POLÍTICA DE **GERENCIAMENTO DE RISCOS**

POL.003 REV.00

Unimed Brasil

POLÍTICA DE

GERENCIAMENTO DE RISCOS

POL.003 REV.00

Unimed Brasil

Diretoria Executiva da Unimed do Brasil

Gestão 2021 – 2025

Omar Abujamra Junior
Presidente

Emilson Ferreira Lorca
Vice-Presidente

Dilson Lamaita Miranda
Diretor de Administração e Finanças

Rubens Carlos de Oliveira Junior
Diretor de Desenvolvimento de Mercado

Marcos de Almeida Cunha
Diretor de Gestão de Saúde

Silvio Porto de Oliveira
Diretor de Intercâmbio

Claudio Laudares Moreira
Diretor de Regulação, Monitoramento e Serviços

Aprovações:

Glauco Samuel Chagas
Superintendente Executivo

Eduardo Pioltine Rachid
Gerente de Gestão Estratégica

Leandro dos Santos Silva
Coordenador de Governança Corporativa

Sumário

1. Objetivo

A presente Política de Gestão de Riscos tem como objetivo estabelecer um conjunto de princípios, diretrizes, papéis e responsabilidades relacionados às práticas de Gestão de Riscos adotados pela Unimed do Brasil, considerando aspectos como:

a. Transmitir conhecimento entre todos os colaboradores quanto aos principais riscos inerentes às suas respectivas atividades.
b. Incorporar uma abordagem consistente, integrada e abrangente para o Gerenciamento de Riscos, considerando o papel de todos os colaboradores.
c. Alinhar o apetite a risco, definido pela cooperativa, com seu planejamento e estratégia de negócios, a fim de auxiliar a Unimed do Brasil no processo de decisão.
d. Estabelecer instrumentos para identificação, avaliação, medição, tratamentos de ocorrência e respostas, bem como a comunicação dos riscos, relacionados às categorias definidas neste documento, assegurando proteção contra causas que resultem em exposições indesejáveis e que possam afetar os produtos, serviços e a estratégia de negócio.

A Unimed do Brasil considera que garantir a gestão de riscos, de forma legítima, correta e conforme, é de extrema relevância para a boa execução dos processos em cada uma de suas áreas, bem como para resguardar a imagem e a credibilidade da cooperativa perante colaboradores, clientes, terceiros e demais partes que se relacionam com a cooperativa.

2. Abrangência

Esta política se aplica e deve ser observada por colaboradores, clientes, terceiros e demais partes que se relacionam com a cooperativa, sendo estabelecida como base cultural e procedimental em relação à gestão de riscos e controles internos.

Havendo conflito entre as disposições desta política e a legislação aplicável, esta última prevalecerá.

3. Terminologia e Conceitos

Siglas e abreviações:

ANS: Agência Nacional de Saúde Suplementar.

MD: Modelo.

RN: Resolução Normativa.

POL: Política.

3.1. Definições gerais

ANS

A Agência Nacional de Saúde Suplementar (ANS) é o órgão responsável pela normalização, controle, regulação e fiscalização das atividades relativas à assistência privada à saúde.

Apetite a risco

É a quantidade de riscos, no sentido mais amplo, que a organização está disposta a aceitar em sua busca para agregar valor aos negócios. Ou seja, é análise da organização em assumir riscos versus o potencial de retorno de sua tratativa.

Cadeia de valor

A cadeia de valor demonstra, de forma macro, a relação dos processos institucionais, de negócio e apoio, a fim de satisfazer as necessidades dos clientes e partes interessadas no negócio.

COSO

Committee of Sponsoring Organizations of the Treadway Commission (COSO), organização dedicada à melhoria dos relatórios financeiros, sobretudo pela aplicação da ética e efetividade na aplicação e no cumprimento dos controles internos. Seu framework tem sido amplamente aplicado em todo o mundo. É reconhecida como uma estrutura modelo para desenvolvimento, implementação e condução do controle internos, bem como avaliação da sua eficácia.

Categoria de risco

É a classificação do grupo de riscos determinados no "Dicionário de riscos" da organização.

