3

Instituto Brasileiro de Governança Corporativa

Cadernos de Governança Corporativa

Guia de Orientação para Gerenciamento de Riscos Corporativos

O IBGC, dando seqüência a seus "Cadernos de Governança Corporativa", lança o "Guia de Orientação para Gerenciamento de Riscos Corporativos".

O objetivo desta iniciativa é trazer ao mercado informações práticas que contribuam para o processo da governança corporativa e auxiliem conselheiros e demais administradores a desempenhar melhor as suas funções. Contribui, assim, para aprimorar o funcionamento do mercado, gerar maior confiança dos investidores e, conseqüentemente, propiciar maior fluidez de recursos para as empresas.

IBGC | Instituto Brasileiro de Governança Corporativa

IBGC | Instituto Brasileiro de Governança Corporativa

Guia de Orientação para Gerenciamento de Riscos Corporativos

IBGC | Instituto Brasileiro de Governança Corporativa

2007

Instituto Brasileiro de Governança Corporativa

O IBGC é uma organização exclusivamente dedicada à promoção da governança corporativa no Brasil e o principal fomentador das práticas e discussões sobre o tema no País, tendo alcançado reconhecimento nacional e internacional.

Fundado em 27 de novembro de 1995, o IBGC – sociedade civil de âmbito nacional, sem fins lucrativos – tem o propósito de "ser referência em governança corporativa, contribuindo para o desempenho sustentável das organizações e, influenciando os agentes de nossa sociedade no sentido de maior transparência, justiça e responsabilidade".

Para mais informações sobre o Instituto Brasileiro de Governança Corporativa, visite o site: **www.ibgc.org.br.** Para associar-se ao IBGC ligue para (11) 3043 7008.

I59g Instituto Brasileiro de Governança Corporativa
Guia de orientação para o gerenciamento de riscos corporativos / Instituto Brasileiro de Governança Corporativa; coordenação: Eduarda La Rocque. São Paulo, SP: IBGC, 2007 (Série de Cadernos de Governança Corporativa, 3).

48p.

ISBN: 978-85-99645-04-8

1. governança corporativa. 2. governança corporativa - risco - gestão
I. Título. II. La Rocque, Eduarda, coord. CDD – 658.4

Bibliotecária responsável: Mariusa F. M. Loução – CRB-12/330

Créditos

Este trabalho foi desenvolvido pelo Subcomitê de Gerenciamento de Riscos Corporativos do Comitê de Finanças e Contabilidade do IBGC.

Durante sua elaboração, este documento passou por processo intenso de discussão e audiência pública, tendo recebido diversas contribuições e sugestões.

Agradecemos à Bovespa, pela cessão de suas instalações no Rio de Janeiro para algumas das reuniões de trabalho e ao *staff* do IBGC, especialmente Simone Novotny Couto Pereira e Angela Rita Franco Donaggio, que secretariaram os trabalhos. Agradecemos todos os membros do Subcomitê de Gerenciamento de Riscos Corporativos, principalmente à Eduarda La Rocque, que coordenou a organização deste documento.

Contribuições:
Antonio Laporta
Antonio Moura
Camila Nogueira
Carlos Antonio Rocca
Clarissa Lins
Eduardo de Vasconcellos
Heloisa B. Bedicks
Ives Pereira Muller
João Carlos Orzzi Lucas
Jose Luiz de Souza Motta
Lúcio Carlos de Pinho Filho
Moacyr Carmo
Paulo Baraldi
Paulo Conte Vasconcellos
Roberto Lamb

Coordenação:
Eduarda La Rocque

Contribuições especiais:
Este guia contou com a participação extremamente relevante de Antonio Cocurullo, Eduardo Lins de Carvalho, Jorge Luiz de Carvalho Brandão e Lucia Hauptman, e com a inestimável colaboração de Carlos Eduardo Lessa Brandão para tornar o texto o mais didático possível, aproximando-o do que deveria ser um guia do IBGC.

Índice

Apresentação

O Instituto Brasileiro de Governança Corporativa - IBGC, em comemoração aos 10 anos de sua fundação, completados em 2005, lançou a série de publicações denominada Cadernos de Governança.

O objetivo desta iniciativa é trazer ao mercado informações práticas que contribuam para o processo da governança corporativa e auxiliem conselheiros e demais administradores a desempenhar melhor as suas funções, contribuindo para aprimorar o funcionamento do mercado, gerar maior confiança dos investidores e, conseqüentemente, propiciar maior fluidez de recursos para as empresas.

Os Cadernos de Governança do IBGC são editados, de acordo com seu conteúdo, em três séries:

sobre parte dos conceitos envolvidos[1], e as práticas entre as empresas são as mais variadas. Desta forma, julga-se necessário divulgar os conceitos para, em seguida, introduzir e disseminar a cultura de gerenciamento de riscos corporativos. A partir do entendimento e alinhamento dos conceitos e da formação de um linguajar comum, deve-se implantar o que melhor se aplica à realidade de cada organização no contexto em que se encontra e atua. Dispor de um modelo mental e de termos e jargão adequados para viabilizar a discussão das aplicações práticas do gerenciamento integrado de riscos (especialmente entre os conselheiros de administração e especialistas no tema), representa uma das principais contribuições deste Guia para as organizações.

O IBGC acredita que as reflexões e sugestões trazidas com este Guia contribuirão para o aperfeiçoamento do ambiente empresarial, por se tratar de uma valiosa ferramenta de gestão para o desenvolvimento sustentável das organizações, beneficiando todas as partes interessadas.

1

Introdução

1 Introdução

As atividades envolvidas no Gerenciamento de Riscos Corporativos ("GRCorp") devem contribuir para a perenidade da organização, atendendo aos seus objetivos estatutários e estratégicos.

As recomendações e sugestões contidas neste Guia de Orientação para Gerenciamento de Riscos Corporativos (Guia) devem ser avaliadas diante da realidade de cada organização. Apesar de destinar-se primariamente a empresas com fins lucrativos, os conceitos e sugestões poderão ser utilizados também por entidades do primeiro e do terceiro setores. Aspectos específicos relacionados a organizações financeiras são tratados brevemente no Anexo A.2.

Este Guia também sugere que as organizações disponham de uma estrutura mínima de governança corporativa, ou seja, um conselho de administração, conselho deliberativo ou conselho consultivo.

As sugestões deste documento contam com a atuação do conselho de administração no processo de gerenciamento dos riscos. O Guia visa orientá-lo tanto para a implantação de um modelo de GRCorp como para a avaliação e introdução de melhorias em modelos existentes.

De forma geral, as práticas sugeridas pelo Instituto Brasileiro de Governança Corporativa – IBGC vão além do cumprimento legal e regulatório e pressupõem que a organização atenda a todas as exigências desta natureza.

A estrutura do Guia se inspirou no item 2.38, 3ª edição, do Código das Melhores Práticas de Governança Corporativa do IBGC ("Código do IBGC"):

> "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".

Para que o conselho de administração possa efetivamente identificar, priorizar e garantir a gestão eficaz da exposição da organização aos diversos riscos que podem afetar o seu negócio, deve apresentar uma atitude pró-ativa, requerendo informações baseadas no modelo de GRCorp. Isto se tornará possível na medida em que os conselheiros tenham conhecimento suficiente sobre o tema e consigam avaliar os modelos, ferramentas e medidas utilizadas. O Código do IBGC propõe que pelo menos um dos conselheiros

apresente bons conhecimentos sobre o assunto[2], sendo recomendável que os demais também disponham de conhecimento mínimo sobre o tema.

Após introdução conceitual sobre riscos, detalha-se, no capítulo 2, o processo de identificação, avaliação e resposta aos riscos. O capítulo 3 visa a auxiliar na implementação de um modelo de GRCorp que respeite o estágio de desenvolvimento e a estratégia de longo prazo de cada organização.

1.1 Conceituação de Risco

O termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar (*to dare*, em inglês). Costuma-se entender "risco" como possibilidade de "algo não dar certo", mas seu conceito atual envolve a quantificação e qualificação da incerteza[3], tanto no que diz respeito às "perdas" como aos "ganhos", com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações:

> "Quando investidores compram ações, cirurgiões realizam operações, engenheiros projetam pontes, empresários abrem seus negócios e políticos concorrem a cargos eletivos, o risco é um parceiro inevitável. Contudo, suas ações revelam que o risco não precisa ser hoje tão temido: administrá-lo tornou-se sinônimo de desafio e oportunidade". (Bernstein, P., p. VII, 3ª edição,1996)

O risco é inerente a qualquer atividade na vida pessoal, profissional ou nas organizações, e pode envolver perdas, bem como oportunidades. Em Finanças, a relação risco-retorno indica que quanto maior o nível de risco aceito, maior o retorno esperado dos investimentos. Esta relação vale tanto para investimentos financeiros como para os negócios, cujo "retorno" é determinado pelos dividendos e pelo aumento do valor econômico da organização.

Empreender significa buscar um retorno econômico-financeiro adequado ao nível de risco associado à atividade. Ou seja, o risco é inerente à atividade de negócios, na qual a consciência do risco e a capacidade de administrá-lo, aliadas à disposição de correr riscos e de tomar decisões, são elementos-chave. Assumir riscos diferencia empresas líderes, mas também pode levá-las a estrondosos fracassos. O resultado das iniciativas de negócios revela que o risco pode ser gerenciado a fim de subsidiar os administradores[4] na tomada de decisão, visando a alcançar objetivos e metas dentro do prazo, do custo e das condições pré-estabelecidas.

2 – A composição do conselho de administração (segundo item 2.17 do Código do IBGC) deve buscar diversidade de experiências, conhecimentos e perfis, de maneira que se possa reunir, dentre outros fatores, experiência em administrar crises e experiência em identificação e controle de riscos.

3 – Risco: evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência. Incerteza: evento futuro identificado, ao qual não é possível associar uma probabilidade de ocorrência. Ignorância: eventos futuros que, no momento da análise, não poderão sequer ser identificados, muito menos quantificados (exemplo: eventos decorrentes de sistemas complexos como o climático – as conseqüências do aquecimento global são imprevisíveis). Faber, Manstetten e Proops, 1996, p. 209-211.

4 – Administradores: conselheiros de administração e diretoria. Também chamada de alta administração.

A aplicação do conceito de risco no contexto empresarial requer a definição de indicadores de desempenho (geração de fluxo de caixa, valor de mercado, lucro, reclamações de clientes, quebras operacionais, fraudes, entre outros) associados a níveis de volatilidade, ou seja, à variação dos resultados em torno de uma média. Essas possibilidades, tanto de ganho como de perda, que podem ter causas de natureza externa (ambiente competitivo, regulatório, financeiro) ou de natureza interna (diferencial tecnológico, controles, capacitações, conduta) são oriundas do contexto em que cada organização atua.

O modelo de GRCorp é um instrumento de tomada de decisão da alta administração que visa a melhorar o desempenho da organização pela identificação de oportunidades de ganhos e de redução de probabilidade e/ou impacto de perdas, indo além do cumprimento de demandas regulatórias.

