iii) facilidade de telecomunicações; (iv) facilidade de auditoria; (v) capacidade técnica; (vi) facilidade de testes; (vii) segurança organizacional; (viii) classificação e controle dos ativos de informação; (ix) segurança em pessoas; (x) segurança física e do ambiente; (xi) gerenciamento das operações e comunicação; (xii) controle de acesso; (xiv) gestão da continuidade do negócio. Cada critério foi pontuado conforme escala (1-não atende; 1,2-atende parcialmente; 1,5-atende; e 2-excede).

O resultado dessa análise indicou a Opção 1 – Site de Contingência de Terceiro como a de maior pontuação e, portanto, a mais recomendada para desenho dos planos de resposta.

3.3 Análise Crítica da Estrutura de GCN da XY Telecom (Pré-teste do modelo de GCN da BS25999-1)

Após a apresentação da estrutura de GCN da empresa XY Telecom, foi realizada uma análise crítica dessa estrutura com o objetivo de identificar as principais dificuldades encontradas nessa implantação, assim como necessidades de melhoria. Essa análise crítica representa um pré-teste do modelo de GCN da BS25999-1 (ou ciclo de vida de GCN) cujo resultado servirá de referência para o desenvolvimento da proposta de estrutura de apoio de SGCN, objeto do presente trabalho.

3.3.1 Metodologia da Análise Crítica

A análise crítica da estrutura de GCN da XY Telecom foi realizada em três etapas. A primeira etapa envolveu o levantamento de informações adicionais sobre a implantação de cada uma das fases da estrutura de GCN da XY Telecom. Essa etapa foi realizada através de entrevistas com colaboradores da XY Telecom participantes do projeto de GCN em 2008, que foram questionados a respeito das deficiências ou necessidades de melhoria observadas durante ou após a implantação da estrutura de GCN.

A segunda etapa envolveu uma verificação da aderência da estrutura de GCN da XY Telecom à norma de referência BS25999-1. Essa etapa foi realizada a partir da análise das informações existentes sobre a estrutura de GCN da XY Telecom, comparação com as recomendações para cada um dos elementos do ciclo de vida de GCN apresentado na norma BS25999-1 e identificação das principais não-conformidades (*gaps*) dessa estrutura.

A terceira etapa envolveu a consolidação de informações. Nessa etapa foram consolidadas as respostas obtidas nas entrevistas, bem como os *gaps* identificados na estrutura da XY Telecom, em um quadro segmentado por fase de implantação e principais elementos.

3.3.2 Resultados da Análise Crítica

Conforme a metodologia descrita, foi realizada a análise crítica da estrutura de GCN da XY Telecom. Os resultados dessa análise são apresentados no Quadro 7.

Quadro 7 – Resultados da Análise Crítica da Estrutura de GCN da XY Telecom

Fases da Estrutura	Elemento	Dificuldades/Necessidades Observadas	*GAPS* com relação à BS25999-1
Fase I – Definição do Escopo e Planejamento	Escopo	Escopo de 50 processos e 25 sistemas foi muito grande para uma implantação inicial, o que impactou nos prazos de desenvolvimento das fases III e IV e encareceu os custos com a consultoria do projeto.	Escopo contemplou alguns processos administrativos ou de apoio, não relacionados diretamente aos produtos e serviços fundamentais da companhia.
Fase II – Documentação da Gestão de Continuidade de Negócios	Política de GCN	Política não foi publicada e divulgada aos colaboradores. Portanto, as diretrizes e responsabilidades definidas não foram de fato afirmadas na companhia.	Não identificado.
	Regulamento de GCN	Não foi publicado.	Não identificado.
	Procedimento de GCN	Não foi publicado.	Não identificado.
Fase III – Análise de Riscos e Análise de Impacto no Negócio (BIA)	Análise de Riscos	Escopo amplo de processos gerou uma amostra grande para análise, dificultando sua execução nos prazos. Lógica e critérios para cálculo dos riscos é de *software* de terceiro, gerando dificuldades para atualização ou customização.	Análise de Riscos concentrou-se em ativos de TI e de infra-estrutura prediais, desprezando outros ativos importantes tais como pessoas e suprimentos.
	Análise de Impacto de Negócios (BIA)	Escopo amplo de processos gerou um grande número de entrevistas com gestores, dificultando a execução do BIA nos prazos.	Não identificado.
Fase IV – Estratégias de Continuidade	Estratégias de Continuidade	Estratégia de Continuidade não foi aprovada pela Alta Direção, impedindo sua implementação, bem como a evolução das demais etapas do ciclo de GCN.	Elaboração de estratégias de continuidade concentrou-se no contingenciamento de ativos de TI e de infra-estrutura prediais, desprezando outros recursos importantes tais como pessoas e suprimentos.

Fonte: elaborado pelo autor

Com base nos resultados apresentados, pôde-se constatar a necessidade de algumas melhorias na estrutura de GCN da XY Telecom que devem ser consideradas numa futura remodelagem desse processo.

Em contrapartida, as etapas implantadas de GCN na XY Telecom demonstram uma relativa consistência com as boas práticas de GCN previstas na BS25999-1. Além disso, pôde-se observar na apresentação da estrutura de GCN da XY Telecom a aplicação de técnicas e métricas bastante interessantes e pertinentes aos objetivos determinados, como no caso do procedimento de GCN, do BIA ou das estratégias de GCN.

O projeto de GCN da XY TELECOM não foi continuado no ano seguinte ao de 2008. Portanto, a grande deficiência observada na estrutura de GCN da companhia em estudo deve-se ao fato de que sua implantação foi incompleta. Fazendo-se um paralelo com o modelo de ciclo de vida de GCN da norma BS25999-1, vista no capítulo 2, faltam ainda serem

totalmente implantadas as seguintes etapas: implementação e operação (onde devem ser confeccionados os planos de gestão de incidentes e o plano de continuidade de negócios), a etapa de teste, análise crítica e manutenção dos preparativos de GCN, a etapa de gestão do programa de GCN e a etapa de aculturamento de GCN na organização.

Essa deficiência observada remete à reflexão de que talvez uma melhor estratégia de convencimento da alta direção para o patrocínio do projeto, a definição de objetivos mais consistentes sobre GCN e o estabelecimento do conceito de manutenção e melhoria contínua das etapas já implantadas (elementos presentes num modelo de Sistema de Gestão de Continuidade de Negócios) pudessem ter evitado essa interrupção.

Desse modo, a análise comparativa entre os modelos de GCN e SGCN apresentados no capítulo 2, aliada ao estudo e análise crítica do modelo de GCN da XY Telecom servirão como ponto de partida para a elaboração de uma nova de estrutura de GCN nessa companhia.

Como viu-se, a XY Telecom trata-se de uma empresa de grande porte situada em um mercado altamente competitivo e regulado. Caracterizada por uma abordagem por processos bem definida, a empresa apresenta uma estrutura de GCN parcialmente implantada, mas com bons elementos de referência.

No capítulo 4 será elaborada e apresentada uma proposta para implantação de uma nova abordagem de GCN para essa organização, fundamentada num conceito mais consistente com a melhoria contínua, o SGCN. Essa proposta visa retomar e reestruturar o modelo de GCN da XY Telecom de forma a garantir a sua manutenção e aperfeiçoamento constante.

4. Sistema de Gestão de Continuidade de Negócios – Proposta de Estrutura de Apoio à Implantação na XY Telecom

Este capítulo apresenta uma proposta de estrutura de apoio para a implantação de um sistema de gestão de continuidade de negócios, que aborde os aspectos associados ao risco de interrupção dos processos críticos de uma empresa de telecomunicações. Esta proposta está baseada no referencial teórico apresentado no capítulo 2 (com ênfase no modelo de ciclo de vida de GCN da norma BS25999-1 e no modelo de SGCN da norma BS25999-2) e no estudo de caso da estrutura de GCN da XY Telecom apresentado no capítulo 3, considerando os resultados da análise crítica realizada.

A escolha pelo desenvolvimento de uma estrutura de SGCN integrando elementos do ciclo de vida de GCN foi fundamentada inicialmente pelos resultados do comparativo conceitual realizado entre o modelo de SGCN (sistema de gestão) e de GCN (ciclo de vida), apresentado no capítulo 2, onde concluiu-se pela indicação de uma proposta de estrutura mista. Além disso, o estudo de caso e análise crítica da estrutura de GCN da XY Telecom reafirmaram essa indicação, dado que observou-se naquele modelo características importantes a serem aproveitadas, assim como necessidades de aperfeiçoamento no tocante à melhoria contínua.

A estrutura proposta é apresentada na forma de sugestões para cada requisito de apoio à implantação, definidas de acordo com o contexto da empresa em estudo.

Para facilitar a elaboração de sugestões sobre a implantação de um sistema de gestão de continuidade de negócios, foi elaborado um modelo esquemático para representar os níveis de implantação dos requisitos do SGCN.

O sistema proposto, de forma geral, segue a estrutura apresentada por Viegas (2000). O modelo de PDCA desenvolvido por Viegas (2000) é consistente com a melhoria contínua,

evidenciando as etapas de Planejamento, Implementação e Operação, Verificação e Ação Corretiva e Análise Crítica.

Como a estrutura de Viegas (2000) contempla um sistema integrado de qualidade e meio ambiente, foram feitas algumas adaptações no modelo original de forma a contemplar as particularidades dos requisitos de um sistema de gestão de continuidade de negócios, com base no padrão normativo BS25999-2.

O modelo adaptado de implantação dos requisitos do SGCN é apresentado na Figura 9 e é composto de 4 etapas: Planejamento, Implementação e Operação, Análise Crítica e Ação Corretiva. Cada tópico da Figura 9 representa um elemento (requisito) relevante a ser considerado na implantação do sistema.

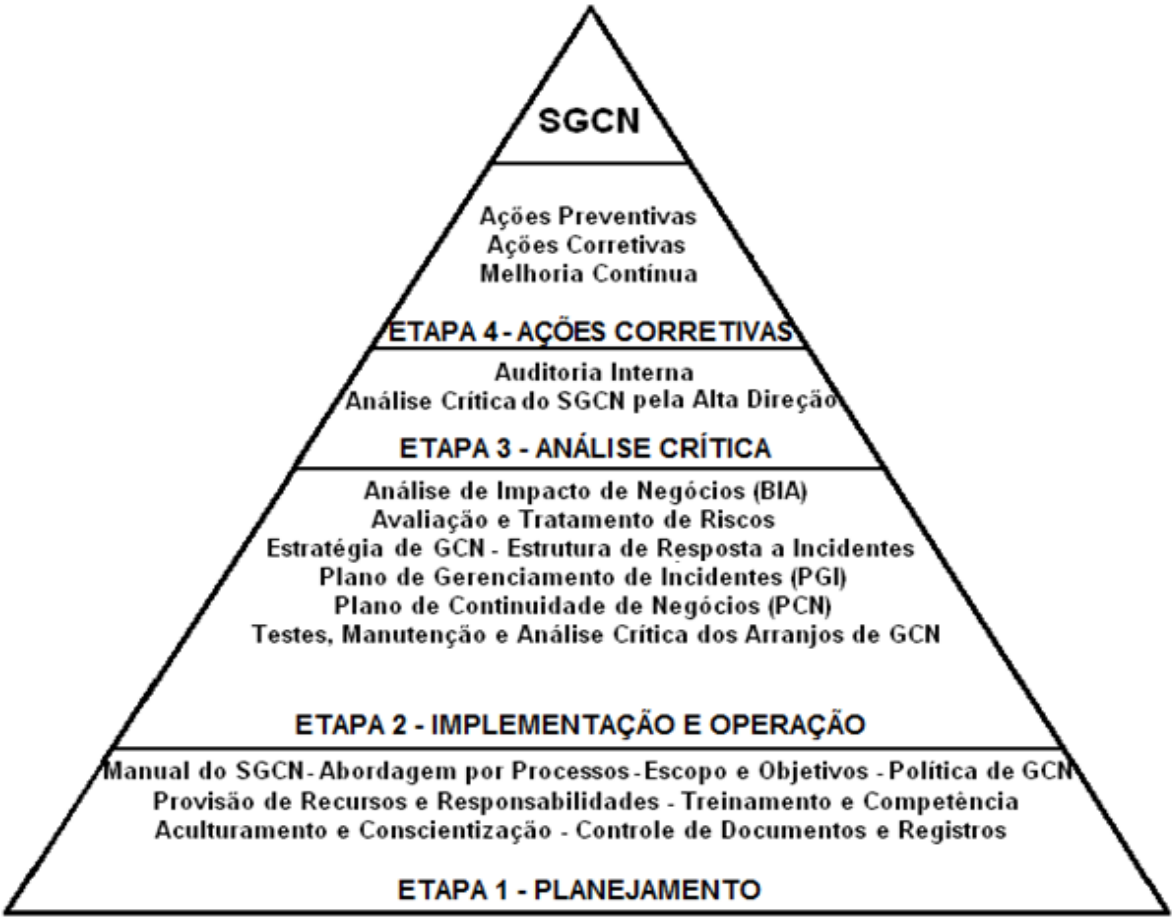

Figura 9 – Proposta de Estrutura de Apoio à Implantação de um SGCN

Fonte: adaptado de Viegas (2000)

O objetivo do modelo proposto, além de apresentar sugestões para a implantação dos requisitos de SGCN, conforme boas práticas de GCN existentes, é também planejar as ações de adequação para a empresa XY Telecom. Para isso, utilizou-se como auxílio quadros do

tipo 3W1H (*what, who, when, how*), incluindo informações sobre: (i) o que fazer; (ii) quem vai fazer; (iii) quando, ou em quanto tempo será feito; e (iv) como será feito.

A seguir, será visto como cada um dos elementos relevantes do SGCN deve ser tratado, de forma a permitir que o sistema proposto funcione adequadamente na empresa de referência.

4.1 Etapa 1 - Planejamento

Nesta etapa serão feitas sugestões e planejadas ações para a implantação dos seguintes requisitos: Manual do Sistema de Gestão de Continuidade de Negócios; Abordagem por Processos; Escopo e Objetivos; Política de GCN; Provisão de Recursos e Responsabilidades; Treinamento e Competência; Aculturamento e Conscientização; Controle de Documentos e Registros. A seguir, cada um desses elementos será brevemente descrito.

