



CODASP

**Política, Metodologia e Processo de Gestão
de Riscos Corporativos**

03 de outubro de 2017

Versão 1.0

Ficha Técnica

Política, Processo e Metodologia de Gestão de Riscos Corporativos da CODASP

| | |
|-----------------------------------|--|
| Projeto: | Estruturação da Política, Processo e Metodologia de Gestão de Riscos Corporativos da CODASP |
| Responsável pela Aprovação | Alexandre Penteado Pires |
| Responsável Técnica | Larissa de Oliveira Viveiros |

São Paulo, 03 de outubro de 2017

APRESENTAÇÃO

A Política, o Processo e a Metodologia de Gerenciamento de Riscos Corporativos da Companhia de Desenvolvimento Agrícola do Estado de São Paulo (CODASP) são instrumentos que contribuem para o aperfeiçoamento da governança e da gestão da Companhia.

A primeira versão desses instrumentos foi concebida no contexto do processo de implantação da Área de Auditoria Interna da CODASP, em observância ao disposto na Lei nº 13.303, de 30 de junho de 2016, como contribuição para o aperfeiçoamento e modernização da gestão da Companhia e como pré-condição para a efetiva disseminação da cultura de gestão de riscos na companhia.

Este trabalho não seria possível sem o patrocínio da Alta Administração da Companhia, que disponibilizou os meios para a sua realização, dando assim um passo importante rumo à profissionalização da gestão na instituição.

Larissa de Oliveira Viveiros
Auditora Interna

Sumário

| | |
|--|----|
| GLOSSÁRIO | 5 |
| 1. INTRODUÇÃO | 14 |
| 2. POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS | 14 |
| Capítulo I - Das Disposições Preliminares | 14 |
| Capítulo II – Dos Princípios..... | 15 |
| Capítulo III - Das Diretrizes e Objetivos | 15 |
| Capítulo IV - Das Responsabilidades e Competências | 16 |
| 3. METODOLOGIA E PROCESSO DE GESTÃO DE RISCOS CORPORATIVOS | 18 |
| 3.1 Identificação dos Riscos..... | 18 |
| 3.2 Categorização dos Riscos..... | 18 |
| 3.3 Avaliação dos Riscos | 23 |
| 3.4 Tratamento dos Riscos..... | 24 |
| 3.5 Monitoramento dos Riscos | 26 |

Glossário

| Termo | Significado |
|--|---|
| Análise de Riscos | Processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades. A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos. |
| Atividade | É a decomposição do trabalho em ações necessárias para produzir um resultado em particular, que, dependendo da complexidade do macroprocesso ou processo, podem ser divididas em tarefas que corresponderão ao passo a passo para a realização de cada atividade. Em outras palavras, as atividades correspondem a “o quê” é feito e “como” é feito durante o processo. |
| Avaliação de Controles Internos | Processo mediante o qual se procura conhecer e avaliar a eficácia do(s) controle(s) interno(s) de uma entidade quanto à sua capacidade para evitar ou reduzir o impacto ou a probabilidade de eventos negativos (riscos) ou aumentar a probabilidade ou o impacto de eventos positivos (oportunidades), na busca de objetivos estabelecidos. <i>(BRASIL. Tribunal de Contas da União (TCU). Voto condutor do Acórdão 1.074/2009- TCU-Plenário. Relator: Ministro Weder de Oliveira.)</i> Disponível em: < https://contas.tcu.gov.br/pesquisaJurisprudencia/#/pesquisa/acordao-completo >. Acesso em: 23 fev 2017. |
| Avaliação de | Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é |

