SISTEMA DE GESTÃO INTEGRADO

Política de Gestão de Riscos e Controles Internos

PL-SGI-04 REV.01

Sumário

Controle de Versões

N°	Data	Aprovado por	Histórico
00	18/06/2025	Carla Oliveira	Emissão Inicial
01	24/06/2025	Arthur Barcelos	Ajustes em formatação

1. Objetivo

A Política de Gestão de Riscos e Controles Internos da **T2M - TEST TO MARKET LTDA** tem como objetivo estabelecer princípios, diretrizes e responsabilidades para a estruturação, implementação, monitoramento e melhoria contínua do processo de gestão de riscos e controles internos da **T2M**.

Esta política visa assegurar que os riscos relevantes às atividades, processos e objetivos estratégicos da organização sejam identificados, avaliados, tratados e comunicados de forma sistemática, promovendo a cultura de integridade, transparência, conformidade regulatória e tomada de decisão baseada em riscos.

Neste sentido, também tem por finalidade assegurar um ambiente de controle eficaz, alinhado às melhores práticas de governança, gestão e compliance, e em consonância com as regulamentações internas e externas aplicáveis.

2. Fundamentos e Referências Normativas

I. **ISO 31000:2018** - Gestão de Riscos.
II. **COSO ERM** - Enterprise Risk Management.
III. **COSO ICIF** - Internal Control Integrated Framework.
IV. **NBR ISO/IEC 27001** - Gestão da Segurança da Informação.
V. **NBR ISO 37301** - Compliance.
VI. **Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018).

3. Termos e Definições

Para fins desta Política, aplicam-se os seguintes termos e definições:

a) **Ambiente Interno:** O ambiente interno é a base para todos os outros componentes do gerenciamento de riscos corporativos, o que propicia disciplina e estrutura. Esse ambiente influencia o modo pelo qual as estratégias e os objetivos são estabelecidos, os negócios são estruturados, e os riscos são identificados, avaliados e geridos. Este influencia o desenho e o funcionamento das atividades de controle, dos sistemas de informação e comunicação, bem como das atividades de monitoramento. (COSO, 2004).
b) **Ambiente Externo:** Representa o contexto no qual a instituição existe e opera. É composto pelos elementos políticos, sociais, culturais, tecnológicos e ambientais.
c) **Apetite a Risco:** Nível de exposição a riscos que a organização está disposta a assumir no desenvolvimento de suas atividades para atingir seus objetivos estratégicos.

d) **Área proprietária de risco (*Risk Owner*)**: Unidade organizacional que possui autoridade e responsabilidade pelo gerenciamento do risco.

e) **Avaliação de Riscos:** Os riscos são avaliados considerando seus efeitos inerentes e residuais, bem como sua probabilidade e seu impacto.

f) **Controles Internos:** Conjunto de políticas, procedimentos, práticas, rotinas sistêmicas, diretrizes, conferências, trâmites e demais mecanismos implementados de forma coordenada pela gestão e pelos colaboradores da organização. Têm como objetivo enfrentar os riscos e fornecer segurança razoável quanto ao alcance dos objetivos institucionais, à integridade das informações, à conformidade e à eficácia operacional.

g) **Gestão de Riscos:** Processo contínuo, sistemático e estruturado de identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos que possam afetar o alcance dos objetivos organizacionais, com base em princípios de governança, integridade e melhoria contínua.

h) **Governança:** Conjunto de mecanismos, processos e estruturas instituídos pela Alta Direção para direcionar, monitorar e avaliar a atuação organizacional, com vistas à geração de valor sustentável, ao cumprimento de obrigações e à proteção dos interesses das partes interessadas.

i) **Incerteza:** Grau de imprevisibilidade associado à probabilidade ou ao impacto de eventos futuros, que pode dificultar a tomada de decisão e o planejamento.

j) **Impacto:** Efeito resultante da ocorrência do evento.

k) **Matriz de Riscos**: Conjunto dos eventos de risco identificados pela empresa, descritos e classificados em categorias.

l) **Mensuração do Risco:** Estimar a probabilidade versus o impacto da ocorrência do risco.

m) **Modelo das Três Linhas:** Estrutura de governança que distribui papéis e responsabilidades na gestão de riscos e controles internos. A primeira linha compreende gestores e colaboradores diretamente responsáveis por identificar e gerenciar riscos em suas áreas. A segunda linha compreende funções que orientam, supervisionam e promovem a padronização dos processos de gestão de riscos e controles. A terceira linha corresponde à auditoria interna, que atua de forma independente avaliando a efetividade dos controles e da governança.

