	Código	Revisão	Emissão	Área	Aprovação
	POL_CGR_001	01/12/2024	30/05/2016	Comitê de Gestão de Riscos	Conselho de Administração
	Política de Gestão de Riscos				

1. OBJETIVO

O objetivo da Política de Gestão de Riscos ("Política") da São Carlos é fornecer os princípios e diretrizes para a gestão dos riscos associados aos negócios da Companhia, definir e documentar os processos e as atividades relacionadas, bem como as principais responsabilidades atribuídas aos diversos órgãos da administração e áreas da Companhia.

2. TERMOS, DEFINIÇÕES E ABREVIATURAS

- **Apetite ao risco** significa o nível de Riscos que a administração da Companhia está disposta a aceitar na condução da sua estratégia de negócios e/ou suas operações
- **Auditoria Interna** significa a consultoria externa contratada para acompanhar a gestão de riscos da Companhia
- **AVCB** significa Auto de Vistoria do Corpo de Bombeiros
- **Código de Ética e Conduta** significa o Código de Ética e Conduta da Companhia, disponibilizado aos órgãos reguladores (CVM e B3 S.A.) e a todos os colaboradores
- **Comitê de Auditoria** significa o Comitê de Auditoria da São Carlos (não estatutário)
- **Companhia ou São Carlos** significa a São Carlos Empreendimentos e Participações S.A., conjuntamente com suas controladas
- **Conselho de Administração** significa o Conselho da Administração da São Carlos
- **Controles Internos** são as ações das áreas para implementar, controlar e mitigar a ocorrência dos riscos
- **Donos dos Riscos (*Risk Owners*)** são os colaboradores (líderes) formalmente definidos pela Companhia e que possuem responsabilidade e autoridade para gerenciar os riscos a ele atribuídos
- **Diretoria Executiva** significa a Diretoria Executiva da São Carlos composta por diretores estatutários e diretores executivos (não estatutários)
- **Gestão de Riscos** significa a aplicação das práticas e procedimentos visando identificar, avaliar, tratar, monitorar e reportar os eventos que possam representar um Risco
- **Impacto do Risco** significa a avaliação qualitativa e/ou quantitativa do efeito ou consequência de materialização de um risco para a Companhia
- **Materialização do Risco** significa perdas e/ou consequências do impacto de um risco que venham a atingir negativamente a Companhia
- **Nível do Risco** significa a análise combinada entre a probabilidade de ocorrência de um risco e seu impacto
- **ISO 31000** é uma norma internacional que fornece diretrizes para a gestão de riscos em organizações de todos os tamanhos e setores. A norma foi desenvolvida pela *International Organization for Standardization* (ISO) e é a base desta Política
- **Probabilidade do Risco** significa a avaliação qualitativa e/ou quantitativa da possibilidade de ocorrência de um risco
- **Risco** significa todo e qualquer evento decorrente de incertezas ao qual a Companhia está exposta e que possa afetar negativamente o cumprimento dos seus objetivos
- **Risco inerente** significa o risco antes da aplicação das ações e medidas de mitigação consideradas pela Companhia

- **Risco residual** significa o risco remanescente após o resultado das ações e medidas de mitigação adotadas pela Companhia

3. DIRETRIZES

3.1 ABRANGÊNCIA

Esta Política é parte dos controles internos da São Carlos e se aplica à Companhia, suas subsidiárias e seus colaboradores.

3.2 PRINCÍPIOS

i. Esta Política foi concebida com base nos padrões internacionais ISO 31000, que fornece diretrizes para a gestão de riscos em organizações de todos os tamanhos e setores. A norma foi desenvolvida pela *International Organization for Standardization* (ISO). A São Carlos adota a abordagem de gestão de riscos prevista na ISO 31000 com flexibilidade suficiente para assegurar que seja capaz de se adaptar à evolução das necessidades dos negócios.

ii. A São Carlos tem como objetivo reduzir sua exposição ao risco a um nível aceitável, avaliar as incertezas dos projetos e mitigar a ocorrência de riscos que possam impactar a realização do seu planejamento estratégico, garantindo que todos os riscos sejam identificados e administrados de forma apropriada.

iii. A São Carlos estabelece e mantém sistemas de gestão de risco adequados à sua natureza, dimensão e complexidade.

iv. A São Carlos acredita que um processo de identificação de riscos bem definido e um reporte rigoroso dos riscos existentes fornecem uma base sólida para gerir os riscos da Companhia de forma eficaz.

