

## POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

**IPT 18652**

Esta cópia é de propriedade do Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A. – IPT.  
Reprodução parcial ou total é proibida. Não pode ser cedido a terceiros sem prévia e formal autorização.

Aprovado pelo Conselho de Administração em 17.10.2022

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

## Sumário

1. Objetivo .....	3
2. Escopo e Diretrizes Gerais da Política de Riscos .....	3
2.1. Escopo .....	3
2.2. Princípios e Diretrizes.....	3
3. Appetite a Risco e Limites Aceitáveis para Riscos .....	4
4. Etapas da Gestão de Riscos.....	5
4.1. Identificação dos Riscos .....	5
4.2. Análise dos Riscos .....	5
4.3. Tratamento dos Riscos .....	6
4.4. Monitoramento dos Riscos e Comunicação.....	6
5. Estrutura Organizacional para a Gestão de Riscos e Instâncias de Governança .....	7
5.1. Estrutura Organizacional, Atribuições e Responsabilidades.....	7
6. Referências.....	10

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

## 1. Objetivo

Estabelecer os princípios da Gestão de Riscos, seus níveis de responsabilidades, os limites aceitáveis e as diretrizes para a identificação, análise, tratamento e monitoramento dos riscos no Instituto de Pesquisas Tecnológicas do Estado de São Paulo S.A. - (IPT).

## 2. Escopo e Diretrizes Gerais da Política de Riscos

### 2.1. Escopo

A Política de Gestão de Riscos do IPT está alinhada à sua estratégia, definida e atualizada no Plano Estratégico Quinquenal e colabora para que seus objetivos sejam alcançados com maior preservação e geração de valor.

A Política de Gestão de Riscos tem abrangência para todo o IPT e aplica-se a todos os colaboradores, incluindo empregados, estagiários, bolsistas e prestadores de serviço.

A gestão de riscos está incluída no compromisso do IPT com a lei federal nº 13.303, de 2016, pelo qual deve assumir responsabilidades com metas e resultados específicos e para que seja possível avaliar e fiscalizar o trabalho desempenhado.

### 2.2. Princípios e Diretrizes

O IPT deve cumprir sua missão, executar suas estratégias de curto e longo prazos, garantir a sustentabilidade e a continuidade de suas atividades, preservar a vida, o ambiente, seus bens e direitos tangíveis e intangíveis.

Além de proteger seu patrimônio físico e humano, o IPT concentra notável valor intangível que deve ser resguardado contra ameaças, intencionais ou não, principalmente contra sua imagem, reputação, integridade, credibilidade, tecnologia, informação e conhecimento acumulado.

A gestão de riscos insere-se no compromisso do IPT em atuar de forma ética, íntegra e em conformidade com os requisitos legais e regulatórios estabelecidos em todas as jurisdições onde atua.

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

A gestão de riscos deve incorporar as particularidades do IPT e dar suporte para a tomada de decisões baseadas no autoconhecimento de competências, no diagnóstico de vulnerabilidades e na tolerância a riscos específicas de suas atividades.

Os riscos devem ser gerenciados de forma proativa e abrangente, por todas as linhas de atuação, para que estejam no nível de exposição aceitável e de acordo com o apetite a risco do IPT.

Os riscos devem ser considerados em todas as decisões do IPT e sua gestão deve ser realizada de maneira integrada, aproveitando as sinergias entre Unidades de Negócios e o efeito da diversificação.

A filosofia de gestão de riscos deve ser incorporada na cultura do IPT para favorecer a comunicação sobre riscos, antecipar ameaças que possam afetar seus objetivos estratégicos e aperfeiçoar as práticas de governança e de gestão.

Os conceitos e métodos empregados na identificação, análise, avaliação e tratamento dos riscos devem ser uniformizados em todo o IPT de forma estruturada e sistemática para melhorar a confiabilidade das informações, a eficiência e eficácia da gestão de riscos.

Considerando a relação entre gestão de riscos e estratégia, os objetivos estratégicos do Plano Anual e do Plano Quinquenal devem ser disponibilizados para conhecimento dos Diretores de Unidade de Negócios, Coordenadores e Gestores. Os objetivos estratégicos das Unidades de Negócio devem estar alinhados aos objetivos estratégicos institucionais. Sobre esse conjunto de objetivos, os riscos serão gerenciados.

### **3. Apetite a Risco e Limites Aceitáveis para Riscos**

A quantidade e o tipo de riscos que o IPT está disposto a assumir para atingir seus objetivos devem ser estabelecidos de acordo com as atribuições e responsabilidades detalhadas no item 5 desta política de gestão de riscos.