n) **Monitoramento de Risco:** A integridade do processo de gerenciamento de riscos corporativos é monitorada e as modificações necessárias são realizadas. Desse modo, a organização poderá reagir ativamente e mudar segundo as circunstâncias. O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes ou uma combinação desses dois procedimentos. Verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças em relação ao nível de desempenho requerido ou esperado. Monitoramento pode ser aplicado a riscos, a controles, à estrutura de gestão de riscos e ao processo de gestão de riscos.

o) **Nível de Risco:** Grau de significância de um risco, resultante da combinação entre a probabilidade de sua ocorrência e o impacto potencial nos objetivos organizacionais.
p) **Objetivo:** Resultado ou condição desejada que orienta a atuação da organização e evidencia o cumprimento da missão institucional e o alcance da visão de futuro.
q) **Política de Gestão de Riscos:** Declaração formal da organização que expressa seu comprometimento, princípios e diretrizes gerais para a gestão de riscos, servindo como referência para todas as áreas e instâncias de governança.
r) **Probabilidade:** Possibilidade de ocorrência de um evento.
s) **Responsável pelo Risco:** Pessoa ou unidade organizacional formalmente designada com autoridade e responsabilidade para gerir riscos específicos, incluindo sua identificação, análise, resposta e reporte.
t) **Risco:** Possibilidade de que um evento, ação ou omissão afete adversa ou positivamente o alcance dos objetivos da organização. O risco é caracterizado por sua probabilidade e impacto e pode originar perdas, oportunidades ou ambos.
u) **Sistema de Gestão de Riscos e Controles Internos:** Conjunto integrado de estruturas, políticas, processos, práticas, pessoas, tecnologias e recursos que sustentam a implementação, operação, monitoramento e aperfeiçoamento contínuo da gestão de riscos e dos controles internos em toda a organização. A presente Política é parte integrante desse sistema.

4. Princípios e Diretrizes da Gestão de Riscos

4.1. Princípios da Gestão de Risco

Os princípios de Gestão de Riscos e Controles Internos que serão observados pela **T2M** na condução de suas atividades são:

I. Integração à governança corporativa.
II. Abordagem estruturada, sistemática e oportuna.
III. Proporcionalidade ao contexto organizacional.
IV. Baseada em evidências.
V. Transparência e comunicação eficaz.
VI. Melhoria contínua.

4.2. Diretrizes da Gestão de Risco

As seguintes diretrizes da Gestão de Riscos e Controles Internos deverão ser observadas pela **T2M**, na condução de suas atividades:

I. O processo de gestão de riscos e controles internos da **T2M** compreende as etapas de estabelecimento de contexto, identificação, análise, avaliação, tratamento, comunicação e consulta, bem como o monitoramento contínuo e a retroalimentação do processo, com foco em melhoria contínua.
II. A execução da gestão de riscos e dos controles internos está baseada em metodologia estruturada e suportada por ferramenta corporativa, devendo seguir fluxos operacionais padronizados e orientações técnicas específicas.
III. Todas as ações de gestão de riscos e de controles internos devem estar plenamente alinhadas ao planejamento estratégico, aos processos finalísticos e de apoio, e às demais políticas e diretrizes institucionais vigentes.
IV. A gestão de riscos e controles internos é parte indissociável dos processos organizacionais e constitui responsabilidade direta de todos os gestores e colaboradores, independentemente de seu nível hierárquico ou unidade de atuação.
V. O Sistema de Gestão de Riscos e Controles Internos será mantido sob ciclos de aprimoramento contínuo, com revisões periódicas que permitam sua adaptação às mudanças no ambiente interno e externo, às necessidades institucionais e à maturidade da organização.
VI. A estrutura de gestão de riscos e controles internos contempla, no mínimo, quatro dimensões essenciais: (i) riscos operacionais, incluindo os relacionados à integridade; (ii) riscos estratégicos; (iii) riscos inerentes ao negócio da organização; e (iv) riscos vinculados aos projetos estratégicos.
VII. A eficácia da gestão de riscos e dos controles internos será medida e acompanhada por meio de relatórios técnicos, painéis gerenciais, indicadores-chave de risco (KRIs), indicadores de desempenho e demais instrumentos de monitoramento.
VIII. A Alta Direção deve demonstrar comprometimento inequívoco com a gestão de riscos e controles internos, assegurando aos responsáveis pela sua implementação o acesso tempestivo, completo e irrestrito às informações e áreas necessárias à execução de suas atribuições, com garantia de autonomia técnica e independência funcional.
IX. Os procedimentos de controles internos serão proporcionais aos riscos e baseados na relação custo-benefício;
X. Realizar a utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais.

