COMPANHIA DO METROPOLITANO DE SÃO PAULO | METRÔ

INSTRUMENTO NORMATIVO

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
POL-01-201	**02**	**GESTÃO DE RISCOS CORPORATIVOS**	**A partir de: 04/08/2022**

DESTINATÁRIO

Todas as Unidades Organizacionais

PRINCIPAIS ALTERAÇÕES

Atualização das diretrizes considerando a legislação pertinente e as melhores práticas do mercado.

UNIDADE GESTORA DO PROCESSO (Assinatura e Carimbo)	DOCUMENTO DE APROVAÇÃO
GRC - original assinado por Marcelo Monteiro Praça	**RCA-020/2022**

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
POL-01-201	**02**	**GESTÃO DE RISCOS CORPORATIVOS**	**A partir de: 04/08/2022**

SUMÁRIO

1 FINALIDADE

Estabelecer diretrizes, conceitos e responsabilidades na identificação, avaliação, tratamento, monitoramento e comunicação de riscos no ambiente corporativo, contribuindo com o aprimoramento da governança corporativa, do planejamento empresarial e, na preservação e geração de valor da organização.

A avaliação de risco envolve um processo dinâmico e iterativo para identificar e analisar os riscos para a realização dos objetivos da entidade. Ela constitui a base para determinar como esses riscos devem ser gerenciados. A Administração leva em conta, em sua análise de riscos corporativos, possíveis mudanças no ambiente externo e no seu próprio modelo de negócio, que podem interferir em sua capacidade de realizar os objetivos.

Os riscos corporativos envolvem as atividades do negócio da empresa, os riscos de integridade e os regulatórios.

2 DEFINIÇÕES

2.1 **ALÇADA**

Nível de competência da autoridade responsável pela aprovação da mensuração e tratamento de riscos corporativos.

2.2 **AVALIAÇÃO DE RISCO**

Processo de avaliação da criticidade do risco que permite a organização considerar até que ponto os fatores de riscos em potencial podem impactar a realização dos objetivos e as estratégias, com vistas a subsidiar tomada de decisão para resposta ao risco.

Nota: A Administração avalia os eventos com base em duas perspectivas – probabilidade e impacto – e, geralmente, utiliza uma combinação de métodos qualitativos e quantitativos.

2.3 **DONO DO RISCO (*RISK OWNER*)**

Autoridade que tem a responsabilidade pela identificação e gerenciamento dos riscos do processo sob sua gestão. Os gestores dos processos são os donos do risco.

2.4 **EVENTO**

Ocorrência ou mudança em um conjunto específico de circunstâncias (ISO 31000:2018).

Incidentes ou ocorrências originadas a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos (Coso ERM).

2.5 **FATOR DE RISCO**

Elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco (ISO 31000:2018).

2.6 GESTÃO DE RISCOS CORPORATIVOS

Processo 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 compatíveis com a exposição de riscos da organização e possibilitar garantia razoável do cumprimento dos seus objetivos.

Os riscos corporativos envolvem as atividades do negócio da empresa, os riscos de integridade e os regulatórios.

Nota: Processo conduzido na Companhia do Metrô pelo Conselho de Administração, Comitê de Auditoria, Diretoria, Comissão de Gestão de Riscos Corporativos, Gerências e demais empregados.

2.7 IDENTIFICAÇÃO DE RISCO

Processo de identificação de riscos que afetam o desempenho dos objetivos e das estratégias empresariais. Envolve a descrição de fatores, consequências potenciais e controles envolvidos.

Nota: A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas experientes, especialistas e as necessidades das partes interessadas.

2.8 IMPACTO

Resultado ou efeito da materialização de um evento de risco sobre os objetivos estratégicos da empresa,

Notas:

(1) Poderá ocorrer uma série de impactos possíveis associados a um evento.

(2) O impacto de um evento pode ser positivo ou negativo em relação aos objetivos correlatos da Companhia do Metrô.

2.9 PRINCIPAIS INDICADORES DE RISCO - KRI (*KEY RISK INDICATOR*)

Medida para avaliar como o risco se comporta e para fornecer alertas de forma rápida e antecipada quanto à exposição, seu potencial de ganho ou perda futura.

2.10 MAPA DE RISCO

Representação formal na qual são registrados os riscos identificados e avaliados, sob a perspectiva de probabilidade e impacto (nível do risco), de forma a permitir a definição das ações necessárias ao seu gerenciamento.

Nota: É representado no plano cartesiano, por pares ordenados (Probabilidade e Impacto), podendo ser definida a quantidade de níveis conforme a análise pretendida. Na Companhia do Metrô, o Mapa de Risco é do tipo 5x5, sendo Eixo X a Probabilidade e o Eixo Y o Impacto.

2.11 MELHORIA CONTÍNUA DA ESTRUTURA

Melhoria na capacidade de gerenciar riscos da organização e em sua cultura de gestão de riscos com base nos resultados do monitoramento e das análises críticas.

2.12 MONITORAMENTO

Avaliação contínua do processo de gestão de riscos com a finalidade de evidenciar as mudanças no nível de desempenho requerido ou esperado, resultantes das ações adotadas pelo gestor.

2.13 NÍVEL DO RISCO / CRITICIDADE

Resultado da combinação de duas dimensões: probabilidade e impacto.

Associa-se a cores diferentes no mapa de riscos conforme seu nível, podendo ser:

- Extrema (vermelho),
- Alta (laranja),
- Média (amarelo),
- Baixa (verde).

O nível de criticidade determina a alçada de tratamento do risco, respectivamente: Conselho de Administração, Diretoria Plena, Diretor e Gerente.