Compliance

A palavra "*compliance*" vem do verbo em inglês "*to comply*", no ambiente corporativo está relacionada à conformidade e à integridade corporativa. Exige adoção de condutas alinhadas com às leis vigentes, regulamentos e diretrizes internas e os imperativos éticos.

Dicionário de riscos

Documento corporativo utilizado pela organização, com o objetivo de padronizar em uma linguagem comum e definir conceitualmente os tipos de riscos mapeados.

ESG

É uma sigla em inglês para "*environmental, social and governance*" (ambiental, social e governança, em português). É usada para se referir às práticas ambientais, sociais e de governança de uma empresa.

Evento

Ocorrência, incidente ou mudança em um conjunto específico de circunstâncias que pode afetar a realização dos objetivos.

Fator de risco

Descrição detalhada da eventual falha que pode acontecer e sua consequência (impacto negativo que será gerado caso esta ocorra).

Frequência

Número de eventos ocorridos em um determinado período.

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.

Governança Corporativa

Estrutura composta pelas áreas Auditoria Interna, Compliance, Gestão da Qualidade e Gestão de Riscos e Controles Internos.

Impacto

São as consequências da ocorrência do evento. No caso dos riscos, representa o valor da perda provável (financeira ou não) de sua materialização.

ISO 31000:2018

Norma desenvolvida pela *International Organization for Standardization* (ISO), que estabelece os princípios e as orientações genéricas sobre gestão de riscos. Possui um framework universal reconhecido para gerenciar os riscos dos diversos processos de uma organização, independentemente de seu porte e segmento.

Matriz de riscos

Consolidação dos riscos associados às atividades da cooperativa que tem por objetivo apresentar o resultado da avaliação dos riscos identificados, mensurando critérios que auxiliarão no estabelecimento das prioridades com relação ao tratamento.

Plano de ação

É a definição das ações corretivas para reduzir a exposição aos riscos residuais, a partir da identificação das deficiências ao longo do ciclo de avaliação do ambiente de controles internos.

Probabilidade

É a possibilidade de um determinado evento de risco ocorrer, considerando o contexto e a frequência de execução da atividade na qual está inserido.

Resposta ao risco

Decisão que será tomada após a identificação do risco inerente ou avaliação do ambiente de controle dos riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de controles internos da organização.

Risco ambiental

É possibilidade de perda causada por agentes físicos (ex. ruído, vibração), químico (ex. poeira, gases) ou biológico (bactéria, fungo que podem causar prejuízos materiais ou imateriais de

ordem natural, social ou tecnológica, sobretudo devido a sua natureza, intensidade ou tempo de exposição.

Risco de integridade

Exposição a penalidades legais, perdas financeiras e de reputação, que podem se materializar caso a empresa não atue dentro da lei, das regras internas e externas, também conhecido como risco de *compliance*.

Risco de crédito

Medida de incerteza relacionada à probabilidade da contraparte de uma operação, ou de um emissor de dívida, não honrar, total ou parcialmente, seus compromissos financeiros, ou de ter a sua classificação de risco de crédito alterada.

Risco estratégico

É definido como a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos relacionados aos objetivos estratégicos, ou seja, eventos que impactam diretamente o cumprimento da estratégia da Unimed do Brasil.

Risco inerente

Risco existente em razão do tipo ou da natureza do negócio ou processo. É o risco ao qual uma atividade estaria exposta se não existissem controles ou outros fatores atenuantes implementados (é o risco bruto ou risco antes dos controles estarem implementados). Origina-se da natureza própria da atividade executada.

Risco legal

Medida de incerteza relacionada aos retornos de uma operadora por falta de um completo embasamento legal de suas operações. É o risco de não cumprimento de leis, regras, regulamentações, acordos, práticas vigentes ou padrões éticos aplicáveis, considerando, inclusive, o risco de que a natureza do produto/serviço prestado possa tornar a operadora particularmente vulnerável a litígios.

Risco de mercado

Medida de incerteza relacionada à exposição a perdas decorrentes da volatilidade dos preços de ativos, tais como cotações de ações, taxas de juros, taxas cambiais, preços de commodities e preços de imóveis.