1.2 Benefícios do Modelo de GRCorp

A adoção de um modelo de GRCorp visa a permitir que a alta administração e demais gestores da organização lidem eficientemente com a incerteza, buscando um balanceamento ótimo entre desempenho, retorno e riscos associados.

A implantação do GRCorp traz vários benefícios para a organização:

a) Preserva e aumenta o valor da organização, mediante a redução da probabilidade e/ou impacto de eventos de perda, combinada com a diminuição de custos de capital que resulta da menor percepção de risco por parte de financiadores e seguradoras e do mercado em geral;

b) Promove maior transparência, ao informar aos investidores e ao público em geral os riscos aos quais a organização está sujeita, as políticas adotadas para sua mitigação, bem como a eficácia das mesmas;

c) Melhora os padrões de governança, mediante a explicitação do perfil de riscos adotado, em consonância com o posicionamento dos acionistas e a cultura da organização, além de introduzir uma uniformidade conceitual em todos os níveis da organização, seu conselho de administração e acionistas.

Além dos benefícios listados acima, a implementação de um modelo de GRCorp eficaz apresenta ainda vários outros resultados positivos para a organização:

d) Desenho de processos claros para identificar, monitorar e mitigar os riscos relevantes;

e) Aprimoramento das ferramentas de controles internos (sistemas de controles) para medir, monitorar e gerir os riscos;

f) Melhoria da comunicação entre as áreas da organização;

g) Identificação e priorização dos riscos relevantes (exposição líquida, já considerando os impactos interrelacionados e integrados a diversos tipos de riscos);

h) Definição de uma metodologia robusta para mensurar e priorizar riscos;

i) Definição e implementação do modelo de governança para gerir a exposição (fóruns de decisão, políticas e processos e definição de alçadas);

j) Identificação de competências para antecipar riscos relevantes e, se for o caso, mitigá-los após uma análise custo-benefício;
k) Melhor entendimento do posicionamento competitivo da organização;
l) Promoção de transparência para os *stakeholders*[5], em relação aos fatores que possam valorizar ou prejudicar a organização.

Em resumo, o GRCorp preserva e agrega valor econômico à organização, contribuindo fundamentalmente para a realização de seus objetivos e metas de desempenho, representando mais do que um mero conjunto de procedimentos e políticas de controle. Além disso, facilita a adequação da organização aos requerimentos legais e regulatórios, fatores críticos para sua perenidade.

5 – *Stakeholders* - partes interessadas: públicos relevantes com interesses pertinentes à organização, ou ainda, indivíduos ou entidades que assumam algum tipo de risco, direto ou indireto, em face da organização. São elas, além dos acionistas, os funcionários, clientes, fornecedores, credores, governos, entre outros.

2 Metodologia da Implantação

Utilizando-se da definição proposta pelo COSO II[6], o GRCorp é um processo desenhado para identificar e responder a eventos que possam afetar os objetivos estratégicos da organização. Suas diretrizes devem ser estabelecidas pelo conselho de administração e as ações decorrentes devem ser implementadas pelos gestores, com o objetivo de prover, com razoável segurança, a realização das metas da organização a partir de um adequado alinhamento da estratégia com o seu apetite a riscos.

Em função desta ampla definição há distintas metodologias e estruturas para o desenvolvimento e implantação do GRCorp. A bibliografia anexa inclui exemplos de metodologias e estruturas que atendem às boas práticas de GRCorp. O Guia se propõe a apresentar aspectos relevantes destas metodologias e estruturas. Os aspectos referentes a estruturas adequadas e de como implementar um modelo de GRCorp são tratados no capítulo 3. Neste capítulo descrevem-se seis etapas fundamentais em uma metodologia de implantação de um modelo de GRCorp: identificação e classificação, avaliação, mensuração, tratamento, monitoramento, informação e comunicação dos riscos.

Para mapear, analisar e principalmente tomar decisões em termos de priorização e alocação de recursos em consonância com o gerenciamento de riscos, recomenda-se a categorização destes eventos por "natureza" e "origem" (na etapa de identificação dos riscos) e por relevância (nas etapas de avaliação e mensuração dos riscos), sempre associados aos objetivos estratégicos da organização.

Cabe realçar que o processo de identificação de riscos (item 2.1) pode resultar na identificação de oportunidades, o que requer a participação de pessoas qualificadas, com visão holística dos negócios da organização nos seus diferentes níveis. Os riscos corporativos identificados devem ser conhecidos por toda a organização e, portanto, devidamente comunicados pela alta administração.

Após a identificação dos riscos, torna-se necessário adotar uma métrica que permita a avaliação da relevância dos mesmos através de informações relacionadas à sua exposição e correspondentes fontes de incertezas. Para determinar a relevância dos riscos deve-se avaliar seu impacto (não apenas no desempenho econômico-financeiro do período, mas também o impacto intangível) e a probabilidade de ocorrência (item 2.2).

Uma vez definidos os objetivos estratégicos da organização, estes são traduzidos num conjunto de planos e metas organizados e ordenados de ações sob os pontos de vista físico e econômico-financeiro. O modelo de GRCorp deve buscar quantificar a incerteza envolvida neste planejamento econômico-financeiro e projetar os resultados da empresa em cenários alternativos de preços, condições macroeconômicas e operacionais (etapa de mensuração dos riscos – item 2.3).

Depois de avaliados e mensurados, deve-se definir qual o tratamento que será dado aos riscos (item 2.4) e como os mesmos deverão ser monitorados (item 2.5) e informados às diversas partes interessadas (item 2.6).

6 – COSO - *The Committee of Sponsoring Organizations of the Treadway Commission* - entidade sem fins lucrativos dedicada, num primeiro momento, à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa. No COSO II amplia-se a abordagem para tratar do GRCorp - ver Anexo A.4.

2.1 Identificação e Classificação dos Riscos

Trata-se da definição do conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis[7]. É importante ressaltar que sempre existirão riscos desconhecidos pela organização. O processo de identificação e análise geral de riscos deve ser monitorado e continuamente aprimorado.

2.1.1 - Associação com os Objetivos Estratégicos e Perfil de Riscos

Os objetivos estratégicos orientam como a organização deverá trabalhar para criar valor a todos que investiram na organização, o que depende crucialmente do perfil de riscos corporativos.

A definição do perfil de riscos é prerrogativa do conselho de administração que, por sua vez, reflete a posição dos acionistas. O perfil de riscos significa em quanta exposição ao risco se aceita incorrer, o que envolve tanto o nível de apetite quanto o de tolerância a riscos[8].

O perfil de riscos deverá estar refletido na cultura da organização e, para isto, cabe ao conselho de administração outorgar um mandato claro para a diretoria administrá-lo. A implantação de um modelo de GRCorp requer o envolvimento ativo de ambos (conselho de administração e diretoria), aprimorando o processo de tomada de decisão da organização, tanto no contexto da elaboração do seu planejamento estratégico, como na sua execução e monitoramento.

Para determinar o perfil de riscos de uma organização são necessárias definições claras de indicadores de desempenho e índices de volatilidade, divididos em dois grupos: um de natureza financeira (valor de mercado, geração de caixa operacional, distribuição de dividendos, etc.) e outro de natureza qualitativa (transparência, idoneidade, reconhecimento de marca, ambiente de trabalho, responsabilidade socioambiental, etc.).

2.1.2 - Categorização dos Riscos

Dentre os vários critérios alternativos para a classificação dos riscos, há dois componentes que se inter-relacionam: Pessoas – principalmente como causas – e a Reputação – principalmente como conseqüência – do bom ou mau gerenciamento dos riscos.

O risco associado às Pessoas é um componente causal presente na grande maioria dos riscos da

7 – "Ativos intangíveis" podem ser entendidos como os ativos e métodos responsáveis pela diferença entre o *market value* (valor de mercado) e o *book value* (valor contábil) da organização. São direitos, sem representação física, que dão à organização uma posição exclusiva ou preferencial no mercado, ou seja, contribuem para o seu valor econômico. Exemplos: carteira de clientes, reputação, relacionamentos, imagem, processos, capacidade de inovação, softwares, marcas e patentes, direitos autorais, licenças, concessões, pesquisa e desenvolvimento, etc.

8 – Enquanto "apetite ao risco" está associado ao nível de risco que a organização pode aceitar na busca e realização de sua missão/visão (análise *ex-ante*), "tolerância ao risco" diz respeito ao nível aceitável de variabilidade na realização das metas e objetivos definidos (atividade mais associada ao monitoramento, *ex-post*).

organização. Por exemplo, a falha na formulação de objetivos claramente entendidos, aceitos e positivamente concatenados dentro da organização como um todo, é um risco que acarreta perda de sinergia e valor empresarial. Por outro lado, a eficácia e eficiência na formulação e/ou execução desses objetivos acarretarão ganho de sinergia e de valor empresarial.

Os eventos que podem atingir criticamente a Reputação da organização – em geral denominados "risco reputacional" ou de "imagem" – na verdade não se constituem num tipo específico de risco, mas sim numa conseqüência do mau gerenciamento dos riscos que se torna público. Exemplo: o impacto negativo sofrido por uma empresa de marca valiosa acusada de práticas tais como o uso de material tóxico para produção de bens, contratação de fornecedores com práticas trabalhistas condenáveis, etc. O impacto negativo sofrido por essa empresa, de marca forte, pode causar impacto positivo nas empresas concorrentes.

Não há um tipo de classificação de riscos que seja consensual, exaustivo e aplicável a todas as organizações; a classificação deve ser desenvolvida de acordo com as características de cada organização, contemplando as particularidades da sua indústria, mercado e setor de atuação. Por exemplo: os estoques de materiais de consumo são menos relevantes para um banco do que para uma indústria, onde pode representar um dos principais fatores de risco. Analogamente, as variáveis relacionadas ao "risco de mercado"[9] são cruciais para um banco e podem não ser tão relevantes para determinada organização manufatureira.

Uma das formas de categorização dos riscos consiste em desenhar uma matriz que considere a origem dos eventos, a natureza dos riscos e uma tipificação dos mesmos, conforme ilustrado hipoteticamente na Figura 1 abaixo:

		Tipos	Natureza dos Riscos		
			Estratégico	Operacional	Financeiro
origem dos eventos	Externo	Macroeconômico			
		Ambiental			
		Social			
		Tecnológico			
		Legal			
	Interno	Financeiro			
		Ambiental			
		Social			
		Tecnológico			
		Conformidade			

Figura 1: Exemplo de Categorização de Riscos

9 – Risco de mercado é a denominação utilizada no sistema financeiro para o tipo de risco associado a perdas no valor da carteira de ativos e passivos (incluindo derivativos) advindas de oscilações de preços de ações, *commodities*, moedas e taxas de juros.

A classificação deve ser feita observando-se algumas diretrizes, normalmente encontradas na literatura sobre gerenciamento de riscos.

2.1.2.1 - Origem dos Eventos

É importante determinar a origem dos eventos (externos ou internos), pois auxilia na definição da abordagem a ser empregada por parte da organização.

2.1.2.1.1 - 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.