5. Papéis e Responsabilidades

I. Alta Direção

- Aprovar esta política, definir os níveis de apetite e tolerância ao risco, supervisionar a gestão.

II. Áreas Proprietárias de Riscos

- Atuar como primeira linha, gerenciando os riscos operacionais inerentes às suas atividades, identificando-os, avaliando-os, tratando-os e monitorando-os, em especial os riscos de operação.
- Comunicar tempestivamente e de forma proativa quaisquer novidades e/ou potenciais riscos que impactem o negócio ao responsável pela gestão de riscos da **T2M**.
- Apoiar a reavaliação do apetite/tolerância com dados e evidências atualizadas.

III. Auditoria Interna

- Avaliação independente sobre a eficácia dos processos, controles internos e demais elementos de governança corporativa (Riscos, Compliance, etc.);
- Auxiliar na verificação e cumprimento dos deveres legais e estatutários;
- Reporte dos resultados e das fragilidades identificadas a Alta Direção da **T2M**;
- Elaboração e executar o plano de auditoria aprovado pela Alta Direção, com base em riscos, transações e processos críticos, sugestões dos executivos e histórico;
- Atuar com independência e imparcialidade; e
- Auxiliar as áreas operacionais a compreender os controles, as normas e as políticas estabelecidas.

IV. Colaboradores

- Conscientizar-se dos Riscos inerentes às suas respectivas áreas de responsabilidade e de seu papel na gestão de Riscos de sua área;
- Reportar imediatamente a identificação de qualquer fato relevante, deficiência, falha ou não conformidade referente aos Riscos da Companhia aos Gestores dos Riscos; e
- Identificar e reportar aos Gestores dos Riscos eventuais Riscos ainda não mapeados.

V. **Compliance**

- Realizar a análise periódica de riscos de corrupção e suborno os quais a **T2M** está exposta, em especial quanto à efetividade e suficiência da estrutura de controles internos e dos processos;
- Implementar as medidas destinadas à correção das deficiências identificadas e melhorias do ambiente de controles no âmbito do monitoramento da **T2M**.

VI. **Gestores**

- Identificar e avaliar riscos, implementar controles, reportar exposições, além de comunicar tempestivamente e de forma proativa quaisquer novidades e/ou potenciais riscos que impactem o negócio ao departamento responsável pela gestão de riscos da **T2M**.
- Coordenar a aplicação da metodologia de riscos, manter registros atualizados.

6. Categorização de Riscos

A categorização de riscos tem por objetivo organizar, facilitar a identificação e possibilitar a avaliação adequada dos riscos que possam impactar os objetivos da organização. Para fins desta Política, os riscos são classificados conforme as seguintes categorias:

I. **Riscos Estratégicos:** Riscos que afetam diretamente os objetivos estratégicos da organização, incluindo decisões de investimento, posicionamento institucional, inovação e sustentabilidade no longo prazo.
II. **Riscos do Negócio:** Riscos que impactam a oferta, desempenho e continuidade dos produtos, serviços ou soluções da organização. Incluem eventos relacionados a mudanças de mercado, dependência excessiva de fornecedores, falhas na inovação, perda de competitividade, interrupções na cadeia de valor ou inadimplência de clientes estratégicos.
III. **Riscos Operacionais:** Riscos decorrentes de falhas, inadequações ou indisponibilidades em processos internos, pessoas, sistemas, infraestrutura ou eventos externos que impactam a operação rotineira da organização.
IV. **Riscos de Compliance (ou Conformidade):** Riscos relacionados ao descumprimento de leis, regulamentos, normativos internos ou compromissos assumidos perante partes interessadas, incluindo riscos de sanções legais e danos à reputação institucional.
V. **Riscos Financeiros:** Riscos associados à gestão financeira da organização, incluindo inadimplência, variações cambiais, riscos de crédito, liquidez e solvência.
VI. **Riscos Cibernéticos e de Segurança da Informação:** Riscos relacionados à proteção da informação, ataques cibernéticos, perda de confidencialidade, integridade e disponibilidade de dados e sistemas tecnológicos.