4.1.1 Manual do Sistema de Gestão de Continuidade de Negócios

Visando descrever a estrutura e o estabelecimento do SGCN, sugere-se a elaboração de um Manual do Sistema de Gestão de Continuidade de Negócios que deverá conter informações relacionadas aos principais requisitos que compõem o SGCN implantado na organização. Esse Manual, em outras palavras, serve como um documento guia para descrição do planejamento e do estabelecimento do sistema de gestão de continuidade de negócios na companhia.

É recomendável que o manual contenha informações sobre a adequação da(s) política(s) à escala das operações, riscos e impactos mais significativos relacionados à continuidade de negócios da organização.

Considerando a integração dos diversos requisitos normativos, o manual também deverá conter o escopo do sistema, a interação dos processos de GCN, a(s) política(s) do sistema de gestão, e fazer referência aos principais documentos e registros que compõem o sistema de gestão de continuidade proposto.

Na prática do estabelecimento do SGCN sugere-se, preliminarmente, realizar-se um esboço desse Manual como um instrumento norteador para o planejamento dos requisitos a serem implantados e que deve ser atualizado na medida em que estes requisitos forem de fato estabelecidos.

Na XY TELECOM não se observou a existência de procedimento para orientar e evidenciar o estabelecimento do SGCN, entretanto constatou-se, na proposta de documento Procedimento de GCN, informações sobre os elementos que compõem a estrutura do ciclo de vida de GCN naquela companhia. Sugere-se, portanto, no Quadro 8, o planejamento da elaboração de um Manual aplicado a uma estrutura de SGCN.

Quadro 8 – Ação para Elaboração do Manual de SGCN na XY Telecom

O que fazer	**Quem**	**Quando**	**Como**
Elaboração do Manual do SGCN	Equipe de Coordenação	1 semana	Analisar as atividades previstas no Procedimento de GCN da XY Telecom. Planejar a estrutura documental para estabelecimento do SGCN. Elaborar o Manual.

Fonte: elaborado pelo autor

4.1.2 Abordagem por processos

É aconselhável que uma abordagem por processos (caracterização, definição de entradas e saídas, métodos de monitoramento, etc.) e a estrutura do Sistema de Gestão de Continuidade de Negócios estejam definidas no Manual do SGCN. Essa caracterização deve considerar os processos relacionados ao negócio e, dentre eles, os processos de GCN, aqueles cuja interrupção possa gerar grandes impactos à organização devido à sua relação direta com os produtos e serviços essenciais da companhia.

Conforme visto no capítulo anterior, os processos da empresa XY TELECOM, bem como a interação entre eles, foram representados graficamente através do modelo eTOM. Como visto, o modelo da XY TELECOM representa o universo de processos da organização através três grupos: o primeiro, denominado estratégia, infra-estrutura, produtos e serviços, contém os agrupamentos de processos que se relacionam diretamente à estratégia da empresa, ao ciclo de vida de infra-estrutura e ao ciclo de vida de produtos e serviços, tais como Estratégia e Compromissos, Gerenciamento do Ciclo de Vida das Infraestruturas, Gerenciamento do Ciclo de Vida dos Produtos, Gerenciamento de Marketing e Oferta, Desenvolvimento e Gerenciamento de Serviços, Desenvolvimento e Gerenciamento de Recursos e Desenvolvimento e Gerenciamento de Canais de Fornecimento.

O segundo grupo, denominado operações, contém os agrupamentos de processos que se relacionam diretamente ao cliente, ao aprovisionamento, à garantia da qualidade e ao ciclo de receita da XY TELECOM, tais como Implantação, Garantia, Faturamento, Suporte e Facilidades da Operação, Gerenciamento do Relacionamento com Clientes, Gerência e

Operação de Serviços, Gerência a Operação de Recursos e Gerenciamento do Relacionamento com Fornecedores/Parceiros.

O terceiro grupo, denominado gestão empresarial, contém os processos relacionados indiretamente ao negócio e diretamente à gestão e suporte da organização, tais como Planejamento Estratégico e Empresarial, Gerenciamento de Marca, Pesquisa Mercado e Propaganda, Gestão da Qualidade, Processos, Planejamento e Arquitetura de TI, Pesquisa, Desenvolvimento e Aquisição de Tecnologia, Gestão Financeira e de Ativos, Gerenciamento de Relacionamentos Externos e Outros Interessados, Gestão de Recursos Humanos e Gestão de Fraudes, Segurança e Restauração de Desastres.

Após essa abordagem inicial dos processos da organização, sugere-se, portanto, que a XY TELECOM identifique e detalhe brevemente seus processos de GCN no Manual do SGCN ou em procedimento específico, juntamente com as análises que suportaram a inclusão dos mesmos (Mapeamento de Recursos, Análise de Impactos, Avaliações Qualitativas em Processos, etc.).

Assim, propõe-se no Quadro 9 a ação relacionada à abordagem por processos para a XY TELECOM.

Quadro 9 – Ação para apoiar a Abordagem de Processos de GCN na XY Telecom

O que fazer	**Quem**	**Quando**	**Como**
Descrever a abordagem de processos de GCN	Equipe de Coordenação	1 semana	Detalhar no Manual de SGCN a abordagem de processos de GCN.

Fonte: elaborado pelo autor

4.1.3 Escopo e objetivos

Sugere-se que o escopo do SGCN também esteja documentado no Manual de SGCN, identificando-se os produtos e serviços principais da organização.

Conforme BUSINESS CONTINUITY INSTITUTE (2008), o propósito de se definir o escopo é garantir claramente quais áreas da organização são incluídas no escopo do sistema de SGCN. A documentação de escolhas para cada produto e serviço é recomendável para explicitar a forma como a organização tem a intenção de proteger (ou não) a sua capacidade de manter a sua entrega, de modo que esta decisão esteja disponível para o exame externo, por exemplo, clientes ou órgãos reguladores.

O escopo pode ser definido pela identificação de quais produtos e serviços estão incluídos dentro da mesma. Esta focaliza os critérios chave para o sucesso da maioria das organizações - a entrega de produtos ou serviços. Locais podem também ser utilizados para definir o escopo de SGCN para incluir ou excluir um ou mais sites. No entanto, não é lógico

excluir um site que desempenha um papel na entrega de um produto ou serviço que está incluído no escopo (BCI, 2008).

A limitação do escopo, segundo BCI (2008), deve ser visto como uma tática que permite uma abordagem por etapas de desenvolvimento para a introdução do SGCN em toda uma organização. Se um produto ou serviço é identificado no escopo, então todas as atividades de apoio à sua entrega devem, por conseguinte, ser incluídas no sistema de GCN.

Conforme pode ser visto na Figura 10, de BCI (2008), se for decidido que o Produto B e o Serviço C estão dentro do escopo do programa, então as atividades sombreadas estão necessariamente total ou parcialmente dentro do escopo.

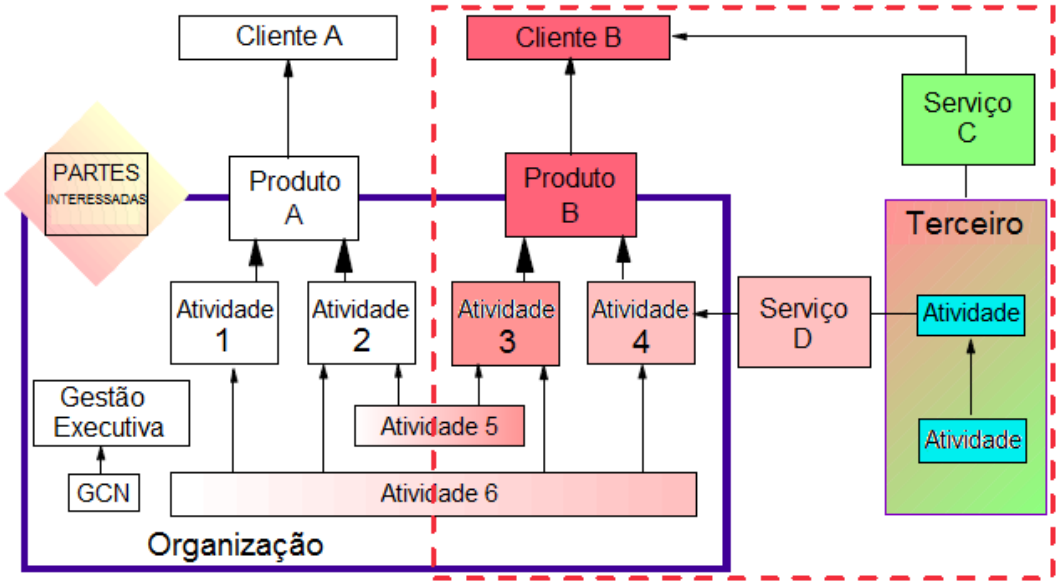

Figura 10 – Diagrama de interação entre produtos e atividades de uma organização conforme a BS25999

Fonte: BCI – Business Continuity Institute (2008)

No caso da empresa em estudo, optou-se pela definição do escopo por processo, já que os processos da empresa estão bem definidos e existe uma área responsável pelo mapeamento e manutenção destes de acordo com o modelo de arquitetura de processos vigente.

No ano de 2008 a XY TELECOM definiu como escopo inicial para os trabalhos de SGCN em torno de 50 processos que eram suportados por 25 sistemas. Conforme visto no capítulo 3, a escolha desse amplo escopo de processos trouxe algumas dificuldades para viabilizar as etapas subseqüentes da estrutura de GCN.

Sugere-se, portanto, a utilização de um escopo mais reduzido de processos e sistemas (escopo piloto) de modo a viabilizar a implantação completa da estrutura de SGCN proposta. Para essa delimitação é importante a utilização de premissas e critérios consistentes e bem

formalizados para garantir que os processos que estão sendo incluídos no escopo são realmente representativos.

Já os objetivos e metas devem conduzir à evolução do Sistema de Gestão de Continuidade de Negócios, de acordo com seu desempenho. Dentre os fatores que contribuem para a sistemática de definição dos objetivos e metas de SGCN deve-se considerar: a)requisitos para a continuidade de negócios; b) objetivos e obrigações da organização; c) nível de risco aceitável; d) responsabilidades legais, regulamentares e contratuais; e d)interesses das suas partes interessadas principais.

Para monitorar o atingimento dos objetivos e metas deve ser criado um programa de gestão. Os programas de gestão nada mais são do que planos de ação que transformam as boas intenções da política e dos objetivos e metas em realidade. Os programas de gestão devem ser compostos pela ação, o responsável, o prazo e o acompanhamento do cumprimento das ações previstas.

Com relação à definição de objetivos e metas não foram identificados na XY TELECOM registros ou evidências de definição e de acompanhamento. Sugere-se, então, que a gestão dos objetivos e metas do SGCN seja implantada e fique sob a responsabilidade de um representante, indicado pela Diretoria da empresa, que monitore e reporte periodicamente a evolução do programa de gestão nas reuniões de análise crítica do SGCN.

Com base nas sugestões apresentadas no tocante ao escopo e objetivos, o Quadro 10 detalha as ações a serem desenvolvidas na XY TELECOM.

Quadro 10 – Ações para apoiar o Escopo e Objetivos de SGCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Definição do escopo de processos	Equipe de Coordenação	1 semana	Avaliação dos processos de GCN e delimitação do escopo de processos.
Definição do escopo de sistemas	Equipe de Coordenação	1 semana	Avaliação dos sistemas de GCN e delimitação do escopo de sistemas.
Definição dos objetivos e metas de SGCN	Equipe de Coordenação	1 semana	Definição, formalização e acompanhamento de objetivos e metas de SGCN

Fonte: elaborado pelo autor

4.1.4 Política de GCN

Presente em todos os padrões normativos de referência, a política é a base para a implantação de um sistema de gestão. Para isso, a alta direção possui papel fundamental no sentido de estabelecer e demonstrar um compromisso com a política de gestão da continuidade de negócios.

Conforme preconiza a BS25999-2, ou NBR15999-2, a política de GCN deve incluir ou fazer referência a: a) os objetivos da continuidade de negócios da organização; e b) o escopo da continuidade de negócios, incluindo as limitações e exclusões (ABNT, 2008).

Recomenda-se que a política seja: a) documentada no manual do SGCN; b) aprovada pela alta direção; c) comunicada a todas as pessoas que trabalham para ou em nome da organização; e d) analisada criticamente em intervalos planejados e quando ocorrerem mudanças significativas (ABNT, 2008).

Em se tratando de empresa de telecomunicações, não se deve esquecer-se de incluir na política o comprometimento em atender requisitos do órgão regulador ANATEL (Agência Nacional de Telecomunicações), que regulamenta o setor.

Conforme visto no capítulo 3, a XY TELECOM definiu, em 2008, uma proposta de política de GCN. De lá para cá ocorreram mudanças importantes na estrutura e na estratégia da XY TELECOM que demandaram a necessidade de revisão da proposta de política de GCN. Necessita-se, também, que a política seja documentada e referenciada no "Manual de SGCN", além de divulgada e compreendida por todos colaboradores.

São planejadas, portanto, no Quadro 11, as ações de adequação para a política de GCN da XY Telecom.

Quadro 11 – Ações para apoiar a definição e divulgação da Política de SGCN na XY Telecom

O que fazer	Quem	Quando (Prazo)	Como
Revisão da Política de GCN	Equipe de Coordenação e Grupo Executivo	1 semana	Reunião com as Equipes para revisão da política e discussão de possíveis alterações/exclusões.
Aprovação da Política de GCN	Diretoria	1 semana	Análise do documento revisado e aprovação formal da política.
Divulgação da Política de GCN	Equipe de Coordenação	1 semana	Publicação do documento final no sistema de documentos da Companhia e inclusão das diretrizes da política de GCN no material a ser divulgado na atividade de conscientização.

Fonte: elaborado pelo autor

4.1.5 Provisão de Recursos e Responsabilidades

A provisão de recursos humanos, financeiros e tecnológicos, conforme definido nos padrões normativos, é fundamental para o adequado funcionamento de um sistema de gestão. Por isso, é recomendável que estes recursos sejam garantidos pela Alta Direção da empresa e

esse comprometimento esteja definido no Manual do Sistema de Gestão de Continuidade de Negócios.

A estrutura organizacional também deverá figurar no Manual do Sistema de Gestão de Continuidade de Negócios, assim como a definição de responsabilidades departamentais em relação aos processos e requisitos normativos.

Conforme visto no capítulo 3, foram previstas em procedimentos específicos algumas responsabilidades sobre a estrutura de GCN que concentraram-se, principalmente, na equipe de coordenação do projeto.

