BOAS PRÁTICAS DE CONTROLE INTERNO, GESTÃO DE RISCOS *E COMPLIANCE*

SUMÁRIO

1. DISPOSIÇÕES PRELIMINARES

Este documento visa à previsão de estruturas e definição de boas práticas de controle interno, gestão de riscos e *compliance* na SCParticipações e Parcerias S.A. - SCPar.

2. FINALIDADE

Dispor sobre os procedimentos a serem observados em um Sistema de Gestão de Riscos,Controles Internos e *Compliance.*

3. ASPECTOS LEGAIS

Lei 13.303 de 30 de junho de 2016 – Lei das Estatais.
Decreto do Estado de Santa Catarina nº 1.007 de 20 de dezembro de 2016.
Decreto do Estado de Santa Catarina nº 1.025 de 18 de janeiro de 2017.

4. CONCEITOS BÁSICOS

4.1. Controle Interno

"Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade." (COSO)

Essa definição reflete alguns conceitos fundamentais. O controle interno é:

4.1.1. Conduzido para atingir objetivos em uma ou mais categorias – operacional, divulgação e conformidade.

4.1.2. Um processo que consiste em tarefas e atividades contínuas – um meio para um fim, não um fim em si mesmo.

4.1.3. Realizado por pessoas – não se trata simplesmente de um manual de políticas e procedimentos, sistemas e formulários, mas diz respeito a pessoas e às ações que elas tomam em cada nível da empresa para realizar o controle interno.

4.1.4. Capaz de proporcionar segurança razoável - mas não absoluta, para a estrutura de governança e alta administração de uma empresa.

4.1.5. Adaptável à estrutura da empresa – flexível na aplicação para toda a empresa ou para uma subsidiária, divisão, unidade operacional ou processo de negócio em particular.

4.2. Risco

Risco é definido como sendo o "efeito da incerteza nos objetivos" (ISO 31000).

O Risco também pode ser definido como "o evento futuro e incerto que, caso ocorra, pode impactar negativamente o alcance dos objetivos da organização." (COSO II).

> "O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos."(COSO)

Essas definições refletem certos conceitos fundamentais. O gerenciamento de riscos corporativos é:

4.2.1. Um processo contínuo e estruturado, que flui através da empresa.

4.2.2. Conduzido pelos profissionais em todos os níveis da empresa, considerando os fatores humanos e culturais.

4.2.3. Aplicadoà definição das estratégias, sendo base confiável para apoio de tomada de decisões e planejamento.

4.2.4. Aplicado em toda a empresa, em todos os níveis e unidades, e inclui a formação de uma visão de portfólio de todos os riscos a que ela está exposta, abordando explicitamente as incertezas.

4.2.5. Formulado para identificar eventos em potencial, cuja ocorrência poderá afetar a empresa, e para administrar os riscos de acordo com seu apetite a risco.

4.2.6. Capaz de propiciar garantia razoável para o Conselho de Administração e a Diretoria Executiva daempresa.

4.2.7. Orientado para a realização de objetivos em uma ou mais categorias distintas, mas dependentes, ou seja, o gerenciamento de riscos desdobra da estratégia e dos objetivos empresariais para os processos/atividades a eles vinculados, incorporando demais riscos existentes.

4.3. Compliance

Do verbo anglo-saxão "*tocomply*", significa cumprir, executar, satisfazer, realizar o que foi imposto. *Compliance* é estar em conformidade, é o dever de cumprir regulamentações internas e externas impostas às atividades da instituição. "Estar *compliance*" é estar em conformidade com leis e regulamentações internas e externas. "Ser e estar *compliance*" é acima de tudo, uma obrigação individual de cada colaborador dentro da empresa.

Cada empresa deverá garantir a existência de uma estrutura (área) competente para desenvolver e atuar em programas efetivos de conformidade e integridade que contemplem mecanismos e medidas de prevenção, de detecção de condutas irregulares, ilícitas e antiéticas, mediante a formalização prévia de processos que definam os órgãos, as competências, o âmbito de atuação e as responsabilidades da alta administração, de empregados e terceiros (fornecedores, prestadores de serviços, agentes intermediários e parceiros em geral) relacionados ao seu negócio.

Em caso de existência de subsidiárias é responsabilidade da empresa trabalhar para que as demais empresas do grupo estejam igualmente operando em conformidade.