VII. **Riscos de Integridade e Ética:** Riscos associados à ocorrência de fraudes, corrupção, conflito de interesses, assédio, nepotismo e outras condutas que possam comprometer os princípios éticos e a integridade institucional.
VIII. **Riscos de Projetos:** Riscos relacionados ao planejamento, execução e controle de projetos institucionais, incluindo riscos de escopo, prazos, orçamentos e entrega de valor.
IX. **Riscos Ambientais, Sociais e de Governança (ESG):** Riscos que envolvem impactos negativos no meio ambiente, aspectos sociais e práticas de governança, com potencial de afetar a sustentabilidade e a imagem da organização.

Essa categorização poderá ser revisada periodicamente, de acordo com o grau de maturidade da gestão de riscos, o contexto organizacional e os fatores externos relevantes.

7. Estrutura de Governança dos Riscos

A estrutura de governança da gestão de riscos e controles internos da **T2M** adota o modelo consagrado das Três Linhas, conforme orientações do *Institute of Internal Auditors* (IIA), da ISO 31000 e do *framework* COSO. Este modelo estabelece papéis e responsabilidades claras para assegurar a efetividade do gerenciamento de riscos, a integridade dos controles e a eficiência da governança organizacional:

- **1ª Linha – Propriedade e Gestão de Riscos:** Compreende os gestores e colaboradores das áreas operacionais, responsáveis diretos por identificar, avaliar, tratar, monitorar e reportar os riscos em suas atividades. São também responsáveis por implementar e manter os controles internos no âmbito de suas funções.
- **2ª Linha – Supervisão e Suporte à Gestão de Riscos:** Inclui as áreas especializadas de gestão de riscos, compliance, segurança da informação, controles internos, integridade e demais funções de controle. Estas áreas estabelecem metodologias, normas, políticas e prestam orientação técnica, promovendo a consistência e a padronização da gestão de riscos na organização.
- **3ª Linha – Avaliação Independente:** É representada pela Auditoria Interna, que atua com independência e objetividade para avaliar a adequação e a eficácia dos processos de governança, gestão de riscos e controles internos. A Auditoria Interna também contribui com recomendações para o aprimoramento contínuo da estrutura de controle e do sistema de governança.

A articulação entre as três linhas visa assegurar que os riscos sejam geridos com responsabilidade, transparência e efetividade, promovendo a geração de valor e a sustentabilidade institucional.

8. Apetite e Tolerância a Riscos

A definição do apetite e da tolerância a riscos é essencial para guiar as decisões estratégicas, orientar a alocação de recursos e estabelecer os limites aceitáveis para exposição a riscos na **T2M**.

8.1. Apetite a Riscos

O apetite a risco representa o nível de risco que a organização está disposta a aceitar no cumprimento de seus objetivos estratégicos. Esse nível é definido pela Alta Direção e deve estar alinhado à missão, visão, valores institucionais, bem como ao ambiente interno e externo de atuação.

O apetite a risco pode variar entre áreas e tipos de riscos (estratégicos, operacionais, financeiros, reputacionais, entre outros), sendo formalizado por meio de documento específico aprovado pela instância competente de governança.

8.2. Tolerância a Riscos

A tolerância ao risco refere-se ao desvio aceitável em relação ao nível de exposição desejado (apetite), representando os limites quantitativos ou qualitativos dentro dos quais a organização opera sem comprometer seus objetivos.

Esses limites devem ser definidos com base em critérios objetivos, estar integrados ao processo decisório, aos sistemas de monitoramento e aos indicadores-chave de risco (KRIs), permitindo o acompanhamento da exposição real frente aos parâmetros estabelecidos.

8.3. Monitoramento e Revisão

Os níveis de apetite e tolerância a riscos devem ser monitorados periodicamente e revisados sempre que ocorrerem alterações significativas na estratégia, nos processos ou no ambiente organizacional. Mudanças nos perfis de risco, no mercado ou em legislações aplicáveis também motivam a reavaliação.

A aderência aos limites definidos será verificada por meio de relatórios gerenciais, com comunicação tempestiva de exposições excessivas às instâncias responsáveis.