Para agilizar a implantação da nova estrutura de SGCN e, visando adequar-se ao padrão normativo de referência (BS25999-2), sugere-se uma maior distribuição dessas responsabilidades.

O primeiro passo encontra-se na nomeação de um representante da Direção, cuja presença é indispensável para relatar o desempenho à alta administração, bem como assegurar que o SGCN seja estabelecido, implementado e mantido.

No caso da empresa XY TELECOM, devido à sua composição *multi-site* e diversidade de processos sugere-se que, além de um representante da Direção para todo o SGCN, a responsabilidade pela gestão de desempenho dos processos críticos de SGCN deve ser compartilhada com os profissionais líderes desses processos. Desta forma, sugere-se que o representante de SGCN seja responsável pelos assuntos mais estratégicos relativos ao sistema, tais como política e análise crítica pela Direção, ao passo que os líderes de processos sejam responsáveis pela implementação e manutenção propriamente dita do SGCN.

Trazendo essa recomendação para a realidade prática, devem ser definidas equipes que responderão pelo planejamento, implementação e manutenção do sistema em toda a organização. Estas equipes deverão ter um caráter multidisciplinar para melhor distribuição das atividades e aproveitamento de habilidades e conhecimentos de cada um.

A definição das equipes deve ocorrer em, no mínimo, 3 níveis, para que o projeto consiga alcançar a importância e abrangência necessária para sua implementação.

No primeiro nível deve ser nomeado o grupo executivo responsável pelo projeto, com a indicação dos representantes da diretoria e gerências responsáveis pela coordenação do projeto.

No segundo nível deve ser nomeada a equipe de coordenação do projeto. Essa equipe deve responder diretamente ao grupo executivo e ter como atribuições a coordenação, planejamento, estruturação, definição das principais ações, além de dar direcionamentos sobre a implementação e manutenção para a equipe de GCN. Deve integrar também a equipe de coordenação o representante da direção para o SGCN.

No terceiro nível deve ser nomeada a equipe de implementação do projeto, ou equipe de GCN. Essa equipe deve responder aos dois níveis anteriores e ter como atribuições o desenvolvimento das atividades de implementação, manutenção e melhoria contínua do sistema, além de servir como elemento multiplicador dos conceitos de SGCN dentro da empresa.

Sugere-se, ainda, que todas essas definições de responsabilidades do sistema de gestão de continuidade de negócios sejam representadas na XY TELECOM através de uma matriz de responsabilidades e autoridades, devidamente documentada no Manual de SGCN ou em procedimento específico.

Com base nessas considerações, propõem-se no Quadro 12 as ações para apoiar os recursos humanos e responsabilidades de SGCN na XY TELECOM.

Quadro 12 – Ações para apoiar a definição de Recursos Humanos e Responsabilidades de SGCN na XY Telecom

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Definição do Grupo Executivo e responsabilidades	Diretoria	1 semana	Escolha formal dos integrantes do Grupo Executivo do Projeto em Reunião de Diretoria.
Definição da Equipe de Coordenação e responsabilidades	Grupo Executivo	1 semana	Escolha formal dos integrantes da Equipe de Coordenação e do representante da direção em reunião do Grupo Executivo.
Definição da Equipe de GCN e responsabilidades	Grupo Executivo e Equipe de Coordenação	1 semana	Escolha formal dos integrantes da Equipe de GCN.
Matriz de Responsabilidades	Equipe de Coordenação	1 semana	Elaboração da Matriz de Responsabilidades e Documentação no Manual de SGCN.

Fonte: elaborado pelo autor

4.1.6 Treinamento e Competência

A sistemática de treinamento e desenvolvimento de colaboradores de GCN na organização deve ser definida através de um procedimento, tendo como principais etapas a identificação das demandas de desenvolvimento, planejamento, execução, registro das ações de desenvolvimento e avaliação da eficácia (ABNT, 2008).

Para preservar a eficácia do SGCN, e considerando que o setor de telecomunicações possui terceirização de muitos de seus processos, sugere-se garantir que o treinamento, desenvolvimento e competência dos contratados estejam no mesmo nível aplicado aos

colaboradores próprios. Nesse aspecto, a área de gestão e desenvolvimento de fornecedores da empresa possui papel fundamental.

A gestão das competências deve ser iniciada pela definição das características necessárias aos ocupantes de cada cargo/função da organização. Esta definição deve incluir registros sobre educação/escolaridade, treinamento, habilidade, experiência e qualificações dos colaboradores envolvidos no SGCN.

No caso da XY TELECOM, o desenvolvimento da sua estrutura inicial de GCN contou com o apoio de consultoria especializada e, portanto, não foram observadas informações sobre a definição de competências específicas ou programas de treinamento aos colaboradores relacionados ao projeto GCN.

Dessa forma, sugere-se que a XY TELECOM, na nova estrutura de SGCN, defina inicialmente as competências dos colaboradores envolvidos, através de perfil de função, utilizando-se o conceito do CHA (Conhecimento, Habilidade, Atitudes). Em seguida, sugere-se a realização de uma comparação entre as necessidades para cada função e qualificação dos funcionários que ocupam cada função no momento, podendo ser documentada através de uma matriz de treinamentos.

Após a determinação das equipes responsáveis pelo planejamento, implantação e manutenção do SGCN, faz-se necessária a capacitação dessas equipes através de treinamento formal. Dessa forma, a opção por cursos *in company* é uma alternativa interessante, pois elimina custos com deslocamentos e hospedagens, além de proporcionar condições mais favoráveis para o desenvolvimento de idéias e discussões sobre assuntos e atividades específicas da empresa.

Visando otimizar o desenvolvimento das equipes, sugere-se que a capacitação destas seja realizada através de dois tipos treinamentos. O primeiro, específico para a equipe de coordenação e grupo executivo, com conteúdos mais detalhados sobre a coordenação, planejamento e acompanhamento do projeto. Já o segundo, direcionado para a equipe de implementação, com conteúdos mais detalhados sobre a elaboração dos planos de resposta (PGI e PCN) e testes de eficácia.

A pessoa selecionada para ministrar os cursos, além do conhecimento sobre boas práticas de SGCN (normas BS25999 e Guia BCI) deve possuir alguma experiência na implementação de SGCN em empresas. A carga horária mínima para capacitação das equipes deve ser de 24 horas.

A contratação de consultoria externa é considerada uma boa opção para o desenvolvimento da atividade de capacitação na XY TELECOM, pois permite que os colaboradores sejam treinados de acordo com a *expertise* da consultoria em relação às

melhores práticas de mercado. Além disso, permite que os colaboradores com conhecimento em SGCN direcionem esforços à implementação de outras ações no projeto.

Após a realização das atividades de qualificação (treinamentos, conclusão de cursos, experiências adquiridas), sugere-se que a avaliação da eficácia destas atividades seja registrada, conforme estabelecido na norma de referência (ABNT, 2008).

Propõe-se, portanto, no Quadro 13, ações para apoiar a definição de treinamento e competência de SGCN na XY TELECOM.

Quadro 13 – Ações para apoiar a definição de treinamento e competência de SGCN na XY Telecom

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Definição dos requisitos de competência do pessoal envolvido no SGCN	Equipe de Coordenação	1 semana	Elaboração do perfil de função do pessoal envolvido no SGCN.
Programação de Treinamentos	Equipe de Coordenação	1 semana	Levantamento das Necessidades de Treinamentos. Elaboração da Matriz de Treinamentos.
Seleção e Contratação de Consultoria para Treinamento "In Company" de SGCN	Equipe de Coordenação	2 semanas	Cotação com empresas que prestam esse serviço, definição do preço e contratação formal.
Treinamento da Equipe de Coordenação e Grupo Executivo	Consultoria Externa	1 semana	Desenvolvimento do curso de SGCN direcionado às duas equipes (10 pessoas) com duração mínima de 20h
Treinamento da Equipe de GCN	Consultoria Externa	1 semana	Desenvolvimento do curso de SGCN direcionado à equipe (20 pessoas) com duração mínima de 20h

Fonte: elaborada pelo autor

4.1.7 Aculturamento e Conscientização do SGCN

Conforme preconiza a BS25999-2, ou NBR15999-2, para assegurar que a GCN torne-se parte de seus valores fundamentais e de gestão eficaz, a organização deve: a) elevar, reforçar e manter a conscientização através da manutenção de um curso de educação e um programa de informação em GCN para todos os empregados e estabelecendo um processo para avaliar a eficácia da conscientização em GCN realizada; b) comunicar a todos os empregados a importância do alcance dos objetivos da continuidade de negócios, da conformidade com a política de continuidade de negócios e da melhoria contínua; e c)

assegurar que todos os empregados estão conscientes de como eles contribuem para o alcance dos objetivos de continuidade de negócios (ABNT, 2008).

Portanto, após a capacitação das equipes de coordenação e de implementação, é necessário que os demais colaboradores da companhia também recebam treinamento ou conscientização sobre SGCN garantindo, assim, o aculturamento em todos os níveis funcionais da organização.

No caso da XY TELECOM, não foi identificada a implantação de ações nesse sentido em sua estrutura de GCN. Dessa forma, propõe-se o estabelecimento de um programa de conscientização e aculturamento a ser desenvolvido através de cursos ou palestras com duração e nível de detalhamento menores que o de capacitação das equipes. Sugere-se que esses cursos ou palestras sejam internos, podendo ter membros das equipes de coordenação e implementação atuando como instrutores multiplicadores.

Sugere-se que os horários e turmas sejam montados de forma a permitir a integração e a participação dos colaboradores. O conteúdo do curso pode incluir temas como: políticas, objetivos e metas; processos críticos de GCN; produtos e serviços fundamentais; eventos, riscos e impactos relacionados à continuidade de negócios da organização; documentação de GCN; comunicação de GCN; planos de gerenciamento de incidentes e continuidade de negócios; auditorias de SGCN; análise crítica, etc. Além disso, sugere-se que sejam mantidos registros da realização desses cursos ou palestras pelos colaboradores.

A forma escolhida para apresentar o conteúdo do curso deve ser a mais adequada para a realidade de cada empresa. No caso da XY TELECOM, que possui abrangência nacional, os recursos mais utilizados para esse fim podem ser *e-learnings* e *workshops*.

Assim, propõem-se no Quadro 14 as ações para apoiar o aculturamento e a conscientização de SGCN na XY TELECOM.

Quadro 14 – Ações para apoiar o Aculturamento e Conscientização de SGCN na XY Telecom

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Programa de Aculturamento e Conscientização de Colaboradores sobre SGCN	Equipe de Coordenação e Equipe de GCN	1 mês	*E-learning* sobre o SGCN da Telecom
			Workshop itinerante de SGCN nas regiões de abrangência da Telecom

Fonte: elaborado pelo autor

4.1.8 Controle de Documentos e Registros

Conforme define a norma BS25999-2, os registros e documentos tem como propósito fornecer clara evidência da operação eficaz do SGCN e da implementação eficaz da GCN na organização (ABNT, 2008).

Seguindo esse propósito, sugere-se que o controle de documentos e de registros ocorra de maneira centralizada para documentos e descentralizada para registros, sendo necessária a elaboração de procedimentos detalhando essas atividades.

Para o controle de documentos, segundo a norma de referência BS25999-2, devem ser considerados aspectos como aprovação, publicação, disponibilização, versão, revisão, e hierarquia de procedimentos (ABNT, 2008).

No caso da XY TELECOM, visando atender ao aspecto de controle de documentos de maneira centralizada, foi implantado pela área de Processos da companhia um *software* de gerenciamento eletrônico de documentos disponível aos colaboradores via *Intranet* cuja funcionalidade está descrita em procedimento documentado. Avaliando-se essa evidência, observou-se que essa ferramenta pode ser utilizada para o controle dos documentos de SGCN, pois atende ao que a norma BS25999-2 exige sobre esse aspecto.

Para o controle de registros, conforme a norma de referência, devem ser considerados aspectos como a identificação, armazenamento, proteção, recuperação, tempo de retenção e descarte dos registros aplicáveis ao SGCN (ABNT, 2008).

No caso da XY TELECOM, sugere-se para atendimento desse requisito a inserção de tabelas de controle de registros no final de cada procedimento aplicável ao SGCN e a elaboração de documento para evidenciar esse procedimento. Essa prática descentralizada facilita o controle, haja vista que o método de registro só pode ser alterado na revisão do procedimento em que ele está inserido e a responsabilidade da gestão do registro varia conforme o gestor de cada procedimento.

Portanto, propõe-se no Quadro 15 as ações para apoiar o controle de documentos e registros de na XY TELECOM.

Quadro 15 – Ações para apoiar o Controle de Documentos e Registros na XY Telecom

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Controle de Documentos de SGCN	Equipe de Coordenação	1 semana	Utilização da ferramenta informatizada existente na companhia para o controle de documentos de SGCN.
Controle de Registros do SGCN	Equipe de Coordenação	1 semana	Incluir tabela de controle de registros ao final de cada procedimento aplicável ao SGCN

Fonte: elaborado pelo autor

4.2 Etapa 2 - Implementação e Operação

Nesta etapa serão feitas sugestões e planejadas ações para a implantação dos seguintes requisitos: Análise de Impacto de Negócios (BIA); Avaliação e Tratamento de Riscos; Estratégia de GCN; Estrutura de Resposta a Incidentes; Plano de Gerenciamento de Incidentes; Plano de Continuidade de Negócios; Testes, Manutenção e Análise Crítica dos Arranjos de GCN. A seguir, cada um desses requisitos será brevemente descrito.

4.2.1 Análise de impacto de negócios (BIA)

Conforme preconiza a norma BS25999-2, ou NBR15999-2, deve ser definido um método documentado e apropriado para determinar o impacto de uma interrupção nas atividades que suportam os produtos e serviços essenciais da organização. Esse processo é comumente conhecido como análise de impacto de negócios, ou BIA - *Business Impact Analysis* (ABNT, 2008).

