1. OBJETIVOS

1.1. Estabelecer diretrizes, conceitos e competências para a condução do processo de gestão de riscos, de acordo com a metodologia definida pela Sabesp, gerando valor para a organização e aperfeiçoando as práticas de governança, de forma sistemática, estruturada e integrada aos valores e diretrizes empresariais; e

1.2. Considerar a visão de riscos na tomada de decisões, alinhada com as boas práticas de mercado.

2. DIRETRIZES

2.1. A gestão de riscos deve ser integrada e alinhada à cultura e ao planejamento estratégico da Companhia, considerando seus valores, objetivos, tomada de decisão, modelo de negócio, operação, estrutura organizacional, nível de exposição e tolerância a riscos.

2.2. Para a elaboração e revisão do Mapa de Riscos Corporativos, a Diretoria Executiva deverá utilizar a metodologia vigente que considera a identificação dos riscos e causas que possam impactar a capacidade da Companhia de atingir os objetivos estratégicos

2.3. A magnitude do risco será definida pela avaliação do impacto, probabilidade de ocorrência e criticidade. Com base nessa avaliação, os Responsáveis pelos Riscos devem definir as ações de mitigação para mantê-los no nível aceitável. A implementação dessas ações será acompanhada pela área de Riscos e Controles Internos.

2.4. A gestão, comunicação e monitoramento dos riscos fica a cargo da área de Riscos e Controles Internos, responsável por apoiar e instrumentalizar a gestão, assegurando a aderência da metodologia de gerenciamento de riscos aos objetivos de negócios da Companhia, propondo atualizações, quando necessário.

2.5. Os riscos devem ser identificados e classificados por sua natureza (estratégica, financeira, operacional, conformidade e climático) e categoria (governança, político/econômico e negócio; contábil, crédito, liquidez e mercado; ambiental, processo e infraestrutura, pessoal, informação e tecnologia; regulamento e legislação; mudanças climáticas).

2.6. Os Riscos Corporativos possuem o Responsável pelo Risco, responsáveis pela aprovação da mensuração, tratamento dos riscos corporativos. O monitoramento do nível de risco e responsabilidade pelas ações de mitigação são definidas por níveis de alçada estabelecidos com base no nível de criticidade do risco.

2.7. Os administradores da Companhia devem zelar pela adequação dos recursos necessários à área de Riscos e Controles Internos para execução das atividades e implantar as ações necessárias para a mitigação dos riscos.

2.8. O Mapa de Riscos Corporativos deve ser atualizado bienalmente e/ou na ocorrência de eventos internos ou externos que afetem os objetivos estratégicos da Companhia e submetido para aprovação do Conselho de Administração.

2.9. Os Riscos Corporativos classificados como críticos (Impacto: Alto, indepentendente da Probabilidade de Ocorrência; Impacto: Significativo e Probabilidade de Ocorrência: Provável ou Quase Certa; e Impacto: Moderado e Probabilidade de Ocorrência: Quase Certa) devem ser acompanhados pelo Comitê de Auditoria, por meio de relatórios periódicos elaborados pela área de Riscos e Controles Internos.

2.10. Os colaboradores que desempenham funções relacionadas à gestão de riscos devem ser capacitados, conforme os princípios e procedimentos definidos na metodologia adotada pela Companhia. A área de Gestão de Riscos deverá assegurar a implementação de programas de treinamento, com periodicidade mínima anual ou sempre que ocorrer atualização relevante na metodologia.

2.11. Os riscos aos quais a Companhia está sujeita devem ser acompanhados pelo Conselho de Administração, Comitê de Auditoria, Diretorias, Área de Riscos e Controles Internos, Auditoria Interna e demais comitês de assessoramento do Conselho de Administração envolvidos na estrutura de gerenciamento de riscos, tais como o Comitê de Transações com Partes Relacionadas e o Comitê de Sustentabilidade, por meio de relatórios periódicos das atividades de cada órgão, conforme aplicável.

Gestão de Riscos Financeiros (exclusivo da Diretoria Financeira e de Relação com Investidores)

2.12. A proteção dos fluxos financeiros que apresentem indexação a variáveis de mercado que possam levar com sua flutuação, ao comprometimento de metas anteriormente estabelecidas de custos e/ou rentabilidade, poderá ser realizada por meio de operações com derivativos.