9. Processo de Gestão de Riscos

O processo de gestão de riscos da **T2M** está estruturado com base nas diretrizes da ISO 31000 e consiste em um ciclo contínuo, dinâmico e iterativo, composto pelas seguintes etapas:

I. **Estabelecimento do Contexto:** Compreende a definição dos objetivos organizacionais, a compreensão do ambiente interno e externo, a delimitação do escopo da análise e o alinhamento com os critérios de risco previamente definidos.
II. **Identificação de Riscos:** Fase de mapeamento e descrição dos eventos que possam afetar positiva ou negativamente os objetivos da organização, considerando ameaças, oportunidades, causas e consequências.
III. **Análise de Riscos:** Avaliação qualitativa e/ou quantitativa da probabilidade de ocorrência e do impacto dos riscos identificados. Pode incluir análise de causas-raiz, cenários de risco e interdependência entre eventos. Cada risco deve ser analisado individualmente quanto à probabilidade de ocorrência e impacto, e deve ser alocado na matriz de risco construída pela **T2M**.
IV. **Avaliação de Riscos:** Comparação dos níveis de risco estimados com os critérios de risco da organização, visando priorizar os riscos significativos que exigem tratamento e apoiar a tomada de decisão. Isto pode levar a uma decisão de: (i) aceitar o risco; (ii) considerar as opções de tratamento de riscos; (iii) transferir o risco; (iv) manter os controles existentes; e (v) reconsiderar os objetivos.
V. **Tratamento de Riscos:** Definição e implementação de respostas ao risco, tais como mitigação, aceitação, transferência ou eliminação, com base em planos de ação que contenham responsáveis, prazos e recursos.
VI. **Comunicação e Consulta:** Processo contínuo de troca de informações com as partes interessadas internas e externas, promovendo entendimento mútuo, engajamento e apoio ao processo decisório.
VII. **Monitoramento e Análise Crítica:** Acompanhamento contínuo da exposição aos riscos, da eficácia das ações de tratamento e da adequação do processo como um todo. Inclui a revisão de riscos, atualização de registros e ajuste de estratégias.

Esse processo é aplicado de forma integrada aos processos organizacionais, com suporte da área responsável por riscos e controles internos, visando a criação de valor e o fortalecimento da governança institucional.

9.1. Análise e Avaliação de Riscos

A análise e avaliação de riscos têm por finalidade compreender a natureza e as características dos riscos identificados, considerando suas causas, incertezas, probabilidade de ocorrência, consequências potenciais e a eficácia dos controles existentes. A análise pode ser qualitativa, quantitativa ou híbrida, de acordo com a complexidade e os dados disponíveis.

Cada risco deve ser posicionado na matriz de riscos da organização, com base na combinação entre impacto e probabilidade, possibilitando sua priorização. Com isso, a companhia poderá implementar, de forma efetiva, o Programa de Gestão de Riscos e de Controles Internos.

A avaliação, por sua vez, visa comparar os resultados da análise com os critérios previamente definidos, orientando a tomada de decisão quanto ao tratamento (i) aceitar o risco; (ii) considerar as opções de tratamento de riscos; (iii) transferir o risco; (iv) manter os controles existentes; e (v) reconsiderar os objetivos.

9.1.1. Definição de Escala de Impacto x Probabilidade

Para a avaliação dos riscos a **T2M** utiliza da métrica "impacto x probabilidade", onde:

- **Impacto:** Considera-se uma avaliação quantitativa e qualitativa do risco nos quesitos de conformidade legal, reputacional, socioambiental e impacto econômico.
- **Escala de impacto:** Crítico, Alto, Médio e Baixo.
- **Probabilidade:** Define-se como a probabilidade de materialização do evento de risco durante um determinado período, considerando o histórico de ocorrências ou previsões futuras.
- **Escala de Probabilidade:** Muito provável, Provável, Pouco Provável e Improvável.

9.1.2. Análise de Risco Inerente e Residual

Desta forma, a **T2M** utiliza 2 (dois) cenários para avaliação dos riscos, sendo:

- **Risco Inerente:** É o resultado da avaliação dos riscos (impacto x probabilidade) considerando um cenário em que não há nenhuma ação da companhia para mitigá-lo, ou seja, em seu estado potencial, ausente de controles.

- **Risco Residual:** É o resultado da avaliação dos riscos (impacto x probabilidade) considerando os controles existentes e seu potencial de mitigação destes riscos. A atuação dos controles, se efetiva, tende a reduzir o impacto dos riscos e ou a probabilidade de ocorrência.

9.1.3. Severidade dos Riscos

A severidade do risco é definida a partir do cruzamento das notas atribuídas de impacto e probabilidade, sendo classificada conforme escala de severidade: Crítico, Alto, Médio e Baixo.

Riscos classificados no quadrante **crítico** da matriz deverão possuir planos de ação para tratamento, visando redução de severidade.