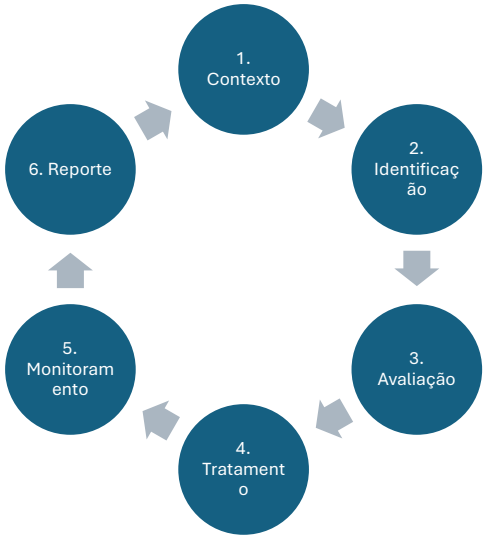
3.3 LIMIAR DE RISCO

Limiar de risco de uma companhia refere-se a sua capacidade de absorver os riscos associados aos seus negócios. De um modo geral, quanto maior a companhia, maior o limiar do risco. O limiar de risco está relacionado à classificação de risco residual, no qual o nível de exposição está equilibrado com a oportunidade potencial do negócio.

3.4 PROCESSO DE GESTÃO DE RISCO

O processo de gestão de riscos da São Carlos é composto por 6 etapas, conforme figura 1 abaixo:

Figura 1 – Etapas da Gestão de Risco



3.4.1 Estabelecimento do contexto

Delimitar o escopo de identificação de um risco, analisando o contexto interno, que envolve a estrutura organizacional, processos, metas e objetivos de longo prazo, sistemas e relações com *stakeholders* internos, assim como o contexto externo, que envolve a análise do ambiente cultural, legal, social, político, financeiro, tecnológico e econômico no qual a Companhia está inserida, seja em âmbito regional, nacional ou internacional.

A São Carlos desenvolve anualmente um plano de negócios que define as suas metas para os próximos 3 anos. Com base neste plano, a Companhia identifica quais riscos serão enfrentados e qual será sua abordagem para endereçá-los.

3.4.2 Identificação de riscos

Identificar um risco envolve realizar uma série de questionamentos sobre cada área ou negócio da Companhia:

(a) o que poderia acontecer de inesperado na área / Companhia?
(b) como é que isso aconteceria?
(c) por que isso aconteceria?
(d) quantas vezes isso já aconteceu na Companhia?
(e) quantas vezes isso já aconteceu no mercado?
(f) qual seria o impacto?
(g) quais são as ações existente para o controle de risco deste impacto?

Os gestores das áreas, com assistência do Comitê de Gestão de Riscos, serão responsáveis por criar uma lista de riscos que possam comprometer a São Carlos em termos operacionais, financeiros ou reputacionais, no presente ou futuro. Com o apoio do Comitê de Gestão de

Riscos, para cada risco, serão definidos controles a serem monitorados como forma de mitigar os riscos.

Esta lista será revisada em reunião pelos diretores de cada unidade de negócio juntamente com o Comitê de Gestão de Riscos para que façam a revisão, mensuração, exclusão e inserção de novos riscos.

Tipos de Risco

As categorias de riscos a serem consideradas pela Companhia com o objetivo de classificar quanto a origem são:

• Riscos Financeiros (RF) – significam os riscos cuja materialização resulte em perdas de recursos financeiros pela Companhia

• Riscos Operacionais, Tecnológicos ou Ambientais (OTA) – significam os riscos cuja materialização resulte em perdas de recursos operacionais atrelados a processos, pessoas e/ou sistemas em decorrência de falhas, deficiências e/ou inadequações diversas

• Risco Estratégico Político (EP) – se refere ao cumprimento dos objetivos da companhia e risco reputacional. Ex.: novos competidores, modelos de negócio disruptivo (modelos novos, rompem a normalidade)

• Riscos Regulatórios (RR) – significam os riscos associados às sanções legais ou regulatórias, de perda financeira ou de reputação, resultante de alguma falha no cumprimento de leis, acordos, regulamentos, do Código de Ética e Conduta e/ou de políticas ou normas internas da Companhia

3.4.3 Avaliação de riscos

O processo de avaliação dos riscos consiste na definição da probabilidade de ocorrência e do impacto de um risco.