Risco

Medida da incerteza a respeito de um evento ao qual a empresa está exposta. Representado pela possibilidade de perdas diretas ou indiretas, decorrentes de processos internos, pessoas e sistemas inadequados ou falhos, ou ainda de eventos externos.

Risco operacional

Medida de incerteza que compreende os demais riscos enfrentados pela operadora relacionados aos procedimentos internos, tais como risco de perda resultante de inadequações ou falhas em processos internos, pessoas e sistemas.

Risco residual

Risco remanescente após considerarmos os controles implementados e as ações mitigatórias (planos de ação) definidas para os riscos inerentes.

Risco social

É possibilidade de violação de relações pautadas em equidade, direitos humanos, direitos trabalhistas, saúde e segurança dos stakeholders, como colaboradores, fornecedores, clientes e comunidades onde a organização atua.

Risco de subscrição

Medida de incerteza relacionada a uma situação econômica adversa que contraria as expectativas da operadora no momento da elaboração de sua política de subscrição quanto às incertezas existentes na estimação das provisões técnicas e relativas à precificação.

4. Diretrizes

4.1. Disposições gerais

A Unimed do Brasil está comprometida com a adoção das boas práticas de governança, com o mais alto nível de cuidado, confidencialidade e conformidade com as legislações aplicáveis.

Como parte da Unimed do Brasil, no exercício de suas atividades, nossos colaboradores, gestores e administradores sempre devem garantir a adoção da gestão de riscos em suas operações em conformidade com a lei e com esta política.

Caso você tenha alguma dúvida em relação às suas obrigações, aos seus direitos e deveres em relação à gestão de riscos e controles internos, entre em contato com nosso time responsável por meio do e-mail gestao.riscos@unimed.coop.br.

4.2. Princípios Norteadores da Gestão de Risco e Controles Internos

A Política de Gestão de Riscos observa os seguintes princípios:

I. Agregar valor e proteger o ambiente institucional;
II. Ser transparente e conclusiva;
III. Ser parte integrante dos processos organizacionais;
IV. Apoiar a melhoria contínua das áreas da Unimed do Brasil;
V. Subsidiar a tomada de decisões.

A Unimed do Brasil cuida para que todas as atividades de gestão de riscos e controles internos estejam em conformidade com os princípios de governança trazidos pela ANS por meio da resolução normativa de nº 518 (e suas atualizações) e demais normas que vierem a tratar o mesmo tema.

4.3. Metodologia da Gestão de Riscos

O processo de Avaliação de Riscos e Controles da empresa tem como base os componentes e princípios do COSO ERM e ISO 31000:2018, bem como suas respectivas alterações, que têm como objetivo propiciar uma gestão integrada e eficaz, em linha com as melhores práticas utilizadas nos mercados nacional e internacional, para a proposição e implementação do modelo corporativo de gestão de riscos e controles internos.

4.3.1. COSO ERM 2017

O *framework* consiste em cinco componentes inter-relacionados do gerenciamento de riscos. Cada componente inclui princípios que se aplicam à criação, preservação e realização de valor, conforme figura, abaixo:

Governança e cultura

1. Conselho/direção exerce supervisão de estratégia e riscos
2. Estabelece estruturas operacionais
3. Define a cultura desejada
4. Demonstra compromisso valores fundamentais
5. Atrai, desenvolve e retém indivíduos capazes

Estratégia e definição de objetivos

6. Analisa o contexto de negócios
7. Define o apetite ao risco
8. Avalia estratégias alternativas
9. Formula objetivos de negócios

Desempenho

10. Identifica riscos
11. Avalia a gravidade do risco
12. Prioriza riscos
13. Implementa respostas ao risco
14. Desenvolve a visão do portfólio

