POLÍTICA DE GERENCIAMENTO DE RISCOS, CONTROLES INTERNOS E CONFORMIDADE

- **Responsável pela elaboração e controle:** Diretoria Executiva e Gerência de Governança, Riscos e Controles Internos.
- **Abrangência:** Esta Política alcança todos os membros de órgãos de governança, gestores, colaboradores, patrocinadoras, beneficiários, fornecedores e empresas parceiras, partes relacionadas e demais pessoas ou entidades que, de qualquer forma, desempenhem atividades vinculadas à Organização.
- **Regulamentação:**
  - Resolução Normativa – RN° 526/2022;
  - Resolução Normativa – RN° 518/2022;
  - ABNT NBR ISO 31000:2018;
  - Código de Ética - SIM;
  - *Commitee of Sponsoring Organizations of the Treadway Commission – COSO;*
  - Código das Melhores Práticas de Governança Corporativa – IBGC;
  - Lei n° 13.709/2018 - Lei Geral de Proteção de Dados – LGPD;
  - Lei n° 8.078/1990 - Código de Defesa do Consumidor;
  - Lei n° 12.846/2013 - Lei Anticorrupção.
- **Periodicidade:** Esta Política deverá ser revisada anualmente e submetida ao Conselho Deliberativo para aprovação. Extraordinariamente essa política poderá ser revisada a qualquer tempo.

1. Apresentação

Esta Política estabelece diretrizes para garantir que a SIM mantenha um sistema estruturado de gerenciamento de riscos, controles internos e conformidade, em consonância com as melhores práticas de governança. Nosso compromisso é identificar, avaliar, tratar e monitorar riscos de forma contínua, assegurando a eficácia dos controles e a aderência às normas internas e à legislação aplicável.

2. Conceitos

- Conformidade: refere-se ao dever de cumprir e fazer cumprir leis e regulamentos externos e internos, impostos às atividades da Organização;
- Controles Internos: procedimentos que visam assegurar o alcance dos objetivos estratégicos, a salvaguarda dos ativos, o atingimento das metas de desempenho financeiro e operacional, a fidedignidade das informações gerenciais e contábeis e a aderência às políticas definidas pela Administração, com o objetivo de evitar erros, fraudes e ineficiências;

- COSO: Committee of Sponsoring Organizations of the Treadway Commission, entidade sem fins lucrativos, dedicada à melhoria contínua da confiabilidade dos dados apresentados nas demonstrações financeiras, por instrumento da ética, efetividade dos controles internos e Governança Corporativa;
- Cultura de Gestão de Riscos: conjunto de normas, atitudes e comportamentos relacionados com a consciência de riscos assumidos e gerenciados pela SIM;
- Declaração de Apetite a Riscos: instrumento que formaliza os riscos que a organização decide aceitar, evitar, mitigar ou compartilhar para atingir seus objetivos estratégicos, estabelecendo limites, diretrizes e indicadores que orientam a gestão e o monitoramento da exposição a riscos.
- Estrutura de Gestão de Riscos: conjunto de componentes que subsidia a concepção, implementação, monitoramento, avaliação e melhoria contínua da gestão de riscos na Organização;
- Exposição ao Risco: quantificação da possibilidade da Organização ser afetada por um determinado risco;
- Fatores de Risco: fatores internos ou externos que podem originar os riscos;
- Gestão de Riscos: processo de identificação, análise, avaliação, priorização, tratamento e monitoramento de riscos que possam afetar, positiva ou negativamente, os objetivos de processos de trabalho e/ou de projetos de uma operadora nos níveis estratégicos, tático e operacional;
- Apetite a Riscos: Nível de risco que a organização está disposta a aceitar na busca de seus objetivos, materializado por diretrizes e indicadores que definem a visão agregada da exposição a riscos. Esse apetite orienta a escolha de estratégias de resposta, como evitar, mitigar, compartilhar ou aceitar riscos.
- Tolerância a Riscos: nível de variação aceitável em relação ao apetite a riscos, definido por limites e indicadores que permitem monitorar e controlar a exposição.
- Nível de Risco: medida da importância ou significância do risco, considerando o produto resultante entre a probabilidade e impacto.
- Risco Inerente: risco natural a que uma organização está exposta antes de qualquer ação de controle ou mitigação.
- Risco Residual: risco que permanece após a aplicação de controles, políticas e medidas de mitigação.
- Riscos Relevantes: riscos capazes de ameaçar o atingimento de objetivos estratégicos ou impactar a sustentabilidade da Organização;
- Matriz de Riscos: consiste em um inventário dos riscos mapeados pela SIM, classificados de acordo com sua probabilidade e impacto, que tem por objetivo apresentar o resultado da avaliação dos riscos identificados, mensurando critérios que auxiliarão no estabelecimento das prioridades com relação ao tratamento;
- Impacto: refere-se ao resultado ou consequência caso ocorra a materialização de um evento de risco. O impacto do risco é analisado em diferentes esferas, conforme a régua definida;
- ISO 31.000:2018: norma da família de Gestão de Risco criada pela International *Organization for Standardization.* O objetivo da ISO 31.000:2018 é estabelecer princípios e orientações genéricas sobre Gestão de Riscos;