2.12.1. Para tomada de riscos financeiros e de tesouraria devem ser avaliados produtos a serem utilizados exclusivamente para proteger ativos, passivos e fluxos financeiros indexados da Companhia e de suas controladas contra descasamentos e flutuações de mercado.

2.12.2. A utilização de derivativos fica restrita à proteção de riscos, ficando vedadas operações especulativas.

2.13. Para fins de alçada de aprovação, deve ser considerado valor nominal (*notional* / valor de face) de cada operação com derivativo e observada a política de alçadas vigente.

2.14. A Companhia deve buscar a redução do impacto nos resultados econômicos e financeiros de variáveis que indexem ativos, passivos ou contratos, atuando tempestivamente para que as soluções de mitigação apresentem a efetividade esperada.

2.15. Para controle do Risco de Contraparte:

a) A Companhia utilizará as classificações de risco divulgadas pelas agências *Standard & Poor's* (S&P), *Moody's* ou *Fitch* para definir os limites de exposição máxima das operações de derivativos;

b) O limite de exposição a uma determinada contraparte em operações com derivativos deverá obedecer aos seguintes critérios:

- ✓ *Rating local* mínimo de AA+ ou equivalente, de acordo com a contraparte;
- ✓ Caso alguma contraparte não possua rating local, será utilizada equivalência de seu rating internacional para o rating local.

2.15.1. Eventuais exceções ao quanto previsto no item 2.13 deverão ser submetidas à aprovação do Diretor Presidente e do Diretor Financeiro e de Relações com Investidores.

3. REFERÊNCIAS

- COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management;
- ABNT NBR ISO 31000 – Gestão de Riscos – Diretrizes;
- ABNT NBR ISO 31073 – Gestão de Riscos – Vocabulário;
- Regulamento do Novo Mercado – B3;
- Comissão de Valores Mobiliários – CVM;
- Securities and Exchange Commission – SEC;
- Estatuto Social da Sabesp.

Avaliação de riscos	Processo de avaliação que permite que uma organização considere até que ponto os fatores de riscos em potencial podem impactar a realização dos objetivos estratégicos. A Administração avalia os eventos com base em duas perspectivas – impacto e probabilidade, geralmente, utiliza uma combinação de métodos qualitativos e quantitativos, que resulta no nível de criticidade do risco.
Administradores	Consideram-se Administradores os membros do Conselho de Administração e da Diretoria.
Apetite ao risco	O nível de exposição a riscos que a Companhia está disposta a assumir para alcançar seus objetivos de negócio.
Boas Práticas de Governança	Orientações publicamente reconhecidas, com o objetivo de alcançar e manter transparência, equidade e qualidade das informações, bem como manter reputação positiva perante o mercado e um diferencial na preservação e geração de valor.
Controle	Conjunto de políticas, procedimentos e atividades implementadas para que os riscos sejam gerenciados dentro dos limites do apetite ao risco da Sabesp e que os objetivos estratégicos sejam alcançados de maneira eficaz e eficiente.
Derivativo	Contrato entre as partes, onde ficam estabelecidas as condições futuras de negociação de um determinado ativo-objeto.
Fator de Risco	Fator que tem uma grande influência no risco. Geralmente, utilizado para identificar quais são as possíveis causas que podem materializar um risco.
Gestão de Riscos Corporativos	Processo conduzido pela Administração e supervisionado pelo Conselho de Administração, Comitê de Auditoria e demais comitês de assessoramento ao Conselho de Administração envolvidos na estrutura de gerenciamento de riscos (tais como o Comitê de Transações com Partes Relacionadas e o Comitê de Sustentabilidade), Diretoria Executiva, Diretorias, Gerências Executivas, Gerências, Área de Riscos e Controles Internos e a Auditoria Interna, bem como os demais colaboradores. A gestão de riscos corporativos visa identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com a exposição de risco da organização para assegurar o cumprimento dos seus objetivos. A gestão de risco está diretamente relacionada ao crescimento sustentável, a rentabilidade, a preservação e a geração de valor para a Companhia e seus acionistas, dado que este processo permite a identificação não só de ameaças, como também de oportunidades de aprimoramento e desenvolvimento do negócio.
Identificação de risco	Processos de busca, reconhecimento e descrição de riscos. A identificação de riscos envolve a descrição de fatores e consequências potenciais. Proporcionará gerar uma lista abrangente de riscos (portfólio) baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.
Impacto	Resultado ou efeito de um evento de risco. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos de negócio da Companhia.