| Termo | Significado |
|---------------------------------|--|
| Riscos | <p>aceitável ou tolerável.</p> <p><i>(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO 31000:2009: Gestão de Riscos – Princípios e diretrizes. Rio de Janeiro, 2009.)</i></p> |
| Cadeia de Valor | <p>i. Conjunto de macroprocessos que se compõem em corporativos finalísticos e corporativos de suporte, executados de forma inter-relacionada que criam valor para o usuário final.</p> <p>ii. Conjunto de atividades inter-relacionadas que criam valor para o cliente, segmentado em um conjunto de atividades primárias e outro de atividades de suporte. As atividades primárias são aquelas relacionadas à produção de bens ou serviços e à logística de entrega de insumos e produtos. As atividades de suporte dizem respeito à gestão de recursos e de infraestrutura para a produção. (Porter, 1991).</p> |
| Competências Necessárias | <p>Competência é a mobilização de conhecimentos, habilidades e atitudes do servidor, no contexto de trabalho, para, individualmente ou em equipe, alcançar os resultados esperados pela organização.</p> <p>Competências necessárias, tratam do conjunto de qualidades ou características idealmente necessárias para executar as atividades de determinada ocupação (ou de um conjunto de ocupações) em uma organização e que influenciam o desempenho apresentado pelo colaborador/gestor. É a referência, o ideal para determinado indivíduo exercer o conjunto de atividades que lhe são atribuídas.</p> <p><i>(Ver também: Perfil profissional desejado. BRASIL. Tribunal de Contas da União - TCU. Glossário de termos do controle, 2012. Disponível em:</i></p> |

| Termo | Significado |
|---------------------------------|--|
| | <p><i><http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/scalizacao_controle/normas_auditoria/Glossario_termos_ce.pdf>.</i> <i>Acesso em: 1 Out. 2013.)</i></p> |
| Controles Internos | <p>Ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos. Compreende o plano de organização e todos os métodos e procedimentos utilizados pela Administração e conduzidos por todos os seus agentes para salvaguardar ativos, desenvolver a eficiência nas operações, avaliar o cumprimento dos programas, objetivos, metas e orçamentos, verificar a exatidão e a fidelidade das informações e assegurar o cumprimento da lei.</p> <p><i>(COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Internal Control: Integrated Framework. United States of America, 2013.</i></p> <p><i>BRASIL. Lei Complementar nº 856, de 16 de maio de 2017. Dispõe sobre a reorganização da estrutura organizacional da Secretaria de Estado de Controle e Transparência - SECONT, órgão central do sistema de controle interno do Poder Executivo do Estado do Espírito Santo. Diário Oficial dos Poderes do Estado, 17 mai 2017.)</i></p> |
| Estratégia Institucional | <p>Conjunto de objetivos, finalidades, metas, diretrizes fundamentais e os planos para atingir os objetivos da organização como um todo.</p> |
| Gestão | <p>Estruturas responsáveis pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a consecução de seus</p> |

| Termo | Significado |
|-------------------------|---|
| | <p>objetivos, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas. A gestão consiste em planejar, construir, executar e monitorar atividades alinhadas com a direção estratégica estabelecida pela governança para atingir os objetivos de negócios. Na maioria das organizações, a gestão é responsabilidade da gerência executiva, sob a liderança do chefe diretor executivo (CEO).</p> <p><i>(BRASIL. Tribunal de Contas da União (TCU). Referencial Básico de Governança: Aplicável a Órgãos e Entidades da Administração Pública. Versão 2. Brasília, 2014. Disponível em: <http://portal.tcu.gov.br/comunidades/governanca/entendendo-a-governanca/referencial-de-governanca/>. Acesso em: 23 fev 2017. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. United States of America, 2012).</i></p> |
| Gestão de Riscos | <p>Conjunto de princípios, estruturas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere aos riscos. (www.pmimf.fazenda.gov.br)</p> <p>Atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. A gestão de riscos pode ser aplicada a toda uma organização, em suas várias áreas e níveis, a qualquer momento, bem como a funções, atividades e projetos específicos.</p> <p><i>(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário. Rio de Janeiro, 2009. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ISO NBR 31000:2009: Gestão de Riscos – Princípios e diretrizes. Rio de Janeiro, 2009).</i></p> |

