

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS		Código: SUT.POL.GO.01.01
			Aprovação: 03/03/2022
Fluxo de Valor:	Governança	Elaborado por:	Vannessa Silva
Área de Origem:	Governança, Risco e Compliance	Aprovado por:	Conselho de Administração

POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

SUMÁRIO

1 – OBJETIVO.....	3
2 - APLICAÇÃO.....	3
3 - DEFINIÇÕES.....	3
4 - DESCRIÇÃO DAS DIRETRIZES E REGRAS.....	7
4.1 - Papeis e Responsabilidade.....	7
4.2 - Processo de Avaliações de Riscos e Controles Internos.....	8
4.3 - Mapeamento dos Processos.....	10
4.4 - Escopo.....	10
4.5 - Contexto Interno e Externo.....	10
4.6 - Identificação dos Riscos.....	11
4.7 - Identificação dos Controles.....	12
4.8 - Identificação das Deficiências.....	12
4.9 - Autoavaliação de Riscos e Controles Internos.....	13
4.10 - Mensuração do Impacto e Probabilidade.....	13
4.11 - Cálculo do Risco.....	15
4.12 - Resposta ao Risco.....	16
4.13 - Avaliação do Ambiente de Controle.....	17
4.14 - Efetividade do Controle.....	20
4.15 - Planos de Ação.....	20
4.16 - Registro e Reporte.....	22
4.17 - Análise Crítica.....	23
5 – DOCUMENTOS E REGISTROS ASSOCIADOS.....	23
6 - HISTÓRICO DAS REVISÕES.....	23
7 - DICIONÁRIO DE RISCOS.....	22

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

1. OBJETIVO

O objetivo deste documento é garantir que a política de Gestão de Riscos e Controles Internos da Unimed Teresina esteja formalizada, atualizada e disponível para consulta de todos os colaboradores, de forma que estes reconheçam suas funções e responsabilidades no processo. Além disso, busca-se assegurar que os controles internos sejam efetivos e consistentes com a natureza, complexidade e riscos das operações. Ademais, pretende-se orientar os procedimentos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades dos colaboradores, incorporando aviso de riscos à operação e à tomada de decisões estratégicas, visando a sustentabilidade do negócio alinhado às melhores práticas de mercado.

2. APLICAÇÃO

As disposições desta Política se aplicam aos colaboradores da Unimed Teresina.

3. DEFINIÇÕES

Agente de Conformidade: colaborador interno designado para apoiar as áreas operacionais no gerenciamento dos riscos relacionados à execução das atividades cotidianas, servindo como suporte e facilitador da área de Governança, Riscos e *Compliance*.

Autoavaliação de Riscos e Controles (CSA – *Control Self Assessment*): consiste na avaliação semestral, realizada pelos gestores que administram as áreas da Unimed Teresina, com intuito de identificar os riscos e avaliar o ambiente de controles. A avaliação dos gestores é revisada pela área de Governança, Riscos e *Compliance*, por meio de técnicas como *walkthrough*, testes de aderência e/ou resultados de trabalhos sobre o ambiente de controles internos, como os processos de fiscalização de Órgãos Reguladores e trabalhos das auditorias internas e externas.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

Cadeia de Valor: consiste na forma como as atividades, processos e negócios da Unimed Teresina estão organizados, de modo a gerar valor às partes interessadas, como acionistas, fornecedores, colaboradores, órgãos reguladores e consumidor final.

Código de Conduta Ética: conjunto de princípios, valores e normas que regem as relações da Unimed Teresina com todos os seus stakeholders.

Categoria de Risco: é a classificação do grupo de riscos determinados no “Dicionário de Riscos” da Unimed Teresina.

Comitê de Governança, Riscos e Compliance: reunião que tem por objetivo garantir a transparência e a ética na Unimed Teresina, zelando pela efetiva adoção das melhores práticas de governança, assim como avaliar os riscos inerentes aos seus negócios, incluindo avaliações qualitativa e quantitativa, de forma a assegurar a boa gestão dos recursos, a proteção e a valorização do seu patrimônio.