Mapa de Riscos Corporativos	Representação gráfica referente ao processo de análise de riscos no ambiente corporativo. No caso da Sabesp, é apresentado graficamente no layout de mapa 4 X 4, através de posicionamento do nível do risco em quadrante com cor correspondente. Representado no plano cartesiano, por pares ordenados (Impacto e Probabilidade): Eixo Y: Impacto: 4 – Alto (vermelho), 3 – Significativo (laranja), 2 – Moderado (amarelo), 1 - Baixo (verde claro) Eixo X: Probabilidade: 4 - Quase Certa (vermelho), 3 - Provável (laranja), 2 - Possível (amarelo), 1 – Baixa (verde claro).
Metodologia de Gestão de Riscos	Conjunto de definições de padrões na identificação, análise, avaliação, tratamento e monitoramento dos riscos, com base na aplicação do modelo do COSO ERM "Enterprise Risk Management – Integrated Framework", nas normas ABNT NBR ISO 31000 e ABNT NBR ISO 31073 – Gestão de riscos – Vocabulário, de forma flexível às características e peculiaridades da Sabesp e de seu ambiente de negócios.
Nível de Alçada	É o nível de acompanhamento e monitoramento dos riscos e dos respectivos planos de ação mitigatórios: Em relação aos riscos classificados com criticidade Baixa, compete às Diretorias. Em relação aos riscos classificados com criticidade Moderada, compete às Diretoria Executivas. Em relação aos riscos classificados com criticidade Crítica, compete ao Comitê de Auditoria.
Probabilidade	Chance de um evento acontecer. Na terminologia de gestão de riscos, a palavra "probabilidade" é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período).
Rating	Refere-se à avaliação da capacidade de uma organização cumprir suas obrigações financeiras, expressa por uma nota atribuída por agências especializadas (Standard & Poor's – S&P, Moody's ou Fitch.
Responsável pelo risco/ Dono do Risco	Área responsável por identificar, avaliar, tratar, comunicar, monitorar riscos corporativos ou de processos e elaborar planos de ação para mitigação dos riscos.
Resultados econômicos	Está relacionado ao resultado de lucro ou prejuízo contábil, medindo a eficiência operacional do negócio ao considerar receitas e despesas, independentemente do fluxo de caixa.
Resultados financeiros	Representa a liquidez e a capacidade da empresa de gerar caixa, levando em conta os fluxos de entrada e saída de dinheiro.
Risco corporativo	Risco que pode comprometer a capacidade da Companhia de atingir seus objetivos estratégicos.

1. **Conselho de Administração**
   a) aprovar as diretrizes e a Política Institucional de Gestão de Riscos Corporativos;
   b) analisar e deliberar sobre o mapa de riscos corporativos da Companhia apresentado pela Diretoria Executiva, bem como sobre os planos de ação para mitigação dos riscos aos quais a Companhia está sujeita;
   c) supervisionar, com suporte do Comitê de Auditoria, a efetividade da estrutura e do processo de gerenciamento dos riscos; e
   d) comunicar, assim que possível, à área de Riscos e Controles Internos sobre novos riscos que possam surgir.

2. **Comitê de Auditoria**
   a) avaliar o mapa de riscos corporativos da Companhia;
   b) observado o Nível de Alçada, avaliar os planos de ação para mitigação dos riscos a serem deliberados pelo Conselho de Administração;
   c) acompanhar o plano anual de trabalho de gestão de riscos corporativos;
   d) acompanhar e avaliar a evolução de implantação dos planos de ação mitigatórios dos riscos corporativos de seu Nível de Alçada;
   e) assegurar a autoridade, autonomia, independência e responsabilidade da área de Riscos e Controles Internos; e
   f) comunicar, no menor prazo possível, a área de Riscos e Controles Internos caso identificados novos riscos.