| Termo | Significado |
|-------------------------------|--|
| Governança | <p>Compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade. É o sistema pelo qual as organizações são dirigidas e controladas. Pode ser entendido como o conjunto de ações e responsabilidades exercidas pela alta administração da empresa, órgão ou entidade, com o objetivo de oferecer orientação estratégica e garantir que os objetivos sejam alcançados, com simultânea gerência de riscos e verificação de que os recursos são utilizados de forma responsável.</p> <p><i>(BRASIL. Tribunal de Contas da União (TCU). Referencial Básico de Governança: Aplicável a Órgãos e Entidades da Administração Pública. Versão 2. Brasília, 2014. Disponível em: <http://portal.tcu.gov.br/comunidades/governanca/entendendo-a-governanca/referencial-de-governanca/>. Acesso em: 23 fev 2017. BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.)</i></p> |
| Macroprocesso | <p>Conjunto de processos por meio dos quais a organização cumpre a sua missão, implementa suas estratégias, gerando valor ao seu usuário final.</p> |
| Objetivos Estratégicos | <p>São os fins a serem perseguidos pela organização para o cumprimento de sua missão e o alcance de sua visão de futuro. Constituem elo entre as diretrizes de uma organização e seu referencial estratégico. Traduzem, consideradas as demandas e expectativas dos clientes, os desafios a serem enfrentados num determinado período.</p> <p><i>(BRASIL. Tribunal de Contas da União (TCU). Referencial Básico</i></p> |

| Termo | Significado |
|---------------------------|---|
| | <p><i>de Governança: Aplicável a Órgãos e Entidades da Administração Pública. Versão 2. Brasília, 2014. Disponível em: <http://portal.tcu.gov.br/comunidades/governanca/entendendo-a-governanca/referencial-de-governanca/>. Acesso em: 23 fev 2017).</i></p> |
| Plano de Auditoria | <p>Documento resultante da fase de planejamento da auditoria, contendo o registro dos resultados das atividades desenvolvidas nessa fase e programa de trabalho para a fase de execução, incluindo: o objetivo de auditoria; a visão geral do objeto e do seu ambiente, inclusive do controle interno; a determinação da materialidade; a análise de problema ou avaliação de riscos utilizada para definir os objetivos de auditoria específicos e determinar a natureza, época e extensão dos procedimentos de auditoria e o programa de auditoria contendo esses procedimentos; a estimativa de prazos, a agenda ou o cronograma detalhado do trabalho; a alocação de recursos, inclusive de especialistas, quando for o caso, e a estimativa do custo da fiscalização.</p> <p><i>(INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI): ISSAI 100 a 400. Tradução de Secretaria de Relações Internacionais do TCU. Disponível em: <http://www.intosai.org/fileadmin/downloads/downloads/4_documents/ISSAI_100_Portugues.pdf>. Acesso em: 23 fev 2017.</i></p> <p><i>INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Normas Internacionais das Entidades Fiscalizadoras Superiores (ISSAI): ISSAI 1300, 1315 e 1330. JOHANNESBURG, 2010. Disponíveis em: <http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm>. Acesso em: 23 fev 2017. CONSELHO</i></p> |