Controle (barreira): conjunto de políticas, metodologias e normas, além de atividades de acompanhamento (automatizadas ou não) com vistas a reduzir o grau de exposição a risco, subsidiar o cumprimento dos objetivos estabelecidos por uma organização, assegurar a existência de conformidade com as leis e regulamentos, assim como promover a confiabilidade dos relatórios gerenciais.

Controle chave: elementos essenciais ou mais importantes de controle em um processo ou subprocesso. Esses controles mitigam diretamente o risco para uma percentagem elevada das transações ou valores processados.

Controle compensatório: controle que não é considerado “chave”, mas que, na falta ou inexistência de um controle chave, reduz a frequência ou gravidade de um incidente/risco.

Controle detectivo: mecanismos que demonstram a existência de anomalias ou de desvios em relação às metas ou objetivos estabelecidos pela organização.

Controle preventivo: conjunto de políticas, normas e procedimentos estabelecidos pela organização com o objetivo de reduzir, preventivamente, o grau de exposição aos riscos.

COSO (Committee of Sponsoring Organizations of the Treadway Commission): entidade sem fins lucrativos dedicada à melhoria contínua da confiabilidade dos dados apresentados nas

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

demonstrações financeiras, por instrumento da ética, efetividade dos controles internos e governança corporativa. Desenvolveu, em 1992, o *framework* “*Internal Control - Integrated Framework*”, posteriormente revisado e relançado no ano de 2013, o qual se tornou referência mundial para o estudo e a aplicação de controles internos efetivos.

Deficiência de controle: irregularidades na execução do controle, identificadas ao longo dos procedimentos de avaliação do ambiente de controles (ausência de controle, de evidência, de política, deficiência no desenho, entre outros).

Dicionário de riscos: documento corporativo utilizado pela Unimed Teresina com o objetivo de padronizar em uma linguagem comum e definir conceitualmente os tipos de riscos mapeados.

Fator de risco: descrição detalhada ou causa que contribui para a materialização do risco no subprocesso.

Frequência: número de eventos ocorridos em um determinado período.

Impacto: é o volume do prejuízo/ganho financeiro e a extensão do desgaste/conservação da imagem institucional da Unimed Teresina provocados por um determinado evento, por descumprimento de demandas regulatórias e/ou por não atendimento dos objetivos estratégicos.

Indicador de risco: métrica baseada em aspectos quantitativos ou qualitativos. É também uma medida que, ao longo do tempo, serve como um alerta inicial para a materialização de possíveis eventos/incidentes futuros com impactos potencialmente adversos e avaliação histórica da evolução do ambiente de controles.

ISO 31000:2018: norma desenvolvida pela *International Organization for Standardization (ISO)* que estabelece os princípios e orientações genéricas sobre gestão de riscos. Possui um *framework* universal reconhecido para gerenciar os riscos dos diversos processos de uma organização, independentemente do seu porte e segmento.

Mapa de Riscos: demonstração gráfica dos riscos associados às atividades da Unimed Teresina que tem por objetivo apresentar o resultado da avaliação dos riscos identificados, mensurando os critérios que auxiliarão no estabelecimento das prioridades com relação ao tratamento.

Patrimônio Líquido: Patrimônio Líquido ou Capital Próprio é o que representa o valor contábil devido pela pessoa jurídica, aos sócios ou acionistas, com base no Princípio da Entidade. No balanço patrimonial, esse termo consiste na diferença entre o valor dos ativos e dos passivos.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

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.

Política de Gestão de Riscos e Controles Internos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

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

Programa de Integridade: conjunto de ações que visam organizar, documentar e gerenciar os princípios, valores e normas contidos no Código de Conduta Ética da Unimed Teresina.