2.1.2.1.2 - 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.

2.1.2.2 - Natureza dos Riscos

Igualmente importante é classificar a natureza dos riscos, o que permite sua agregação de uma forma organizada e de acordo com a sua natureza - estratégica, operacional ou financeira - em função da(s) área(s) da organização que é(são) afetada(s) pelos eventos. Cabe mencionar que os riscos podem pertencer a categorias distintas e em alguns casos poderão se encaixar em duas ou até mesmo em todas as categorias concomitantemente. Em alguns segmentos de negócio mais regulados, notadamente os bancos, o órgão regulador estabelece como boa parte dos riscos devem ser agrupados.

2.1.2.2.1 - Riscos Estratégicos

Os riscos estratégicos estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização[10]. 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.

10 – Segundo o estudo *Disarming the Value Killers* (Deloitte, 2006), o risco estratégico é o principal motivador para a perda de valor das ações do grupo de 100 empresas, entre as mil maiores organizações globais, que registraram as maiores quedas no preço das ações em períodos de um mês, ao longo do decênio 1994-2003.

2.1.2.2.2 - Riscos Operacionais

Os 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 negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais.

2.1.2.2.3 - Riscos Financeiros (mercado, crédito e liquidez)

Os riscos financeiros são aqueles associados à exposição das operações financeiras da organização. É o risco 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*.

Existem também outras categorias de risco descritas na literatura relacionadas à combinação ou decorrência de eventos e riscos já descritos, e que não foram gerenciados de forma adequada. É comum que se destaque como uma das categorias – principalmente na literatura dedicada ao cumprimento da Lei Sarbanes-Oxley (Anexo A4) – o risco associado à confiabilidade das informações transmitidas nos relatórios financeiros divulgados pelas organizações.

É igualmente relevante enfocar na qualidade das informações que circulam internamente, destacando-se como categoria de risco as informações para tomada de decisão (estratégicas, financeiras e operacionais). Incertezas sobre a relevância e a confiabilidade nas informações que dão suporte ao processo decisório, que devem estar disponíveis no momento oportuno, podem ser fontes de risco. Deve existir, também, um adequado fluxo de informações que assegure à alta administração que nenhuma informação relevante deixou de ser considerada.

2.1.2.3 Exemplos de Tipos de Riscos

Essa tipificação visa assegurar a definição de uma linguagem comum de riscos dentro da organização, considerando uma descrição ampla dos tipos de risco. Como ilustração, citam-se alguns exemplos abaixo:

2.1.2.3.1 - Tecnologia: representado por falhas, indisponibilidade ou obsolescência de equipamentos e instalações produtivas ou fabris, assim como de sistemas informatizados de controle, comunicação, logística e gerenciamento operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização, ao longo da sua cadeia de valor (clientes, fornecedores, parceiros e unidades regionais). Pode estar também associado a erros ou fraudes, internas ou externas, nos sistemas informatizados ao capturar, registrar, monitorar e reportar corretamente transações ou posições.

2.1.2.3.2 - Ambiental: associado à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos. Nesses casos, a empresa se vê impedida de operar até que a causa do dano ambiental seja remediada, podendo inclusive ser acionada por terceiros em função de lucro cessante, ou tendo que arcar com esforço adicional de reparar o prejuízo causado às comunidades do entorno. Os riscos ambientais não se resumem a catástrofes ou desastres ambientais, mas também ao potencial de efeitos decorrentes do aquecimento global sobre os negócios, que podem inviabilizar novos empreendimentos ou a expansão da capacidade produtiva.

2.1.2.3.3 - Conformidade: relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos. Por incluir as normas e procedimentos internos, apresenta um contexto mais amplo do que o tipo de risco mais usualmente citado, o risco legal/regulatório, decorrente da aplicação da legislação trabalhista, tributária, fiscal, referentes a relações contratuais, regulamentação de mercado e de prestação de serviços.

● ● ● 2.2 Avaliação dos Riscos

Para se definir qual o tratamento que será dado a determinado risco, o primeiro passo consiste em determinar o seu efeito potencial, ou seja, o grau de exposição da organização àquele risco. Esse grau leva em consideração pelo menos dois aspectos[11]: a probabilidade de ocorrência e o seu impacto (em geral medido pelo impacto no desempenho econômico-financeiro do período). Deve-se incorporar também o impacto "intangível" à análise (Figura 2).

A quantificação do grau de exposição nem sempre é trivial, podendo haver interdependência entre os riscos em dois níveis: a) os eventos podem não ser independentes; b) um determinado evento pode gerar "impactos múltiplos", ou seja, efeitos sobre diferentes tipos de riscos, em diversas áreas. Neste caso, o grau de exposição irá depender do impacto financeiro consolidado e da probabilidade conjunta de todos os eventos e deve ser medido quantitativamente de acordo com a metodologia proposta no item 2.3.

Para o caso de eventos independentes que tenham efeito sobre uma única área – como a maior parte dos riscos operacionais - o grau de exposição financeira é calculado simplesmente pelo valor aproximado do impacto financeiro multiplicado pela probabilidade de ocorrência do evento. Os riscos associados a estes eventos podem ser controlados para cada processo isoladamente. Incorpora-se ainda na abordagem o impacto intangível de cada um dos processos, tal como ilustrado nas figuras ao lado.

11 – Metodologias especializadas consideram três como sendo os aspectos fundamentais para uma boa análise da importância e priorização do controle de risco: capacidade de detecção e/ou prevenção, probabilidade e impacto.

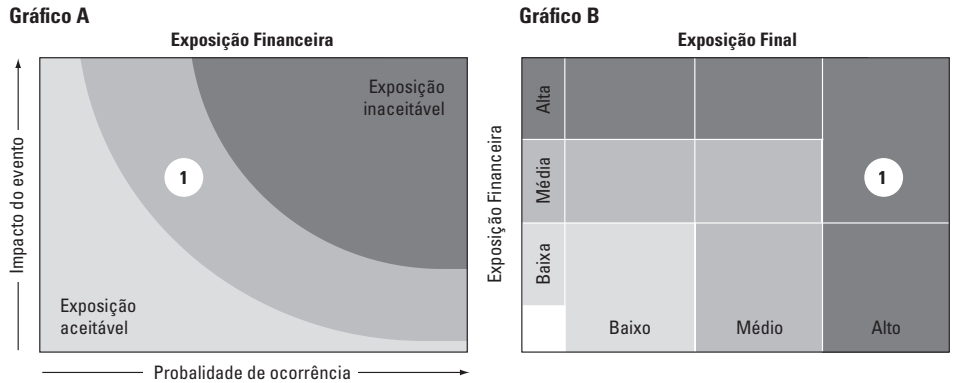

Figura 2 – Exemplo Ilustrativo de Mapa de Avaliação dos Riscos

O Gráfico A, Exposição Financeira, representa o espaço no qual são expostos os eventos de riscos identificados em função do nível da probabilidade de ocorrência (eixo horizontal) e do valor do impacto do evento (eixo vertical). Os tons denotam o grau de importância que se deve dar a cada um dos eventos em função da região que ocupam no gráfico (um evento de alta probabilidade e alto impacto se dispõe na região escura, devendo ser monitorado com muito cuidado).

No Gráfico B, Exposição Final, a **exposição financeira** mensurada no eixo vertical já é o resultado do impacto multiplicado pela probabilidade (Gráfico A). A partir de então, incorpora-se o impacto intangível de cada um dos eventos. O evento 1, que numa primeira análise foi classificado como de média importância (região intermediária no Gráfico A), caso tenha um impacto intangível alto, passa a se enquadrar na região escura no Gráfico B, pois a Exposição Final (Exposição Financeira + Impacto Intangível) é considerada alta.

A elaboração de um Mapa de Avaliação dos Riscos, tal como ilustrado na figura 2, é uma etapa fundamental na priorização do gerenciamento de riscos e na definição de tratamento que deve ser dado a cada um dos riscos identificados (vide item 2.4).

2.3 Mensuração dos Riscos (cálculo do impacto financeiro consolidado)

Uma primeira abordagem para o gerenciamento de riscos pode adotar uma visão mais qualitativa sobre os objetivos estratégicos da organização e os impactos dos eventos de riscos sobre eles (avaliação aproximada da "exposição" alta, média ou baixa, tal como ilustrado na Figura 2). Entretanto, uma vez definido o direcionamento estratégico da organização, este pode ser traduzido em termos quantitativos (objetivos, indicadores de desempenho e metas financeiras) que orientarão o seu planejamento (projeção do orçamento e do plano plurianual).

A atividade de planejamento envolve detalhar, além de outros dados, as receitas e as despesas operacionais, os custos, investimentos e o fluxo de caixa projetado. Para isto é necessário que se projetem cenários sobre as tendências de mercado, trajetórias das variáveis macroeconômicas e financeiras, bem como as premissas operacionais. Consolida-

se, assim, um conjunto organizado e ordenado de planos e metas das ações, sob o ponto de vista físico, econômico e financeiro. O modelo de GRCorp deve buscar quantificar as incertezas envolvidas na fase de planejamento e projetar os resultados da organização em cenários alternativos de preços, condições macroeconômicas e operacionais.

O impacto financeiro consolidado dos riscos na organização pode ser medido quantitativamente em termos da variação potencial do seu valor econômico, fluxo de caixa e resultado econômico, através de uma metodologia que se denomina "planejamento sob incerteza". Para viabilizar tal quantificação é necessário que a organização (i) tenha o seu negócio modelado em alguma ferramenta que possibilite simulações e (ii) seja capaz de gerar cenários das principais variáveis e consistentes entre si.

A modelagem passa pela identificação detalhada de cada um dos fatores que afetam as transações e indicadores de desempenho da organização, incluindo todos os tipos de riscos identificados, e pela determinação da dinâmica de impacto de cada uma das operações nas contas de resultados.

A geração de cenários envolve o conhecimento e previsões de cada área estratégica da organização e deve expressar a evolução conjunta das variáveis. A área financeira pode traçar previsões para as variáveis macroeconômicas; a área de crédito, para a inadimplência de cada tipo de cliente; a área comercial, para as vendas; e estas, em conjunto com a de planejamento, para os preços, índices de consumo, eficiência, capacidade, etc. Associando-se probabilidades aos cenários gerados, é possível quantificar o risco e estimar a probabilidade de que qualquer métrica de desempenho fique abaixo das metas orçadas em cada período (ex.: geração ou necessidade de caixa, resultado contábil, etc.). É recomendável buscar a identificação e o gerenciamento dos riscos integralmente, não apenas os riscos isolados, mas também os riscos múltiplos e comuns a diferentes áreas[12].

O processo de GRCorp passa a envolver, a partir de então: o monitoramento das exposições, a avaliação antecipada do impacto de novas operações ou diferentes cenários de mercado e a comparação com os resultados efetivos, para identificação das fontes de desvio e reavaliação do modelo. Obtém-se, assim, maior autoconhecimento e, conseqüentemente, um processo decisório antecipado de redução de perdas e aumento de ganhos, como também uma previsibilidade maior para os resultados futuros da organização.