| Termo | Significado |
|--|--|
| | <p><i>FEDERAL DE CONTABILIDADE. Normas Brasileiras de Contabilidade de Auditoria Independente (NBC TA): 300, 315 e 330. Disponível em: <http://portalcfc.org.br/wordpress/wpcontent/uploads/2013/01/NBC_TA_AUDITORIA.pdf>. Acesso em: 23 fev 2017).</i></p> |
| Processo | <p>Grupo de atividades efetuadas logicamente e que produz bens/serviços de valor para o cliente - Hammer e Champy (1994).</p> |
| Processo de Apoio ou de Suporte | <p>São aqueles que dão suporte a alguma atividade-fim da organização, tais como a gestão de pessoas, a gestão de compras, o planejamento e o acompanhamento das ações institucionais etc.</p> <p><i>(Visão Prática: Conceitos Fundamentais em Gestão por Processos. Disponível em <http://www.administradores.com.br/artigos/negocios/visaopratica-conceitos-fundamentais-em-gestao-por-processos/29427/>. Acessado em 13/03/2017. PROCESSOS FINALÍSTICOS E DE APOIO: CONSIDERAÇÕES. Disponível em <https://arfn10.blogspot.com.br/2012/10/processos-finalisticos-e-de-apoio.html>. Acessado em 13/03/2017.)</i></p> |
| Processo de Negócio | <p>Um processo que pertence e é executado pelo negócio. Um Processo de Negócio contribui para a entrega de um produto ou Serviço aos Clientes de negócio.</p> <p><i>(OFFICE OF GOVERNMENT COMMERCE. IT Service Management. Glossário Information Technology Infrastructure Library (ITIL). Versão v3 1.2).</i></p> |
| Processo de Trabalho | <p>Conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos/serviços (saídas) com valor agregado. Processos são geralmente planejados e</p> |

| Termo | Significado |
|--|---|
| | realizados de maneira contínua para agregar valor na geração de produtos e serviços. Processos podem ser agrupados em macroprocessos e subdivididos em subprocessos. <i>(BRASIL. Tribunal de Contas da União (TCU). Padrões de Levantamento. Portaria-Segecex nº 11/2011).</i> |
| Processo Finalístico | Processo associado às atividades-fim da organização ou diretamente envolvido no atendimento às necessidades dos seus clientes”. Referem-se ao conjunto de atividades que representam a essência da organização, caracterizam a atuação da organização e estão diretamente relacionados às grandes funções da organização e aos seus objetivos estratégicos e à geração de produto/serviço para o cliente interno ou externo. <i>(Visão Prática: Conceitos Fundamentais em Gestão por Processos. Disponível em <http://www.administradores.com.br/artigos/negocios/visaopratica-conceitos-fundamentais-em-gestao-por-processos/29427/>. Acessado em 13/03/2017. PROCESSOS FINALÍSTICOS E DE APOIO: CONSIDERAÇÕES. Disponível em <https://arfn10.blogspot.com.br/2012/10/processos-finalisticos-e-de-apoio.html>. Acessado em 13/03/2017.)</i> |
| Projeto | Esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. |
| Projeto de Transformação Organizacional | Intervenção em um processo para fins de melhoria e/ou inovação. |
| Risco | Efeito da incerteza sobre os objetivos (www.pmimf.fazenda.gov.br). Possibilidade de um evento ocorrer e afetar adversamente a |

| Termo | Significado |
|----------------------------|--|
| | <p>realização de objetivos (COSO, 2004).</p> <p>Possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido em termos de consequências e probabilidades (TCU, 2010f); efeito da incerteza nos objetivos (ABNT, 2009).</p> |
| Tratamento de Risco | <p>Processo de modificar um risco (ABNT, 2009). Consiste em selecionar e implementar uma ou mais opções de resposta a riscos para modificar os níveis de risco (INTOSAI, 2007). Definição das ações para reduzir a probabilidade de ocorrência dos eventos ou suas consequências (BRASIL, 2017).</p> <p><i>(ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ISO NBR 31000:2009 – Gestão de Riscos – Princípios e diretrizes. Rio de Janeiro, 2009. INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). INTOSAI GOV 9130 - Guidelines for Internal Controls Standards for the Public Sector: further information on entity risk management. PSC Subcommittee on Internal Control Standards. 2007. Disponível em:<http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm>. Acesso em: 23 fev 2017.</i></p> <p>BRASIL. Secretaria de Gestão do Ministério do Planejamento - Seges/MP. Instrução Normativa 5/2017. Art. 25.)</p> |

1. Introdução

O presente documento tem por objetivo estabelecer os requisitos mínimos da Política, do Processo e da Metodologia de Gestão de Riscos a serem utilizadas na CODASP.