Revisão e reavaliação

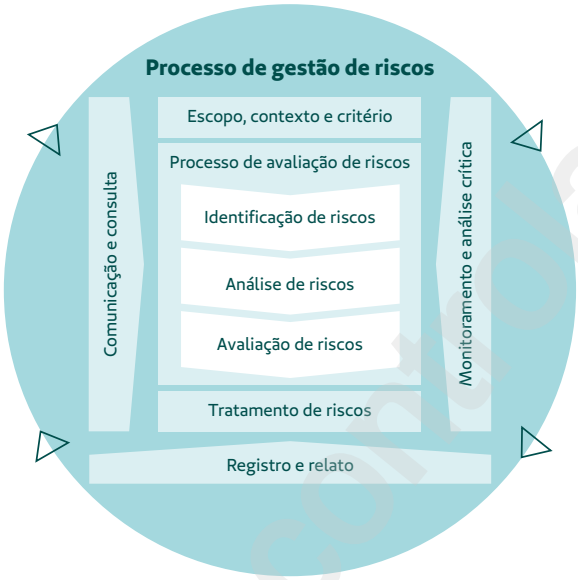
15. Avalia mudança substancial
16. Revê Risco e Desempenho
17. Busca melhoria na gestão de riscos corporativos

Informação, comunicação e relatórios

18. Alavanca a informação e a tecnologia
19. Comunica informações de risco
20. Relatórios de risco, cultura e desempenho

4.3.2. ISO 31000:2018

O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos, conforme ilustrado, a seguir:



4.4. Gerenciamento de Riscos

O gerenciamento de riscos corporativos é um processo conduzido pelo Conselho de Administração, Diretoria e demais empregados, aplicado no estabelecimento de estratégias formuladas para identificar eventos em potencial, em toda a organização, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. De forma sintética, pode-se dizer que o sistema de gerenciamento de riscos é composto pelas seguintes fases:

4.4.1. Análise do Ambiente e dos Objetivos

Nessa etapa, são identificados os objetivos relacionados ao processo organizacional e definidos os contextos – externo e interno – a serem levados em consideração ao gerenciar riscos. É importante apontar quais resultados são alcançados pelos processos organizacionais e possuem relação com os objetivos estratégicos da cooperativa.

Caso o processo a ser avaliado não esteja mapeado e disponível na Cadeia de valor da Unimed do Brasil, caberá à área de Gestão de Riscos executar suas atividades sem essa documentação. Nesse cenário, deverá ser comunicado à área de Gestão da Qualidade e Processos, para que possam apoiar a respectiva área no mapeamento do fluxograma, possibilitando a associação dos riscos e fatores de risco às atividades, conforme o padrão adotado pela empresa.

4.4.2. Identificação de Eventos

Uma vez mapeados os processos, a próxima etapa é identificar quais são os eventos que podem afetar o alcance dos objetivos da Unimed do Brasil, bem como o ambiente de controles necessário para geri-los. Sendo assim, o principal objetivo dessa atividade é identificar os riscos dos processos, seus respectivos fatores de riscos, impactos e probabilidades de ocorrência.

Identificados os fatores de riscos, seus impactos e probabilidades de ocorrência, devem ser classificados de acordo com o Dicionário de riscos da Confederação, contendo, as no mínimo, as seguintes classificações de riscos:

a. Risco de subscrição
b. Risco de crédito
c. Risco de mercado
d. Risco legal

e. Risco operacional
f. Risco estratégico
g. Risco de integridade
h. Risco social
i. Risco ambiental

NOTAS:

1. A avaliação dos riscos de integridade e legal também serão analisados pela área de Compliance em conformidade com a *POL.006 – Política de Compliance*, que estabelece o Programa de Integridade com finalidade de prevenir, identificar e mitigar atos de corrupção, fraudes, desvios de conduta e atos ilícitos que podem prejudicar a organização.
2. A avaliação dos riscos social e ambiental será foco da área de Sustentabilidade, além da análise de um conjunto de categorias de riscos disponíveis e sinalizadas no dicionário de riscos.