2.4 Tratamento dos Riscos[13]

Depois de identificados, avaliados e mensurados, deve-se definir qual o tratamento que será dado aos riscos. Na prática, a eliminação total dos riscos é impossível. Nesse contexto, a elaboração de um mapa de riscos (tal como o esboçado na Figura 2) apóia a priorização e visa direcionar os esforços relativos a novos projetos e planos de ação elaborados, a fim de minimizar os eventos que possam afetar adversamente e maximizar aqueles que possam trazer benefícios para a organização. É recomendável alinhar a estrutura de controles

12 – Para efeito de ilustração de uma situação em que os impactos são múltiplos, podemos avaliar o efeito do evento "variação da cotação do dólar" em uma organização que tenha tanto contratos comerciais quanto financeiros "dolarizados". Caso haja aumento da cotação da moeda norte-americana, tanto o contrato financeiro como o comercial serão afetados e deve-se determinar a exposição consolidada da organização à taxa de câmbio, que não é independente de outros eventos, tais como mudanças na trajetória da taxa de juros, no preço da matéria-prima, preço do produto vendido, etc.

13 – Os termos "tratamento dos riscos" ou "resposta aos riscos" são usados indistintamente ao longo deste guia.

internos aos objetivos estratégicos e ao nível de exposição desejado pela organização. A alta administração poderá determinar seu posicionamento frente aos riscos, considerando seus efeitos, grau de aversão e resposta, complementada por uma análise de custo-benefício.

As várias alternativas para tratamento dos riscos são descritas abaixo, iniciando-se pelo dilema básico: evitar ou aceitar o risco.

2.4.1 - Evitar o Risco: decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Exemplo: uma organização decide se desfazer de uma unidade de negócios.

2.4.2 - Aceitar o Risco: neste caso, apresentam-se quatro alternativas: reter, reduzir, transferir/ compartilhar ou explorar o risco.

2.4.2.1 - Reter: manter o risco no nível atual de impacto e probabilidade. Exemplo: a diretoria da empresa decide nada investir em melhorias da área de informática, assumindo que as perdas e erros atualmente sabidos e esperados de informações internas para o processo de decisão e de gestão são (riscos) toleráveis.

2.4.2.2 - Reduzir: ações são tomadas para minimizar a probabilidade e/ou o impacto do risco. Exemplo: uma organização financeira identificou e avaliou o risco de seus sistemas permanecerem inoperantes por um período superior a três horas e concluiu que não aceitaria o impacto dessa ocorrência. A organização investiu no aprimoramento de sistemas de auto-detecção de falhas e de *backup* para reduzir a probabilidade de indisponibilidade do sistema.

2.4.2.3 - Transferir e/ou Compartilhar: atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco. Exemplo: uma concessionária de energia elétrica identificou e avaliou os riscos de falhas naturais com danos elétricos em seus equipamentos turbo-geradores e de potência de grandes usinas. Após analisar a melhor estratégia a ser adotada no que tange às despesas possíveis com franquia *vis-à-vis* os prêmios de risco a serem contratados, constitui-se um seguro destes equipamentos junto ao mercado, transferindo este risco operacional categorizado como de alto impacto e baixa freqüência, inerente ao processo de operação e manutenção.

Devem ser transferidos por meio de seguro os riscos tidos como catastróficos (riscos de baixa freqüência e alta severidade), os riscos de alta freqüência que provoquem cumulativamente perdas relevantes e todos aqueles cujo custo de transferência seja inferior ao custo de retenção. Os custos de seguro obtidos no mercado podem subsidiar a decisão sobre retenção *versus* transferência dos riscos. Além de identificar os riscos que deseja transferir, os gestores de seguros precisam conhecer profundamente a dinâmica das operações da organização e o fluxo de informações que garantirá a adequação do contrato de seguro por toda a vigência das apólices, normalmente de

12 meses. A transferência do risco não necessariamente elimina todas as potenciais perdas e, por isto, é necessário dispor de um adequado plano de contingência (Anexo B).

2.4.2.4 - Explorar: aumentar o grau de exposição ao risco na medida em que isto possibilita vantagens competitivas. Exemplo: uma empresa produtora de petróleo usa as informações sobre o mercado futuro para especular no mercado de derivativos, aumentando sua exposição ao preço da *commodity*.

2.4.3 - Prevenção e Redução dos Danos

Os riscos podem ser reduzidos pela prevenção – diminuição da probabilidade de ocorrência e/ou diminuição do impacto financeiro esperado sobre a organização, caso o evento ocorra – e/ou pela remediação – controle dos danos após a ocorrência do evento. Para o risco cujo impacto possa afetar adversamente a continuidade da operação, faz-se necessária a elaboração de um plano de contingência adequado e continuamente testado. Ainda mais amplo do que um plano de contingência, as organizações devem avaliar a adoção de uma metodologia para a "Gestão da Continuidade de Negócios" (Anexo B).

As decisões sobre evitar, reter, reduzir, transferir ou explorar riscos estão baseadas na avaliação do impacto dos mesmos sobre os indicadores de desempenho escolhidos e sobre a imagem da organização vis-à-vis os custos de se estabelecerem controles internos.

Um dos objetivos da GRCorp é buscar um nível confortável e balanceado de retenção, redução, exploração e transferência de riscos, adequado a seu apetite definido estrategicamente, envolvendo os objetivos, os riscos respectivos e os controles internos. Da mesma forma, pode haver critérios distintos para enfocar o conceito e práticas de controles internos, que quando acentuados podem gerar custos, muitas vezes excessivos. Na questão do equilíbrio riscos *versus* controles *versus* custos, são muito utilizadas as "melhores práticas" aplicáveis aos tipos específicos ou categorias de risco, segmento de negócios ou tecnologias em questão. As melhores práticas são geradas e disseminadas por institutos independentes, internacionais ou nacionais, associações de indústria ou profissionais e organismos de normatização e por entidades regulatórias, tais como as citadas nos Anexos.

Desta forma, a organização terá uma resposta específica para cada evento significativo. Deverão ser avaliados e monitorados os impactos positivos e negativos da ocorrência dos eventos, considerando:

- **Risco inerente:** risco natural; ausência de qualquer ação que a direção possa realizar para alterar a probabilidade de ocorrência ou de impacto.
- **Risco residual:** resultante do processo de tomada de ações e aplicação das melhores práticas de controles internos ou da reposta da organização ao risco.

2.4.4 Capacitação

Na avaliação dos riscos deve-se considerar a capacitação da organização em lidar com os mesmos, o que significa ser capaz de identificá-lo, antecipá-lo, mensurá-lo, monitorá-lo e, se for o caso, mitigá-lo. Como exemplo, um incêndio pode ser classificado como um evento de alta magnitude para uma organização do setor florestal. Porém, se a organização possui forte capacitação interna para prevenir e

controlar um incêndio, o evento, inicialmente classificado como de alto impacto, pode ser reclassificado para médio ou baixo impacto.

A avaliação da capacitação se dá em duas dimensões principais: pessoas e processos. O exercício de avaliação de capacitação requer uma análise comparativa às melhores práticas, com a identificação de eventuais lacunas de capacitação. Uma vez definido o grau de tolerância ao risco da organização, deve-se adotar um plano de ação para eliminar as lacunas inaceitáveis para assegurar um gerenciamento de riscos eficaz.

● ● ● 2.5 Monitoramento dos Riscos

Cabe à alta administração a avaliação contínua da adequação e da eficácia de seu modelo de GRCorp. Este deve ser constantemente monitorado, com o objetivo de assegurar a presença e o funcionamento de todos os seus componentes ao longo do tempo.

O monitoramento regular ocorre no curso normal das atividades gerenciais. Já o escopo e a freqüência de avaliações ou revisões específicas dependem, normalmente, de uma avaliação do perfil de riscos e da eficácia dos procedimentos regulares de monitoramento. Vulnerabilidades e deficiências no GRCorp devem ser relatadas aos níveis superiores de gestão e, dependendo da gravidade, reportadas à alta administração.

De um modo geral, os controles internos se estruturam em controles gerais e atividades de controles específicos, como por exemplo, reconciliações e confirmações de posições ou fluxos contábeis, procedimentos de testes, etc. Uma das metodologias para dar suporte a este processo de avaliação é o uso de Matrizes de Controles de Riscos, que evidenciam os objetivos e os riscos associados. Estas atividades de controle têm o propósito de determinar em que proporção, através de distintos atributos, os objetivos considerados relevantes pela administração estão sendo efetivamente gerenciados.

A alta administração deve dedicar especial atenção e fornecer diretrizes que orientem:[14]

- a extensão e o conteúdo da documentação formal relativa a GRCorp na organização: manuais de políticas e procedimentos, organogramas, descrições de funções e responsabilidades, instruções operacionais, diagramas de fluxo, resultados de avaliações, análises e testes realizados;
- o relato, a documentação interna e externa (quando aplicável) de deficiências encontradas, assim como, o respectivo nível de ameaça ou exposição, percebida, potencial ou real, e oportunidades associadas para reforço ou revisão dos controles utilizados; e
- o conteúdo dos relatórios relativos a GRCorp e os níveis de informação estratégica: significância de problemas ou fatos anormais, princípios da cultura, implicações práticas e comportamentais, informação aos níveis superiores, laterais, diretoria, conselho de administração, comitê de auditoria, auditores e outras entidades externas.

14 – Exemplos práticos, tabelas e relatórios típicos, relativos ao tópico "Monitoramento" podem ser encontrados no COSO II, *Application Techniques*, 09/2004, pp. 85-91. Aos conselheiros e executivos interessados em um aprofundamento no tema gerenciamento de riscos corporativos, no que tange a papéis e responsabilidades específicas típicas, recomenda-se a leitura dos Capítulos 10 (*Roles and Responsibilities*) e 11 (*Limitations of Enterprise Risk Management*) do mesmo documento.

2.6 Informação e Comunicação

A comunicação ágil e adequada com as diversas partes interessadas, acionistas, reguladores, analistas financeiros e outras entidades externas tem a finalidade de permitir avaliações mais rápidas e objetivas a respeito dos riscos a que está exposta a organização. O conteúdo da comunicação com o ambiente externo e interno reflete as políticas, a cultura e as atitudes desejadas e valorizadas pela alta administração.

Devem ser veiculadas a filosofia e a abordagem do GRCorp na organização, assim como delegações claras de responsabilidade e autoridade. A divulgação de processos e procedimentos deve alinhar atitudes e reforçar a cultura da organização. Mecanismos devem ser implementados e geridos de modo a estimular, e não a reprimir, a comunicação de desvios ou suspeitas de violações dos códigos de conduta ou dos princípios de ordem ética da organização por todos os colaboradores, como por meio de exemplos e pelo reforço de atitudes positivas pela alta administração. Entre outros aspectos, devem ser veiculados de forma eficaz:

- A importância e a relevância de um gereciamento efetivo dos riscos corporativos;
- Os objetivos da organização neste domínio;
- O apetite e a tolerância a riscos da empresa;
- Uma linguagem comum para o assunto "riscos";
- As funções e responsabilidades dos diferentes componentes do modelo de GRCorp.