5. PROCEDIMENTOS GERAIS

5.1. Procedimentos de Controle Interno

Os procedimentosde controle interno na SCPar deverão considerar:

5.1.1. Seleção dos processos a serem trabalhados na empresa para documentar e implementar os controles. A empresa deve definir qual será o critério de seleção:a) por meio de materialidade das demonstrações contábeis; b) por julgamento profissional; c) por critérios de criticidade; ed) outros.

5.1.2. Conhecimento mínimo necessário dos processos selecionados. Esse conhecimento pode se dar por entrevistas, narrativas, fluxogramas. É importante conhecer o processo e identificar o que e em qual etapa algo pode dar errado (riscos do processo).

5.1.3. A partir da identificação dos riscos dos processos, deve-se documentar/formalizar os controles existentes e os controles necessários de serem implementados.

5.1.4. Um controle interno, necessariamente, precisa atender a 3(três) quesitos:

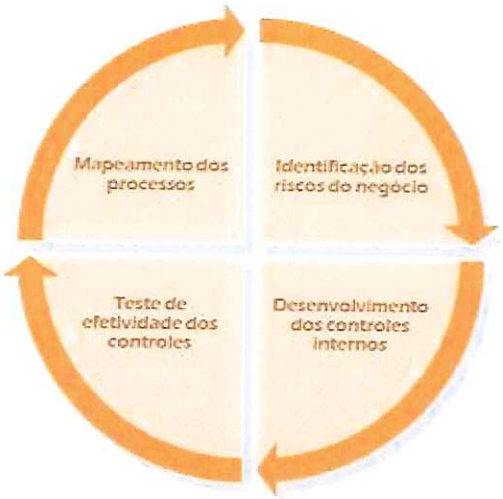
a) deve ser formalizado/documentado;
b) deve ter evidência de sua execução; e
c) deve ser mensurável.

5.1.5. Para cada controle identificado devem ser efetuados testes de efetividade conforme amostras. Os testes confirmam se os controles são executados conforme sua descrição e se de fato são efetivos.

5.1.6. Os responsáveis pelos processos de negócios são os donos dos riscose controles, cabendo a estes o papel de conduzir o processo e seus controles com efetividade.

5.1.7. O Processo de Controles Internos é um ciclo contínuo. Os processos trabalhados, seus riscos e controles devem ser revisados e atualizados sempre que houver alterações ou sempre que surgir um evento novo.

Figura I: Ciclo de Gestão de Riscos de Processos e Controle Interno



5.1.8. Na implementação da Gestão de Riscos de Processos a empresa poderá concentrar seus recursos e esforços nos processos considerados críticos e que impactam mais fortemente na eficiência e eficácia organizacional, ou seja, nas estratégias e objetivos empresariais desdobradas até a unidade, podendo se utilizar da Matriz de Importância e Desempenho, demonstrada na **Figura 2**.

Figura 2: Matriz de Importância x Desempenhona Gestão de Riscos de Processos

Matriz de Importância x Desempenho

Importância	*Descrição*
Alta	O processo é de extrema importância para consecução do propósito e dos objetivos da Unidade. Pode ser considerado processo-chave e crítico para o negócio da organização.
Média	É importante processo para a Unidade. Os seus resultados afetam diretamente os processos-chave da organização.
Baixa	É processo que tem baixo impacto nos processos-chave.

Matriz de Importância x Desempenho

Desempenho	Descrição
Ótimo	Os resultados do processo são substancialmente livres de erros. A performance é superior quando comparada com os processos dos concorrentes e de outras empresas.
Bom	As principais melhorias já foram implantadas, com resultados mensuráveis realizados. O processo pode se adaptar facilmente às mudanças.
Estável	O processo é eficaz (atende às expectativas do cliente) e eficiente (menor custo, menor tempo). Não existem problemas operacionais significativos.
Razoável	O processo apresenta alguns problemas operacionais, mas suas deficiências podem ser corrigidas a curto prazo.
Crítico	O processo é ineficaz ou ineficiente, tem grandes problemas de desempenho que requerem ação corretiva imediata.

Com base na matriz utiliza-se os seguintes fatores:

a) Fator Importância:

• qual é a importância deste processo para atingirmos nossos objetivos?

• este processo impacta diretamente nos nossos resultados?

• é um processo-chave do nosso negócio?

•é um processo de suporte "crítico" em relação aos processos finalísticos?

b) Fator Desempenho:

• este processo tem atingido os resultados esperados?