4.4.2.1. Dicionário de Riscos

Para auxiliar na identificação e no monitoramento dos riscos, foi criado um dicionário de riscos a ser utilizado por todas as áreas da Unimed do Brasil, elaborado com base nas exigências da Agência Nacional de Saúde Suplementar (ANS) e objetivos estratégicos da organização. São eles: *TB.086 - Dicionário de Riscos Corporativos - Unimed do Brasil* e *TB.102 - Dicionário de Riscos de TI - Unimed do Brasil.*

Caso um colaborador identifique algum risco que, a princípio, não conste no dicionário de riscos estabelecido, pode comunicar à área de Gestão de Riscos e Controles Internos, via e-mail gestao.riscos@unimed.coop.br, para que sejam tomadas as devidas providências. O dicionário de riscos da Unimed do Brasil será revisado anualmente pela área de Gestão de Risco e Controles Internos, ou sempre que necessário.

NOTA:

Com o objetivo de melhor direcionar o foco para os riscos de TI, o dicionário de riscos disponível no documento "Inventário de Riscos de Tecnologia da Informação" (*MD.473 - Inventário de Risco de TI*) conta com subcategorias que visam facilitar a visualização e identificação das categorias pela equipe responsável de TI.

4.4.3. Avaliação e Mensuração de Risco

Mensurar os riscos permite identificar as prioridades, além de facilitar o conhecimento das características dos riscos. É possível implementar melhor as atividades de controle conhecendo se os riscos têm maior impacto ou ocorrem com mais frequência. Para possibilitar a visualização dos riscos mais relevantes identificados, foram desenvolvidos os critérios de mensuração dos riscos. Essa mensuração é composta por duas variáveis: probabilidade X impacto.

NOTAS:

1. Caso cada critério de probabilidade e/ou impacto seja classificado em diferentes níveis, o nível mais alto prevalecerá no resultado final da classificação.
2. A mensuração dos riscos para a área de Tecnologia da Informação (TI), seguem critérios específicos disponíveis para consulta no documento Inventário de Riscos.

4.4.3.1. Probabilidade

São as chances de ocorrência de um evento. A tabela a seguir é utilizada para determinação da escala, considerando a quantidade de vezes em que o risco possa se materializar e/ou o percentual de ocorrências que possa acontecer em relação ao total das atividades ao qual a empresa está exposta:

ESCALA DE PROBABILIDADE			
Nível	**Descrição**	**Possibilidade de Ocorrência**	**% ocorrências**
1 Muito Baixa	Evento extraordinário, sem histórico de ocorrência.	1	Até 10%
2 Baixa	Evento casual, sem histórico de ocorrência.	Até 2	Entre 11% a 25%
3 Média	Evento esperado, de pouca frequência, com histórico de ocorrência parcialmente conhecido.	Até 6	Entre 26% a 75%
4 Alta	Evento esperado, com histórico de ocorrência amplamente conhecido.	Até 12	Entre 76% a 90%
5 Muito Alta	Evento repetitivo e constante.	Acima de 12	Acima de 90%

4.4.3.2. Impacto

São as consequências da ocorrência do evento. No caso dos riscos, representa o valor da perda provável (financeira ou não) de sua materialização. A tabela abaixo é utilizada para determinação da escala, considerando quais são as dimensões (custo, prazo, escopo, qualidade, perda) do objetivo do processo ao qual se está exposto ao risco.

ESCALA DE IMPACTO NOS OBJETIVOS DO PROCESSO					
Nível	**Aumento no custo/ prazo (%)**	**Perda financeira (em reais)**	**Interferência no escopo/ procedimentos**	**Regulatório**	**Imagem**
1 Muito Baixo	Até 5%	Até R$ 5.000	Insignificante	-	-
2 Baixo	Entre 6% e 10%	Entre R$ 5.001 e R$ 10.000	Pouca (atrasos de algumas horas)	-	-
3 Médio	Entre 11% e 15%	Entre R$ 10.001 e R$ 50.000	Relevante (interrupção temporária/atrasos de até 2 dias)	-	-
4 Alto	Entre 16% e 20%	Entre R$ 50.001 e R$ 100.000	Muito relevante (interrupção temporária/ atrasos de até 1 semana)	-	Prejudicial à imagem da UB
5 Muito Alto	Acima de 20%	Acima de R$ 100.000	Grave (descontinuidade das atividades por tempo indeterminado)	Descumprimento às Normas da ANS ou Legislação Brasileira	Prejudicial à imagem do Sistema Unimed

4.4.3.3. Avaliação dos Riscos

O risco será avaliado considerando sua relação entre probabilidade x impacto, utilizando-se como base a "Matriz de Classificação do Risco", assim, obtém-se a definição do nível do risco.