O sistema de GRCorp exerce um papel fundamental como instrumento para a homogeneização de linguagem, possibilitando: (i) relatórios direcionados para os diversos níveis de gestão; (ii) e o estabelecimento de um canal claro de comunicação, em duas vias, entre a diretoria e o conselho de administração. Este canal é o instrumento pelo qual o conselho irá orientar a gestão da diretoria em termos de limites de exposição ao risco e também receber análises qualitativas e quantitativas quanto aos riscos identificados, oportunidades e retornos esperados das diversas operações sob análise.

Com relação à comunicação externa, o aumento da transparência para o mercado sobre os mecanismos de gerenciamento de riscos adotados pela organização constitui-se num diferencial, mesmo quando se trata de uma obrigação legal.

Deve-se considerar que entidades regulatórias do exterior e do Brasil (SEC - Securities and Exchange Commission, CVM - Comissão de Valores Mobiliários, Banco Central do Brasil, etc.) estabelecem níveis de divulgações em notas explicativas às demonstrações financeiras sobre gerenciamento de riscos de um modo amplo ou sobre determinadas contas ou transações[15].

15 – Exemplos práticos, tabelas, relatórios, diagramas e gráficos típicos, relativos ao tópico "Informação e Comunicação", também podem ser encontrados no documento COSO II, 2004, pp.67-84.

3

Implementação e Estruturas Adequadas para o Gerenciamento de Riscos

3 Implementação e Estruturas Adequadas para o Gerenciamento de Riscos

Não existe uma única forma para implementar um modelo de GRCorp, nem uma única estrutura adequada para tal, dependendo de uma análise custo-benefício em função do porte, especificidades e nível de complexidade de cada organização. Uma organização que lida fortemente com *commodities* negociadas em bolsa de valores e que apresenta uma gestão ativa do seu caixa, ou uma estrutura complexa de dívidas e operações envolvendo o mercado de derivativos, por exemplo, pode requerer sistemas de controle de riscos financeiros sofisticados.[16]

Por outro lado, para fazer frente aos riscos operacionais, não se pode comparar os esforços e recursos que uma grande empresa sujeita à adoção da Lei Sarbanes-Oxley (SOX)[17] com as exigências e necessidades das pequenas empresas.

O importante é introduzir na organização a prática de tratar crítica, qualitativa e quantitativamente os riscos, identificando-os, avaliando-os, tratando-os e calculando seus impactos de uma forma integrada. A implantação de um modelo de GRCorp é um processo de longa duração, que deve ser continuamente aprimorado, dinâmico, interativo e integrado ao processo de planejamento estratégico da organização.

O item 3.1 trata da implementação do modelo de GRCorp, descrevendo a formulação da arquitetura para o GRCorp. O item 3.2 aborda algumas tendências em termos de estrutura funcional e o item 3.3 revisa o papel do conselho de administração no processo de GRCorp.

3.1 Arquitetura para o GRCorp

Para implantar um modelo de GRCorp e promover uma cultura de gerenciamento de riscos na organização deve-se elaborar uma arquitetura para facilitar e viabilizar o gerenciamento do risco propriamente dito, cuja concepção e implementação trazem inúmeros benefícios para a organização, tais como:

- Aderência dos processos internos ao perfil de riscos estabelecido pelo conselho de administração;
- Clareza quanto às regras de governança para gerir a exposição;
- Endereçamento de lacunas de capacitação de pessoas, processos e sistemas;
- Implementação de sistemas de controles eficazes.

16 – Ver Anexo A.2.

17 – Ver Anexo A.4.

Pode-se dividir a formulação da arquitetura para o GRCorp em cinco dimensões distintas que devem girar em torno e se condicionar aos objetivos estratégicos e metas de desempenho da organização. Abaixo, listam-se as questões que devem ser abordadas com referência aos objetivos e metas e em cada uma das dimensões da arquitetura de risco identificadas:

Objetivos estratégicos e metas de desempenho:

- Os objetivos estratégicos e metas de desempenho estão definidos, comprometidos e gerenciados?
- A gestão dos objetivos e das metas estratégicas norteia as prioridades dos riscos, seus respectivos controles e dos demais componentes da arquitetura de risco?
- As mudanças no ambiente de negócios são antecipadamente gerenciadas em termos de objetivos, metas, riscos e controles?

3.1.1 Processos Críticos (para o GRCorp)

a) Quais são os macroprocessos identificados como relevantes na fase de levantamento dos riscos?
b) Quais são os princípios que irão nortear eventual redesenho dos processos?
c) Qual é o mecanismo para se descontinuar e/ou criar processos novos a partir da implantação do modelo de GRCorp?
d) Quais são as ações críticas para mitigar os riscos relevantes?

3.1.2 Governança de Gerenciamento de Riscos (ver 3.3)

a) Quais são os fóruns de decisão envolvidos?
b) Quais são os papéis e responsabilidades desses fóruns?
c) Qual é a composição desses fóruns?
d) Quais são as alçadas?
e) Quais são as políticas necessárias para tomada de decisão ágil e eficaz?

3.1.3 Organização e Pessoas

a) Existem as capacitações necessárias? Quais são as lacunas? Como endereçá-las?
b) O modelo organizacional facilita a identificação, monitoramento e mitigação dos riscos relevantes?
c) Como está sendo tratada a questão da sucessão de postos/pessoas-chave na organização?

3.1.4 Sistemas de Controle

a) Existem controles adequados para mensurar a exposição?
b) Os relatórios gerenciais facilitam a identificação, monitoramento e mitigação dos riscos?
c) Os sistemas de TI (Tecnologia da Informação) são adequados?

3.1.5 Comunicação

a) Há comunicação adequada com os colaboradores?
b) Existe uniformidade conceitual quanto ao modelo de GRCorp?
c) O perfil de riscos e seus benefícios estão devidamente comunicados para a organização?
d) Há um claro alinhamento entre o perfil de riscos e os valores e cultura corporativa?
e) As responsabilidades e direitos decisórios estão devidamente explicitados e comunicados?
f) Há comunicação adequada com os *stakeholders* externos?

3.2 Estrutura Funcional

Existem várias alternativas para a construção de uma estrutura de gerenciamento de riscos e cada organização deverá desenhar aquela mais adequada ao seu perfil. Observa-se, no entanto, a tendência pela criação de uma unidade responsável por esta nova função. O gerenciamento dos riscos de um determinado processo é uma atividade a ser atribuída aos gestores desse processo, cabendo à unidade executiva responsável pelo GRCorp integrar e orientar os vários esforços, bem como interagir com a alta administração. Esta unidade executiva pode ser um departamento, núcleo, área[18] ou unidade funcional composta por representantes de diversas áreas (comitê)[19]. Caso se crie um comitê executivo para o gerenciamento de riscos, este deve ter função ativa no processo decisório diário da organização, apoiando a tomada de decisões mais difíceis ou complexas. Sugere-se que o comitê executivo seja coordenado pelo presidente ou diretor executivo da organização e tenha como membros o diretor financeiro, os diretores operacionais, assessores e outros responsáveis pelas áreas envolvidas com riscos. Esta composição depende do nível de complexidade das operações da organização.

É importante realçar a distinção entre as funções deste comitê executivo para o gerenciamento de riscos e as funções de um comitê de riscos do conselho de administração. Este último teria uma abordagem mais vinculada à estratégia da organização, sendo que em alguns casos o comitê de auditoria assume esta função. Ver Anexo C.

3.3 O Gerenciamento de Riscos e o Conselho de Administração

O conselho de administração deve ser o responsável por determinar os objetivos estratégicos e o perfil de riscos da organização. Definir seu perfil consiste em identificar o grau de apetite a riscos da organização, bem como as faixas de tolerância a desvios em relação aos níveis de riscos determinados como aceitáveis. O conselho de administração deve estabelecer também a política de responsabilidade da diretoria em: (i) avaliar a quais riscos a organização pode ficar exposta; e (ii) desenvolver procedimentos para administrá-los.

O papel fundamental de implementar uma sólida estrutura de gerenciamento de riscos e controle é

18 – Nas pequenas e médias empresas, a função pode ser exercida por uma única pessoa.

19 – Os comitês (do conselho de administração) se propõem a estudar assuntos de sua competência e preparam propostas para o conselho de administração, do qual normalmente fazem parte. É muito comum existirem nas organizações diversos comitês executivos que, não necessariamente, contam com a presença de membros do conselho de administração.

delegado aos gestores, com o comitê de auditoria (ou instância que desempenha sua função), em nome do conselho de administração, exercendo a função de supervisão.

Como ponto de partida para análise do modelo de GRCorp praticado atualmente pela organização, ou para instituí-lo, sugere-se que o conselho de administração discuta o tema com a diretoria, abordando pontos tais como os elencados a seguir.

Este item serve, desta forma, como uma conclusão, ao revisar os temas abordados ao longo do Guia (em seguida a cada pergunta sugerida, é feita referência ao item correspondente neste Guia).

Em um primeiro momento deve-se indagar sobre itens que revelem o escopo e a maturidade do modelo de GRCorp existente na organização, conforme sugerido a seguir:

a) A organização considera os riscos de maneira global e integrada ao planejamento estratégico? (vide 2.1.1)
b) Os riscos são considerados de maneira ampla (não apenas os riscos financeiros)? (vide 2.1.2)
c) Os ativos intangíveis são considerados (ex: reputação)? (vide 2.1.2)
d) Que métodos e ferramentas utilizam? (vide 2.3 e 2.4.3)
e) Como se controlam os riscos financeiros? (vide 2.3 e Anexo A.2)
f) A organização tem o gerenciamento de riscos como parte integrante da agenda de seus gestores e comitês? (vide 3.2)
g) A quem a gerência/unidade de risco se reporta? (vide 3.2)
h) Como é disseminada a cultura de gerenciamento de riscos? (vide 2.6)
i) As pessoas-chave são preparadas e cumprem seus papéis? (vide 2.4.4 e 3.1.3)

s) Como são estabelecidos os limites de tolerância a riscos que pautam os controles e a supervisão das operações?
t) O conselho de administração reflete explicitamente sobre riscos em seus processos decisórios?

Essas reflexões são necessárias para que os membros do conselho de administração, além de evitar penalidades e conseqüências danosas à organização e aos seus próprios membros, atentem para os riscos que devem ser por ele analisados e para o seu papel dentro da estrutura de GRCorp da organização, uma vez que a preocupação com riscos é fundamental para que ele cumpra bem a sua missão de "proteger e valorizar o patrimônio, bem como maximizar o retorno do investimento" (conforme item 2.3 do Código do IBGC).

4

Referências

4 Referências

BASILÉIA II (Basel II): *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, 2005. Disponível em: http://www.bis.org .

BERNSTEIN, P. **Desafio aos deuses: a fascinante história do risco**, 3ª edição,Campus, Rio de Janeiro, 1996.