9.2. Tratamento de Riscos

Concluídas as etapas de identificação, análise e avaliação, deve-se definir e implementar estratégias para o tratamento dos riscos. O tratamento visa selecionar e aplicar medidas para modificar o risco, por meio de um processo iterativo que compreende:

I. Formulação e seleção das opções de resposta ao risco;
II. Planejamento e implementação das ações;
III. Avaliação da eficácia dos tratamentos adotados;
IV. Análise da aceitabilidade do risco remanescente; e
V. Adoção de medidas adicionais, caso necessário.

A escolha das opções deve considerar o equilíbrio entre os benefícios da mitigação e os custos, impactos operacionais e estratégicos, avaliando a viabilidade tanto sob a ótica micro (local/processual) quanto macro (organizacional). As principais estratégias de tratamento incluem:

- Evitar o risco;
- Reduzir a probabilidade ou o impacto;
- Remover a fonte de risco;
- Compartilhar ou transferir o risco (ex.: seguros, parcerias);
- Reter o risco de forma consciente, com monitoramento apropriado;
- Assumir ou até ampliar o risco, quando estrategicamente vantajoso.

As decisões de tratamento devem estar documentadas, justificadas e alinhadas ao apetite de risco institucional.

9.2.1. Planos de Ação de Riscos e Controles Internos

Com base nas avaliações periódicas de riscos e na análise dos ambientes de controles, assim como nas ações originadas das auditorias internas e externas — independentemente da fonte da avaliação — surge a necessidade de elaborar e implementar planos de ação voltados para a melhoria contínua do ambiente de controles internos e para a redução dos riscos à **T2M**.

As ações a serem adotadas são definidas pelos gestores responsáveis pela mitigação dos riscos devem conter prazos claros para sua efetiva conclusão.

Durante a análise dos planos de ação, pode ocorrer que determinados riscos estejam dentro do apetite de risco da companhia, ou seja, são considerados aceitáveis, não sendo necessárias ações de mitigação específicas.

O monitoramento dos planos de ação é responsabilidade da área de Riscos e Controles Internos, que realiza periodicamente follow-ups junto às áreas de negócio para acompanhar o andamento das ações.

9.3. Comunicação e Consulta

A **T2M** adotará práticas sistemáticas de monitoramento, comunicação e aprimoramento contínuo no âmbito da gestão de riscos e dos controles internos, visando garantir a eficácia, a atualização e a evolução do seu sistema de governança corporativa.

- **Monitoramento Contínuo:** A eficácia do sistema de gestão de riscos e controles internos será monitorada de forma contínua por meio de indicadores, autoavaliações periódicas, auditorias internas e externas, testes de controles e revisões independentes. O monitoramento permitirá a identificação tempestiva de deficiências, desvios e oportunidades de melhoria.
- **Comunicação Transparente:** A **T2M** assegurará uma comunicação clara, tempestiva e objetiva entre as áreas envolvidas na gestão de riscos e controles internos. Informações relevantes sobre eventos de risco, planos de ação, auditorias, conformidade regulatória e desempenho dos controles serão compartilhadas com os níveis hierárquicos apropriados, incluindo a alta administração e os comitês de governança, quando aplicável.
- **Escalonamento e Tratamento de Exceções:** Falhas significativas ou riscos com impacto elevado deverão ser prontamente comunicados à Alta Direção. As exceções a políticas ou desvios relevantes de controles devem ser formalmente registradas, analisadas e tratadas com medidas corretivas adequadas.

9.4. Monitoramento e Análise Crítica

A **T2M** realiza o acompanhamento contínuo da exposição aos riscos, da eficácia das ações de tratamento e da adequação do processo como um todo. Inclui a revisão de riscos, atualização de registros e ajuste de estratégias:

- **Registro e Rastreabilidade:** Todas as atividades de monitoramento, avaliações, auditorias e melhorias implementadas deverão ser registradas de forma organizada e rastreável, permitindo a reconstrução dos processos decisórios e a prestação de contas frente às partes interessadas.
- **Aprimoramento Contínuo:** A estrutura de gestão de riscos e controles internos será objeto de constante evolução, acompanhando mudanças no ambiente regulatório, nas estratégias empresariais, nos processos internos e nos riscos emergentes. As lições aprendidas e os resultados das avaliações servirão de insumo para o redesenho de processos, políticas e controles.