- Modelo de Três Linhas: conceito desenvolvido pelo IIA (Institute of Internal Auditors), amplamente utilizado no mercado, onde as atribuições de Gestão de Riscos e de Controles Internos fica dividida por linhas de atuação e funções dentro da Organização;
- Partes Interessadas (stakeholders): pessoa ou entidade que pode afetar, ser afetada ou perceber- se afetada por uma decisão ou atividade da SIM;
- Proprietário do Risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco na primeira linha de defesa;
- Risco: efeito da incerteza, sobre os objetivos da organização, que pode ser expresso em termos de uma combinação de consequências de um evento e a probabilidade de ocorrência associada;
- Vulnerabilidade: extensão à qual a SIM está exposta ou desprotegida em relação aos impactos negativos decorrentes de falha e/ou inexistência de controles;
- Ética: refere-se ao valor institucional que busca promover os atos considerados os melhores e mais justos, sem distinção ou discriminação de qualquer natureza, com base nos princípios morais;
- Gestão da Integridade: conjunto de medidas de prevenção de possíveis desvios de conduta na entrega dos resultados organizacionais;
- Governança: combinação de processos e estruturas implantadas pela alta administração da Organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;
- ESG (*Environmental, Social and Governance*): conjunto de práticas ambientais, sociais e de governança que orientam as organizações a atuarem de forma sustentável, ética e responsável, equilibrando resultados econômicos com impactos positivos na sociedade e no meio ambiente.

3. Objetivos

Estabelecer diretrizes e responsabilidades para identificar, avaliar, monitorar e mitigar riscos que possam comprometer a sustentabilidade da SIM – Caixa de Assistência à Saúde, o cumprimento das normas legais e regulatórias, a eficiência operacional e financeira, a continuidade dos negócios e a qualidade dos serviços prestados aos beneficiários. Busca-se, ainda, fortalecer a governança corporativa, integrar a gestão de riscos à estratégia organizacional, prevenir fraudes, corrupção e falhas de controles, além de promover uma cultura de integridade, ética, transparência e conformidade em todos os níveis da Organização.

4. Princípios

4.1 Conformidade e Integridade – garantir que todas as práticas estejam em aderência a normas, leis e padrões éticos.

4.2 Responsabilidade e Transparência – assumir impactos das decisões e manter clareza em processos e controles.

4.3 Segurança e Resiliência – proteger pessoas, processos e informações, estando preparados para responder a imprevistos.

5. Diretrizes

5.1 Manter a estrutura de gerenciamento de riscos, controles internos e conformidade compatível com a natureza e complexidade das operações da Organização;

5.2 Estabelecer indicadores para gerenciamento de riscos, com foco nos riscos relevantes e reportes periódicos à Alta Administração;

5.3 Adotar modelo de gerenciamento integrado de riscos, controles internos e conformidade;

5.4 Integrar o gerenciamento de riscos e a estratégia, incorporar a gestão de riscos ao processo de definição do planejamento e seleção de iniciativas e projetos estratégicos, bem como, acompanhar e revisão dos objetivos estratégicos;

5.5 Identificar, analisar, avaliar e monitorar fatores de riscos que podem comprometer a integridade, a disponibilidade e a continuidade das atividades da Entidade, adotando medidas tempestivas para mitigação dos riscos;

5.6 Basear o Modelo de Gerenciamento de Riscos, Controles Internos e Conformidade nas etapas de estabelecimento de contexto, identificação, análise, avaliação, tratamento, monitoramento, comunicação e consulta dos riscos, em consonância com os preceitos da ISO 31.000.

5.7 Buscar embasar as nossas avaliações de riscos preferencialmente em informações quantitativas, contemplando dados históricos e projeções, que resultem em métricas que combinem probabilidade de ocorrência e impactos associados em um horizonte de tempo definido;

5.8 Assegurar que os limites e alçadas corporativas, previamente definidos, serão observados no processo de gestão de riscos;

5.9 Documentar nossos riscos relevantes em inventário de riscos, aprovado pelo Conselho Deliberativo;

5.10 Revisar periodicamente o inventário de riscos, de maneira a assegurar que os riscos mais relevantes e/ou aqueles aos quais possuímos maior exposição, receberão gerenciamento proporcional ao seu potencial de impacto na Organização;

5.11 Definir nosso apetite a riscos a partir da estratégia da Organização;

5.12 Manter nosso apetite a riscos formalizado através de Declaração de Apetite a Riscos, aprovada pelo Conselho Deliberativo;

5.13 Estabelecer ações de tratamento para riscos avaliados em nível superior ao apetite definido;

5.14 Disponibilizar e divulgar, tempestivamente, informações consistentes, fidedignas e relevantes sobre o gerenciamento de riscos, controles internos e conformidade à Alta Administração e às entidades externas de fiscalização e controle;

5.15 Disseminar a cultura de gerenciamento de riscos, controles internos e conformidade e incentivar a capacitação e qualificação do público interno em todos os níveis.