2. Política de Gestão de Riscos Corporativos

Capítulo I - Das Disposições Preliminares

A gestão de riscos corporativos deverá alinhar-se ao planejamento estratégico e à cadeia de valor da CODASP.

O Plano Anual de Auditoria Interno da CODASP deverá ser alinhado à Política, ao Processo e à metodologia de gestão de Riscos corporativos da Companhia.

Para os efeitos da Política de Gestão de Riscos, entende-se por:

I - **risco**: efeito da incerteza sobre os objetivos;

II - **gestão de riscos**: conjunto de princípios, estruturas, processos e atividades coordenados para dirigir e controlar uma organização no que se refere aos riscos;

III - **processo de gerenciamento de riscos**: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, identificação, análise, avaliação, tratamento e monitoramento;

IV - **estrutura de gestão de riscos**: conjunto de componentes que fornecem os fundamentos, metodologias e arranjos organizacionais para a gestão de riscos; e

V - **gestor do risco**: agente que tem a responsabilidade e a autoridade para gerenciar determinado risco.

Capítulo II – Dos Princípios

A Gestão de Riscos observará os seguintes princípios:

- I - agregação e proteção de valor;
- II - integração a todos os processos organizacionais;
- III - subsídio e auxílio aos tomadores de decisão;
- IV - abordagem explícita da incerteza, como prática de gestão sistemática, estruturada e oportuna, subordinada ao interesse público;
- V - uso das melhores informações disponíveis;
- VI - alinhamento com o contexto interno e externo da organização;
- VII - consideração dos fatores humanos e culturais;
- VIII - transparência e participação;
- IX - dinamismo, iteração e capacidade de reagir a mudanças; e
- X - melhoria contínua da organização.

Capítulo III - Das Diretrizes e Objetivos

São diretrizes e objetivos da gestão de riscos:

- I - subsidiar de forma integrada a elaboração do planejamento estratégico institucional, seus desdobramentos e a cadeia de valor;
- II - contribuir para o desempenho dos processos e das políticas da organização;
- III - executar periodicamente as etapas que compõem o processo de gerenciamento de riscos;

- IV - estabelecer instrumentos de medição de desempenho da gestão de riscos, mediante atividades contínuas ou de avaliações independentes ou a combinação de ambas;
- V - utilizar-se de metodologia, ferramentas e conhecimento para o apoio à gestão de riscos convergentes com as melhores práticas;
- VI - promover o desenvolvimento contínuo dos agentes em gestão de riscos, no âmbito da CODASP;
- VII - prover soluções tecnológicas de forma integrada e eficiente para sustentar os processos de gerenciamento de riscos;
- VIII - estabelecer responsabilidades e competências para os agentes envolvidos no processo de gerenciamento de riscos;
- IX - assegurar que os responsáveis pela tomada de decisão, em todos os níveis organizacionais, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização;
- X - estabelecer níveis adequados de exposição a riscos;
- XI - proteger o ambiente corporativo para a realização demonstrável dos objetivos estratégicos e a melhoria do desempenho institucional;
- XII - aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis;
- XIII - estabelecer controles proporcionais ao risco, observada a relação custo-benefício; e
- XIV - promover a cultura de gestão de riscos na Companhia.

Capítulo IV - Das Responsabilidades e Competências

A responsabilidade e a competência para a estruturação e efetivação da gestão de riscos são do dirigente máximo de CODASP.

Cada risco deve estar associado a um gestor de risco com alçada suficiente para o seu gerenciamento.

São responsabilidades do gestor de risco:

I - assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos

estabelecida na organização;

II - monitorar e documentar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na exposição ao risco em níveis adequados; e

III - garantir que as informações relevantes e suficientes sobre o risco estejam disponíveis para subsidiar o processo de tomada de decisão.