- **Engajamento Organizacional:** A melhoria contínua será sustentada pelo engajamento dos colaboradores, com estímulo à cultura de controle, ética e responsabilização. A contribuição ativa das equipes será valorizada por meio de programas de capacitação, canais de comunicação interna e incentivo à identificação de riscos e proposição de soluções.
- **Revisão Periódica da Política:** Esta política será revisada periodicamente, ou sempre que houver mudanças relevantes no ambiente externo ou interno da empresa, garantindo sua aderência às melhores práticas de mercado, às normas vigentes e à realidade operacional da **T2M**.

10. Gestão de Controles Internos

A gestão de controles internos da **T2M** tem como objetivo assegurar a conformidade das operações, a confiabilidade das informações, a proteção de ativos e a eficácia dos processos organizacionais, por meio de um sistema estruturado, contínuo e integrado à gestão de riscos.

10.1. Objetivos dos Controles Internos

Os objetivos dos controles internos da gestão são:

I. Prover suporte à missão, à continuidade e à sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos da **T2M**;
II. Proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica das operações;
III. Assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas;
IV. Assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria **T2M**; e
V. Salvaguardar e proteger bens, ativos e recursos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

10.2. Princípios dos Controles Internos

Os controles internos da gestão da **T2M** devem ser desempenhados e implementados em consonância com os seguintes princípios:

I. Aderência à integridade e a valores éticos;
II. Coerência e harmonização da estrutura de competências e reponsabilidades dos diversos níveis de gestão da **T2M**;
III. Clara definição de objetivos que possibilitem o eficaz gerenciamento de riscos;

IV. Identificação e avaliação das mudanças internas e externas a **T2M** que possam afetar significativamente os controles internos da gestão;
V. Desenvolvimento e implementação de atividades de controle que contribuam para a obtenção de níveis aceitáveis de riscos; e
VI. Utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão.

10.3. Diretrizes dos Controles Internos

A estrutura de controles internos da **T2M** será baseada em princípios de governança corporativa, transparência, conformidade regulatória e eficácia operacional, com o objetivo de assegurar a integridade dos processos, a proteção dos ativos, a confiabilidade das informações e a mitigação de riscos.

I. **Modelo das Três Linhas de Defesa:** Os controles internos da **T2M** serão estruturados com base no modelo das três linhas de defesa, com definição clara de responsabilidades entre as áreas executoras, a função de gestão de riscos e a auditoria interna, promovendo independência e eficácia no monitoramento.
II. **Formalização e Padronização de Processos:** Os processos organizacionais deverão ser formalizados, padronizados e atualizados periodicamente, garantindo a rastreabilidade das atividades, a segregação de funções e a prevenção de falhas operacionais ou desvios éticos.
III. **Avaliação e Monitoramento de Riscos:** A avaliação e o monitoramento contínuo dos riscos servirão como base para o desenho e a implementação de controles proporcionais à criticidade dos processos e alinhados ao apetite de risco institucional.
IV. **Prevenção de Fraudes e Irregularidades:** Serão utilizados mecanismos de prevenção e detecção de fraudes, falhas e irregularidades, como controles automatizados, trilhas de auditoria, revisões independentes e restrições de acesso aos sistemas e dados corporativos.
V. **Controles Tecnológicos:** Os sistemas de informação deverão possuir controles tecnológicos robustos, voltados à integridade, confidencialidade e disponibilidade das informações, incluindo políticas de segurança cibernética e gestão de acessos.
VI. **Conformidade Regulatória:** A conformidade com normas legais, regulatórias e internas será garantida por meio da atuação coordenada das áreas de compliance, auditoria e controles internos, assegurando aderência às exigências dos órgãos de controle e fiscalização.
VII. **Capacitação e Cultura de Controles:** A empresa promoverá treinamentos e ações contínuas de capacitação voltadas à disseminação da cultura de controle interno, fortalecendo o comprometimento dos colaboradores com os princípios de integridade e responsabilidade.
VIII. **Tratamento de Deficiências:** Deficiências ou fragilidades nos controles identificadas em auditorias, avaliações internas ou externas deverão ser

tratadas com planos de ação tempestivos, assegurando a melhoria contínua e a efetividade do sistema de controle.

10.4. Classificação dos Controles Internos

Os controles internos na **T2M** são classificados em:

I. **Controles Preventivos**: visam evitar a ocorrência de erros, fraudes ou não conformidades (ex.: segregação de funções, parametrizações sistêmicas, treinamentos).
II. **Controles Detectivos**: identificam eventos após sua ocorrência, permitindo sua análise e resposta (ex.: auditorias, conciliações, revisões, alarmes).
III. **Controles Corretivos**: tratam falhas ou problemas identificados, promovendo sua remediação (ex.: planos de ação corretiva, ajustes operacionais).