MATRIZ DE CLASSIFICAÇÃO DO RISCO		IMPACTO				
		1 Muito Baixo	**2 Baixo**	**3 Médio**	**4 Alto**	**5 Muito Alto**
PROBABILIDADE	**5 Muito Alta**	5	10	15	20	25
	4 Alta	4	8	12	16	20
	3 Média	3	6	9	12	15
	2 Baixa	2	4	6	8	10
	1 Muito Baixa	1	2	3	4	5
NÍVEL DO RISCO		Irrelevante (1)	Baixo (2 a 4)	Médio (2 a 4)	Alto (10 a 15)	Crítico (16 a 25)

4.4.3.4. Avaliação dos Controles Internos

Para concluir a avaliação do risco, é necessário verificar a eficácia do ambiente de controles internos, pois determinado risco inerente pode sofrer alteração em sua classificação se existirem controles para mitigá-lo, ou seja, pode ser que o risco residual seja de menor impacto, diminuindo o nível do risco. Para isso, a eficácia dos controles será considerada da seguinte forma:

AMBIENTE DE CONTROLE			
Eficácia	**% de falhas identificadas**	**Descrição**	**Multiplicador no Risco Inerente**
Ineficiente	Acima de 75%	Ausência de controle efetivo para mitigar o risco	1
Frágil	26 a 75%	O desenho do controle necessita de melhorias para mitigar o risco	0,8
Compensatório	1 a 25%	Controle manual desenhado adequadamente para mitigar o risco, no entanto, deve ser avaliado tempestivamente pois pode apresentar falhas	0,6
Eficaz	0	Controle sistêmico avaliado pela área GRC que mitiga o risco do processo	0,2

4.4.4. Priorização dos Riscos

A combinação da probabilidade de ocorrência e da magnitude de impacto define a criticidade dos riscos identificados e permite sua priorização, partindo dos riscos de alta para os de baixa severidade. Os riscos serão priorizados conforme o nível de severidade e que apresentam um maior impacto para a organização em caso de ocorrência.

Para os identificados em níveis crítico e alto, é obrigatória a formalização de um ou mais controles, com a finalidade de evitar, mitigar ou transferir o risco. Ao priorizar um risco em relação a outro, deve ser considerado o apetite a riscos da organização.

4.4.4.1. Apetite a riscos

O apetite a risco é a quantidade de riscos, no sentido mais amplo, que a Unimed do Brasil está disposta a aceitar em sua busca para agregar valor aos negócios. Uma vez definido, esse parâmetro poderá ser alterado somente pela Diretoria Executiva, ou por Comitê específico designado por ela. A Alta Administração escolhe os tratamentos aos riscos, desenvolvendo uma série de medidas para alinhá-los com a tolerância e com o apetite a risco. É importante que o apetite a risco seja estabelecido no início do processo de gerenciamento de riscos. Uma vez definido, a empresa declara que:

I. Todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada.
II. Todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

A tabela abaixo representa o apetite a risco que a Unimed do Brasil está disposta a aceitar. A partir desse apetite, será dada a tratativa de acordo com os critérios estabelecidos pela Diretoria.