Fundamentados pela visão e pelos valores históricos do IPT, o nível de apetite para riscos político-legais, éticos e de imagem-reputação devem ser mínimos, assim como para os riscos financeiros.

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

## 4. Etapas da Gestão de Riscos

Para a gestão de riscos, o IPT considera seu planejamento estratégico, seus ambientes de valor e de negócios e seu apetite a risco, de acordo com o escopo, princípios e diretrizes apresentados no item 2 dessa política. Para isso, utiliza como estrutura conceitual para a integração entre estratégia e desempenho, para o apetite a risco e para as etapas da gestão de riscos, os princípios do *Committee of Sponsoring Organizations of the Treadway Commission* - COSO. Também utiliza as diretrizes do Instituto Brasileiro de Governança Corporativa - IBGC para a elaboração de políticas de gestão de riscos, o modelo de três linhas de atuação em riscos do *Institute of Internal Auditors* - IIA (diferencia três grupos envolvidos no gerenciamento de riscos, seus papéis, responsabilidades e relacionamentos) e os conceitos da norma NBR ISO 31.000.

### 4.1. Identificação dos Riscos

Os riscos são identificados por meio de uma matriz de riscos que considera as ameaças aos objetivos estratégicos definidos para o IPT. A matriz de riscos é composta por agentes dos ambientes de valor e de negócios do IPT e de uma taxonomia que considera riscos Tecnológicos, Político-legais, Econômicos, Ambientais, Sociais, de Imagem-reputação, Financeiros, Operacionais, Éticos, de Inovação, Estratégicos e Digitais. O levantamento de riscos deve perpassar todos os agentes com potencial para destruição de valor e pelas categorias de riscos presentes na taxonomia, não sendo obrigatória a identificação de riscos em todos os elementos dessa matriz.

### 4.2. Análise dos Riscos

Os riscos elencados na matriz de riscos do IPT são analisados por meio de cinco dimensões: quanto à possibilidade de o evento de consequência negativa ocorrer na organização (Possibilidade de Ocorrência); quanto à consequência negativa da materialização do risco nos objetivos do IPT (Impacto); quanto ao lapso de tempo entre a materialização do risco e a percepção de seus efeitos pelo IPT (Tempo de Percepção do Risco); quanto ao nível de preparação para enfrentar ou mitigar o risco (Vulnerabilidade ao Risco); e quanto à disposição

IPT 18652	Revisão: 00	Data de Aprovação: 17.10.2022
Elaborado por: Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		Aprovado por: Conselho de Administração do IPT

dos tomadores de decisões relacionadas ao risco para aceitá-lo na perseguição de seus objetivos (Tolerância a Risco).

Os riscos são então categorizados por meio de relações entre essas cinco dimensões e analisados quantitativamente pela Severidade (relação entre Possibilidade de Ocorrência e Impacto) e pelo Risco Residual (relação entre Severidade e Vulnerabilidade ao Risco). Também são analisados de forma qualitativa pela ponderação entre as cinco dimensões no contexto das estratégias adotadas e dentro das diretrizes desta política.

### **4.3. Tratamento dos Riscos**

Todos os riscos categorizados como prioritários a partir da matriz de riscos devem ter uma ou mais ações associadas, que em conjunto definem a resposta ao risco. As ações podem ser dos seguintes tipos: evitar, reduzir, transferir ou aceitar o risco.

Todos os riscos categorizados como prioritários devem ter um gestor associado e denominado “dono do risco”.

Os riscos com Severidade Muito Alta, Alta, ou Média devem ter um gestor associado ao dono do risco e que garanta seu acompanhamento e a eficácia das ações de resposta ao risco. O dono do risco é responsável por executar a ação de resposta no prazo definido. Caso as ações de resposta envolvam mais de uma área, o dono do risco é responsável pela articulação junto às demais áreas.

Na eventualidade de não ser viável a definição de ações para os riscos categorizados como prioritários, o dono do risco deve justificar o motivo de manter-se tolerante ao risco, devendo escalonar a comunicação conforme a estrutura organizacional para a gestão de riscos e instâncias de governança do item 5 desta política.

Os prazos para tratamento dos riscos devem ser definidos em procedimentos específicos.

### **4.4. Monitoramento dos Riscos e Comunicação**

O IPT deve planejar o monitoramento e a comunicação como parte integrante do gerenciamento de riscos. O monitoramento dos riscos tem como objetivo acompanhar a implantação e eficácia

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

das ações implementadas como resposta que, em última instância, permite verificar a evolução dos riscos ao longo do tempo e identificar novos riscos.