Dessa forma, conforme ABNT (2008), recomenda-se à organização:

> a)identificar as atividades que suportam seus principais produtos e serviços; b)identificar os impactos resultantes dessa interrupção nessas atividades e determinar como as atividades seriam afetadas ao longo do tempo; c) estabelecer o período máximo tolerável de interrupção para cada atividade (ou *MTPD – Maximum Tolerable Period of Disruption*), identificando: o período de tempo máximo após o início de uma interrupção em cada atividade que necessita ser retomada; o nível mínimo em que cada atividade precisa funcionar após o seu reinício; o período de tempo para que sejam retomados os níveis normais de operação; d) classificar as atividades de acordo com a prioridade para a recuperação e identificar as atividades críticas; e) identificar todas as dependências relevantes para as atividades críticas, incluindo fornecedores e parceiros; f) para fornecedores e parceiros responsáveis por atividades críticas, determinar os arranjos de GCN que existem localmente para os produtos e serviços relevantes que eles fornecem; g) fixar os tempos objetivos de recuperação (ou RTO – *Recovery Time Objective*) para o reinício das atividades críticas considerando o período máximo tolerável de interrupção; h) estimar os recursos que cada atividade crítica vai exigir para o seu reinício. (ABNT, 2008, p.9)

É recomendável que informações sobre a identificação das atividades que suportam os principais produtos e serviços, os impactos resultantes de uma interrupção nessas atividades, o período máximo de interrupção em cada atividade, os tempos objetivos de recuperação, a classificação das atividades prioritárias e a estimativa de recursos sejam levantadas através de entrevistas com os gestores de cada processo. A adoção desta prática justifica-se pela visão privilegiada que cada gestor possui do seu respectivo processo e, como visto no capítulo 3, foi bem sucedida para a estrutura inicial de GCN da XY TELECOM.

No tocante às informações sobre dependências relevantes para atividades críticas e instalações de fornecedores responsáveis por atividades críticas, sugere-se a prática de

inspeções *in loco*, visando diagnosticar a capacidade e a estrutura de proteção dessas instalações.

Como produto final, sugere-se que o BIA seja apresentado e documentado conforme prática adotada pela XY TELECOM na sua estrutura inicial de GCN, através de relatório contemplando as informações sobre a análise realizada e uma tabela com o *ranking* de processos críticos, de acordo com os tempos objetivos de recuperação e respectivos impactos financeiros ou não-financeiros. Essa prática é apresentada no Quadro 16.

Quadro 16 – Quadro modelo de *ranking* de processos críticos após a Análise de Impacto de Negócios

Processo de Negócio	**Gestor Responsável**	**RTO**	**Impacto $**
Processo 1	João	4 horas	10 milhões
Processo 2	Sérgio	8 horas	1 milhão
Processo 3	Paulo	1 dia	100 mil

Fonte: adaptado de XY TELECOM (2008)

No caso da XY TELECOM, conforme visto no capítulo 3, o BIA foi realizado para um escopo de 50 processos. Devido a recentes aquisições da empresa, que culminou com o redesenho ou criação de novos processos, faz-se necessária a atualização dessa análise. Além disso, conforme observado anteriormente, a definição de um escopo mais reduzido para essa análise pode otimizar o seu desenvolvimento.

Propõe-se, portanto, no Quadro 17, as ações para apoiar a análise de impacto de negócios na nova estrutura de SGCN da XY TELECOM.

Quadro 17 – Ações para apoiar a Análise de Impacto de Negócios na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Agendamento de Entrevista com Gestores	Equipe de Coordenação	1 semana	Agendamento via e-mail com gestores dos processos de SGCN do novo escopo
Revisão do Questionário de Avaliação	Equipe de Coordenação	1 semana	Análise e atualização do questionário de avaliação
Aplicação do Questionário de Avaliação com Gestores	Equipe de Coordenação	2 semanas	Entrevista com gestores e coleta dos dados de avaliação (impactos e tempos) de cada processo
Elaboração do Relatório BIA	Equipe de Coordenação	2 semanas	Consolidação dos dados de avaliação, definição dos processos críticos e elaboração do relatório BIA

Fonte: elaborado pelo autor

4.2.2 Avaliação e tratamento de riscos

Conforme a BS25999-2, ou NBR15999-2, deve haver um método apropriado, definido e documentado para avaliação de riscos que irá permitir à organização compreender as ameaças e vulnerabilidades de suas atividades críticas e recursos necessários, incluindo aqueles provenientes de fornecedores e parceiros (ABNT, 2008).

Para isso, a organização deve compreender o impacto que poderia ocorrer caso uma ameaça identificada venha a tornar-se um incidente e cause uma interrupção do negócio. A decisão do método de avaliação de riscos é da organização, mas é importante que ele seja apropriado às políticas internas, estratégias e demais requisitos da companhia. Em seguida, a organização deve escolher e implementar tratamentos de risco adequados para cada atividade crítica e de acordo com seus níveis de aceitação de risco (ABNT, 2008).

Atualmente, existe na XY TELECOM uma área específica para o levantamento, monitoramento e tratamento de riscos de toda a organização, inclusive riscos associados à continuidade do negócio, e que adota uma matriz padrão (5x5) de impacto versus probabilidade para definir o nível de exposição de cada risco.

A Figura 11 representa a matriz de nível de risco da XY TELECOM, onde a probabilidade é graduada por faixas percentuais de incerteza e o impacto por faixas percentuais relacionadas ao impacto financeiro do risco. O produto de impacto x probabilidade representa o nível de exposição ao risco, ou grau final do risco.

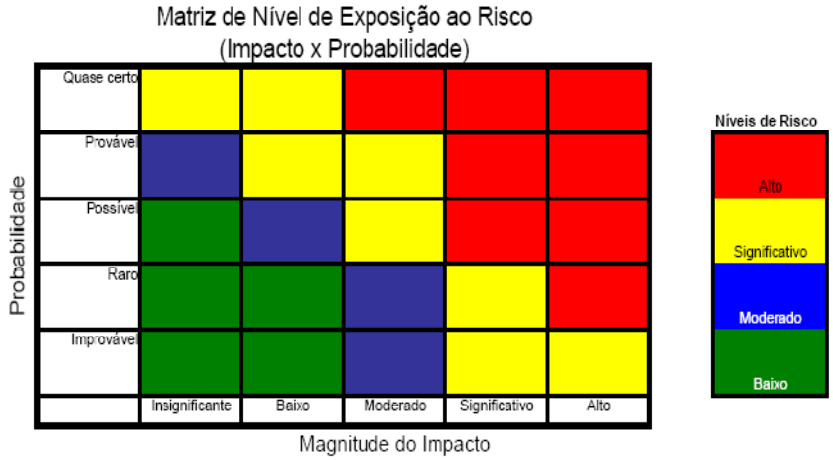

Figura 11 – Matriz de Nível de Exposição ao Risco da XY TELECOM

Fonte: XY TELECOM (2008)

Recomenda-se que para cada uma das suas atividades críticas a organização deva identificar tratamentos de riscos eficazes que: a) reduzam a probabilidade de interrupção; b) diminuam o período de interrupção, e c) limitem o impacto de uma interrupção nos produtos e

serviços principais da organização. Além disso, a organização deve escolher e implementar apropriados tratamentos de risco e adequados para cada atividade crítica de acordo com seus níveis de aceitação de risco e que essas atividades sejam documentadas e monitoradas (ABNT, 2008).

Na estrutura inicial de GCN da XY TELECOM, conforme visto no capítulo 3, a análise de riscos foi iniciada através de um mapeamento dos principais ativos (infra-estrutura predial e de TI) que suportam os processos do escopo. Então, para cada ativo mapeado foi calculado o seu grau de exposição de risco com o auxílio de um *software* de avaliação de risco especializado fornecido pela consultoria do projeto. A adoção dessa prática, conforme viu-se, encontrou como dificuldades o escopo amplo da análise e a impossibilidade de atualização e customização das lógicas e critérios de cálculo utilizados no *software* fornecido pela consultoria. Além disso, foi observado um *gap* no tocante à ausência de análise de riscos em outros ativos existentes como pessoas ou suprimentos, conforme recomenda a BS25999-1.

Portanto, em virtude de nova definição de escopo para a estrutura de SGCN proposta, faz-se necessária a atualização da análise e tratamento dos riscos da XY TELECOM contemplando, além dos ativos de TI e prediais, pessoas e suprimentos. Adicionalmente, sugere-se a definição e documentação em procedimento próprio, os critérios para cálculo dos riscos em ativos da companhia, alinhada com a atual matriz de nível de exposição ao risco da organização, e aplicação dessa metodologia com o auxílio de ferramenta informatizada customizável. Essa medida visa garantir que a base de conhecimento e os critérios de avaliação sobre os riscos sejam da própria companhia e possam ser sempre melhorados e atualizados pela mesma.

Propõe-se, portanto, no Quadro 18, as ações para apoiar a avaliação e tratamento de riscos na nova estrutura de SGCN da XY TELECOM.

Quadro 18 – Ações para apoiar a Avaliação e Tratamento de Riscos de SGCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Elaboração de Procedimento de Identificação, Avaliação e Tratamento de Riscos	Equipe de Coordenação	1 semana	Elaboração de procedimento próprio da companhia sobre identificação, avaliação e tratamento de riscos em ativos.
Atualização do mapeamento dos ativos de TI, prediais e demais ativos	Equipe de Coordenação	1 semana	Análise e atualização da documentação dos ativos de TI, prediais e demais recursos conforme novo escopo.

Avaliação de Risco nos ativos	Equipe de Coordenação	2 meses	Customização do *software* para cálculo dos riscos em ativos, conforme critérios definidos no procedimento da companhia
			Atualização da avaliação de riscos em ativos (TI, prediais, pessoas e suprimentos) conforme novo escopo.
Atualização do Relatório de Avaliação de Risco	Equipe de Coordenação	2 semanas	Consolidação dos dados de avaliação e atualização do relatório de riscos.
Determinação das Medidas de Tratamento de Risco	Equipe de Coordenação	2 semanas	Atualização das medidas de tratamento recomendadas no relatório de riscos.
Implementação das Medidas de Tratamento de Risco	Equipe de Coordenação	A definir.	Implementação das medidas de tratamento recomendadas no relatório de riscos.

Fonte: Elaborado pelo autor

4.2.3 Estratégia de Gestão de Continuidade de Negócios

Conforme ABNT (2007), recomenda-se que a abordagem da organização para determinar suas estratégias de GCN: a) implemente as medidas apropriadas, de forma a reduzir a probabilidade de ocorrência de incidentes e/ou reduzir os potenciais efeitos desses incidentes; b) mantenha um registro das medidas de resiliência e mitigação; c) forneça continuidade para as atividades críticas durante e após um incidente; e d) mantenha um registro das atividades que não foram identificadas como críticas.

Recomenda-se, ainda, que a organização considere opções estratégicas para suas atividades críticas e para os recursos que cada atividade consumirá durante sua recuperação. As estratégias apropriadas dependem de uma série de fatores, como: a) o período máximo de interrupção tolerável de atividade crítica; b) os custos de implementação de uma ou mais estratégias; e c) as conseqüências de não se agir (ABNT, 2007).

O objetivo da fase de Estratégia de Continuidade é o desenvolvimento das estratégias para o restabelecimento dos serviços críticos, em uma restauração compatível com tempo objetivado de recuperação – RTO. Este tempo é o objetivo a ser alcançado quando da ativação da operação em regime de contingência.

Segundo a ABNT (2007), as estratégias de continuidade podem ser necessárias para diversos recursos da organização, tais como pessoas, instalações, tecnologia, suprimentos e partes interessadas. Para cada caso a organização precisa reduzir a probabilidade de

implementar uma solução de continuidade de negócios que possa ser afetada pelo mesmo incidente que causou a interrupção no negócio. Considerando uma empresa de telecomunicações, devido à complexidade de processos e sistemas que suportam o negócio, sugere-se que seja dada atenção especial às estratégias relacionadas às instalações e tecnologias.

No caso da XY TELECOM, conforme visto no capítulo 3, a identificação e apresentação das estratégias de continuidade foi feita, em sua estrutura de GCN original, através da definição da macro-estratégia de continuidade, do mapeamento dos ativos a serem contingenciados, do levantamento de alternativas de contingência e da escolha da estratégia mais indicada para implementação, sendo essas informações documentadas no Relatório de Estratégia de Continuidade de Negócios. O *gap* identificado nessa atividade, deveu-se à falta de avaliação de estratégias de continuidade em outros ativos importantes, tais como pessoas ou suprimentos.

Além disso, observou-se que a implementação da estratégia de continuidade escolhida na estrutura de GCN original da XY TELECOM não foi realizada devido à falta de aprovação formal dessa estratégia pela Alta Direção, fato que comprometeu o desenvolvimento das etapas seguintes do ciclo de vida de GCN.

Portanto, faz-se necessária a atualização das estratégias de continuidade da empresa em estudo de modo a contemplar todos os tipos de ativos relevantes para o negócio e garantir a aprovação pela Alta Direção da estratégia mais indicada.

Propõem-se, assim, no Quadro 19, as ações para apoiar a definição de estratégias de GCN na nova estrutura de SGCN da XY TELECOM.

Quadro 19 – Ações para apoiar a definição de Estratégias de SGCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Atualização do levantamento de sites alternativos e infra-estrutura de contingência	Equipe de Coordenação	1 mês	Análise e atualização das alternativas de contingência para ativos (pessoas, instalações prediais, TI, suprimentos).
Escolha das Estratégias	Equipe de Coordenação	1 mês	Avaliação das alternativas e escolha da estratégia mais indicada.
Atualização do Relatório de Estratégias de Continuidade	Equipe de Coordenação	1 semana	Atualização do documento com as informações levantadas.
Aprovação formal das estratégias de continuidade determinadas	Grupo Executivo e Diretoria	1 semana	Aprovação em reunião de Diretoria das Estratégias de Continuidade determinadas

Fonte: elaborado pelo autor

4.2.4 Estrutura de resposta a incidentes

Conforme ABNT (2008), a organização deve nomear o pessoal de resposta a incidentes, com a necessária responsabilidade, autoridade e competência para gerenciar um incidente. A estrutura de resposta a incidentes deve ter elementos para que as pessoas possam:

> a) confirmar a natureza e extensão de um incidente;
> b) colocar em funcionamento uma resposta de continuidade de negócios apropriada;
> c) possuir planos, processos e procedimentos para a ativação, operação, coordenação e comunicação da resposta a incidentes;
> d) possuir recursos disponíveis para suportar os planos, processos e procedimentos para gerenciar um incidente; e
> e) comunicar-se com as partes interessadas. (ABNT, 2008, p.11)

Recomenda-se que essa estrutura emita uma resposta de continuidade de negócios adequada, que pode ser chamada de equipe de gerenciamento de incidentes ou equipe de gerenciamento de crise (EGC). Essas equipes devem possuir planos, processos e procedimentos de gerenciamento de incidentes, suportados por ferramentas de continuidade de negócios, de forma a permitir a continuidade e a recuperação de atividades críticas (ABNT, 2008).