Nível do Risco	Descrição	Resposta ao Risco
Crítico	**Risco inaceitável**, expõe a empresa a danos severos com impactos de difícil correção, impossibilitando o alcance dos objetivos estratégicos.	**Evitar:** Descontinuação das atividades que geram os riscos. **Mitigar:** Medidas para reduzir a probabilidade dos riscos. **Transferir:** Transferir uma parte do risco a terceiro.
Alto	**Risco inaceitável**, expõe a empresa a danos graves, dificultando o alcance dos objetivos estratégicos.	
Médio	**Risco aceitável**, pode expor a empresa a danos graves, o que dificulta o alcance dos objetivos do processo.	**Mitigar:** Medidas para reduzir a probabilidade dos riscos. **Transferir:** Transferir uma parte do risco a terceiros.
Baixo	**Risco aceitável**, pode expor a empresa a danos de menor relevância, no entanto, não deve dificultar o alcance dos objetivos do processo.	**Aceitar:** Nenhuma medida é adotada para afetar a probabilidade.
Irrelevante	**Risco irrelevante**, embora existente, não expõe a empresa a perdas significativas.	

4.4.5. Respostas aos Riscos

Responder aos riscos envolve a identificação das alternativas mais adequadas para modificar o nível do risco e o planejamento do conjunto de medidas a serem implementadas para tratá-los. A área de Gestão de Riscos e Controles Internos auxilia as áreas a dar a resposta mais adequada aos riscos identificados alinhado ao apetite a risco definido pela cooperativa, de forma que os objetivos não sejam impactados. As opções de respostas aos riscos são:

Evitar o risco	Descontinuação das atividades que geram os riscos. Ação para evitar totalmente o risco.
Mitigar o risco	Adoção de medidas para reduzir a probabilidade ou o impacto dos riscos, como por exemplo, implementação de controles para assegurar que determinado risco residual esteja de acordo com o apetite a riscos da empresa
Transferir o risco	Compartilhar ou transferir uma parte do risco a terceiros. Como por exemplo contratação de apólices de seguros ou terceirização de uma atividade.
Aceitar o risco	Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos, pois o nível do risco é considerado irrelevante, a capacidade da organização para tratá-lo é limitada, ou o custo é desproporcional ao benefício.

A decisão sobre a estratégia adotada para tratar cada risco depende principalmente do grau de apetite a risco da empresa, previamente aprovado pela Diretoria Executiva.

4.4.5.1. Tratamento ao Risco

Para os riscos identificados nas áreas da Unimed do Brasil que necessitem de controles para mitigá-los, serão abertos planos de ação que deverão conter, no mínimo, as seguintes informações:

a. Descrição da falha ou GAP identificado;
b. Indicação da área responsável pelo risco;
c. Descrição do plano de ação elaborado pela área gestora da ocorrência;
d. Prazo para implementação do plano;
e. Responsável pela implementação.

Os planos de ação deverão ser formalizados nos relatórios da Auditoria Interna, devidamente aprovados pelo gestor responsável pela área.

4.4.6. Comunicação e Monitoramento dos Riscos

4.4.6.1. Comunicação

A comunicação durante as etapas do processo de gestão de riscos deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pela legislação vigente. Além disso, a Unimed do Brasil promoverá comunicações que assegurem:

I. Compreensão clara a todas as áreas quanto ao papel, aos objetivos, às funções e às responsabilidades da área de Riscos.
II. Entendimento das pessoas chave sobre seu papel de atuação e suas responsabilidades no processo de Gestão de Riscos.
III. Esclarecimento sobre a implantação de planos de ação, com o intuito de minimizar o risco de a cooperativa não estar em conformidade com as leis e os regulamentos (internos e externos), especialmente nos casos em que haja exposição a multas e/ou sanções de órgãos reguladores.

O colaborador que identificar, durante suas atividades, qualquer situação que possa expor a Unimed do Brasil a algum risco deve comunicar à área de Gestão de Riscos e Controles Internos imediatamente, por meio do e-mail gestao.riscos@unimed.coop.br, para que seja avaliado e tomadas as devidas tratativas de mitigação e/ou correção do risco. A Unimed do Brasil está comprometida com a comunicação sobre a avaliação da gestão de riscos e seus controles internos, conforme determinado pelas resoluções normativas definidas pela ANS para esse fim.

4.4.6.2. Monitoramento

No âmbito do processo de gerenciamento de riscos, o monitoramento deve ser realizado principalmente pela área responsável pelo processo organizacional, de forma a:

I. Garantir que os controles sejam eficazes e eficientes;
II. Analisar as ocorrências dos riscos;
III. Detectar mudanças que possam requerer revisão dos controles e/ou do plano de ação;
IV. Identificar os riscos emergentes.