A GECON deve acompanhar a gestão dos riscos do IPT por meio de relatórios, indicadores, marcos críticos definidos nos planos de ação ou outros meios por ela estabelecidos. Também deve estabelecer uma agenda propositiva para uniformizar, de forma estruturada, os conceitos e metodologias empregados na identificação, análise, tratamento, monitoramento e comunicação dos riscos.

## **5. Estrutura Organizacional para a Gestão de Riscos e Instâncias de Governança**

### **5.1. Estrutura Organizacional, Atribuições e Responsabilidades**

O **Conselho de Administração** tem as seguintes atribuições e responsabilidades:

- i. Estabelecer as diretrizes gerais das estratégias de gestão de riscos do IPT;
- ii. Avaliar e aprovar a Política de Gestão de Riscos e suas revisões;
- iii. Avaliar e aprovar as diretrizes gerais para estabelecimento dos limites aceitáveis para exposição a riscos (Apetite a risco do IPT) e suas revisões;
- iv. Supervisionar as atividades relacionadas ao gerenciamento de riscos executadas pelo Comitê de Auditoria Estatutário (CAE) e Diretoria;
- v. Avaliar a adequação da estrutura destinada ao processo de gerenciamento de riscos: recursos humanos, financeiros e infraestrutura;
- vi. Tomar decisões em casos que envolvam assunção de risco.

O **Comitê de Auditoria Estatutário (CAE)** tem as seguintes atribuições e responsabilidades:

- i. Auxiliar o Conselho de Administração nas definições gerais das estratégias de gestão de riscos do IPT e promover suas revisões;
- ii. Avaliar e supervisionar o processo de gestão de riscos desempenhado pela Diretoria, inclusive através dos trabalhos da Auditoria Interna e da Gerência de Conformidade, Gestão de Riscos e Controle Interno (GECON);

<b>IPT 18652</b>	<b>Revisão: 00</b>	<b>Data de Aprovação: 17.10.2022</b>
<b>Elaborado por:</b> Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		<b>Aprovado por:</b> Conselho de Administração do IPT

- iii. Monitorar, avaliar e informar periodicamente o Conselho de Administração sobre os riscos prioritários identificados pela Diretoria, pela Auditoria Interna ou pela Gerência de Conformidade, Gestão de Riscos e Controle Interno (GECON), bem como os planos de ação e recomendações aplicáveis;
- iv. Supervisionar, avaliar e monitorar a qualidade e a integridade dos mecanismos utilizados para a gestão de riscos com observância do cumprimento dos dispositivos legais e normativos aplicáveis, além de regulamentos e normas internas do IPT;
- v. Avaliar a adequação da estrutura destinada ao processo de gerenciamento de riscos: recursos humanos, financeiros e infraestrutura;
- vi. Elaborar e propor ao Conselho de Administração a Política de Gestão de Riscos do IPT e promover suas revisões;
- vii. Avaliar e propor ao Conselho de Administração os limites aceitáveis para exposição a riscos (Apetite a risco do IPT) e promover suas revisões.

A **Diretoria**, coordenada pelo Diretor-Presidente, tem as seguintes atribuições e responsabilidades:

- i. Promover a integração da gestão de riscos com o planejamento estratégico do IPT e garantir a implantação de um modelo eficiente de gestão de riscos, alinhado aos objetivos estratégicos e metas operacionais;
- ii. Priorizar e administrar riscos nas diretorias, considerando as particularidades dos seus processos, para garantir que estejam dentro do Apetite a risco do IPT e alinhados as diretrizes gerais estabelecidas pelo Conselho de Administração;
- iii. Supervisionar os controles existentes, monitorar sua efetividade e prestar contas ao Conselho de Administração;
- iv. Supervisionar a Gerência de Conformidade, Gestão de Riscos e Controle Interno (GECON) e a Auditoria Interna a respeito da gestão de riscos e seus controles;
- v. Promover a cultura de gestão de riscos no IPT e implementar a estrutura destinada ao processo de gerenciamento de riscos com investimento em recursos humanos, financeiros e infraestrutura;

IPT 18652	Revisão: 00	Data de Aprovação: 17.10.2022
Elaborado por: Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		Aprovado por: Conselho de Administração do IPT

vi. Revisar, contribuir e encaminhar ao Conselho de Administração o Apetite a risco do IPT com o apoio da Gerência de Conformidade, Gestão de Riscos e Controle Interno (GECON).

