



CÓDIGO <b>POL-01-201</b>	REVISÃO <b>01</b>	TÍTULO <b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	VIGÊNCIA <b>A partir de: 05/02/2019</b>
-----------------------------	----------------------	--	--

## 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)

**GRC - original assinado por Marcelo Monteiro  
Praça**

DOCUMENTO DE APROVAÇÃO

**RCA-004/2019**

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
<b>POL-01-201</b>	<b>01</b>	<b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	<b>A partir de: 05/02/2019</b>

## SUMÁRIO

1 FINALIDADE.....	3
2 DEFINIÇÕES.....	3
2.1 ALÇADA .....	3
2.2 AVALIAÇÃO DE RISCO .....	3
2.3 DONO DO RISCO ( <i>RISK OWNER</i> ) .....	3
2.4 GESTÃO DE RISCOS CORPORATIVOS .....	3
2.5 IDENTIFICAÇÃO DE RISCO .....	3
2.6 IMPACTO.....	4
2.7 INDICADOR DE RISCO - KRI ( <i>KEY RISK INDICATOR</i> ) .....	4
2.8 MAPA DE RISCO .....	4
2.9 MELHORIA CONTÍNUA DA ESTRUTURA.....	4
2.10 MONITORAMENTO .....	4
2.11 NÍVEL DO RISCO / CRITICIDADE.....	4
2.12 NÍVEL DE TOLERÂNCIA AO RISCO.....	4
2.13 PROBABILIDADE.....	4
2.14 RISCO .....	5
2.15 TRATAMENTO DE RISCO .....	5
3 DIRETRIZES .....	5
4 DOCUMENTOS DE REFERÊNCIA .....	6
5 DOCUMENTOS VINCULADOS .....	6
6 DISPOSIÇÕES FINAIS.....	6
QUADRO DE REVISÕES .....	7
REVISORES .....	7

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
POL-01-201	01	POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS	A partir de: 05/02/2019

## 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.

## 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 relativa àqueles que necessitam de tratamento.

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

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

### 2.5 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.

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
<b>POL-01-201</b>	<b>01</b>	<b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	<b>A partir de: 05/02/2019</b>

## 2.6 IMPACTO

Resultado ou efeito de um evento de risco.

### Notas:

- (1) Poderá haver 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 de uma empresa.

## 2.7 INDICADOR 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.

## 2.8 MAPA DE RISCO

Representação formal onde 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.

## 2.9 MELHORIA CONTÍNUA DA ESTRUTURA

Melhoria contínua da estrutura de gestão de riscos visando seu aperfeiçoamento e a disseminação da cultura na Companhia.

## 2.10 MONITORAMENTO

Avaliação contínua do processo de gestão de riscos com a finalidade de evidenciar as mudanças no nível de desempenho requerido ou esperado.

## 2.11 NÍVEL DO RISCO / CRITICIDADE

Resultado da combinação de pesos das duas perspectivas: probabilidade e impacto.

**Nota:** Associa-se a cores diferentes no mapa de riscos conforme seu nível. Na Companhia do Metrô as réguas de classificação de riscos são:

- a) Impacto: Alto (vermelho), Significativo (laranja), Moderado (amarelo), Baixo (verde claro) e Mínimo (verde escuro);
- b) Probabilidade: Quase Certo (vermelho), Provável (laranja), Possível (amarelo), Baixa (verde claro) e Improvável (verde escuro).

## 2.12 NÍVEL DE TOLERÂNCIA AO RISCO

Nível de variação no desempenho quanto à realização dos objetivos.

## 2.13 PROBABILIDADE

Grau de possibilidade de que um evento de risco ocorra.

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
<b>POL-01-201</b>	<b>01</b>	<b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	<b>A partir de: 05/02/2019</b>

## **2.14 RISCO**

Risco é a possibilidade de um evento ocorrer e afetar a realização dos objetivos da Organização.

## **2.15 TRATAMENTO DE RISCO**

Processo de seleção e implementação de medidas para aceitar/monitorar, 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 descrito 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 Corporativos (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 estabeleça planos de contingência 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.

CÓDIGO	REVISÃO	TÍTULO	VIGÊNCIA
<b>POL-01-201</b>	<b>01</b>	<b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	<b>A partir de: 05/02/2019</b>

- 3.12 Garantir a classificação dos riscos por origem de eventos (internos ou externos), natureza (estratégico, operacional, financeiro e conformidade), 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.
- 3.16 Assegurar a revisão desse instrumento normativo anualmente ou a qualquer momento quando de alguma alteração de processo ou legislação.

#### **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 – Enterprise Risk Management Framework*.
- 4.3 ABNT NBR ISO 31000:2009 – Gestão de Riscos – Princípios e Diretrizes.
- 4.4 ABNT ISO GUIA 73:2009 – 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**

Não há

#### **6 DISPOSIÇÕES FINAIS**

- 6.1 As situações não previstas neste Instrumento Normativo serão analisadas e deliberadas pela Gerência de Gestão de Riscos Corporativos, Segurança da Informação e Conformidade (GRC).
- 6.2 Este Instrumento Normativo revoga e substitui o de código POL-00-201 - Rev. 00 – Gestão de Riscos Corporativos, de 28/01/2009, e demais disposições em contrário.

<b>CÓDIGO</b> <b>POL-01-201</b>	<b>REVISÃO</b> <b>01</b>	<b>TÍTULO</b> <b>POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS</b>	<b>VIGÊNCIA</b> <b>A partir de: 05/02/2019</b>
------------------------------------	-----------------------------	---	---

**QUADRO DE REVISÕES**

<b>CÓDIGO DO IN</b>	<b>REV.</b>	<b>VIGÊNCIA</b>	<b>MOTIVO</b>
POL-01-201	00	28/01/2009	Instrumento Normativo implementador

**REVISORES**

<b>Nome</b>	<b>Reg.</b>	<b>Área</b>
Silvio Valdrighi	33.610-0	GRC/RCG
Maria Silvia Soares de Oliveira Mondolfo	09.046-1	GRC/RCG
Lísias Ruiz Martins Barbosa	12.008-5	GRC/RCG
Jana Eleonora Brando D'Avila	27.581-0	GRC/RCC
Rui Pastor	11.877-3	GRC/RCC
Sergio Anunciação Ortona	03.764-1	GRC/RCC