COSO Report, *Internal Control – Integrated Framework*, 1997. Disponível em: http://www.coso.org

COSO II, *ERM - Enterprise Risk Management*, 2004. Disponível em: http://www.erm.coso.org

DELOITTE Research, *Disarming the Value Killers*, 2005. Disponível em: http://www.deloitte.com/dtt/article/0,1002,sid%253D2002%2526cid%253D72667,00.html. Consulta em 05/10/2006.

GALESNE, F. e LAMB, R., **Decisões de Investimentos da Empresa**, Atlas, 1999.

IBGC, **Código das Melhores Práticas de Governança Corporativa**, 3ª edição. São Paulo, 2004.

SARBANES-OXLEY ACT, *Public Company Accounting Reform and Investor Protection Act of 2002*, EUA, 2002.

4.1 Literatura Relacionada

4.1.1 - Livros

BARALDI, P. **Gerenciamento de Riscos Empresariais**. Rio de Janeiro: Elsevier (Editora Campus), 2ª edição revista e ampliada, 2005.

BREALEY, R. e MYERS, S., **Financiamento e Gestão de Risco**, Bookman, 2005.

BRIGHAM, E.F., GAPENSKI, L.C. e EHRARDT, M.C., **Administração Financeira, Teoria e Prática**, Atlas, 2001.

CROUHY M., GALAI D., MARK R., **Gerenciamento de risco: abordagem conceitual e prática: uma visão integrada dos riscos de crédito e de mercado**. Rio de Janeiro: Qualitymark: São Paulo: SERASA, 2004.

FABER, M., MANSTETTEN, R. e PROOPS, J., **Ecological economics: concepts and methods**. Cheltenham: Edward Elgar Publishing Ltd. 1996.

GRINBLAT, M. e TITMAN, S., **Mercados Financeiros e Estratégia Corporativa**, Bookman, 2005.

JORION, P., **Value-at-Risk: A nova fonte de referência para a gestão do risco financeiro**, BM&F, 2003.

NEIL D., **Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk**, 1ª Edição, Mc Graw Hill.

SCOTT H., **Risk Management and Insurance**, 2ª Edição, Mc Graw Hill.

VAUGHAN E., VAUGHAN T., **Fundamentals of Risk and Insurance**, 9ª Edição, Wiley, 2003.

4.1.2 - Artigos e Documentos Técnicos

BACCI, L. C., ***Gerenciamento corporativo de riscos***. São Paulo: TCC/FGV, 2003.

COCURULLO, A., *COSO Report e ERM – Comparação entre duas metodologias.* Risk Update, 10ª Edição, ano 2, janeiro de 2006.

_____, *Gestão de riscos corporativos,* 3ª Edição, São Paulo: Scortecci, 2004. 230 p., ISBN 85-7372-766-7

COCURULLO, A., VANCA, P., *A importância da gestão de riscos nos processos de auditoria*. São Paulo: IBRACON - no. 286 – mai./jun. 2002

CARVALHO, E.J.L, *FMEA: Metodologia para Auto – Avaliação - Risco Operacional*. Risk Update, 8ª Edição, ano 1, outubro de 2005.

DELOITTE (Consultas em 05/10/2006), *When Corporate Risk Becomes Personal*, Corporate Board Member, Special Supplement, 2005. Disponível em: http://www.deloitte.com/dtt/article/0,1002,sid%253D5604%2526cid%253D91334,00.html. Publicado em 08/02/2006 - site EUA.

_____, *Value-Based EnterpriseRisk Management*, Deloitte Consulting, September 2005. http://www.deloitte.com/dtt/article/0,1002,sid%253D2132%2526cid%253D94647,00.html. Publicado em 14/02/2006 - site EUA.

_____, *ERA - A Guide to Risk in the Organization for the C-Suite and the Boardroom*, Deloitte, August 2005. Disponível em: http://www.deloitte.com/dtt/article/0,1002,sid=2132&cid=99958,00.html. Publicado em 14/02/2006 - site EUA.

_____, *In the Dark - What boards and executives don't know about the health of their businesses*, A Survey by Deloitte in Cooperation with the Economist Intelligence Unit, October 2004. Disponível em: http://www.deloitte.com/dtt/whitepaper/0,1017,sid%253D1007%2526cid%253D62386,00.html; publicado em 16/01/2006 - global site.

_____, *Assessing the Value of EnterpriseRisk Management*, Economist intelligence Unit, October2004. Disponível em: http://www.deloitte.com/dtt/budget/0,2299,sid%253D20241%2526cid%253D67257,00.html. Publicado em novembro de 2004 - site Deloitte França.

HENRIQUES, J.P., *É preciso gestão estratégica*. Coimbra, Portugal: 1997. Disponível em: http://student.dei.uc.pt

J.P. MORGAN, *RiskMetrics Technical Document*, 1995, Fourth Edition., New York.

LIMA DE PAULO, W., FERNANDES, F.C., RODRIGUES, L.G.B. e EIDT, J., *Controles internos: Uma metodologia de mensuração dos níveis de controles de riscos*, 6º Congresso de Controladoria e Contabilidade – Departamento de Contabilidade e Atuaria – FEA- USP – 2006. Disponível em: www.riskoffice.com.br.

LA ROCQUE, E. e LOWENKRON, A., *Métricas e particularidades da Gestão de Risco em corporações*, Artigos RiskControl - Lista de Riscos nº 4, 2004. Disponível em: http://www.riskcontrol.com.br.

PRICEWATERHOUSECOOPERS (PwC), *Cadernos promocionais sobre gestão de riscos e prestação de serviços profissionais de auditoria e consultoria*. USA: de 2002 à 2006.

ROCCA, C.A., *Volatilidade e Gestão de Risco em empresas não financeiras*, Trabalho apresentado no seminário "Gestão de riscos em empresas não financeiras" promovido pela ABRASCA, realizado na BOVESPA em 19/11/2004. Disponível em: www.riskoffice.com.br.

RISKMETRICS GROUP, *Corporate Metrics*, 1998.

4.1.3 - Algumas Normas Relacionadas ao Tema

AS/NZS HB 203:2004 Environmental Risk Management – Principals and process.

_____, 205:2004 OHS Risk Management Hand Book.

_____, 221:2004 Business Continuity Management.

_____, 240:2004 Guidelines for managing risk in outsourcing utilizing the AS/NZS 4360 process.
_____, 254:2004 Guide to control assurance and risk management.
_____, 4360:2004 Risk Management (Trad.: Gestão de Riscos, Risk Tecnologia, 1ª Edição, Junho de 2003). Risk Management Guidelines – Companion to ASA/NZS 4360:2004.
_____, 4810.1 Medical devices - Risk management - Application of risk analysis.
BS 6079-3 Project Management - Part3: Guide to the management of business related project risk.
BSI - PD6668 Managing Risk for Corporate Governance.
BSI PAS 56:2003 Guide to Business Continuity Management.
CSA Q 850:1997 Risk Management Guidelines for Decision Makers.
IEC 60300-3-9 Risk analysis of technological systems – Application guide.
IEC 62198 Project risk management – Application guidelines.
ISO 10006 Quality management systems – Guidelines for quality management in Projects.
ISO/IEC Guide 51:1999 Safety aspects – Guidelines for their inclusion in standards.
_____, 73:2002 Risk management – Vocabulary - guidelines for use in standards.
JISQ 2001:2001 Guidelines for development and implementation of risk management system.
PCOAB, Public Company Accounting Oversight Board Auditing - Standard 2: disponível em: http://www.pcaobus.org.
ONR 49000 Risk management for organizations and systems -Terms and principles.
_____, 49001 Risk management for organizations and systems -Elements of the risk Management system.
_____, 49002-1 Risk management for organizations and systems, Part 1: Guidelines for risk.
_____, 49002-2 Risk management for organizations and systems, Part 2: Guidelines for the integration of risk management into the general management system.
_____, 49003 Risk management for organizations and systems, - Qualification of the risk manager.
SNZ HB 8669:2004 Guideline for Risk Management in Sport and Recreation.

4.1.4 - Alguns *Websites* Relacionados ao Tema

http://www.airmic.com
http://www.erm.coso.org
http://www.ferma-asso.org
http://www.listaderiscos.com.br/lr/portal/
http://www.orx.org
http://www.pcaobus.org
http://www.rims.org
http://www.risktech.com.br
http://www.rmmagazine.com
http://www.theirm.org

Anexos

● ● ● A1 Introdução

O gerenciamento de riscos é uma prática usual e antiga que faz parte da rotina de qualquer empresário desde tempos muito remotos (vide Bernstein, p. 1996). Uma vasta literatura foi historicamente elaborada para a área de seguros (vide, por exemplo, Vaughan & Vaughan, 2003) e, mais recentemente, o tema entrou em voga e tem se desenvolvido como uma metodologia estruturada a partir de várias vertentes, dentre as quais se destacam: Finanças, Auditoria e Tecnologia da Informação.

A idéia do seguro nos remete a uma época anterior a Cristo, com os seguros de transportes que foi impulsionada pela navegação marítima comercial. Os sucessivos incêndios em Hamburgo (1672 a 1676) coincidem com os primeiros seguros patrimoniais e com a fundação da ainda existente Hamburger Feuerkasse, a mais antiga seguradora do mundo. Pode-se medir a prosperidade da indústria do seguro, iniciada com a Revolução Industrial e sustentada pelo progresso e desenvolvimento do século XX, pelas inúmeras seguradoras e resseguradoras existentes e pelos volumes extraordinários de recursos movimentados por esta indústria.

A criação do *Federal Deposit Insurance Corporation* (FDIC) em 1933 proveu garantias governamentais incondicionais à maioria dos bancos credores. A taxa fixa (sem riscos) das garantias de depósitos auxiliou na diminuição dos requerimentos de capitais de mercados, assegurando aos depositários a garantia do pagamento, mesmo que seus bancos viessem a falir.

A preocupação com a busca de soluções para avaliação de processos e/ou controles internos nas empresas continua. Em 1947 surge a Organização Internacional de Normatização, ISO (*International Organization for Standardization*). Desde então, novas abordagens vêm sendo desenvolvidas com o objetivo de incorporar novos conceitos nas empresas e adequá-las às exigências do mercado e de órgãos reguladores, conforme demonstrado na figura abaixo. Importante ressaltar que o cronograma não tem a pretensão de indicar todas

as metodologias e/ou abordagens disponíveis, mas sim apresentar uma visão histórica de marcos regulatórios importantes surgidos recentemente. A seguir, alguns *links* úteis:

www.acionista.com.br/mercado/fidc.htm
www.bcb.gov.br
www.bis.org/bcbs/index.htm
www.bouzas.com.br/2554_Integral.htm
www.group30.org/home.php
www.ic.coso.org/
www.isaca.org/cobit/
www.iso.org/iso/en/ISOOnline.frontpage
www.pch.gc.ca/progs/em-cr/verif/2003/2003_12/2_e.cfm?nav=0
www.sarbanes-oxley.com/section.php?level=1&pub_id=SEC-Rules

● ● ● A.2 Vertente Financeira

Na indústria financeira, o incentivo a implementar os sistemas de gerenciamento de riscos surgiu, na década de 80, com a preocupação crescente do *Bank of England* e do *Federal Reserve Board* com a exposição dos bancos relacionadas às operações *off-balance-sheet,* conjugados com problemas de empréstimos para os países do terceiro mundo. O *Bank of International Settlements* (BIS) continuou o processo iniciado pelo *Federal Reserve Bank* e pelo *Bank of England* enviando prévias de propostas para os bancos e demandando comentários e sugestões. Os primeiros resultados deste processo vieram em 1988, com o Acordo da Basiléia e suas emendas subseqüentes a partir de 1996.