São responsabilidades da Auditoria Interna:

I - propor política, normas e metodologias de gestão de riscos;

II - facilitar e monitorar a implementação do processo de gerenciamento de riscos;

III - acompanhar o desempenho institucional referente à gestão de riscos do órgão ou entidade; e

IV - promover a disseminação da cultura de gestão de riscos.

3. Processo Metodologia de Gestão de Riscos Corporativos

3.1 Identificação dos Riscos

Riscos podem ser entendidos como um conjunto de eventos, externos ou internos, que podem impactar os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis. 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.

3.2 Categorização dos Riscos

Os riscos devem ser categorizados com relação à sua origem, natureza e tipo.

3.2.1 Origem

| Origem | Definição |
|----------------|---|
| Externa | São associados 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. |

| Origem | Definição |
|----------------|---|
| Interna | São 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 proativa. |

3.2.2 Natureza

| Natureza | Definição |
|---------------------|--|
| Estratégicos | São associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização. Os riscos decorrentes da má gestão empresarial muitas vezes resultam em fraudes relevantes nas demonstrações financeiras. Exemplos: falhas na antecipação ou reação ao movimento dos concorrentes causadas por fusões e aquisições; diminuição de demanda do mercado por produtos e serviços da empresa causada por obsolescência em função de desenvolvimento de novas tecnologias/produtos pelos concorrentes. |
| Financeiros | São 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. |

| Natureza | Definição |
|---------------------|--|
| Operacionais | São 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. |

3.2.3 Tipo

| Tipo | Definição |
|---------------------|---|
| Ambiental | São associados 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. 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. |
| Conformidade | São relacionados 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 |

| Tipo | Definição |
|-----------------------|---|
| | 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. |
| Legal | São relacionados à mudanças na legislação vigente que possam vir a comprometer a operação e funcionamento da organização e/ou o alcance dos seus objetivos estratégicos. |
| Macroeconômico | São relacionados a situações na economia do país que levariam a perdas importantes para empresas, investidores e demais residentes do país. |
| Pessoas | São normalmente relacionados à falta de pessoal qualificado e de profissionais preparados para exercer suas funções. Existe a possibilidade desses erros serem intencionais, isto, é fruto de uma conduta duvidosa. Os principais riscos de pessoal são: <ul style="list-style-type: none">– não intencionais, resultado de omissão ou negligência;– de qualificação, isto é, o profissional não tem condição de desempenhar corretamente suas tarefas por falta de capacidade ou habilidade e– fraude, quando a conduta não atende intencionalmente as normas da empresa, se caracterizando por desvios de materiais ou valores, divulgação de inverdades etc. |
| Tecnológico | São relacionados a falhas, indisponibilidade ou |

| Tipo | Definição |
|------|--|
| | 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. |

3.2.4 Tabela Resumo

| | | Tipos | Natureza dos Riscos | | |
|--------------------|---------|----------------|---------------------|-------------|------------|
| | | | Estratégico | Operacional | Financeiro |
| Origem dos Eventos | Externo | Macroeconômico | | | |
| | | Ambiental | | | |
| | | Tecnológico | | | |
| | | Legal | | | |
| | Interno | Ambiental | | | |
| | | Pessoas | | | |
| | | Tecnológico | | | |
| | | Conformidade | | | |