10.5. Implementação e Monitoramento dos Controles Internos

A implementação dos controles internos é de responsabilidade das áreas executoras dos processos, sendo obrigatória sua documentação, manutenção e revisão periódica. O monitoramento da eficácia dos controles ocorre por meio de:

I. Testes de controles (rotineiros ou amostrais);
II. Avaliações internas ou por auditoria independente;
III. Indicadores de desempenho e de controle;
IV. Registros de não conformidades e planos de ação.

10.6. Integração dos Controles Internos com a Gestão de Riscos

A gestão de controles internos está intrinsecamente ligada à gestão de riscos, pois os controles são mecanismos para mitigar os riscos identificados. A análise da efetividade dos controles influencia diretamente na avaliação do nível de risco remanescente e na priorização de ações.

11. Ferramentas e Instrumentos para a Gestão de Riscos

A efetividade da gestão de riscos e controles internos depende da adoção de ferramentas e instrumentos adequados que viabilizem a sistematização, o monitoramento e a melhoria contínua dos processos. A **T2M** adota um conjunto integrado de ferramentas que apoiam a governança, promovem a transparência e facilitam a tomada de decisão baseada em riscos.

11.1. Sistema Corporativo de Gestão de Riscos e Controles Internos

Plataforma informatizada institucionalmente definida, utilizada para registrar, avaliar, tratar e monitorar riscos e controles. Deve permitir:

I. A rastreabilidade das informações inseridas;
II. A geração de relatórios e painéis gerenciais;
III. A identificação de responsáveis e prazos;
IV. A integração com outros sistemas (quando aplicável);
V. A manutenção de histórico das ações adotadas.

11.2. Matriz de Riscos e Controles

Documento estruturado que relaciona os riscos aos objetivos estratégicos, processos e áreas da organização, descrevendo:

I. Eventos de risco;
II. Causas e consequências potenciais;
III. Controles existentes e sua efetividade;
IV. Classificação de riscos (probabilidade e impacto);
V. Ações de tratamento e responsáveis.

11.3. Indicadores de Risco (KRIs)

Conjunto de métricas utilizadas para monitorar a exposição a riscos e antecipar tendências. Devem ser:

I. Relevantes e alinhados aos riscos prioritários;
II. Periodicamente monitorados;
III. Utilizados como base para decisões preventivas e corretivas.

11.4. Plano de Ação e Mitigação

Instrumento que consolida as medidas previstas para reduzir, transferir ou aceitar os riscos identificados. Cada plano deve conter:

- Ações detalhadas;
- Responsáveis e prazos;
- Indicadores de acompanhamento;
- Critérios de conclusão e validação.

11.5. Relatórios Gerenciais e Dashboards

Ferramentas visuais e analíticas utilizadas para consolidar informações, apresentar evolução da gestão de riscos e controles e subsidiar a Alta Administração na tomada de decisões. Incluem:

- Painéis interativos de riscos estratégicos e operacionais;
- Comparativos entre períodos;
- Análises de efetividade dos controles.

11.6. Manual e Metodologia de Gestão de Riscos

Documento técnico que detalha o processo adotado pela organização, os critérios, os instrumentos de apoio, os responsáveis e o ciclo de revisão. Deve ser amplamente divulgado e revisado periodicamente.

11.7. Capacitação e Sensibilização

A **T2M** investe na capacitação contínua e na sensibilização de seus colaboradores como pilares para a efetiva gestão de riscos e controles internos. Para isso, podem ser utilizados instrumentos como trilhas de aprendizagem, treinamentos presenciais ou virtuais, materiais de apoio, guias rápidos, simulações e estudos de caso, promovendo a cultura de riscos de forma acessível, prática e alinhada aos objetivos organizacionais.

12. Revisão e Atualização da Política

A **T2M** manterá mecanismos de revisão periódica desta política para garantir sua aderência a alterações legais, regulatórias ou institucionais, assegurando o compromisso contínuo com a conformidade e a ética empresarial.

Esta Política entra em vigor na data de sua aprovação pela Diretoria e Compliance e, revoga quaisquer normas e procedimentos em contrário.

Aprovado em 18 de junho de 2025.

Arthur Barcelos
Compliance Officer