Conforme viu-se no capítulo 3, a estrutura de GCN original da XY TELECOM contemplou numa proposta de procedimento a formação da EGC através de equipes funcionais, que são as equipes com responsabilidade para atuar em resposta aos diferentes tipos e níveis de eventos que possam ocorrer na companhia. Essas equipes seriam divididas em 3 Grupos: (i) Grupo Executivo; (ii) Grupo de Gestão/Decisão; e (iii) Grupo de Execução. No entanto, a ausência de implementação dessas equipes não permitiu uma avaliação mais concreta da eficácia dessa formação.

Propõe-se, portanto, a adoção da formação da equipe de gerenciamento de crises recomendada pelo BCI (2008). Segundo orientação deste autor, a equipe de gerenciamento de crises recomendada é formada por 3 times de resposta: o time de resposta a incidentes - TRI (responsável pelas ações de resposta a incidente do PGI – Plano de Gerenciamento de Incidentes), o time de continuidade de negócios - TCN (responsável pelas ações previstas no PCN – Plano de Continuidade de Negócios) e o time de gestão executiva da crise - TGEC (responsável pelas decisões de nível executivo para tratar incidentes com proporções de crise).

No caso da XY TELECOM, a equipe de gerenciamento de crise poderá ser formada por membros da diretoria, da coordenação do projeto de SGCN e por colaboradores oriundos de áreas da organização responsáveis pelos recursos que suportam os processos do escopo do SGCN. Por exemplo, o processo de faturamento da XY TELECOM possui como principais ativos pessoas, sistemas informatizados, instalações prediais e de telecomunicações. Então, se este processo pertencer ao escopo do SGCN, a equipe de gerenciamento de crise deverá

possuir integrantes específicos das áreas de Gente, Tecnologia da Informação, Administração Predial e Serviços Gerais que darão suporte na definição de estratégias e planos de resposta para os eventos que possam afetar aqueles ativos.

Além disso, a equipe de gerenciamento de crise da XY TELECOM poderá contar com membros de áreas como Jurídico, Comunicação, Segurança Empresarial, Auditoria e Gestão de Riscos para tratar de crises com conseqüências à companhia: como sanções regulatórias, danos à imagem da companhia, ocorrências criminais, danos ambientais, etc. Membros de outras áreas da organização também poderão ser chamadas para compor a equipe em caso de crise, dependendo do seu tipo e gravidade. É necessário, portanto, que se estabeleçam claramente quais são os membros efetivos e consultivos da EGC e, principalmente, que se estabeleça um líder.

Diante dessas sugestões, propõe-se no Quadro 20 a ação para apoiar a definição da estrutura de resposta a incidentes do novo modelo de SGCN da XY TELECOM.

Quadro 20 – Ação para apoiar a Estrutura de Resposta a Incidentes na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Definição da Equipe de Gerenciamento de Crises	Equipe de Coordenação	1 semana	Elaboração, Aprovação e Publicação de Procedimento definindo a EGC e seu funcionamento

Fonte: Elaborado pelo autor

4.2.5 Plano de gerenciamento de incidentes (PGI)

Conforme ABNT (2008), a organização deve possuir planos documentados que detalhem a forma como a organização irá gerenciar um incidente e como ela irá recuperar ou manter as suas atividades a um predeterminado nível, em caso de uma interrupção. Conforme o autor, cada plano deve possuir um escopo definido, ser acessível e compreensível, possuir um responsável por sua análise crítica, atualização e aprovação; e estar alinhado com as estratégias de contingência definidas.

Além disso, segundo ABNT (2008), os planos deverão conter coletivamente:

> a) identificação das linhas de comunicações;
> b) principais tarefas e informações de referência;
> c) definição dos papéis e responsabilidades das pessoas e equipes com autoridade durante e após um incidente;
> d) diretrizes e os critérios relacionados aos indivíduos que possuem autoridade para invocar cada plano, e em que circunstâncias;
> e) um método pelo qual cada plano é invocado;
> f) locais de encontros alternativos, detalhes atualizados de contatos e mobilização para agências relevantes, organizações e recursos necessários para suportar a resposta;
> g) um processo de retirada assim que o incidente terminar;

> h) uma referência para os detalhes de contatos essenciais para todas as partes interessadas principais;
> i) detalhes para gerenciar as conseqüências imediatas de uma interrupção de negócios, com atenção aos seguintes elementos:
> 1) bem-estar dos indivíduos;
> 2) opções estratégicas e táticas para responder a uma interrupção, e
> 3) prevenção de novas perdas ou indisponibilidade de atividades críticas;
> j) detalhes para o gerenciamento de um incidente, incluindo:
> 1) provisão de assuntos de gestão durante um incidente, e
> 2) processos para permitir a continuidade e a recuperação das atividades críticas.
> k) detalhes sobre como e em que circunstâncias a organização irá comunicar-se com os funcionários e seus parentes, principais partes interessadas e contatos de emergência;
> l) detalhes sobre meios de comunicação de resposta na organização após um incidente, incluindo:
> 1) estratégia de comunicação de incidentes;
> 2) preferências de interface com os meios de comunicação;
> 3) modelo ou guia de orientação para a elaboração de uma declaração à mídia; e
> 4) porta-vozes adequados;
> m) um método para a gravação de informações vitais sobre o incidente, ações realizadas e decisões tomadas;
> n) detalhes de ações e tarefas que precisam ser desempenhadas;
> o) detalhes dos recursos requeridos para a continuidade e recuperação de negócios em momentos distintos;
> p) priorização dos objetivos em termos de recuperação de atividades críticas, cronograma de recuperação e os níveis necessários à recuperação de cada atividade crítica. (ABNT, 2008, p.11-12)

Sugere-se que o plano de gerenciamento de incidentes possua uma matriz de níveis de crise ou níveis de acionamento. A matriz consiste em um quadro com níveis que possibilitam avaliar um evento e acionar ou não determinado procedimento para gerenciar o incidente, tornando esse processo mais eficaz. Dessa forma, os envolvidos na gestão de incidentes podem usar a matriz para avaliar se é necessário acionar procedimentos para reposta a crises ou tratar o evento como parte da operação normal da gestão de incidente.

Para essa finalidade, pode ser utilizada como referência na proposta de SGCN a adoção do modelo de níveis de acionamento da estrutura original de GCN da XY TELECOM, apresentado no Quadro 4 da subseção 3.2.2.

Outro elemento essencial para a administração do incidente e que deve constar do PGI é o estabelecimento do Centro de Comando. Entende-se por Centro de Comando o local onde serão realizadas as reuniões deliberativas do time de gestão executiva da crise (TGEC). Numa emergência com proporções de crise, os membros do TGEC deverão reunir-se no Centro de Comando para avaliar a situação e tomar as decisões cabíveis. Tratando-se de crise, o seu gerenciamento será mais eficiente se as reuniões dos membros do TGEC forem presenciais.

As instalações do Centro de Comando deverão conter, no mínimo, os requisitos especificados no Procedimento da Estrutura de GCN original da XY TELECOM apresentada na subseção 3.2.2.

Além disso, conforme a ABNT (2007), recomenda-se que a estratégia de comunicação da organização com a mídia seja documentada no PGI, ou em documento à parte chamado de plano de comunicação. Segundo o autor, é importante que o plano de comunicação inclua:

> a) a estratégia de comunicação de incidentes;
> b) a interface com a mídia escolhida pela organização;
> c) um guia ou modelo para a criação de uma minuta de declaração a ser fornecida à mídia na primeira oportunidade viável após os incidente;
> d) uma quantidade apropriada de porta-vozes competentes que sejam nomeados e autorizados a liberar as informações autorizadas para a mídia;
> e) a definição, quando for viável, de um local apropriado para realizar o contato com a mídia ou com grupos de pessoas interessadas. (ABNT, 2007, p.29)

Outra recomendação importante sobre o PGI é que, após a sua elaboração, ele deve ser comunicado e operado através de treinamentos junto à equipe de gerenciamento de crises. É recomendável que a atualização das equipes de resposta ocorra de maneira continuada em intervalos planejados, durante os testes dos preparativos ou após a ocorrência de incidentes. Esta medida visa garantir que o plano de resposta esteja sempre disponível para operação e possua a eficácia desejada, caso seja solicitada a sua utilização.

Diante dessas sugestões, e considerando a ausência de um plano de gerenciamento de incidentes implementado na XY TELECOM, propõe-se no Quadro 21 as ações para apoiar a elaboração do PGI nessa empresa.

Quadro 21 – Ações para apoiar o Plano de Gerenciamento de Incidentes na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Elaboração do Plano de Gerenciamento de Incidentes	Equipe de Coordenação Equipe de GCN	Variável conforme escopo do SGCN	Planejamento, Elaboração e Aprovação do PGI
Treinamento dos times integrantes do PGI	Equipe de Coordenação Equipe de GCN	Variável conforme escopo do SGCN	Planejamento e Realização do Treinamento em PGI aos times integrantes

Fonte: elaborado pelo autor

4.2.6 Plano de continuidade de negócios (PCN)

Conforme ABNT (2007), através da norma NBR15999-1, ou BS25999-1, o Plano de Continuidade de Negócios (PCN) é conceituado como a documentação de procedimentos e informações desenvolvida, consolidada e mantida para estar pronta para o uso caso ocorra um incidente, e permitindo que a organização mantenha suas atividades críticas em um nível aceitável de funcionamento.

Desse modo, recomenda-se, segundo ABNT (2007), que o PCN inclua uma lista estruturada de ações e tarefas em ordem de prioridade, destacando-se:

> a) como o PCN é ativado;
> b) as pessoas responsáveis por ativar o plano de continuidade de negócios;
> c) o procedimento que esta pessoa deve adotar ao tomar esta decisão;
> d) as pessoas que devem ser consultadas antes desta decisão ser tomada;
> e) as pessoas que devem ser informadas quando a decisão for tomada;
> f) quem vai para onde e quando;
> g) quais serviços estão disponíveis, aonde e quando, incluindo como a organização mobilizará seus recursos externos e de terceiros;
> h) como e quando esta informação será comunicada;
> i) se relevante, procedimentos detalhados para soluções manuais, recuperação de sistemas, etc. (ABNT, 2007, p.31)

Além disso, os recursos necessários para a continuidade e recuperação dos negócios precisam ser identificados em diferentes posições no tempo, incluindo-se: (i) pessoas; (ii) instalações; (iii) tecnologia; (iv) informações; (v) suprimentos; e (vi) partes interessadas (ABNT, 2007).

O Plano de Continuidade de Negócios diferencia-se do Plano de Gerenciamento de Incidentes por ser o plano que vai garantir o restabelecimento das atividades essenciais da organização que foram descontinuadas pelo evento e recuperá-las aos seus níveis normais de funcionamento. Tratam-se das ações tomadas após a avaliação e contenção dos danos, com duração variando de minutos a dias e que, dentre outros, tem o intuito de estabelecer o contato com clientes e fornecedores, recuperar os processos críticos e refazer o trabalho perdido (ABNT, 2007).

Durante a execução do plano de continuidade e, após a retomada dos processos críticos da organização, o ambiente de crise da organização torna-se mais controlado e a extensão dos danos causados pelo incidente ficam mais evidentes, o que facilita o planejamento das ações de recuperação do negócio. Estas ações de recuperação geralmente duram de semanas a meses e objetivam, dentre outras, reparar ou substituir os danos causados aos ativos da organização, realocar as pessoas ao local de trabalho permanente e recuperar os custos de seguros. A Figura 12, adaptada de ABNT (2007), apresenta um esquema com a linha de tempo de um incidente onde pode-se evidenciar mais claramente a diferença no tempo e função de cada plano.

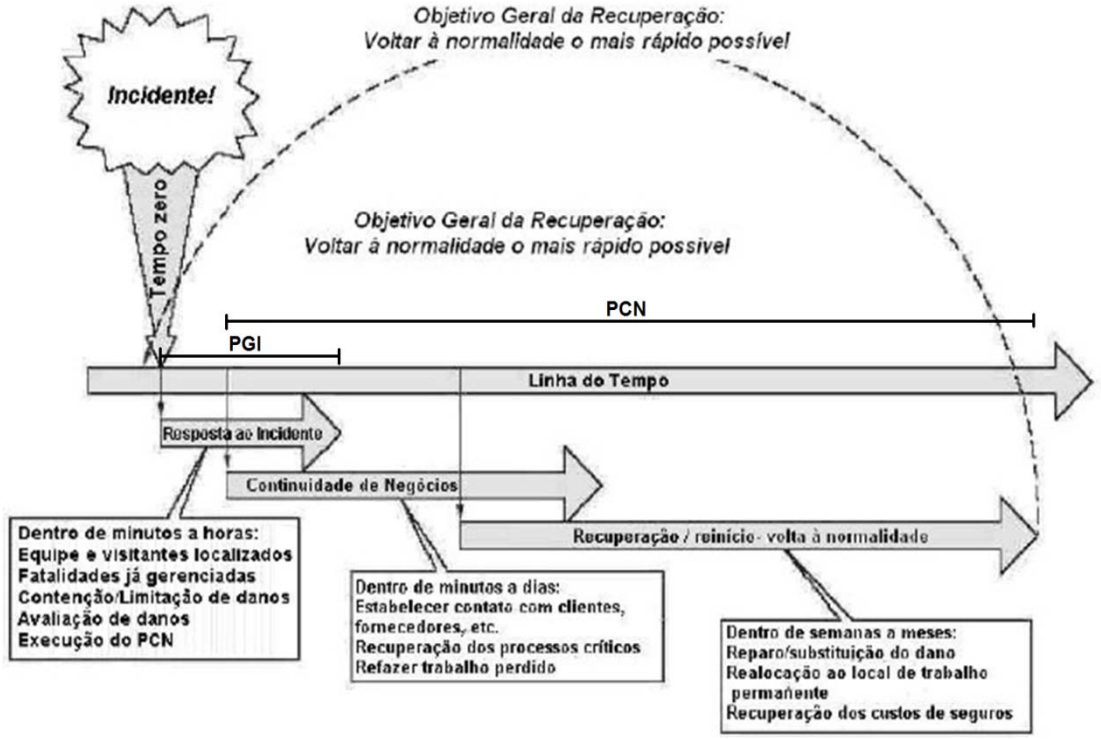

Figura 12 – Linha de tempo de um incidente

Fonte: adaptado de ABNT (2007)

No caso da XY TELECOM, não foi evidenciada a existência de um PCN documentado ou de equipe implantada para tratar desse assunto. Portanto, demanda-se a necessidade de elaboração do plano de continuidade de negócios e de implantação do time de continuidade de negócios, formada por membros da equipe de gerenciamento de crises. Além disso, a exemplo do PGI, o PCN depois de elaborado deverá ser comunicado e operado através de treinamentos. É recomendável que a atualização do time de continuidade de negócios ocorra de maneira continuada em intervalos planejados, durante os testes dos preparativos ou após a ocorrência de incidentes.