3.3 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: a probabilidade de ocorrência e o seu impacto (em geral medido pelo impacto no desempenho econômico-financeiro do período). Seguem abaixo as ferramentas a serem utilizadas para a avaliação do nível de exposição da Companhia aos riscos identificados:

| Legenda Nível de Risco Extremo Alto Médio Baixo | | Probabilidade | | | | |
|---|------------------|------------------|------------|------------|-----------|------------------|
| | | 1 Muito Baixa | 2 Baixa | 5 Média | 8 Alta | 10 Muito Alta |
| Impacto | 10 Muito Alto | 10 | 20 | 50 | 80 | 100 Extremo |
| | 8 Alto | 8 | 16 | 40 | Alto 64 | 80 |
| | 5 Médio | 5 | 10 | Médio 25 | 40 | 50 |
| | 2 Baixo | 2 | 4 | 10 | 16 | 20 |
| | 1 Muito Baixo | 1 | 2 | 5 | 8 | 10 |

| Magnitude | Descrição | P |
|-------------|--|---|
| Muito Baixa | Evento Improvável de ocorrer. Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade | 1 |
| Baixa | Evento Raro de ocorrer. O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade. | 2 |
| Média | Evento possível de ocorrer. Há elementos e ou informações que indicam moderadamente essa | 5 |

| Magnitude | Descrição | P |
|------------------|--|----------|
| | possibilidade. | |
| Alta | Evento provável de ocorrer. É esperado que o evento ocorra, pois os elementos e informações disponíveis indicam de forma consistente essa possibilidade | 8 |
| Muito Alta | Evento praticamente certo de ocorrer. Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade | 10 |

3.4 Tratamento dos Riscos

As várias alternativas para tratamento dos riscos são descritas abaixo:

| Alternativa | Definição |
|------------------------|---|
| 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. |
| Aceitar o Risco | Neste caso, apresentam-se quatro alternativas: reter, reduzir, transferir/compartilhar ou explorar o risco. |
| Retter | 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. |

| Alternativa | Definição |
|-------------------------------------|---|
| Reduzir | <p>Ações são tomadas para minimizar a probabilidade e/ou o impacto do risco.</p> <p>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 autodetecção de falhas e de backup para reduzir a probabilidade de indisponibilidade do sistema.</p> |
| Transferir e/ou Compartilhar | <p>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 franquias 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 frequência, inerente ao processo de operação e manutenção.</p> <p>Devem ser transferidos por meio de seguro os riscos tidos como catastróficos (riscos de baixa frequência e alta severidade), os riscos de alta frequência 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</p> |

| Alternativa | Definição |
|--------------------|---|
| | 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 |
| Explorar | Aumentar o grau de exposição ao risco na medida em que isto possibilita vantagens competitivas. |

3.5 Monitoramento dos Riscos

O monitoramento dos riscos ocorre no curso normal das atividades gerenciais. Já o escopo e a frequência 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 nesse processo devem ser relatadas aos níveis superiores de gestão e, dependendo da gravidade, reportadas à Alta Administração.

Segue abaixo modelos referenciais de ferramentas para suporte ao monitoramento de riscos na CODASP:

COMPANHIA DE DESENVOLVIMENTO AGRÍCOLA DE SÃO PAULO
Secretaria de Agricultura e Abastecimento

Formulário de Registro de Risco:

| Formulário de Registro de Risco | | | | | | | | | |
|--|---------------|----------|-----------------------------------|--------|--------------|--------------------|-----------------------|---------------------------|------|
| Responsável pela identificação do risco: | | | Responsável pela gestão do risco: | | | | | | |
| Origem: | Natureza: | | Tipo: | | | Data do Registro: | | | |
| Identificação do Risco | | | | | | Avaliação do Risco | Tratamento do Risco | | |
| Cadeia de Valor | Macroprocesso | Processo | Causa | Evento | Consequência | (P x I) | Mecanismo de Controle | Alternativa de Tratamento | Ação |

Relatório Gerencial de Monitoramento de Riscos:

| Relatório Gerencial de Monitoramento de Riscos | | | |
|--|-------------------|-------------------------|--|
| Data de Elaboração: | | | |
| Responsável pela Elaboração | | | |
| Evento | Avaliação (P x I) | Responsável pela Gestão | Status (Sob controle, Alerta, Efetivado) |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