O primeiro Acordo, de 1988, tinha como foco a alocação de capital para fazer frente a riscos de crédito. A partir de 1993, introduziram-se regras para o "risco de mercado" – (vide definição na nota de rodapé nº 9) – que tem como grande referência a publicação pelo *JP Morgan do RiskMetrics* (vide www.riskmetrics.com) em outubro de 1994. O documento veio em resposta aos grandes desastres financeiros do início dos anos 90 (casos conhecidos como os da Procter & Gamble, Orange Count, Barings, etc) (ver Jorion, p. 2003 no item 4.1.1), e introduziu o conceito de *Value-at-Risk* ("VaR").

O VaR mede a perda potencial do valor de uma carteira com determinada probabilidade num dado intervalo de tempo. A grande vantagem em geral atribuída ao VaR é o de ser uma métrica de risco que consegue num único número resumir todo o "risco de mercado" da instituição. Entretanto, o gerenciamento de riscos em empresas não-financeiras é bem mais complexo. Desde a publicação do *RiskMetrics* observa-se um intenso debate sobre como adaptar o conceito de VaR para estas empresas, e o único consenso atingido foi o de que o VaR não seria suficiente, poia o gerenciamento de riscos em empresas necessariamente envolveria múltiplas facetas, não apenas quantitativas, mas também qualitativas.

O conceito de VaR está muito associado à marcação a mercado de ativos e passivos; e a falta de liquidez dos ativos de uma empresa faz com que a mesma esteja mais preocupada com o fluxo de caixa ou com o resultado em risco do que com o valor presente em risco. Desenvolveram-se, então, conceitos

tais como CfaR (*Cashflow-at-Risk*), EaR (*Earnings-at-Risk*) e PaR (*Profit-at-Risk*). Ver RISKMETRICS GROUP (1998) e LA ROCQUE, E. e LOWENKRON, A. (2004).

Em junho de 1999, o *Basle Committee on Banking Supervision* do BIS, ou Comitê da Basiléia, propôs uma uma nova estrutura para a adequação do capital, cuja publicação substituiu o acordo de 1988. Os objetivos do novo acordo são:

- Promover segurança e equilíbrio no sistema financeiro mediante a manutenção de pelo menos o mesmo nível de capital que os bancos mantêm no sistema atual;
- Aprimorar o nível de competitividade de forma eqüitativa. As novas regras não devem oferecer incentivos para que reguladores em alguns países elaborem regras mais atraentes para impulsionar os investimentos em seus países. Por exemplo, dois bancos com o mesmo portifólio deveriam ter o mesmo capital onde quer que eles estejam atuando;
- Constituir abordagem mais ampla para o gerenciamento de riscos, objetivando aprimorar o Acordo de 1988, mediante a incorporação de novas dimensões de risco (por exemplo, os riscos operacionais);
- Focalizar em bancos que sejam internacionalmente ativos. Os princípios desta abordagem devem ser flexíveis o suficiente para atender instituições financeiras com distintos níveis de complexidade e sofisticação.

Para alcançar estes objetivos, o Comitê da Basiléia propôs uma estrutura apoiada em três pilares: o primeiro trata da adequação do capital regulatório mínimo com base nos riscos de mercado, de crédito e operacionais; o segundo reforça a capacidade dos supervisores bancários em avaliar e adaptar o capital regulatório às condições de cada instituição financeira; e o terceiro atribui à transparência e à divulgação de informações um papel importante e relevante no fomento à disciplina de mercado.

● ● ● A.3 Ramo de Auditoria

Paralelamente a este desenvolvimento pelo ramo financeiro, auditores, contadores e legisladores têm devotado atenção crescente aos controles internos. O Financial Accounting Standards Board (FASB) publicou guias encorajando a divulgação de demonstrações financeiras mais completas, demonstrando o que tem sido feito para mitigar os riscos e o modelo de governança instaurado para o gerenciamento desses riscos entre outras iniciativas.

Um grupo de reguladores e profissionais têm publicado guias importantes relativos aos controles internos e ao gerenciamento de riscos. Dentre os esforços notáveis incluem-se:

- **Relatório COSO (1992):** elaborado previamente pelos contadores profissionais dos Estados Unidos, estabelece padrões para que os controles internos assegurem operações eficientes, relatórios financeiros confiáveis e conformidade legal. Entre os aspectos de controles internos são descritos em detalhes a mitigação e o monitoramento dos riscos. [mais informações sobre o COSO no item A.4]

- **Relatório Cadbury (1992):** o documento inglês recomenda aos diretores que confirmem nos relatórios anuais de suas empresas a revisão da efetividade dos controles internos corporativos.
- **Kon Trag (1994) e Turnbull (1999):** documentos de origem alemã e inglesa, respectivamente, propiciam uma abordagem ampla e robusta para o gerenciamento de riscos. Os conceitos e diretrizes constantes desses documentos assemelham-se aos princípios emanados pelo COSO II – ERM.

Além destas, outras importantes iniciativas foram introduzidas nos últimos dez anos. Como exemplo, o estudo do grupo dos 30 (G-30) publicado em julho de 1993, que propiciou uma abordagem abrangente e avançada para gerenciamento de riscos. O estudo do G-30 provê um guia prático contendo 20 recomendações, relacionadas principalmente ao gerenciamento de instrumentos derivativos.

A.4 Lei Sarbanes-Oxley

Em resposta aos escândalos corporativos do início do século XX (Enron, WorldCom, Adelphia, entre outros), surge em 2002 nos Estados Unidos a Lei Sarbanes-Oxley ("SOX"). Formulada por dois congressistas americanos, Paul Sarbanes e Michael Oxley, enfatizou o papel fundamental dos controles internos e fez com que boas práticas de governança corporativa se transformassem em exigência legal.

A SOX foi aprovada e promulgada pelo Congresso Americano em julho de 2002, afetando todas as empresas americanas e estrangeiras que possuiam títulos e ações negociados em bolsas americanas. Tal lei serviu de base para regulamentações locais ao redor do mundo, colocando em voga toda a metodologia que a área de auditoria vinha desenvolvendo para aprimorar os controles internos. A SOX recomenda e, portanto, não obriga, que o *framework* de controles internos a ser utilizado pelas empresas seja baseado no COSO – *The Committee of Sponsoring Organizations of the Tradeway Commission.*

O COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa.

Seu primeiro objeto de estudo foram os controles internos. Em 1992 publicou o trabalho "Controles Internos – Estrutura Integrada", com o objetivo de auxiliar as entidades corporativas e demais organizações a avaliar e aprimorar seus sistemas de controles internos. Esta publicação (COSO I) tornou-se referência mundial para o estudo e a aplicação dos controles internos.

Em setembro de 2004, foi lançado o documento "Gerenciamento de Riscos Corporativos – Estrutura Integrada". Conhecido como COSO II, busca um foco mais robusto e extensivo no tópico de gerenciamento de riscos corporativos.

Esta metodologia de aplicação dos controles internos e gerenciamento de riscos foi adotada pelo PCAOB – *Public Company Accounting Oversight Board*, que é o órgão criado pela SOX para supervisionar as empresas de auditoria das companhias abertas com títulos negociados nas bolsas de valores americanas. Pode-se dizer que as metodologias propostas pelo COSO tornaram-se uma grande referência para mapeamento e avaliação dos controles internos das empresas que querem se certificar como aderentes aos requisitos da SOX. De acordo com esta metodologia, o controle interno é parte integrante do gerenciamento de riscos corporativos.

A.5 Tecnologia da Informação

No campo da tecnologia da informação constitui referência unânime, embora não-obrigatória, a Norma ISO/IEC 27001, que trata de diretrizes e princípios para a gestão da segurança da informação, em seus diversos aspectos de riscos, vulnerabilidades e mecanismos de controle recomendados.

Da mesma forma, a Norma ISO/IEC 20000 estabelece as bases para a boa gestão dos recursos e serviços de tecnologia da informação, e respectiva mensuração de desempenho, *vis-a-vis* os requisitos das áreas de negócios de qualquer organização.

Ainda no que toca a mitigação de riscos, prevenção e redução de danos relacionados com tecnologia da informação, através de processos, objetivos de controle e indicadores de desempenho, constitui referência essencial o COBIT (*Control Objectives for Information and Related Technologies*), desenvolvido inicialmente pelo ISACA (*Information Systems Audit and Control Association*) e hoje, em sua versão 4.0, publicado e mantido pelo ITGI (*Information Technology Governance Institute*).

A.6 Norma ISO 31000

Encontra-se em estágio de desenvolvimento (em *WD-Working Draft*) a norma ISO 31000: *General Guidelines for Principles and Implementation of Risk Management*. Seu desenvolvimento atribuiu-se a um comitê especial, denominado ISO *Technical Management Board on Risk Management*, composto por delegações de 35 países, formadas por profissionais de diversos setores de atividades como: financeiro, indústria, governança corporativa, segurança, agronegócios, qualidade, meio ambiente, tecnologia, projetos, saúde, defesa e seguros, dentre outros. O ISO/IEC *Guide* 73 também será submetido à revisão como conseqüência dos trabalhos de construção da ISO 31000.

O Brasil, representado pela ABNT (Associação Brasileira de Normas Técnicas), está entre os países participantes e colabora com o desafio de tornar a ISO 31000 uma norma geral de gerenciamento de riscos, através da consolidação de diferentes conceitos e terminologias, da apresentação de diretrizes e princípios para a implementação de estruturas de gerenciamento de riscos aplicáveis às organizações, independentemente de seu tamanho, segmento ou área de atuação.

A finalização dos trabalhos está prevista para 2008. A perspectiva é que, futuramente, as normas ISO das áreas que tratem de gerenciamento de riscos reflitam os mesmos conceitos da ISO 31000.

B Gestão da Continuidade de Negócios

Décadas de esforços empresariais em prevenção e redução de riscos de diversas origens e fontes, principalmente de riscos operacionais, geraram não só experiência significativa neste campo, como também no campo do gerenciamento de impactos adversos e situações de interrupção ou ameaça iminente à continuidade das operações de diversas organizações.

Este corpo de conhecimentos, melhores práticas, habilidades e certificações profissionais constitui hoje a disciplina denominada de Gestão da Continuidade de Negócios, GCN (ou BCM, de *Business Continuity Management*), englobando e consolidando conceitos e práticas, relacionados, desde os anos 80, a planos de contingência, planos de recuperação de desastres, planos de *backup*, resposta a emergências e gerenciamento de crises, entre outros.