• qual o nível de satisfação dos clientes em relação a este processo?

• têm sido registradas reclamações, elogios, sugestões de melhoria?

5.2. Procedimentos de Gestão de Riscos Estratégicos

A empresa além da definição da missão e visão, também estabelece objetivos estratégicos, isto é, metas de alto nível que alinham e apoiam as decisões para o cumprimento destes.

O gerenciamento de riscos corporativos é um processo conduzido pelo conselho de administração, diretoria executiva e empregados, sendo aplicado no estabelecimento de estratégias no âmbito da empresa.

O gerenciamento de riscos corporativos requer que a empresa adote uma visão de portfólio dos riscos, procedimento que poderá exigir a participação de cada um dos gerentes responsáveis por unidades de negócios, funções, processos ou outras atividades que envolvam avaliação de risco, a qual poderá ser quantitativa ou qualitativa. Com uma visão combinada de cada nível da empresa, a alta administração é capaz de avaliar se a carteira de riscos é compatível com o apetite a risco da empresa.

Os procedimentos de Gestão de Riscos Estratégicos na SCPar deverão considerar:

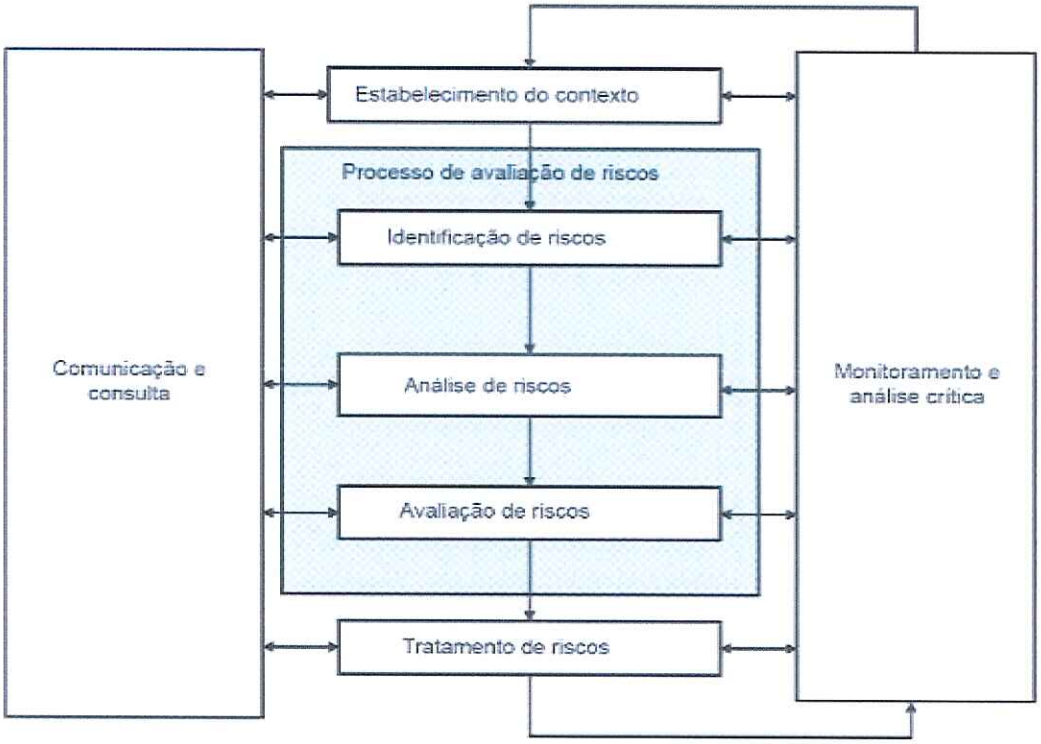
5.2.1. A criação de uma Política de Gestão de Riscos Estratégicos e o estabelecimento,de forma clara,dos objetivos, responsabilidades, princípios e diretrizes.

As técnicas de gestão de riscos são aplicadas nessa etapa para ajudar a administração a avaliar e a selecionar a estratégia e os objetivos a ela associados.

5.2.2. Que o processo de gestão de riscos estratégicos seja parte integrante da gestão, incorporado na cultura e nas práticas, e adaptado aos processos

de negócios da empresa, podendo ser utilizado para tanto o framework:ISO 31000 e/ou COSO ERM (Enterprise Risk Manager).