Diante dessas considerações, são propostas no Quadro 22 as ações para apoiar a elaboração do plano de continuidade de negócios na XY TELECOM.

Quadro 22 – Ações para apoiar a elaboração do Plano de Continuidade de Negócios na XY Telecom

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Elaboração do Plano de Continuidade de Negócios	Equipe de Coordenação Equipe de GCN	Variável conforme escopo do SGCN	Planejamento, Elaboração e Aprovação do PCN
Treinamento do Time de Continuidade de Negócios	Equipe de Coordenação Equipe de GCN	Variável conforme escopo do SGCN	Planejamento e Realização do Treinamento no PCN do Time de Continuidade de Negócios

Fonte: elaborado pelo autor

4.2.7 Testes, manutenção e análise crítica dos arranjos de GCN

A organização, segundo ABNT (2008), deve testar seus arranjos de GCN para assegurar que eles atendem aos requisitos do negócio. Portanto, segundo o autor, recomenda-se à organização:

> a) desenvolver testes que sejam consistentes com o escopo do SGCN;
> b) possuir um programa aprovado pela alta direção para garantir que os testes são realizados a intervalos planejados e quando ocorrerem mudanças significativas na organização;
> c) realizar uma série de testes diferentes para validar o conjunto de arranjos de continuidade de negócios;
> d) planejar os testes de modo que o risco de ocorrência de um incidente como resultado direto do teste seja minimizado;
> e) definir as metas e objetivos de cada teste;
> f) proceder uma análise crítica após a realização de cada teste, que irá avaliar o alcance das metas e objetivos de cada exercício.
> g) produzir um relatório escrito do teste, os resultados e feedback, incluindo ações requeridas. (ABNT, 2008, p.13)

Para orientar a definição dos testes, é exibida no Quadro 23 um modelo da ABNT (2007) com uma série de abordagens para testar as estratégias de GCN.

Quadro 23 – Tipos e métodos de teste das estratégias de GCN

Complexidade	**Teste**	**Processo**	**Variações**	**Freqüência recomendada**
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 ao menos
Complexo	Testar todo o PCN, incluindo o gerenciamento de incidentes	Teste que envolve todo o prédio/campus/zona de exclusão		Anualmente

Fonte: ABNT (2007)

No tocante à manutenção, recomenda-se que seja estabelecido um programa de manutenção de GCN claramente definido e documentado e que esse programa garanta a

analise crítica de GCN caso ocorram quaisquer mudanças, internas ou externas, que causem algum impacto à organização. Novos produtos e serviços e suas atividades dependentes, também necessitam ser identificados e incluídos no programa de manutenção da GCN (ABNT, 2007).

Além disso, segundo ABNT (2008), a organização deve analisar criticamente, a intervalos planejados e quando ocorrerem mudanças significativas, os arranjos de GCN para assegurar a sua contínua pertinência, adequação e eficácia. Essa análise deve ser regular e conduzida através de auto-avaliação ou auditoria.

Na eventualidade de um incidente que resulte na invocação do PCN ou do PGI, ABNT (2008) recomenda também uma análise crítica pós-incidente para:

> a) identificar a natureza e a causa do incidente;
> b) avaliar a adequação do gerenciamento da resposta;
> c) avaliar a eficácia da organização em alcançar seus tempos objetivos de recuperação;
> d) avaliar a adequação dos arranjos de GCN relativos à preparação dos funcionários para o incidente;
> e) identificar melhorias a serem feitas nos arranjos de GCN. (ABNT, 2008, p.13)

No caso da XY Telecom, ainda não existe um procedimento que defina os testes, manutenção e análise crítica dos arranjos de GCN. Portanto, sugere-se a elaboração de um procedimento documentado abordando essas atividades, incluindo a definição do programa de testes e do programa de manutenção e responsabilidades.

Para realizar os testes, manutenção e análise crítica dos arranjos de GCN, sugere-se que estejam envolvidos, principalmente, os colaboradores dos níveis da Equipe de Coordenação e Equipe de GCN do projeto, incluindo-se a Equipe de Gerenciamento de Crise, além dos Auditores Internos de SGCN.

Diante dessas sugestões, propõe-se no Quadro 24 as ações para apoiar a definição de testes, manutenção e análise crítica dos preparativos de GCN na XY TELECOM.

Quadro 24 – Ações para apoiar a definição de Testes, Manutenção e Análise Crítica dos preparativos de GCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Procedimento de Testes, Manutenção e Análise Crítica dos preparativos de GCN	Equipe de Coordenação	2 semanas	Elaboração, Aprovação e Publicação de Procedimento
Programa de Testes de GCN	Equipe de Coordenação Equipe de GCN	A definir conforme o programa	Planejamento e execução dos testes nos preparativos de GCN

Programa de Manutenção de GCN	Equipe de Coordenação Equipe de GCN	A definir conforme o programa	Planejamento e execução de manutenção nos preparativos de GCN
Realização da Análise Crítica dos preparativos de GCN	Equipe de Coordenação Equipe de GCN Auditores Internos de GCN	Semestralmente ou conforme demanda	Realização da Análise Crítica dos preparativos de GCN

Fonte: elaborado pelo Autor

4.3 Etapa 3 - Análise Crítica

Nesta etapa serão feitas sugestões para a implantação dos seguintes elementos: Auditoria Interna e Análise Crítica do SGCN pela Alta Direção. A seguir, cada um desses elementos será brevemente descrito.

4.3.1 Auditoria Interna

Visando verificar a conformidade dos sistemas de gestão em relação aos requisitos de GCN, bem como a aderência aos requisitos dos padrões normativos de referência, faz-se fundamental a realização de auditorias internas.

Para isso, deve ser estabelecido, implementado e mantido um procedimento definindo as responsabilidades e os requisitos para planejamento, execução e reporte de auditorias internas de SGCN, bem como a manutenção dos registros.

Conforme ABNT (2008), um programa de auditoria de SGCN deve ser planejado levando-se em consideração a situação e a importância dos processos e áreas a serem auditadas, o BIA, avaliação de risco, controle e medidas de mitigação, bem como os resultados de auditorias anteriores. Os critérios da auditoria, escopo, freqüência e métodos também devem ser definidos.

Sugere-se que a XY TELECOM possua procedimento documentado para o processo de auditoria interna de SGCN e, quando possível, o planejamento, programação, preparação, execução e reporte das auditorias internas ocorra de maneira integrada com os demais sistemas de gestão da organização.

Além disso, sugere-se à XY TELECOM que o planejamento das auditorias seja elaborado e divulgado às áreas envolvidas através de um cronograma de auditoria contendo os processos a serem auditados, requisitos da norma BS25999-2 em cada processo, auditores

internos selecionados, período e local da auditoria. A freqüência das auditorias sugerida é semestral e a metodologia de execução da auditoria deve basear-se na norma NBR ISO19011, que é uma norma brasileira de referência para a realização de auditorias em sistemas de gestão.

Para a realização das auditorias internas é importante que seja feito um processo de seleção e capacitação dos auditores internos. Nesse sentido, sugere-se que o auditor interno seja colaborador da companhia e que atenda às características pessoais e de experiência previstas na norma NBR ISO19011. Sugere-se, ainda, que o curso de formação de auditor interno do SGCN possua uma carga horária mínima de 20h e, devido à sua especificidade, seja ministrado por consultoria externa.

Para medir o resultado das auditorias, a sistemática mais usual é de contabilizar as não-conformidades por itens da norma BS25999-2, vinculadas aos processos e regiões onde foram detectadas. Esse método traz uma visão mais clara sobre os elementos do sistema com maior fragilidade, bem como facilita a análise de abrangência das não-conformidades identificadas.

Considerando que na XY TELECOM ainda não foi planejada ou implementada a prática de auditorias internas de SGCN, propõe-se no Quadro 25 as ações para apoiar a implantação dessa atividade.

Quadro 25 – Ações para apoiar a implantação de Auditorias Internas de SGCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Procedimento de Auditorias Internas	Equipe de Coordenação	2 semanas	Elaboração, Aprovação e Publicação de Procedimento
Formação de Auditores Internos	Consultoria Externa	1 semana	Desenvolvimento do curso de auditor interno de SGCN (20 pessoas) com duração mínima de 20h
Realização de Auditorias Internas	Auditores Internos	1 mês	Planejamento da Auditoria e Divulgação do Cronograma
			Execução das Auditorias
			Registro das Não-Conformidades

Fonte: elaborado pelo autor

4.3.2 Análise Crítica do SGCN pela Alta Direção

Conforme ABNT (2008), a Alta Direção deve analisar criticamente o sistema de gestão de continuidade de negócios da organização, em intervalos planejados, para assegurar sua contínua compatibilidade, adequação e eficácia.

A pauta de uma reunião de análise crítica de SGCN, segundo ABNT (2008), deve incluir:

> a) resultados de auditorias e análises críticas do SGCN, incluindo os principais fornecedores e parceiros; b) realimentação das partes interessadas, incluindo observações independentes; c) técnicas, produtos ou procedimentos que podem ser usados na organização para melhorar o desempenho e a eficácia do SGCN; d) situação das ações preventivas e corretivas; e) nível de risco aceitável e de risco residual; e) vulnerabilidades ou ameaças não contempladas adequadamente nas avaliações de risco anteriores; f) acompanhamento das ações oriundas de análises críticas anteriores pela direção; g) quaisquer mudanças que possam afetar o SGCN; h) recomendações para melhoria; i) resultados de testes; j) boas práticas e orientações recentes; k) lições oriundas de incidentes; e l) resultados do programa de treinamento e conscientização. (ABNT, 2008, p.14-15)

No caso da XY Telecom, não foi identificado procedimento a respeito da análise crítica de SGCN pela alta direção. Por isso, sugere-se que a XY TELECOM possua um procedimento específico para a análise crítica do Sistema de Gestão de Continuidade de Negócios incluindo informações sobre as responsabilidades e os assuntos que deverão ser tratados nesta.

Dentre outras responsabilidades, é recomendável que a alta direção do SGCN acompanhe o tratamento de não-conformidades e ações corretivas, defina políticas e objetivos do sistema de gestão, disponibilize recursos, defina as atribuições do representante da direção, bem como a sistemática de reuniões e registros. Sugere-se que a análise crítica pela alta direção seja realizada por intermédio do representante da direção do SGCN que é responsável por reportar o andamento do sistema. Para facilitar essa tarefa, sugere-se que essa atividade seja planejada, de preferência no formato de uma apresentação, contendo todas as informações exigidas para medir e tomar decisões a respeito do sistema. Além disso, para evidenciar a ocorrência da reunião, das decisões tomadas e também do comprometimento da alta direção para com o SGCN é recomendável a elaboração de um modelo de ata padrão de análise crítica. O modelo da ata, assim como a sistemática de controle desse registro deverão constar do procedimento sobre a análise crítica do SGCN.

Diante dessas sugestões, propõe-se no Quadro 26 as ações para apoiar a implantação da análise crítica de SGCN pela alta direção na XY TELECOM.

Quadro 26 – Ações para apoiar a implantação da Análise Crítica de SGCN pela Alta Direção na XY TELECOM

O que fazer	Quem	Quando (Prazo)	Como
Procedimento de Análise Crítica do SGCN	Equipe de Coordenação	1 semana	Elaboração, Aprovação e Publicação do Procedimento
Realização da Análise Crítica de SGCN pela Alta Direção	Representante da Direção e Alta Direção	Semestralmente	Planejamento da Reunião de Análise Crítica pelo Representante da Direção
			Realização e registro em ata da Reunião de Análise Crítica do SGCN

Fonte: elaborado pelo autor

4.4 Etapa 4 - Ações Corretivas

Nesta etapa serão feitas sugestões para a implantação dos seguintes requisitos: Ações Corretivas e Preventivas, e Melhoria Contínua. A seguir, cada um desses elementos será brevemente descrito.

4.4.1 Ações Corretivas e Preventivas

A norma ISO9001:2000, conforme ABNT (2008), preconiza que a organização deve executar ações corretivas e preventivas de modo a eliminar as causas de não-conformidades reais e potenciais e evitar sua repetição. Neste caso, as ações corretivas e preventivas devem ser apropriadas aos efeitos das não-conformidades encontradas e, para ambas, deve ser estabelecido um procedimento documentado.

Em um sistema de gestão de continuidade de negócios não é diferente, e a organização necessita executar ações preventivas e corretivas específicas relacionadas à possibilidade de interrupção na entrega desses produtos ou processos.

Por isso, segundo ABNT (2008), recomenda-se a elaboração de procedimento documentado sobre não-conformidades, definindo os requisitos para:

> a) análise crítica de não-conformidades reais e potenciais; b) determinação das causas de não-conformidades reais e potenciais; c) avaliação da necessidade de ações para assegurar que aquelas não-conformidades não ocorrerão novamente; d) determinação e implementação de ações necessárias; e) registros dos resultados das ações executadas; e) análise crítica de ações corretivas e preventivas executadas; f) identificar os riscos que se modificaram e assegurar que a atenção está voltada para os riscos modificados significativamente; g) garantir que todos aqueles que precisam saber, sejam informados da não-conformidade e ponham em prática a ação preventiva; e h) garantir que a prioridade das ações preventivas seja baseada nos resultados da avaliação de riscos e do BIA. (ABNT, 2008, p.16)

No caso da XY TELECOM, não foi identificado procedimento sobre não-conformidades ou ações corretivas e preventivas de SGCN. Portanto, sugere-se que sejam tratados no SGCN através de um procedimento: (i) a sistemática de constatação e registro de não-conformidades; (ii) a identificação e registro de causas das não-conformidades, incluindo as causas raiz; (iii) a análise e registro da abrangência das não-conformidades; (iv) a elaboração, registro e acompanhamento de ações corretivas e preventivas para eliminar ou prevenir as causas raiz das não-conformidades; (v) e a verificação da eficácia dessas ações.