As **Unidades de Negócios**, as **Áreas administrativas** e os **Colaboradores que atuam nas operações do IPT** reportam-se à Diretoria, compõem a **1ª Linha de Atuação na Gestão de Riscos** e têm as seguintes atribuições e responsabilidades:

- i. Identificar, analisar, tratar e monitorar os riscos relacionados aos processos e à consecução dos objetivos do IPT de acordo com as diretrizes desta política;
- ii. Implantar planos de ação e de controle para que a todos os riscos identificados como prioritários sejam atribuídos um dono e gestor correspondente, se aplicável;
- iii. Comunicar, em tempo hábil, alterações de processos ou informações relevantes relacionadas à gestão de riscos.

A **Gerência de Conformidade, Gestão de Riscos e Controle Interno (GECON)** compõe a **2ª Linha de Atuação na Gestão de Riscos** e tem as seguintes atribuições e responsabilidades:

- i. Coordenar a implementação dos planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;
- ii. Assessorar a Diretoria na identificação, avaliação e análise dos diversos tipos de riscos envolvidos nos processos e na definição de estratégias de gestão destes riscos dentro dos limites definidos pelo Apetite a risco do IPT;
- iii. Dar suporte às Unidades de Negócios e Coordenadorias para a identificação, avaliação, análise e mitigação de riscos utilizando controles e para a implementação da Política de Gestão de Riscos do IPT;
- iv. Monitorar a tolerância a riscos das Unidades de Negócios e Coordenadorias e suas compatibilidades com o apetite a risco do IPT;
- v. Definir o método de gestão de riscos por meio de uma visão integrada, sistêmica e sinérgica das atividades do IPT e fazer sua comunicação apropriada para promover a cultura de gestão de riscos;

IPT 18652	Revisão: 00	Data de Aprovação: 17.10.2022
Elaborado por: Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		Aprovado por: Conselho de Administração do IPT

- vi. Propor a estrutura necessária para o processo de gerenciamento de riscos: recursos humanos, financeiros e infraestrutura;
- vii. Submeter ao Comitê de Auditoria Estatutário (CAE), em conjunto com a Diretoria, as diretrizes gerais para estabelecimento dos limites aceitáveis para exposição a riscos: **Apetite a risco do IPT.**

A **Auditoria Interna** atua na avaliação da aderência e da eficácia do processo de gerenciamento de riscos, de forma independente e objetiva, com a supervisão do Comitê de Auditoria. Compõe a **3ª Linha de Atuação na Gestão de Riscos** e tem as seguintes atribuições e responsabilidades:

- i. Aferir a efetividade do gerenciamento dos riscos, a confiabilidade do processo de identificação, análise, tratamento e monitoramento de riscos e a adequação dos controles internos;
- ii. Fornecer avaliações independentes sobre a gestão de riscos, a adequação dos seus processos de governança e controles internos relacionados.

## 6. Referências

Associação Brasileira de Normas Técnicas: ABNT NBR ISO 31000:2018 **Gestão de Riscos - Diretrizes**, 2018.

Comissão de Valores Mobiliários – CVM, Assessoria de Análise e Pesquisa (ASA). **Gerenciamento de riscos corporativos: uma análise das diretrizes e das práticas**, 2015.

Committee of Sponsoring Organizations of the Treadway Commission: COSO. **Enterprise Risk Management Integrating with Strategy and Performance**, 2017.

Committee of Sponsoring Organizations of the Treadway Commission: COSO. **Enterprise Risk Management Integrated Framework**, 2004.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. **Risk Appetite - Critical to Success: Using Risk Appetite to Thrive in a Changing World**, 2020.

Instituto Brasileiro de Governança Corporativa – IBGC. Série Cadernos de Governança Corporativa, 19. **Gerenciamento de riscos corporativos: evolução em governança e estratégia**, 2017.

IPT 18652	Revisão: 00	Data de Aprovação: 17.10.2022
Elaborado por: Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		Aprovado por: Conselho de Administração do IPT

Oliva, F. L. A Maturity Model for Enterprise Risk Management. **International Journal of Production Economics**, v. 173, p. 66-79, 2016.

The Institute of Internal Auditors - IIA. **Modelo das Três Linhas de do IIA.**

IPT 18652	Revisão: 00	Data de Aprovação: 17.10.2022
Elaborado por: Gerência de Conformidade, Gestão de Riscos e Controle Interno - GECON		Aprovado por: Conselho de Administração do IPT