Resposta ao Risco: decisão que será tomada após a identificação do risco original ou avaliação do ambiente de controle dos riscos residuais, com o objetivo de promover discussões que assegurem a eficiência do ambiente de controles internos da Unimed Teresina.

Risco negativo: medida da incerteza a respeito de um evento ao qual a organização está exposta. Esse risco é representado pela possibilidade de perdas diretas ou indiretas, decorrentes de processos internos, pessoas e sistemas inadequados e/ou falhos ou ainda de eventos externos.

Risco Original: risco existente em razão do tipo ou natureza do negócio ou processo. É o risco que uma atividade estaria exposta se não houvesse 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 positivo: medida da incerteza a respeito de um evento ao qual a organização está exposta. Representado pela possibilidade de ganhos diretos ou indiretos, decorrentes de processos internos, pessoas e sistemas ou eventos externos que possam caracterizar oportunidades.

Risco Residual: risco remanescente após considerarmos os controles implementados e ações mitigatórias (planos de ação) definidas para os riscos originais, ou seja, é o risco líquido.

4. DESCRIÇÃO DAS DIRETRIZES E REGRAS

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

4.1 . PAPÉIS E RESPONSABILIDADES

4.1.1. As responsabilidades no modelo de Gestão de Riscos, Controles Internos e *Compliance* da Unimed Teresina baseiam-se no conceito de três linhas de defesa, conforme posicionamento do Instituto dos Auditores Internos (IIA) a respeito do tema “Gerenciamento Eficaz de Riscos e Controles”. A atuação da área de Governança, Riscos e *Compliance* ocorre na 2ª linha de defesa, de maneira independente, mas não de forma isolada das áreas gestoras, conforme demonstrado na figura a seguir:

Figura 1 - Estrutura de camadas e níveis de reporte



1ª linha de defesa: responsável pelo gerenciamento, monitoramento e ações de respostas aos riscos, sendo essa a área responsável pelos processos/subprocessos, riscos originais e execução de ações para mitigação dos riscos.

2ª linha de defesa: responsável pelo apoio à 1ª linha de defesa, auxiliando na identificação, mensuração, avaliação, mitigação, monitoramento e reporte dos riscos e efetividade dos controles, bem como na aderência ao cenário regulatório, tanto interno quanto externo.

3ª linha de defesa: responsável por fornecer, para a alta administração da organização e os órgãos de governança, as avaliações independentes quanto à eficiência e eficácia dos processos e procedimentos estabelecidos, atuando em conformidade com as normas internacionais reconhecidas para a prática de auditoria interna.

4.1.2. O processo de mapeamento de riscos e controles internos está alinhado às diretrizes e aos

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

valores éticos definidos pelo Código de Conduta Ética, fazendo parte do Programa de Integridade da Unimed Teresina.

4.1.3. As diretrizes voltadas para a gestão dos riscos inerentes às atividades abaixo estão descritas em Políticas específicas:

- i. Desenvolvimento e precificação de produtos;
- ii. Comercialização/disponibilização de produtos;
- iii. Contratação de outras operadoras, seguradoras ou resseguradoras como forma de mitigação de riscos de suas atividades;
- iv. Investimentos;
- v. Gestão de fluxo de caixa;
- vi. Cálculo de provisões técnicas e Teste de Adequação do Passivo (TAP), conforme as premissas estabelecidas pela Agência Nacional de Saúde (ANS);
- vii. Acompanhamento de processos judiciais e suas estimativas de valores a partir do histórico de perdas;
- viii. Transações com partes relacionadas e adiantamentos;
- ix. Relacionamento com prestadores e outros fornecedores;
- x. Gestão de Tecnologia da Informação; e
- xi. Gestão da continuidade dos contratos.