Esse processo é dinâmico e contínuo. Ele é crucial para a boa governança da cooperativa. As pessoas envolvidas em cada área devem ter capacidade e competência para diagnosticar,

priorizar, monitorar e gerir os seus riscos, sempre atentas às mudanças do ambiente (interno e externo) para não serem surpreendidas por riscos desconhecidos ou não controlados.

Portanto, mudanças identificadas durante o monitoramento devem ser encaminhadas à área de Gestão de Riscos e Controles Internos, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais da Unimed do Brasil.

NOTA:

A revisão das matrizes deve ocorrer conforme necessidade das áreas, atualização da eficácia dos controles pela equipe da Auditoria Interna ou no máximo a cada 1 ano, por meio de cronograma elaborado pela área de Gestão de Riscos e Controles Internos.

5. Papéis e Responsabilidades

I. **Diretoria Executiva:** deve tomar ciência periodicamente das diretrizes, estratégias e políticas referentes ao gerenciamento de riscos da cooperativa. Acompanhar, no mínimo, anualmente, a gestão de riscos com o objetivo de garantir sua eficácia e o cumprimento de seus objetivos.

II. **Área de Gestão de Riscos e Controles Internos:** responsável por auxiliar e treinar os responsáveis das áreas no gerenciamento dos riscos corporativos, e monitorar os eventos que possam impactar no cumprimento de seus objetivos. Reavaliar periodicamente o ambiente de controles internos da Unimed do Brasil para que os riscos estejam mitigados de acordo com o apetite a risco definido pela Diretoria Executiva.

III. **Gestores:** responsáveis pela identificação, mensuração, avaliação e gestão dos riscos que possam impactar o cumprimento de seus objetivos estratégicos e operacionais.

IV. **Colaboradores:** responsáveis por identificar os riscos existentes em seus processos e comunicar para seus gestores imediatos e à área de Gestão de Riscos para buscar as devidas tratativas em conjunto. Monitorar a ocorrência dos riscos.

V. **Auditoria Interna:** responsável por aferir, de forma independente, as regras e os procedimentos estabelecidos nesta política, mitigando os riscos quanto às gestões, aos controles e aos processos internos, além de realizar acompanhamento das ações para tratamento do risco.

VI. **Compliance:** responsável por identificar os riscos de integridade e monitora-los definindo as ações de controles, aculturamento e comunicação necessários para mitigá-los.

VII. Sustentabilidade: responsável por estruturar e disseminar o conceito de ESG, e também auxiliar os responsáveis das áreas na associação dos riscos sociais e ambientais à suas rotinas operacionais.

6. Disposições finais

Sem prejuízo das disposições contidas nesta política, a Unimed do Brasil se reserva ao direito de revisá-la, na periodicidade que melhor entender.

6.1. Canal de Ética

Colaboradores, fornecedores ou outros stakeholders que observarem quaisquer desvios às diretrizes desta política poderão relatar o fato ao Canal de Ética, podendo ou não se identificar.

O descumprimento das diretrizes desta política enseja a aplicação de medidas de responsabilização dos agentes que estiverem em desconformidade com este documento, conforme a respectiva gravidade do desvio identificado.

7. Documentos associados ou referências

CÓDIGO E DESCRIÇÃO
POL.006 - Política de Compliance
MD.473 - Inventário de Risco de TI
TB.086 - Dicionário de Riscos Corporativos - Unimed do Brasil
TB.102 - Dicionário de Riscos de TI - Unimed do Brasil

NOTAS:

A. Todos os documentos citados encontram-se disponíveis no sistema eletrônico de documentação vigente, dentro da classificação respectiva, bem como o controle do histórico de revisões.

B. A forma de arquivamento dos registros citados nesse documento se encontra na *TB.020 – Controle de registros e documentos.*

Alameda Santos, 1.827 - 10ª andar - Cerqueira César
01419-909 - São Paulo - SP - Tel.: (11) 3265-4000
www.unimed.coop.br