O gerenciamento da continuidade de negócios é implementado através da elaboração de Planos de Continuidade de Negócios, PCN's (ou BCP's, de *Business Continuity Plans*) para as diversas situações de risco, em geral residual ou externo, identificadas com base na análise dos impactos para a organização, na avaliação de estratégias de continuidade e dos respectivos custos de implementação *vis-a-vis* as perdas a serem evitadas ou benefícios ou ganhos parciais a serem obtidos.

No desenvolvimento e promoção de melhores práticas de GCN, assim como na certificação de profissionais qualificados, destacam-se, nos Estados Unidos, e com ampla aceitação internacional, o BCI, *Business Continuity Institute* e o DRII, ***Disaster Recovery Institute International***. Estes institutos preconizam, conjuntamente, códigos de ética para profissionais de GCN, diretrizes, estruturas e práticas para a elaboração de PCNs por empresas de quaisquer segmentos.

Na Europa, o BSI (*British Standards Institute*) trabalha na elaboração de um Código de Práticas para Gestão de Continuidade de Negócios, atualmente publicado para consulta na forma de *draft proposal* (DPC BS 25999-1).

Especificamente com relação à tecnologia da informação, além de se aplicarem os princípios gerais de GCN, ou PCNs, são adicionalmente definidos e elaborados Planos de Continuidade de Serviços de TI (PCSTI). Tais planos envolvem, em particular, os conceitos de nível de serviço, objetivos de controle, múltiplos equipamentos, centros de processamento de informações e rotas de comunicações, equipes e procedimentos alternativos de operação, comunicação e relacionamento com a comunidade, autoridades e entidades regulatórias, em função da gravidade ou alcance das perdas ou danos, internos ou externos à organização.

Na elaboração de processos e planos de continuidade de TI, constituem ainda referências nucleares as Normas ISO/IEC 20000 e 27001, assim como o COBIT, anteriormente citados (ver anexo A4).

C Comitê(s) de Riscos[20]

Quando o conselho de administração constitui comitês para melhor desempenhar o seu papel de orientação e supervisão do direcionamento estratégico dos negócios e da ação dos gestores, o "comitê de riscos" do conselho de administração será parte deste e, como tal, o escopo de sua atuação estará voltado para a identificação dos riscos decorrentes das estratégias alternativas sob decisão do conselho de administração.

Caberá ao comitê a discussão e a clara definição do apetite a riscos da organização e a direção adequada a ser sugerida como orientação emanada da alta administração. A este comitê também caberá sugerir os limites de tolerância aos diferentes riscos identificados como aceitáveis pelo conselho de administração. Os limites constituirão a ferramenta para a área executiva conduzir as políticas da empresa.

Uma orientação voltada para a tolerância a riscos poderá ser estabelecida, por exemplo, em termos de percentual de prejuízos aceitáveis para cada linha de negócios; neste caso, aproximando-se o limite de tolerância estabelecido, caberá à área executiva propor ao conselho de administração a saída do negócio, com a liquidação dos ativos ou outra saída semelhante (*stop loss*).

No processo decisório diário, os executivos, sob o comando do principal executivo, ou de outro, como, por exemplo, o titular de uma "diretoria de riscos", ou de uma "gerência de riscos", poderão constituir um "comitê executivo para o gerenciamento de riscos". A esse comitê, de caráter executivo, competiria a função de tomada de decisão, de escolha e implementação de políticas alternativas, como por exemplo, decidir a realização de medidas de proteção *(hedge)* de posições e escolher os parceiros mais adequados à decisão. Nessa situação, o comitê executivo toma decisões dentro dos parâmetros de apetite a riscos definidos pelo conselho de administração e administra e controla as posições com base em parâmetros de tolerância previamente definidos.

A distinção das funções de direcionamento estratégico e das funções executivas deve estar presente na formatação dos comitês, na sua composição, nas agendas de trabalho, evitando-se que, ou se aloquem funções executivas a um comitê do conselho de administração ou se estendam atribuições estatutárias a comitês executivos não-estatutários.

Por outro lado, é importante considerar que o comitê de riscos do conselho de administração terá uma dinâmica de trabalho muito diferente da dinâmica de trabalho de um comitê executivo, uma vez que este poderá se reunir, ou tomar decisões conjuntas quase que diariamente, o que geralmente será impossível (e inadequado) para um comitê do conselho de administração.

20 – Os Comitês (do conselho de administração) estudam assuntos de sua competência e preparam propostas para o conselho de administração, do qual fazem parte. Existem, no entanto, comitês executivos, não necessariamente com a presença de membros do conselho de administração.

A responsabilidade pelo GRCorp será, então, distribuída em uma unidade de apoio do conselho de administração – o Comitê de Riscos – e uma unidade executiva encarregada do processo decisório no gerenciamento de riscos da organização.

Nas organizações que não comportem comitês distintos, constituídos por diferentes membros, será importante desenhar processos de gestão e de governança que segreguem funções estratégicas e funções executivas de forma matricial ou, na impossibilidade desta hipótese, desenhar atribuições para os administradores que segreguem essas funções em instâncias distintas, ou em momentos e reuniões distintos.

D Marco Legal e Regulatório no Brasil

Há no Brasil regulamentações que estão em linha com a SOX e Basiléia. A Comissão de Valores Mobiliários (CVM), através da Instrução nº 220/94, definiu regras relacionadas com controles internos de certa forma similares às impostas pela SOX. Para as instituições financeiras, o Conselho Monetário Nacional instituiu, através da Resolução nº 2554/98 do Banco Central do Brasil, a implementação de "Sistema de Controles Internos" para as atividades desenvolvidas e para os Sistemas de Informações, bem como para garantir o cumprimento das normas legais e regulamentares aplicáveis.

O Banco Central definiu também um conjunto de regras que se constituem na "Basiléia" brasileira:

- Res.2099/1994: risco de crédito
- Res.2606/1999: exposição a moedas;
- Res.2804/2000: risco de liquidez;
- Circular 2972/2001: risco pré-fixado;
- Comunicado 12.746/2004 sobre a implementação de Basiléia II no Brasil;
- Resolução 3.380/2006: risco operacional

Há, ainda, as regulamentações referentes ao controle de riscos para fundos de pensão (elaboradas pela SPC) e para seguradoras (SUSEP), que também estão alinhadas com as melhores práticas internacionais.

Deloitte

Deloitte.

A governança corporativa, mais do que um determinante da perenidade dos negócios, é um dos grandes alicerces da atuação da Deloitte, uma das maiores organizações do mundo em seu setor, na prestação de serviços de consultoria e auditoria aos seus clientes. Participar deste guia, que aborda a importância do conselho fiscal no cotidiano das empresas, assim como as melhores práticas para o seu pleno estabelecimento, é uma oportunidade singular para a Deloitte reiterar seu comprometimento com o futuro dos negócios de seus mais de 3.000 clientes em todo o Brasil. No País, a Deloitte atua desde 1911, é uma das líderes de mercado e seus mais de 3.200 profissionais são reconhecidos pela integridade, competência e habilidade em transformar seus conhecimentos em soluções empresariais para seus clientes.

Energias do Brasil

A Energias do Brasil é uma holding que reúne ativos nas áreas de geração, distribuição e comercialização de energia elétrica, mantendo como guia, em seus negócios, um elevado padrão ético, com base em valores como transparência, rigor e eficiência. Dedicada a ser uma das empresas líderes do setor energético brasileiro, sem contudo descuidar da sua responsabilidade sócio-ambiental, a companhia estabeleceu políticas para conduzir suas atividades sem pôr em risco o seu sistema financeiro ou as comunidades por ela afetadas. Sem ferir o seu entorno nem se esquivar de prestar contas de seus atos. É apoiada nesses sólidos princípios que a Energias do Brasil se sente confiante em patrocinar este guia, fonte de orientação para outras companhias que desejem, também, trilhar o caminho das boas práticas empresariais.

KPMG

Os serviços de Enterprise Risk Management (ERM) da KPMG Risk Advisory Services podem ajudar sua organização a criar um programa sustentável para o gerenciamento dos riscos corporativos, auxiliando no desenvolvimento de um roteiro prático, transferindo conhecimento e fornecendo treinamento para sua organização, condições indispensáveis para uma bem-sucedida implementação de ERM. Nossa metodologia baseada em Estruturação, Posicionamento, Governança e Estabelecimento da cultura de gestão de riscos tem sido aplicada em diversas empresas nos mais diversos mercados e atende as necessidades de ser abrangente e prática, atuando no nível conceitual, mas sem estabelecer um processo burocrático. Visite nosso site para maiores informações: www.kpmg.com.br

A&E Consultoria

A iniciativa do IBGC na criação desse Guia e o empenho com que conduziu o trabalho representam uma contribuição imensa para a compreensão de tema tão complexo. O Gerenciamento de Riscos Corporativos possui fundamental importância para o desenvolvimento de um grau elevado de governança e a gestão dos programas de seguros das empresas deverá adquirir relevância nesse contexto. A experiência obtida pela A&E Consultoria com a aplicação do Review, uma ferramenta de análise, diagnóstico e de recomendações sobre os riscos existentes e os seguros adquiridos, levou-nos a perceber sua total aderência aos interesses da boa Governança Corporativa.

SERPRO

A inovação é uma marca indelével dos 42 anos do Serviço Federal de Processamento de Dados (SERPRO), Empresa Pública do segmento de tecnologia da informação, traduzida em sua missão: " Prover e Integrar soluções em Tecnologia da Informação para o êxito da gestão das finanças públicas e da governança do Estado, em benefício da sociedade."

O tema Gestão de Riscos é relativamente recente no Brasil. Participar do esforço para a edição do Guia de Riscos Corporativos do IBGC, é contribuir para a inovação da gestão pública e aprimoramento das práticas de governança nas empresas estatais.

Série

Cadernos de Governança Corporativa

1 Guia de Orientação para o Conselho Fiscal

2 Manual Prático de Recomendações Estatutárias

3 Guia de Orientação para Gerenciamento de Riscos Corporativos

IBGC | Instituto Brasileiro de Governança Corporativa

O IBGC é uma organizacão exclusivamente dedicada à promoção da governança corporativa no Brasil e o principal fomentador das práticas e discussões sobre o tema no país, tendo alcançado reconhecimento nacional e internacional.

Fundado em 27 de novembro de 1995, o IBGC - sociedade civil de âmbito nacional, sem fins lucrativos - tem o propósito de "ser referência em governança corporativa, contribuindo para o desempenho sustentável das organizações e influenciando os agentes de nossa sociedade no sentido de maior transparência, justiça e responsabilidade."

IBGC - Av. das Nações Unidas, 12.551
19º andar, conj. 1910
World Trade Center
04578-903 – São Paulo / SP
Tel.: 55 11 3043-7008

IBGC PARANÁ – Tel.: 55 41 3022-5035
IBGC RIO – Tel.: 55 21 2223-9651
IBGC SUL – Tel.: 55 51 3328-2552
www.ibgc.org.br

Guia de Orientação para Gerenciamento de Riscos Corporativos

Cadernos de Governança Corporativa