5.2.2.1 Framework ISO 31000



a) Comunicação e consulta - A comunicação deve abordar questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los.

b) Estabelecimento do contexto – Avaliar os objetivos da empresa e definir os parâmetros externos e internos a serem levados em consideração ao gerenciar o risco, considerar as estratégias, o escopo e os parâmetros das atividades da empresa.

c) Definição dos critérios de risco - Estabelecer os critérios a serem utilizados para avaliar como a probabilidade e impacto serão definidos; como o nível do risco deve ser determinado e o que é aceitável ou tolerável.

d) Identificação de riscos - Identificar as fontes do risco, áreas de impactos, e suas causas e consequências potenciais. A finalidade desta etapa é construir um Mapa de Riscos Estratégicos que possam comprometer a realização dos objetivos da empresa.

e) Análise de riscos – Analisar as causas e as fontes do risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. Convém que os fatores que afetam as consequências e a probabilidade sejam identificados.

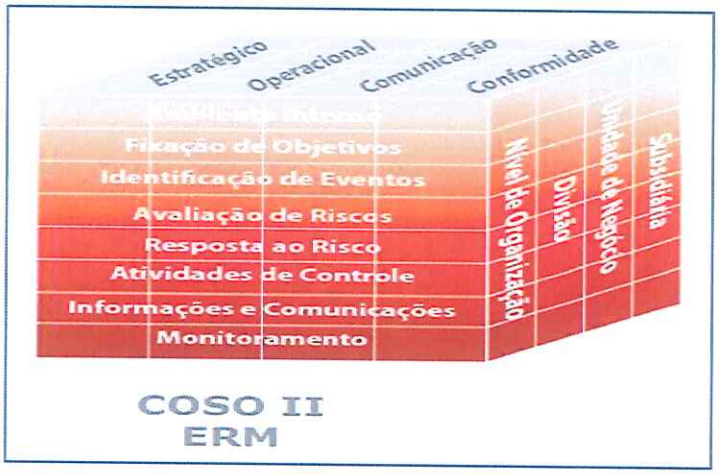
f) Avaliação de riscos - Comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos e decidir sobre o seu tratamento. A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais ricos necessitam de tratamento e a prioridade para a implementação do tratamento.

g) Tratamento de riscos - O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. As opções de tratamento de riscos podem incluir a ação de evitar o risco, tratar, transferir (através de planos de ação) ou aceitar de forma consciente e bem embasada.

h) Monitoramento e análise crítica – Envolve a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico e deve garantir que os riscos estejam sendo gerenciados como o planejado, possibilite detectar mudanças no contexto externo e interno e identificar novos riscos.

i) Registros do processo de gestão de riscos estratégicos - As atividades de gestão de riscos estratégicos devem ser registradas de forma a possibilitar a melhoria dos métodos e ferramentas, bem como de todo o processo.

5.2.2.2 Framework COSO ERM



a) Ambiente Interno - A administração estabelece uma filosofia quanto ao tratamento de riscos e estabelece um limite de apetite a risco. O ambiente interno determina os conceitos básicos sobre a forma como os riscos e os controles serão vistos e abordados pelos empregados da empresa. O coração de toda empresa fundamenta-se em seu corpo de empregados, isto é, nos atributos individuais, inclusive a integridade, os valores éticos e a competência – e, também, no ambiente em que atuam.

b) Fixação de Objetivos – Os objetivos devem existir antes que a administração identifique as situações em potencial que poderão afetar a realização destes. O gerenciamento de riscos corporativos assegura que a administração adote um processo para estabelecer objetivos e que os escolhidos propiciem suporte, alinhem-se com a missão da empresa e sejam compatíveis com o apetite a risco.

c) Identificação de Eventos – Os eventos em potencial que podem impactar a empresa devem ser identificados, uma vez que esses possíveis eventos, gerados por fontes internas ou externas, afetam a realização dos objetivos. Durante o processo de identificação de eventos, estes poderão ser diferenciados em riscos, oportunidades, ou ambos. As oportunidades são canalizadas à alta administração, que definirá as estratégias ou os objetivos.

d) Avaliação de Riscos – Os riscos identificados são analisados com a finalidade de determinar a forma como serão administrados e, depois, serão associados aos objetivos que podem influenciar. Avaliam-se os riscos

considerando seus efeitos inerentes e residuais, bem como sua probabilidade e seu impacto.