4.2. PROCESSO DE AVALIAÇÃO DE RISCOS E CONTROLES INTERNOS

4.2.1. O processo de Avaliação de Riscos e Controles Internos da Unimed Teresina tem como base os componentes e princípios do COSO e ISO 31000:2018, por isso, seu objetivo é propiciar uma gestão integrada e eficaz, alinhada às melhores práticas utilizadas no mercado nacional e internacional para a proposição e implementação do modelo corporativo de gestão de riscos e controles internos.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: 11/10/2022

Figura 2 – Processo de Gestão de Riscos



4.2.2. Destacamos a seguir as etapas do processo:

- Mapeamento dos processos;
- Escopo;
- Contexto interno e externo;
- Identificação dos riscos;
- Identificação dos controles;
- Identificação das deficiências;
- Autoavaliação de riscos e controles pelos gestores;
- Mensuração do impacto e probabilidade;
- Classificação do risco;

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

- x. Resposta ao risco;
- xi. Monitoramento e avaliação do ambiente de controles;
- xii. Registro e reporte; e
- xiii. Análise crítica.

4.3. MAPEAMENTO DOS PROCESSOS

4.3.1. O mapeamento possibilita uma visão detalhada dos processos e subprocessos da Unimed Teresina, bem como o entendimento das principais características das operações, por meio da análise da documentação disponível e com base em entrevistas com gestores e colaboradores importantes que atuam nos processos do negócio.

4.3.2. Os principais objetivos do mapeamento de processos estão relacionados ao entendimento das atividades de negócio, suporte ou gestão, considerando o escopo definido, identificando os eventos efatores de risco, bem como os controles do processo ou do subprocesso. A etapa de mapeamento é essencial para o funcionamento dos controles internos, uma vez que constitui a fase de entendimento sobre o ambiente de negócios e a estrutura de controles.

4.3.3. Os processos estão documentados na Cadeia de Valor da Unimed Teresina.

4.4. ESCOPO

4.4.1. Trata-se dos diversos segmentos da Unimed Teresina que realizam o gerenciamento de riscos conforme seus papéis e responsabilidades.

4.5. CONTEXTO INTERNO E EXTERNO

4.5.1. Os contextos interno e externo da Unimed Teresina estão definidos em seus Planejamentos

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Estratégicos.

4.6. IDENTIFICAÇÃO DOS RISCOS

4.6.1. Uma vez mapeados os processos, é preciso identificar quais são os eventos de riscos que podem afetar o alcance dos objetivos da Unimed Teresina, bem como o ambiente de controles necessário para gerir esses eventos. Sendo assim, a principal finalidade dessa atividade é identificar os riscos dos processos, bem como seus respectivos fatores, impactos e probabilidades de ocorrência.

4.6.2. Caso o subprocesso a ser avaliado não esteja mapeado e disponível na Cadeia de Valor da Unimed Teresina, caberá à área de Governança, Riscos e *Compliance* executar suas atividades sem essa documentação, possibilitando a realização de seus trabalhos. Nesse caso, deve-se alertar a área de Processos, para que possa apoiar a respectiva área no mapeamento do processo, possibilitando a associação dos riscos e fatores de risco às atividades, conforme o padrão adotado pela Cooperativa.

4.6.3. Para auxiliar o levantamento dos riscos e fatores de riscos, a área de Governança, Riscos e *Compliance* deve realizar o seguinte exercício:

- i. Por que o risco pode se materializar?
- ii. O que pode causar a materialização do risco?
- iii. Quais são os agentes causadores?
- iv. O que ocorre caso o fator de risco se materialize?

4.6.4. Identificados os fatores de riscos, seus impactos e as probabilidades de ocorrência, estes aspectos devem ser classificados de acordo com o Dicionário de Riscos da Unimed Teresina, o qual está dividido de acordo com os grupos abaixo e disposto no Anexo I desta Política.

- i. Risco de Crédito;
- ii. Risco de Liquidez;
- iii. Risco de Mercado;
- iv. Risco Estratégico;
- v. Risco de Subscrição;

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

- vi. Risco de Imagem;
- vii. Risco Operacional;
- viii. Risco Legal;
- ix. Risco Ambiental;
- x. Risco de Terceirização.