3. **Diretoria Executiva**
   a) submeter a Política Institucional de Gestão de Riscos Corporativos à aprovação do Conselho de Administração;
   b) implementar as estratégias e diretrizes aprovadas pelo Conselho de Administração em relação ao gerenciamento de riscos, coordenando as demais áreas para este fim, de modo a manter os riscos aos quais a Companhia está sujeita em níveis compatíveis com o seu apetite de riscos;
   c) apoiar a execução dos trabalhos de identificação, análise, avaliação, tratamento, comunicação e monitoramento dos riscos;
   d) elaborar o mapa de riscos corporativos da Companhia e submetê-lo bienalmente ao Conselho de Administração, após a avaliação do Comitê de Auditoria, propondo as medidas necessárias para mitigação dos riscos moderados e críticos;
   e) acompanhar e avaliar a evolução de implantação dos planos de ação mitigatórios dos riscos, de acordo com as informações disponibilizadas pelas demais áreas envolvidas na estrutura de gerenciamento de riscos;
   f) apoiar a disseminação da cultura de gestão de riscos;
   g) comunicar, no menor prazo possível, à área de Riscos e Controles Internos, caso sejam identificados novos riscos; e
   h) exclusivamente em relação ao Diretor Financeiro e de Relações com Investidores, orientar e realizar a análise de investimentos e definição dos limites de exposição a risco,

propositura e contratação de empréstimos e financiamentos, operações de tesouraria e o planejamento e controle financeiro da Companhia.

4. **Diretorias**
   a) conhecer a metodologia e os Níveis de Alçada de riscos que definem as competências para aprovação e tratamento dos riscos;
   b) identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos de sua competência;
   c) implementar e acompanhar a evolução dos planos de ação mitigatórios dos riscos, de sua competência;
   d) propor à Diretoria Executiva o tratamento e os planos de ação mitigatórios dos riscos de sua competência;
   e) definir e acompanhar os indicadores de riscos;
   f) utilizar os resultados das avaliações de riscos para priorizar a elaboração e/ou revisão de planos de contingência;
   g) efetuar reportes periódicos à área de Riscos e Controles Internos sobre os riscos, indicadores e respectivos planos de ação mitigatórios sob sua responsabilidade (possível mudança de impacto, probabilidade e/ou medidas mitigatórias); e
   h) comunicar, no menor prazo possível, à área de Riscos e Controles Internos, caso sejam identificados novos riscos.

5. **Área de Riscos e Controles Internos**
   a) propor revisões à Política Institucional de Gestão de Riscos Corporativos, quando necessário;
   b) assegurar o alinhamento da prática do gerenciamento de riscos com a Missão, Visão, Valores e Diretrizes da Companhia;
   c) elaborar o plano anual de trabalho de gestão de riscos corporativos, de acordo com as orientações do Comitê de Auditoria;
   d) assessorar a Diretoria Executiva na elaboração bienal do Mapa de Riscos Corporativos, consultando as áreas da Companhia, revisando os riscos existentes e incorporando novos riscos identificados;
   e) consolidar e garantir a distribuição do mapa de riscos corporativos, de acordo com os níveis de alçada definidos;
   f) acompanhar a evolução de implantação dos planos de ação mitigatórios;
   g) elaborar o relatório das atividades de gestão de riscos (Mapa de Riscos, Acompanhamentos dos Planos de Ação e Indicadores de Riscos Críticos);
   h) capacitar a liderança e os colaboradores envolvidos nas atividades de gestão de riscos para aplicação da metodologia adotada pela Companhia;
   i) disseminar a cultura de gestão de riscos em todos os níveis da Companhia;
   j) desenvolver, sugerir e revisar diretrizes para o processo de gestão de riscos corporativos da Companhia (classificação do risco, dicionário do risco, sistema informatizado, mapa de risco, metodologia de análise: identificação, análise, avaliação, tratamento, comunicação e monitoramento);

k) apoiar a execução dos trabalhos de identificação, análise, avaliação, tratamento, comunicação e monitoramento dos riscos;

l) acompanhar os indicadores de riscos e desempenho do processo de gestão de riscos; e

m) gerenciar o sistema informatizado de gestão de riscos.

6. Área de Auditoria Interna

a) conhecer o mapa de riscos corporativos;

b) considerar o mapa de riscos corporativos para elaboração da programação do trabalho de auditoria interna da Sabesp; e

c) aferir a qualidade e efetividade do gerenciamento dos riscos e dos processos de governança da Companhia.