e) Resposta a Risco – Os empregados identificam e avaliam as possíveis respostas aos riscos: evitar, aceitar, reduzir ou compartilhar. A administração seleciona o conjunto de ações destinadas a alinhar os riscos às respectivas tolerâncias e ao apetite a risco.

f) Atividades de Controle – Políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos selecionados pela administração sejam executadas com eficácia.

g) Informações e Comunicações – A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permitam que as pessoas cumpram com suas atribuições. Para identificar, avaliar e responder ao risco, a empresa necessita das informações em todos os níveis hierárquicos. A comunicação eficaz ocorre quando esta flui na empresa em todas as direções, e quando os empregados recebem informações claras quanto às suas funções e responsabilidades.

h) Monitoramento – A integridade do processo de gerenciamento de riscos corporativos é monitorada e as modificações necessárias são realizadas. Desse modo, a empresa poderá reagir ativamente e mudar segundo as circunstâncias. O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes ou uma combinação desses dois procedimentos.

A premissa inerente ao gerenciamento de riscos corporativos é de que toda empresa existe para gerar valor às partes interessadas. Todas as empresas enfrentam incertezas, e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes interessadas. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O gerenciamento de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

5.3. Procedimentos de *Compliance*

Os procedimentos de *Compliance* têm o objetivo de avaliar a aderência às normas externas e internas e identificar condutas inadequadas. Para isto, a SCPar deverá:

5.3.1. Ter a estrutura de Compliance interagindo com diversas áreas da empresa para execução das suas atividades, principalmente com Jurídico, Gestão de Riscos e Controle Interno, e Auditoria Interna.

5.3.2. Definir formalmente quais as Leis, Regulamentações e normas internas farão parte do Programa de *Compliance*, e, portanto, serão o escopo de atuação da área de *Compliance*, de acordo com o tamanho e complexidade do negócio, incluindo o Código de Conduta e Integridade.

5.3.3. Verificar na empresa, através de um método formal, a aderência em relação a cada uma das normas internas e externas que fizerem parte do escopo do Programa de *Compliance*.

5.3.4. Propor formalmente ações juntamente com as áreas envolvidas para atendimento das normas internas e externas.

5.3.5. Monitorar o cumprimento do programa e reportar para a administração da empresa sobre o seu desenvolvimento.

5.3.6. Revisar periodicamente o escopo do Programa de *Compliance*, observando novas Leis, Regulamentações e Normas Internas.

5.3.7. Zelar pelo cumprimento de leis, regulamentações e normas internas e por padrões éticos.

5.3.8. Analisar políticas e normas internas com objetivo de evitar conflitos com outras já existentes e com a legislação.

5.3.9. Os responsáveis pelos processos de negócios são os donos dos riscos de *compliance*, cabendo a estes o papel de estar em conformidade nos processos sob sua responsabilidade.

6. DISPOSIÇÕES FINAIS

6.1. O Conselho de Administração ou o Diretor-Presidente, enquanto a SCPar for regida pelo Decreto Estadual nº 1.007/2016, deverá assegurar a identificação, mitigação e monitoramento dos riscos da empresa (inerentes à atuação empresarial e os relacionados com corrupção e fraudes), bem como garantir a integridade do sistema de controles internos da empresa.

6.2. Caberá a SCPar, atendendo, conforme o caso, aos ditames da Lei Federal nº 13.303/16 ou ao Decreto Estadual nº 1.007/2016, definir aárea competentepara a verificação do cumprimento de obrigações (*compliance*), gestão de riscos e controleinterno.

6.3. Os Processos de Controle Interno e Gestão de Riscos e *Compliance* devem ser parte integrante dos processos da empresa, sendo formalizados na estrutura organizacional no âmbito de sua aplicação, para que sejam dinâmicos, interativos e capazes de reagir a mudanças.

6.4. É responsabilidade do Conselho de Administração ou Diretor-Presidente, conforme o caso, aprovar a política de gerenciamento de riscos da empresa conforme a orientação estratégica da empresa. A definição de atribuições das atividades e responsabilidades nos processos de Controle Interno, Gestão de Riscos e *Compliance*deverão estar formalizadas em documento próprio.

6.5. Os treinamentos referentes à gestão de riscos, controles internos e *compliance* devem ser previstos para que todos na empresa participem, e sejam capazes de reagir a mudanças.

6.6. Para atendimento ao disposto neste documento e manutenção da conformidade, a empresa deverá atender, prioritariamente, as exigências/legislação específicas dos seus órgãos reguladores.