O registro das não-conformidades, ações corretivas e preventivas pode ser feito em um formulário padrão denominado RNCP (Relatório de Não-Conformidades Ações Corretivas e Preventivas). Caso a empresa deseje investir nessa funcionalidade, visando facilitar o monitoramento das ações, assim como a comunicação e cobrança das áreas responsáveis, poderá optar por um sistema informatizado.

Diante dessas considerações, propõe-se no Quadro 27 as tarefas para apoiar a implantação de ações corretivas e preventivas de SGCN na XY TELECOM.

Quadro 27 – Planejamento de tarefas para apoiar as Ações Corretivas e Preventivas de SGCN na XY TELECOM

O que fazer	**Quem**	**Quando (Prazo)**	**Como**
Procedimento de Não-Conformidades, Ações Corretivas e Preventivas	Equipe de Coordenação	1 semana	Elaboração, Aprovação e Publicação do Procedimento
Elaboração de Ações Corretivas e Preventivas	Áreas de Negócio envolvidas nos processos de SGCN	Conforme demanda	Elaboração e registro da Ações Corretivas e Preventivas do SGCN do Formulário RNCP
Verificação de Eficácia das Ações Corretivas ou Preventivas	Equipe de Coordenação	Conforme demanda	Verificação da eficácia das ações corretivas ou preventivas e registro no formulário RNCP

Fonte: Elaborado pelo autor

4.4.2 Melhoria Contínua

Conforme preconizam as normas de referência sobre sistemas de gestão, a organização deve continuamente melhorar a eficácia de seus sistemas de gestão. No tocante ao SGCN, segundo ABNT (2008), a eficácia pode ser melhorada por meio do uso da política de continuidade de negócios, objetivos de continuidade de negócios, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas, e análise crítica pela direção.

A evidência dessa melhoria contínua não necessita ser evidenciada e sim percebida por todas as partes interessadas no SGCN e, para isso, o sistema de gestão precisa ser implementado e ganhar maturidade.

Como visto, foi elaborada uma estrutura de apoio à implantação do SGCN na XY TELECOM com o objetivo de estabelecer o conceito de melhoria contínua de GCN na companhia, além de outros conceitos, facilitando, assim a sua aplicação e aperfeiçoamento.

Em geral, a estrutura de apoio proposta procurou atender a diversos requisitos para poder ser entendida e aplicável aos seus usuários na XY Telecom.

Na próxima seção, será visto como foi a aceitação inicial dessa proposta de estrutura de SGCN perante alguns de seus principais usuários nessa companhia.

4.5 Análise Preliminar de Aceitação da Proposta de Estrutura de Apoio de SGCN na XY Telecom

Após a elaboração da proposta de estrutura de apoio de SGCN na empresa XY Telecom, foi realizada uma análise preliminar da aceitação dessa estrutura perante os seus principais futuros usuários na companhia (membros da equipe de coordenação do projeto). O objetivo dessa análise foi constatar o nível de aceitação dessa proposta verificando, assim, a sua possibilidade de implementação. A seguir, serão descritos o método de execução da análise e os seus resultados.

4.5.1 Metodologia da Análise de Aceitação

A análise preliminar de aceitação da estrutura de apoio de SGCN na XY Telecom foi realizada em duas etapas.

A primeira etapa envolveu a disponibilização da proposta elaborada e o levantamento de informações sobre a aceitação dessa estrutura junto aos seus principais usuários. Essa etapa foi realizada através de entrevistas com 3 colaboradores da XY Telecom participantes da equipe do projeto de GCN em 2009, onde foram abordados os seguintes aspectos sobre aceitação:

- Apresentação: se a forma de apresentação da estrutura de apoio ao SGCN proposta está adequada;
- Entendimento: se foi possível entender os elementos, sugestões e ações que compõem a estrutura de apoio de SGCN proposta;

- Fundamentação técnica: se a proposta de estrutura de apoio de SGCN está bem fundamentada, com base em boas práticas de GCN existentes;
- Aplicabilidade: se a proposta de estrutura de apoio de SGCN pode ser aplicada na XY Telecom.

A terceira etapa envolveu a consolidação de informações. Nessa etapa foram consolidadas as respostas obtidas nas entrevistas com os usuários da estrutura proposta em um quadro dividido por aspecto avaliado e obteve-se um parecer final sobre a aceitação.

4.5.2 Resultados da Análise de Aceitação

Conforme a metodologia descrita, foi realizada a análise de aceitação da estrutura de apoio de SGCN proposta na XY Telecom. Os resultados dessa análise são apresentados no Quadro 28.

Quadro 28 – Resultados da Análise de Aceitação da Proposta de Estrutura de Apoio de SGCN na XY Telecom

	Apresentação	**Entendimento**	**Fundamentação Técnica**	**Aplicabilidade**	**Parecer Final**
Proposta de Estrutura de Apoio à Implantação do SGCN	Foi considerada bem apresentada através do diagrama em pirâmide, facilitando a visualização de todos os elementos a serem implantados. Poderia ter sido destacado neste diagrama quais elementos são novos e quais foram atualizados em relação à estrutura de GCN original.	Foi considerada de fácil entendimento através de linguagem objetiva.	Foi considerada bem fundamentada através das normas de referência e boas práticas de GCN aproveitando alguns elementos da estrutura de GCN anterior.	Foi considerada possível de ser aplicada. Demanda um detalhamento maior no tocante aos planos de resposta para facilitar sua implementação.	Aceita

Fonte: elaborado pelo autor

Com base nos resultados apresentados, pôde-se constatar que a proposta de estrutura de apoio à implantação do SGCN na XY TELECOM em geral foi bem aceita pelos seus usuários, necessitando de alguns ajustes pontuais de melhoria.

Essa aceitação inicial perante seus usuários é um retorno importante sobre a possibilidade de aplicação desse modelo, dado que a avaliação foi realizada por pessoas com conhecimento técnico em GCN.

O objetivo deste capítulo foi apresentar uma proposta de estrutura de apoio à implantação de um Sistema de Gestão de Continuidade de Negócios na XY TELECOM. Com essa proposta de SGCN, apresentada através de etapas, elementos, sugestões e ações, foi possível ter-se uma idéia razoável do que necessita ser feito para que esse sistema possa ser implantado na empresa em estudo. No entanto, tão importante quanto ser implantado, o SGCN também precisa ser implementado, ou seja, precisa funcionar, manter-se, possuir eficácia e melhorar-se continuamente. Por isso, o conceito de implementação (palavra que é parônima à implantação) deve ser concretizado.

Em virtude de outros projetos estratégicos da XY TELECOM no ano de 2009, a opção pela implementação da estrutura de apoio proposta não foi priorizada, fato que limitou uma avaliação mais aprofundada da eficácia dessa estrutura. Por isso, cabe à XY TELECOM desenvolver a implementação do SGCN, contemplando a execução das ações planejadas na proposta deste trabalho, de preferência através de um projeto coordenado.

Com um SGCN estabelecido e implementado, o conceito do modelo PDCA começará a se concretizar, garantindo, assim, a melhoria contínua da resiliência organizacional (capacidade da organização de resistir aos efeitos de um incidente e de retomar suas atividades críticas aos níveis normais de funcionamento), a incorporação da cultura e dos aspectos de GCN entre as partes interessadas, o aprimoramento da gestão de riscos e, por conseguinte, da governança corporativa da companhia.

5. Considerações Finais

Os Sistemas de Gestão, de modo geral, além de serem um diferencial competitivo, surgem como uma solução inteligente para as empresas que visam reduzir riscos, custos, otimizar sua estrutura de controles e monitoramento, e sistematizar o atendimento à legislação aplicável às suas atividades.

Como visto, a implantação de um Sistema de Gestão de Continuidade de Negócios (SGCN) reafirma esse conceito e desenvolve a capacidade da organização de responder à ocorrência de eventos, visando administrar e mitigar seus efeitos e retornar à normalidade caso haja uma interrupção de suas atividades. A seguir, serão brevemente apresentadas as considerações finais desse trabalho e as sugestões para trabalhos futuros.

5.1 Conclusões

O presente trabalho foi desenvolvido através de uma abordagem conceitual e de um estudo de caso, visando caracterizar a gestão da continuidade de negócios e as boas práticas existentes sobre o tema, inserida no contexto de gerenciamento de riscos e de governança corporativa, bem como avaliar a estrutura de GCN numa empresa de telecomunicações.

O principal objetivo deste trabalho foi desenvolver uma proposta de estrutura de apoio para a implantação de um SGCN nessa empresa. O desenvolvimento dessa proposta de estrutura baseou-se nas boas práticas sobre Gestão de Continuidade de Negócios e em especial nas diretrizes previstas nas normas da série BS25999 do *British Standards Institution*, considerado atualmente como um dos instrumentos de referência mais importantes sobre o tema.

Através da revisão bibliográfica, apresentou-se um breve resumo sobre os conceitos e práticas de referência em GCN e buscou-se caracterizar como este tema está inserido no contexto do gerenciamento de riscos que, por sua vez, trata-se de um dos mecanismos para o desenvolvimento da governança corporativa. A literatura apresentou que a

gestão de continuidade de negócios surge como uma forma de gestão que visa administrar o risco operacional de interrupção da entrega dos produtos e serviços essenciais da organização e que é desenvolvida através de um *framework* denominado ciclo de vida de GCN com elementos para o seu estabelecimento. Além disso, foi apresentado que o conceito de GCN evoluiu para um sistema de gestão de continuidade de negócios (SGCN), que tem como referência o padrão normativo BS25999-2 com requisitos para sua implantação.

Ainda na revisão bibliográfica, foi realizada uma análise comparativa entre os modelos de SGCN (segundo a norma BS25999-2) e o de GCN (segundo a norma BS25999-1) onde identificou-se como uma das diferenças mais marcantes entre os dois o fato de que o SGCN está fundamentado num conceito mais sólido e abrangente de gestão, concebido a partir do PDCA – *Plan, Do, Check, Act* (Planejar, Fazer, Verificar e Analisar Criticamente – Ciclo de Melhoria Contínua), modelo mundialmente conhecido e comumente aplicado em sistemas de gestão.

No desenvolvimento deste trabalho pôde-se perceber também a similaridade entre o SGCN e outros modelos de sistema de gestão, como de segurança da informação (SGSI), qualidade (SGQ), meio ambiente (SGA) e saúde e segurança (SGSSO). Esses elementos em comum facilitam o planejamento de um sistema integrado, simplificam a documentação e controles relacionados, bem como sistematizam o atendimento à legislação pertinente, tornando o sistema mais otimizado e facilitando o seu gerenciamento.

Através de um estudo de caso na empresa de nome fictício XY TELECOM, pôde-se observar a existência de uma sólida abordagem por processos e uma estrutura de GCN com boas referências, mas implantada parcialmente. Na análise crítica dessa estrutura, observou-se algumas dificuldades na sua implantação, dentre elas o escopo amplo de processos, que dificultou o desenvolvimento das etapas de análise de riscos e BIA. Além disso, constatou-se na estrutura de GCN dessa empresa alguns *gaps* com relação às boas práticas previstas na norma BS25999-1. Esse cenário, aliado aos resultados da análise comparativa realizada, justificou o desenvolvimento na empresa em estudo de uma proposta de estrutura mais consistente, capaz de ser implementada e melhorada continuamente, fundamentada pelo modelo de SGCN e combinado às boas práticas do modelo de GCN.

A estrutura de apoio proposta apresentou-se através de um diagrama em formato de pirâmide segmentada através de quatro etapas principais e seus elementos de implantação. Com ênfase na finalidade de apoio, em cada elemento de cada etapa do diagrama foram apresentadas sugestões para a implantação de um SGCN aplicado às particularidades do cenário da companhia. Essas sugestões fundamentaram o planejamento de ações de adequação que foram apresentadas utilizando-se a ferramenta 3W1H.

A grande limitação do presente trabalho encontrou-se na impossibilidade de implementação prática da estrutura de apoio proposta em virtude de outras prioridades estratégicas na XY TELECOM impedindo, assim, que se faça uma análise mais concreta da eficácia dessa estrutura. No entanto, a constatação positiva pelos usuários na análise de aceitação dessa proposta, aliado ao seu embasamento técnico, trazem razoável segurança para a sua aplicação.

Uma funcionalidade muito importante da estrutura de apoio proposta é que ela pode ser implementada na forma de um projeto, pois observa-se claramente a existência de um seqüenciamento lógico entre as etapas, elementos, sugestões e ações planejadas. Essa característica da estrutura facilita o seu planejamento e o seu gerenciamento caso venha a ser aplicada.

No entanto, para que essa implementação aconteça de fato, a Alta Direção deve comprar a idéia do SGCN, bem como entender o desenvolvimento de cada um dos requisitos que o compõem. Dessa forma, o SGCN poderá ser entendido e disseminado adequadamente, através da abordagem *top down*, permeando todos os processos e níveis hierárquicos da organização e alcançando a eficiência desejada.

Um dos grandes desafios existentes para as empresas atualmente têm sido conseguir conciliar suas necessidades operacionais com seus objetivos estratégicos. E considerando que o conceito de sistema de gestão de continuidade de negócios é algo bastante recente no cenário corporativo mundial a sua implementação torna-se um desafio ainda mais relevante. Desse modo, muitas empresas optam por implementar parcialmente esse sistema, deixando algumas lacunas que podem custar caro caso um evento de grandes proporções se materialize.

Para prevenir esse risco é que foi desenvolvido o presente trabalho, apresentando-se uma estrutura de apoio com os elementos fundamentais que a organização precisa para enfrentar situações de crise e garantir a continuidade do seu negócio.

5.2 Recomendações para Trabalhos Futuros

O trabalho desenvolvido apresentou um conceito para ser implementado. Portanto, para trabalhos acadêmicos futuros sugere-se implementação da estrutura proposta e a avaliação da sua eficácia.

Além disso, o conceito de SGCN pode também ser explorado em trabalhos versando a respeito do relacionamento deste sistema com demais sistemas de gestão e da possibilidade de desenvolvimento de uma proposta de integração entre eles.

Outra oportunidade interessante a ser explorada em trabalhos pode ser a aplicação, em etapas do SGCN, de ferramentas matemáticas utilizadas na Engenharia de Produção como, por exemplo, a análise multicriterial para a determinação do escopo ou de estratégias de continuidade.