Probabilidade

A probabilidade de ocorrência pode ser definida em quatro níveis, de acordo com os seguintes critérios:

- Remota (abaixo de 30%): Chance remota de que o evento ocorra / Histórico de poucas ocorrências ou não possui histórico de materialização do risco
- Possível (entre 31 e 60%): É mais provável que o evento não ocorra do que ocorra / Histórico de moderada frequência de materialização do risco
- Provável (entre 61% e 90%): É mais provável que o evento ocorra que não ocorra / Histórico de alta frequência de materializações do risco
- Muito Provável (acima de 90%): É quase certo que o evento vai ocorrer / Histórico de intensa frequência de materializações do risco

Impacto

O impacto do risco também é definido em quatro níveis: imaterial, moderado, material e catastrófico e deve ser determinado através das seguintes esferas: financeiro, saúde e segurança, meio ambiente, social e cultural, imagem e reputação, clima organizacional e legal.

O resultado da análise dos riscos entre probabilidade e impacto é representado na matriz de riscos, conforme Figura 2 a seguir. A partir desta matriz, define-se o nível do risco: Muito Baixo, Baixo, Médio, Alto e Crítico.

Após identificação e avaliação dos riscos, o Comitê de Gestão de Riscos será o responsável por definir o nível de cada risco, resultado da aplicação da matriz abaixo.

Figura 2 – Matriz de Definição do Nível de Risco

Probabilidade	Imaterial	Moderado	Material	Catastrófico
Muito provável	Médio	Alto	Crítico	Crítico
Provável	Baixo	Médio	Alto	Crítico
Possível	Muito baixo	Baixo	Médio	Alto
Remota	Muito baixo	Muito baixo	Baixo	Médio

Impacto

3.4.4 Tratamento dos Riscos

Esta etapa consiste em verificar qual a tratativa mais adequada para o risco, sendo possíveis as seguintes estratégias:

- **Aceitar**: esta decisão deve ser feita após uma avaliação cuidadosa da probabilidade e impacto do risco, levando em consideração o limiar de risco definido pela Companhia
- **Rejeitar**: neste caso devem ser tomadas todas as medidas consideradas razoáveis para evitar um risco, tais como interromper uma atividade específica ou cancelar um contrato com parceiro
- **Transferir**: envolver um terceiro para compartilhar um investimento e diluir o risco. Ou transferir o risco parcialmente ou completamente com a contratação de um seguro específico para um determinado risco ou grupo de riscos (seguro de patrimônio, D&O, etc)
- **Tratar**: desenvolver mecanismos internos de controle de riscos ou encorajar a revisão do risco de forma adequada. Esses controles podem ser desde pequenos ajustes da cultura de compliance e gestão de risco até a reestruturação de uma área ou negócio.

3.4.5 Monitoramento dos Riscos

Os riscos devem ser monitorados para garantir que o processo de gestão de risco é eficaz. O monitoramento de riscos é uma responsabilidade de toda Companhia, embora com diferentes níveis de responsabilidade que deverão ser definidos na matriz de risco. Todos os riscos deverão ser acompanhados diretamente pelo Comitê de Gestão de Riscos.

Auditoria

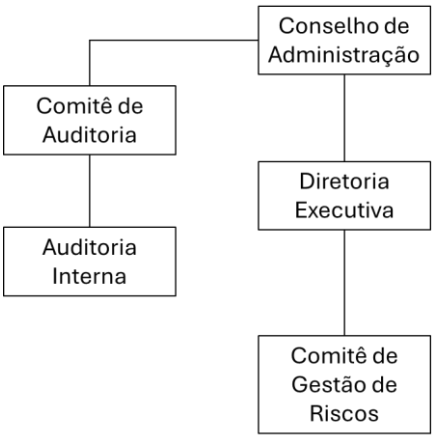
O Comitê de Gestão de Riscos definirá a frequência da auditoria dos controles definidos para cada risco, podendo ser trimestral, semestral ou anual. Nas datas estabelecidas, os gestores farão o reporte do monitoramento dos riscos sob sua gestão. A eficiência dos controles será medida através de testes de efetividade com o responsável pelo risco, conforme definido na matriz de risco.

3.4.6 Reporte

Após a etapa de avaliação, tratamento e monitoramento, o Comitê de Gestão de Riscos apresentará a matriz de riscos final para os responsáveis e para Diretoria Executiva. Neste momento, serão informadas as datas de auditoria e planos de ação, se houver.