5.16 Promover a integridade e a responsabilidade individual e coletiva em todos os níveis da Organização;

5.17 Assegurar conformidade com legislações e normas regulatórias aplicáveis, incluindo ANS, LGPD, Código de Defesa do Consumidor e Lei Anticorrupção;

5.18 Buscar a melhoria contínua dos controles internos, alinhados às melhores práticas de governança;

5.19 Incorporar a sustentabilidade e a responsabilidade socioambiental (ESG) como parte integrante da gestão de riscos e da estratégia institucional.

5.20 Atuar com transparência e ética na gestão de riscos, fortalecendo a confiança das partes interessadas.

6. Instâncias de Supervisão

As Instâncias de Supervisão têm como função apoiar e dar suporte aos diversos níveis hierárquicos da Organização e seus órgãos colegiados com a finalidade de integrar as atividades de Gestão de Risco e Controles Internos nos processos e atividades organizacionais. A SIM adere o modelo das três linhas (MLD) para operacionalizar sua estrutura de Gerenciamento de Riscos e Controles, estabelecidos conforme atuação e nível de responsabilidade dos envolvidos sobre cada processo.

• 1ª Linha– Proporcionada pela área Gestora do Processo, com comprometimento de gerenciar os riscos e, enquanto executora do processo, deve identificar, mensurar e avaliar os riscos do seu negócio.
• 2ª Linha– Atribuída à Gerência de Riscos e Controles Internos e inclui funções de Gerenciamento de Risco e Conformidade, atuando em conjunto com as áreas de negócios para garantir que a 1ª linha tenha identificado, avaliado, tratado e reportado perfeitamente os riscos de seu negócio.
• 3ª Linha– Está a Auditoria Interna, avaliando a eficácia da Governança, do Gerenciamento de Riscos e dos Controles Internos, incluindo a forma como as linhas anteriores alcançam os objetivos de gerenciamento.

7. Responsabilidades

7.1 Conselho Deliberativo

- Aprovar a Política de Gestão de Riscos e Controles Internos da SIM;
- Conhecer o relatório de Gestão de Riscos e Controles Internos submetido pela Diretoria Executiva;
- Aprovar e monitorar as diretrizes referentes ao apetite e à tolerância aos riscos da SIM;
- Conhecer e acompanhar os riscos prioritários e que possuem maior impacto no alcance dos objetivos da Operadora;
- Supervisionar os sistemas de Gestão de Riscos e Controles Internos estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a operadora, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude;
- Emitir à Diretoria Executiva recomendações para o aprimoramento da Gestão de Riscos.

7.2 Conselho Fiscal

- Conhecer e monitorar as diretrizes referentes ao apetite e à tolerância aos riscos da SIM;
- Conhecer o relatório de Gestão de Riscos e Controles Internos submetido pela Diretoria Executiva;
- Emitir à Diretoria Executiva recomendações para o aprimoramento da Gestão de Riscos.

7.3 Diretoria Executiva

- Aprovar a Política de Riscos e Controles Internos e submetê-la para apreciação do Conselho Deliberativo;
- Aprovar os indicadores de avaliação de desempenho da Gestão de Riscos;
- Fomentar a implementação da Gestão de Riscos e controles internos, promovendo sua institucionalização na Organização;
- Estabelecer as diretrizes referentes ao apetite e à tolerância a riscos da SIM e submetê-las para apreciação do Conselho Deliberativo;
- Assegurar os recursos necessários à implementação e execução do Sistema de Gestão de Riscos e Controles Internos da SIM;
- Assegurar o cumprimento dos objetivos estratégicos e da Política de Gestão de Riscos e Controles Internos
- Estabelecer estruturas adequadas para o gerenciamento de integridade, riscos e controle internos em consonância com as diretrizes do Conselho Deliberativo;
- Acolher as recomendações de aprimoramento da Gestão de Riscos emitidas pelos Conselhos Fiscal e Deliberativo, direcionar para os Agentes de Riscos e supervisionar o seu efetivo cumprimento.

7.4 Gestão de Riscos e Controles

- Utilizar metodologia, métodos e ferramentas definidos para identificar, controlar, monitorar e mitigar os riscos inerentes às atividades pelas quais é responsável;
- Refletir, nas Matrizes de Riscos e Controles, os riscos e controles relacionados ao seu processo/área;
- Medir, por meio de testes e indicadores, a efetividade dos controles, que serão acompanhados pela 2ª linha;
- Detectar novos riscos e controles em seu monitoramento, no dia a dia, e fazer refletir na matriz de riscos, mantendo-a atualizada;
- Assegurar o cumprimento das normas internas e regulamentares na prestação de contas, transparência e acurácia das informações, zelando pela efetividade e eficácia dos controles.

7.5 Comitê de Riscos

- Assessorar tecnicamente os administradores no aprimoramento da governança, no estabelecimento dos limites de exposição a riscos globais da Organização, diretrizes, normas e metodologias relacionadas às boas práticas de integridade, de gerenciamento dos riscos e de melhoria dos controles internos.

8. Considerações Finais

- Casos omissos a esta Política deverão ser encaminhados para deliberação do Conselho Deliberativo

Última revisão: 30/10/2025
Vigência: 2 anos
Versão: 4