Notas: Na Companhia do Metrô as réguas de classificação de riscos são:

(1) Impacto: Alto (vermelho), Significativo (laranja), Moderado (amarelo), Baixo e Mínimo (verde);

(2) Probabilidade: Quase Certa (vermelho), Provável (laranja), Possível (amarelo), Baixa e Improvável (verde).

2.14 NÍVEL DE TOLERÂNCIA AO RISCO

Nível aceitável de variação no desempenho quanto a realização dos objetivos. Operar dentro da tolerância ao risco dá à Administração mais confiança que a entidade atingirá seus objetivos.

2.15 PROBABILIDADE

Possibilidade de que um evento de risco ocorra (Coso ERM).

Chance de algo acontecer (ISO 31000:2018).

2.16 RISCO

Possibilidade de um evento ocorrer e afetar desfavoravelmente a realização dos objetivos da organização (Coso ERM).

Conforme Norma ISO 31000:2018, também pode ser definido como efeito da incerteza nos objetivos.

2.17 RISCO INERENTE

Risco que se apresenta a uma organização na ausência de qualquer medida gerencial que poderia alterar a probabilidade ou o impacto de um risco (Coso ERM).

2.18 RISCO RESIDUAL

Risco que resta após a administração ter adotado medidas para alterar a probabilidade ou o impacto dos riscos (Coso ERM).

2.19 TRATAMENTO DE RISCO

Processo de seleção e implementação de medidas para aceitar, reduzir, transferir ou compartilhar e evitar os riscos.

3 DIRETRIZES

3.1 Assegurar que o planejamento estratégico, o plano de negócios e os programas anuais e plurianuais contemplem os riscos e a sua gestão.

3.2 Praticar a gestão de riscos corporativos em todos os processos da empresa, com o uso de linguagem comum e padrões estabelecidos nesta política e procedimentos descritos nos documentos vinculados.

3.3 Difundir a cultura de gestão de riscos em todos os níveis hierárquicos da organização, com uso de linguagem comum, seguindo as boas práticas existentes

3.4 Preparar o capital humano alinhado à estratégia e aos objetivos de negócios, capacitando-o na metodologia utilizada.

3.5 Adotar como oportunidade de melhoria na gestão dos processos de trabalho a identificação e monitoramento dos riscos.

3.6 Assegurar que os riscos corporativos sejam identificados, mensurados e tratados pelos gestores dos processos, em suas áreas de atuação, com o apoio da equipe técnica do Departamento de Gestão de Riscos e Controle Interno (GRC/RCG).

3.7 Assegurar que os níveis de alçada competentes aprovem e acompanhem periodicamente os riscos avaliados.

3.8 Assegurar que toda exposição de riscos seja avaliada, com definição do tratamento e se for o caso, com o estabelecimento de plano de ação, identificando os responsáveis e os indicadores de acompanhamentos dos riscos.

3.9 Garantir que a melhoria contínua da gestão de riscos ocorra por ciclos de avaliações e revisões ou em resposta a um fato específico, aprimorando os processos e controles da Companhia.

3.10 Assegurar que a Companhia do Metrô desenvolva planos de resposta e retomada das atividades para os seus principais processos com base nos resultados das avaliações de riscos.

3.11 Comunicar os riscos corporativos às partes interessadas, por meio dos canais competentes, com critérios alinhados à legislação e às boas práticas de governança corporativa.

3.12 Garantir a classificação dos riscos por origem de eventos (internos ou externos), natureza (estratégico, operacional, financeiro / divulgação e conformidade / regulamentar), categoria e subcategorias.

3.13 Utilizar os riscos para a tomada de decisões estratégicas de forma que contribuam para a realização dos objetivos corporativos.

3.14 Agregar valor à organização, promover maior transparência das informações, aperfeiçoar as práticas de governança e contribuir para a sustentabilidade da Companhia

3.15 Apoiar o Programa de Integridade, observando as diretrizes estabelecidas na legislação sobre fraude e corrupção.

4 DOCUMENTOS DE REFERÊNCIA

4.1 Lei 13.303/16 – Lei das Estatais

4.2 COSO ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Entreprise Risk Manegement Framework*.

4.3 ABNT NBR ISO 31000 – Gestão de Riscos: Princípios e Diretrizes.

4.4 ABNT ISO GUIA 73 – Gestão de Riscos: Vocabulário.

4.5 Estatuto Social da Companhia do Metrô.

4.6 Código de Conduta e Integridade da Companhia do Metrô.

4.7 Regulamento Interno da Companhia do Metropolitano de São Paulo – Metrô.

4.8 Regimento Interno do Comitê de Auditoria.

5 DOCUMENTOS VINCULADOS

5.1 Regulamento de Gestão de Riscos Corporativos da Companhia do Metropolitano de São Paulo – Metrô.

6 DISPOSIÇÕES FINAIS

6.1 As situações não previstas neste Instrumento Normativo serão analisadas e deliberadas pela Gerência de Gestão de Riscos Corporativos e Conformidade (GRC).

6.2 Este Instrumento Normativo revoga e substitui o de código POL-00-201 - Rev. 01 – Gestão de Riscos Corporativos, de 05/02/2019, e demais disposições em contrário.

QUADRO DE REVISÕES

CÓDIGO DO IN	REV.	VIGÊNCIA	MOTIVO
POL-01-201	00	28/01/2009	Instrumento Normativo implementador.
POL-01-201	01	05/02/2019	Atualização das diretrizes considerando a legislação pertinente e as melhores práticas do mercado.

REVISORES

Nome	Reg.	Área
Silvio Valdrighi	33.610-0	GRC/RCG
Maria Silvia Soares de Oliveira Mondolfo	09.046-1	GRC/RCG
Lisias Ruiz Martins Barbosa	12.008-5	GRC/RCG
Silvia Helena Correa Barbosa	29.535-7	GRC/RCC