Por fim, cabe ressaltar que a estrutura proposta nesse trabalho não possui a pretensão de ser definitiva, devendo ser interpretada como um instrumento de apoio para o estabelecimento do SGCN e sendo passível de melhorias a partir de sua implementação, seguindo, assim, a lógica de um sistema de gestão: a lógica do PDCA.

REFERÊNCIAS

AGUIAR, Carlos. **Governança Corporativa e Geração de Valor aos Acionistas**. Rio de Janeiro: 2005. 42 f. Monografia, Instituto de Economia, Universidade Federal do Rio de Janeiro.

ALVES, Sandra. **Os Maiores Erros das Empresas no Planejamento da Continuidade de Negócios.** 2009. Disponível em: <http://www.brasiliano.com.br>. Acesso em: 22 fev. 2010

ARAÚJO, Vagner. **Gestão de Riscos Operacionais**. São Paulo: 2006.168 f. Monografia, Faculdade Carlos Drummond de Andrade.

ASIS INTERNATIONAL. **Business Continuity Guideline: a practical approach for emergency preparedness, crisis management and disaster recovery**. Alexandria: ASIS, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 15999-1:2007 – Gestão de Continuidade de Negócios – Código de Prática**. Rio de Janeiro: ABNT, 2007.

_____. **NBR 15999-2:2008 – Gestão de Continuidade de Negócios – Requisitos**. Rio de Janeiro: ABNT, 2008.

_____. **NBR ISO 9001:2000 – Sistemas de Gestão da Qualidade – Requisitos**. Rio de Janeiro: ABNT, 2000.

_____. **NBR ISO 14001:2004 – Sistemas de Gestão Ambiental – Especificação e diretrizes para uso**. Rio de Janeiro: ABNT, 2004.

_____. **NBR ISO 20000-1 - Tecnologia da Informação – Gerenciamento de Serviços – Parte 1: Especificação**. Rio de Janeiro: ABNT, 2008.

_____. **NBR ISO 20000-2 - Tecnologia da Informação – Gerenciamento de Serviços – Parte 2: Código de Prática**. Rio de Janeiro: ABNT, 2008.

_____. **NBR ISO 31000 – Gestão de Riscos – Princípios e Diretrizes**. Rio de Janeiro: ABNT, 2009.

_____. **NBR ISO/IEC 27001:2006 - Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2006.

_____. **ISO Guia 73 – Gestão de Riscos – Vocabulário**. Rio de Janeiro: ABNT, 2009.

AYRES, Paulo Roberto. **Gestão de Riscos Operacionais**. Porto Alegre: UFRGS, 2007. Artigo, Núcleo de Estudos e Pesquisas em Contabilidade, UFRGS.

BARALDI, Paulo. **Gerenciamento de Riscos Empresariais**. São Paulo: Campus, 2005.

BERGAMINI JUNIOR, Sebastião. Controles Internos como um Instrumento de Governança Corporativa. **Revista do BNDES**, Rio de Janeiro, v. 12, n.24, p.149-188, 2005.

BRASILIANO, Antonio. BCM – Business Continuity Management – Gestão de Continuidade dos Negócios, isto existe no Brasil? **Revista Eletrônica Brasiliano e Associados**, n.27, dez. 2006.

BUCHANAN, Leigh; O'CONNELL, Andrew. **Uma breve história de tomada de decisão**. São Paulo: Harvard Business Review, 2006. Disponível em: <http://www.hbrbr.com.br>. Acesso em: 03 jul. 2008.

CARVALHO, Fernando. COSO x ISO31000. **Revista Gestão de Riscos**, São Paulo, v.44, p.12-16, jun. 2009. Disponível em <http://www.brasiliano.com.br/>. Acesso em 08 out. 2009.

CHAIB, Erick. **Proposta para Implementação de Sistema de Gestão Integrada de Meio Ambiente, Saúde e Segurança do Trabalho em Empresas de Pequeno e Médio Porte: um estudo de caso da indústria metal-mecânica**. Rio de Janeiro: UFRJ, 2005. Dissertação, COPPE, UFRJ.

COCURULLO, Antonio. **Gestão de Riscos Corporativos: riscos alinhados com algumas ferramentas de gestão: um estudo de caso no setor de celulose e papel**. São Paulo: PriceWaterhouseCoopers, 2004.

COMISSÃO DE VALORES MOBILIÁRIOS. **Atribuições**. Disponível em: <http://www.cvm.gov.br/>. Acesso em 11 jul. 2008.

_____. **Cartilha de Recomendações da CVM sobre Governança Corporativa**. Rio de Janeiro: CVM, 2002. Disponível em: <http://www.cvm.gov.br/>. Acesso em 11 jul. 2008.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Gerenciamento de Riscos Corporativos: estrutura integrada**. PriceWaterhouseCoopers, 2007. Disponível em: <http://www.coso.org>. Acesso em: 12 jun. 2008.

CRUZ, Alessandra; SARTORI, Fernando; MILHOMENS, Gabriel; OKADA, Kátia; SILVA, Leonardo; ABRAHÃO, Marília. **Governança corporativa: análise do processo de adequação de uma empresa brasileira do setor elétrico as exigências do mercado de ações norte-americano**. Trabalho apresentado no 26° ENEGEP, Fortaleza, 2006.

DELOITTE TOUCHE TOHMATSU. **Lei Sarbanes-Oxley. Guia para melhorar a governança corporativa através de eficazes controles internos**. São Paulo: Deloitte, 2003.

_____. **Metodologia de Auditoria com Foco em Riscos**. Trabalho apresentado à FEBRABAN, 2003. Disponível em <http://www.febraban.org.br>. Acesso em: 13 jun. 2008

ERBEN, Roland. **Risk Management Standards – role, benefits e applicability**. Trabalho apresentado na 2.ª European Risk Conference, Germany, 2008.

FEDERAÇÃO BRASILEIRA DE BANCOS. Continuidade de Negócios - Os planos dos bancos para garantir uma travessia segura em casos de catástrofe. **Revista CIAB FEBRABAN**, São Paulo, n.16, p. 8-11, abr. 2008. Disponível em <http://www.ciab.org.br/ciab2008>. Acesso em: 08 jul. 2008

FEDERAL EMERGENCY MANAGEMENT AGENCY. **Emergency Management Guide for Business and Industry.** Washington: FEMA, 2005.

FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS. **Norma de Gestão de Riscos**. Bruxelas: FERMA, 2003.

GARCIA, Felix. **Governança Corporativa**. Rio de Janeiro: 2005. 41 f. Monografia, Instituto de Economia, Universidade Federal do Rio de Janeiro.

GUTIERREZ, Wilson. Continuidade de Negócios - Os planos dos bancos para garantir uma travessia segura em casos de catástrofe. **Revista CIAB FEBRABAN**, São Paulo, n.16, p. 8-11, abr. 2008. Entrevista concedida à FEBRABAN.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 4. ed. São Paulo: IBGC, 2009.

_____. **Governança no Brasil**. São Paulo: IBGC, 2008. Disponível em: <http://www.ibgc.org.br/>. Acesso em : 06 jul. 2008.

_____. **Governança no Mundo**. São Paulo: IBGC, 2008. Disponível em: <http://www.ibgc.org.br/>. Acesso em : 06 jul. 2008.

_____. **Guia de Orientação para Gerenciamento de Riscos Corporativos**. São Paulo: IBGC, 2007.

_____. **Origem da Boa Governança**. São Paulo: IBGC, 2008. Disponível em: <http://www.ibgc.org.br/>. Acesso em: 06 jul. 2008.

_____. **Principais Modelos**. São Paulo: IBGC, 2008. Disponível em: <http://www.ibgc.org.br/>. Acesso em : 06 jul. 2008.

LABODOVÁ, Alena. Implementing Integrated Management Systems Using a Risk Analysis based Approach. **Journal of Cleaner Production**, vol. 12, p. 571-580, ago. 2004.

LETHBRIDGE, Eric. **Governança Corporativa**. Brasília: BNDES, 1997. Disponível em <http://www.bndes.gov.br/>. Acesso em: 23 jun. 2008.

MACEDO, Paloma O. **Plano de Contingências do Setor de Tecnologia da Informação para Empresa de Telecomunicações**. Canoas: ULBRA, 2003. Monografia,

MACIEIRA, André. **Gestão Baseada em Riscos: reinventando o papel da gestão de riscos integrada ao negócio**. Rio de Janeiro: ELO GROUP, 2008.

MANAGEMENT WISDOM. **The Deming Library Discussion Guides.** vol. 21. Washington. DVD-ROM.

MINISTÉRIO DA PREVIDÊNCIA SOCIAL. **Modelo Brasileiro de Gerenciamento de Riscos Operacionais da Previdência Social**. Brasília: MPS, 2003.

NATIONAL FIRE PROTECTION ASSOCIATION. **NFPA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs.** Quincy: NFPA, 2007.

OLIVEIRA, Marcelle; RIBEIRO, Maisa; SAMPAIO, Márcia; CARVALHO, Fernanda. **Os efeitos da adoção dos conceitos e das práticas de Governança Corporativa na Transparência das Informações Evidenciadas por Empresas Brasileiras do Setor de Papel e Celulose**. Trabalho apresentado no 4° Congresso USP de Controladoria e Contabilidade, São Paulo, 2004.

OLIVEIRA, Uálison; MARINS, Fernando; ROCHA, Henrique. **Riscos Empresariais Operacionais: percepção no ambiente fabril**. Trabalho apresentado no 26° ENEGEP, Fortaleza, 2006.

PACHECO, Ana Paula; SALLES, Bertholdo; GARCIA, Marcos Antônio; POSSAMAI, Osmar. **O ciclo do PDCA na gestão do conhecimento: uma abordagem sistêmica**. Trabalho apresentado no III Congresso Brasileiro de Sistemas, Florianópolis, 2007. Artigo disponível em <http://www.isssbrasil.usp.br/pdfs2/ana.pdf>. Acesso em fev. 2010.

PADOVEZE, Clovis; BERTOLUCCI, Ricardo. **Proposta de um Modelo para o Gerenciamento do Risco Corporativo.** Trabalho apresentado no 25° ENEGEP, Porto Alegre, 2005.

PEROBELLI, Fernanda. **Um modelo para gerenciamento de riscos em instituições financeiras: aplicação ao setor de distribuição de energia elétrica no Brasil**. São Paulo: USP, 2004. 147 f. Tese de Doutorado, Faculdade de Economia, Administração e Contabilidade, USP, São Paulo, 2004.

RAKE, Michael. A Receita da Boa Governança. **Revista HSM Management**, São Paulo, n.45, ago. 2004.

REGO, Antonio; CARVALHO JUNIOR, Cesar; BRUNI, Adriano; SILVA, Sérgio. **A utilização do COSO na Controladoria: um estudo no Brasil**. Trabalho apresentado no 10° Congresso Internacional de Custos, Lyon, 2007.

SANTANA, Maria Helena. **O Novo Mercado**. São Paulo: BMFBOVESPA, 2006. Disponível em: <http://www.bmfbovespa.com.br>. Acesso em: 16. abr. 2010

SANTOS, Jánison; NASCIMENTO, Hugo. **Implantação de um sistema de gestão de segurança da informação na UFG**. Trabalho apresentado no II Workshop de Tecnologia da Informação das IFES, Gramado, 2008.

SHLEIFER, Andrei; VISHNY, Robert. A Survey of Corporate Governance. **The Journal of Finance**, v. 52, n.2, jun. 1997.

SILVEIRA, Alexandre. **Governança Corporativa, Desempenho e Valor da Governança no Brasil**. São Paulo: USP, 2002. Dissertação de Mestrado, Faculdade de Economia, Administração e Contabilidade, USP, 2002.

SPRING SINGAPORE. **TR19:2005 - Technical Reference for Business Continuity Management (BCM)**. Singapore: SPRING, 2005.

STANDARDS AUSTRALIA; STANDARDS NEW ZEALAND COMMITTEE. **AS/NZS 4360: 2004: Australian/New Zealand Standard Risk Management.** Sidney e Wellington: SA/SNZ, 2004.

_____. **HB221-2004-Business Continuity Management**. Sydney e Wellington: SA/SNZ, 2004.

STANDARDS AUSTRALIA. **HB292 – 2006 – A Practioners Guide to Business Continuity Management**. Sidney: AS, 2006.

TEIXEIRA, Alexandre. A ameaça dos grandes riscos. **Revista Eletrônica Istoé Dinheiro**, ed. 487, jan. 2007. Disponível em <http://www.terra.com.br/istoedinheiro>. Acesso em: 24 jun. 2008.

TELECO. **eTOM: Visão a nível do CEO**. São José dos Campos: TELECO, 2009. Disponível em: <http://www.teleco.com.br/>. Acesso em: 30 mar. 2009.

THE BRITISH STANDARDS INSTITUTION. **BS 25999-1 – Business Continuity Management – Code of Practices.** United Kingdom: BSI, 2006.

_____. **BS 25999-2 – Business Continuity Management – Specification.** United Kingdom: BSI, 2007.

_____. **BS OHSAS 18001:2007 Occupational health and safety management systems. Requirements.** United Kingdom: BSI, 2007.

THE DISASTER RECOVERY INSTITUTE INTERNATIONAL. **Professional Practices for Business Continuity Practitioners**. New York: DRII, 2008. Disponível em: <http://www.drii.org>. Acesso em: 16. abr. 2010

THE FINANCIAL SERVICES AUTHORITY. **Business Continuity Management Practice Guide**. London: FSA, 2006.

THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/PAS 22399 - Societal security — Guideline for Incident Preparedness.** Geneva: ISO, 2007.

TURRIONI, João; BARBEDO, Simone. Sistemas de Gestão da Qualidade no setor de serviços: estudo de aplicabilidade em bibliotecas de ensino superior de uma cidade mineira. **Revista Pesquisa e Desenvolvimento Engenharia de Produção**, Universidade Federal de Itajubá, Itajubá, n.1, p. 63-76, dez. 2003.

VIEGAS, Jaqueline. **Estabelecimento de um sistema integrado de gestão: qualidade e meio ambiente**. Porto Alegre: UFRGS, 2000. Dissertação de Mestrado, Programa de Pós-Graduação em Engenharia de Produção, UFRGS, 2000.

VIEIRA, Solange Paiva; MENDES, André. Governança corporativa: uma análise de sua evolução e impactos no mercado de capitais brasileiro. **Revista do BNDES**, Rio de Janeiro, v. 11, n.22, p.103-122, dez. 2004.