4. ESTRUTURA DE GERENCIAMENTO DOS RISCOS/RESPONSABILIDADES

O organograma a seguir, ilustra a estrutura organizacional de gestão de riscos da Companhia:



Abaixo, encontram-se as responsabilidades das instâncias envolvidas no processo:

4.1 Comitê de Auditoria (não estatutário)

São atribuições do Comitê de Auditoria:

(a) Supervisionar o processo gerencial e de monitoramento de riscos, verificando se a Companhia possui mecanismos internos capazes de identificar, avaliar, tratar e monitorar, como uma maneira de gerenciar o perfil de risco da Companhia
(b) Assessorar o Conselho de Administração no que tange ao processo de gestão de riscos da Companhia
(c) Avaliar os parâmetros do modelo de gestão de riscos da Companhia, assim como seus recursos destinados para o processo de gestão de riscos, além da tolerância máxima determinada pela administração
(d) Supervisionar questões estratégicas do processo de gestão de riscos, como o grau de apetite, assim como avaliar e monitorar as exposições de riscos da Companhia

4.2 Conselho de Administração

São atribuições do Conselho de Administração:

(a) Avaliar anualmente os relatórios de gestão de risco
(b) Sugerir novas práticas que estejam de acordo com as determinações dos acionistas
(c) Considerar em suas análises e tomadas de decisões os reportes recebidos do Comitê de Auditoria
(d) Analisar os relatórios emitidos pela auditoria interna, após a verificação do Comitê de Auditoria
(e) Aprovar a política de gestão de riscos e suas eventuais atualizações
(f) Aprovar as atribuições do Comitê de Auditoria e Auditoria Interna

4.3 Diretoria Executiva

São atribuições da Diretoria Executiva:

(a) Estabelecer o nível de Apetite de Risco da Companhia
(b) Aprovar o sistema de gestão de riscos desenvolvido e implementado pela administração
(c) Conduzir as atividades operacionais e o plano de negócios dentro do limiar de risco
(d) Garantir a manutenção do sistema de gestão de riscos em vigor
(e) Garantir o atendimento à esta Política
(f) Desenvolver e aprovar o plano de negócios e metas definidas para a Companhia
(g) Manter uma estrutura de governança adequada
(h) Apresentar o status do processo de gestão de riscos, anualmente, para o Conselho de Administração

4.4 Auditoria Interna

São atribuições da Auditoria Interna:

(a) Reportar suas atividades ao Conselho de Administração diretamente ou por meio do Comitê de Auditoria

(b) Aferir a qualidade e a efetividade dos processos de gestão de riscos, controle e governança da Companhia
(c) Testar a eficácia dos controles estabelecidos para cada risco e reportar os resultados ao Comitê de Auditoria

4.6 Comitê de Gestão de Riscos

O Comitê de Gestão de Riscos será composto, obrigatoriamente, pelo(a) Diretor(a) Financeiro(a), Gerente de Controladoria e Coordenador(a) de Controladoria.

São atribuições do Comitê de Gestão de Riscos:

(a) Coordenar o processo anual de gestão de riscos
(b) Assessorar as áreas de negócio na identificação e avaliação dos diversos tipos de riscos, assim como suportar na definição dos controles e planos de ação
(c) Definir o nível de cada risco com base na matriz Risco x Impacto (Figura 2)
(d) Definir a frequência da auditoria dos controles dos riscos e realizá-la dentro do período estabelecido
(e) Revisar a eficácia dos controles internos em geral
(f) Revisar a política de gestão de riscos anualmente ou sempre que necessário
(g) Revisar a matriz de risco anualmente ou sempre que necessário
(h) Apresentar o status do processo de gestão de riscos, semestralmente, para Diretoria Executiva
(i) Garantir o cumprimento desta Política
(j) Disseminar, continuamente, a cultura de gestão de riscos na Companhia

4.7 Gestores

São atribuições dos colaboradores da Companhia:

(a) Identificar eventuais novos riscos que possam afetar as suas respectivas áreas, assim como manter os controles de monitoramento dos riscos constantemente atualizados (independente de auditorias realizadas pelo Comitê de Gestão de Riscos)

5 RESPONSABILIDADE

O proprietário desta Política é o(a) Diretor(a) Financeiro(a) da Companhia. Cabe a ele, juntamente com o Comitê de Gestão de Riscos, do qual ele é parte, monitorar e assegurar a aderência à esta Política assim como revisá-la sempre que necessário.

6 REVISÃO

Esta Política será revisada e atualizada anualmente, se necessário, pelo Comitê de Gestão de Riscos, que o fará atendendo a legislação, determinações dos órgãos regulatórios, determinações da Diretoria Executiva, Conselho de Administração e Comitê de Auditoria da

Companhia. Quaisquer alterações na estrutura de negócios atual da Companhia ou eventos naturais adversos irão exigir a revisão desta Política para garantir que permaneça adequada e abrangente a todos os riscos existentes no negócio.

7 APROVAÇÃO

A aprovação desta Política e eventuais alterações é de responsabilidade do Conselho de Administração.

8 VIGÊNCIA

Esta política entra em vigor na data de sua aprovação e poderá ser modificada por recomendação da Diretoria Executiva.