4.6.5. Finalizada a identificação dos riscos, a área de Governança, Riscos e *Compliance* é responsável por associá-los aos processos, alimentando a matriz de riscos e controles.

4.7. IDENTIFICAÇÃO DOS CONTROLES

4.7.1. Paralelamente ao mapeamento/identificação dos riscos, a área de Governança, Riscos e *Compliance* deve identificar os controles existentes na estrutura da Unimed Teresina, os quais possuem objetivo de mitigar a exposição aos riscos identificados.

4.7.2. A partir da identificação dos controles existentes nos processos, estes devem ser associados aos seus respectivos riscos, cadastrados na matriz de riscos e controles.

4.8. IDENTIFICAÇÃO DAS DEFICIÊNCIAS

4.8.1. As deficiências são apontamentos que demandam ação do responsável para correção da ocorrência, podendo decorrer, por exemplo, das ausências de controle e de evidência na execução do controle, da não aderência a uma norma aplicável ou da não execução efetiva de um controle, identificadas pela área responsável pelo processo ou pela área de Governança, Riscos e *Compliance*.

4.8.2. Nesta etapa, a identificação das deficiências pode ser realizada por qualquer membro da 1ª ou 2ª linha de defesa. A área responsável pelo processo para o qual foi apontada uma deficiência, é encarregada de apresentar como resposta uma proposta de solução, traduzida em um plano de ação, o qual será tratado na etapa “Resposta”.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

4.9. AUTOAVALIAÇÃO DE RISCOS E CONTROLES INTERNOS

4.9.1. A autoavaliação é uma ferramenta que visa avaliar e priorizar os riscos mapeados nos processos das áreas de negócio, apoio e/ou gestão, aprimorando o conhecimento dos riscos pelos gestores, de modo a direcionar as ações de mitigação e monitoramento. Essa ferramenta é utilizada pelo gestor (proprietário) dos processos, com o apoio da área de Governança, Riscos e *Compliance*.

4.10 MENSURAÇÃO DO IMPACTO E PROBABILIDADE

4.10.1. Mensurar os riscos permite identificar as prioridades, além de facilitar o conhecimento das características dos riscos. É possível implementar melhor as atividades de controle compreendendo se os riscos têm maior impacto ou ocorrem com mais frequência.

4.10.2. A fim de possibilitar a visualização dos riscos mais relevantes identificados, foram desenvolvidos os critérios de mensuração dos riscos. Esta é composta por duas variáveis (detalhadas a seguir conforme tabelas e gráfico listados):

a) **Impacto**, que significa o valor financeiro ou não, oriundo da materialização dos riscos negativos ou positivos, conforme a tabela a seguir:

Tabela 1 - Mensuração de Impacto

Métricas		Descrição
1	Impacto Baixo	- Impacto Financeiro: R\$ 0,01 a R\$ 100.000,00; - Impacta ligeiramente a imagem da empresa e/ou o alcance de seus objetivos estratégicos.
2	Impacto Moderado	- Impacto Financeiro: R\$ 100.000,01 a R\$ 500.000,00; - Impacta razoavelmente a imagem da empresa e/ou alcance de seus objetivos estratégicos.
3	Impacto Alto	- Impacto Financeiro: acima R\$ 500.000,01; - Impacta profundamente a imagem da empresa, cumprimento de demandas regulatórias e/ou o alcance de seus objetivos estratégicos.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

b) **Probabilidade**, que é a possibilidade de um determinado evento de risco ocorrer, considerando o contexto e a frequência de execução da atividade na qual está inserido, conforme se observa na tabela seguinte:

Tabela 2 - Mensuração de Probabilidade

Métricas	Descrição
1 Rara	O risco poderá se manifestar em circunstâncias excepcionais (por exemplo: até 3 eventos dentro de um período de 12 meses), tendo em vista a efetividade dos controles internos, o monitoramento do processo por meio de indicadores, os relatos de não conformidade e os relatórios gerenciais.
2 Eventual	O risco poderá se manifestar em algum momento (por exemplo: 4 a 10 eventos dentro de um no período de 12 meses), tendo em vista a fragilidade dos controles internos, o monitoramento do processo por meio de indicadores, o histórico de ocorrências, os relatos de não conformidade e os relatórios gerenciais.
3 Frequente	O risco poderá se manifestar com frequência (por exemplo: acima de 10 eventos dentro de um período de 12 meses), tendo em vista a fragilidade ou inexistência dos controles internos, o monitoramento do processo por meio de indicadores, o histórico de ocorrências, os relatos de não conformidade e os relatórios gerenciais.

Nota: ao avaliar a probabilidade de ocorrência do evento, deve ser levada em consideração a frequência de execução dos controles.

Gráfico 1 - Matriz de Riscos



	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Área III (Vermelha): são os riscos com alta significância, podendo ter probabilidade frequente de ocorrência e impacto alto; ter probabilidade frequente de ocorrência e impacto moderado; ou ter probabilidade eventual de ocorrência e impacto alto. Os riscos classificados nessa área exigem a implementação das estratégias de proteção e prevenção (ação corretiva).

Área II (Amarela): são os riscos com média significância, podendo ter probabilidade frequente de ocorrência e baixo impacto; ter probabilidade eventual de ocorrência e impacto moderado; ou ter probabilidade rara de ocorrência e alto impacto. Os riscos classificados nessa área devem ser monitorados de forma rotineira e sistemática, podendo também exigir a implementação das estratégias de proteção e prevenção (ação corretiva)

Área I (Verde): são os riscos com baixa significância, podendo ter probabilidade rara de ocorrência e baixo impacto; ter probabilidade eventual de ocorrência e baixo impacto; ou ter probabilidade rara de ocorrência e impacto moderado. Esses riscos somente devem ser gerenciados e administrados, pois estão com "exposição aceitável".

4.11. CÁLCULO DO RISCO

4.11.1. O Risco leva em consideração as métricas de impacto e probabilidade. O seu valor é resultado da multiplicação dessas duas variáveis, ou seja:

$$\textbf{Risco} = \textbf{Impacto} \times \textbf{Probabilidade}$$

A tabela abaixo apresenta a pontuação e resultado obtido no cálculo do risco, a partir da fórmula acima.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Tabela 3 – Significância do Risco

SIGNIFICÂNCIA DO RISCO
Alto – 6 ou 9
Moderado – 3 ou 4
Baixo – 1 ou 2

Nota: o Risco Original não considera os controles para mitigação, no entanto, o Risco Residual é o que sobra após considerar a efetividade dos controles internos.

4.12 RESPOSTA AO RISCO

b

4.12.1. Para orientar a tomada de decisão, deve ser definida a resposta aos riscos, conforme as categorias descritas abaixo:

- **Eliminar:** só é possível, quando existe a descontinuidade das atividades que geram os riscos;
- **Mitigar:** ações são tomadas para reduzir a probabilidade de materialização e/ou impacto do risco. Esta resposta envolve o aprimoramento ou a criação de controles e melhorias em processos ou subprocessos, por meio da formulação e implementação de planos de ação;
- **Transferência:** redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma parcela de riscos (exemplos: resseguro e terceirização de atividades); e
- **Aceitar (*):** nenhuma ação é tomada para influenciar a probabilidade de ocorrência e/ou impacto do risco.

(*) Em caso de aceitação do risco, ou seja, quando nenhuma ação corretiva for definida para mitigação do risco, a seguinte alçada de aprovação, conforme tabela a seguir, deve ser seguida e formalmente documentada em ata de reunião de algum dos fóruns executivos da Unimed Teresina:

Tabela 4 – Alçada de aprovação

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Alçada	Risco Residual		
	Baixo	Moderado	Alto
Gerentes	X	X	
Superintendentes e Diretoria			X

Nota: a assunção dos riscos classificados como “Altos” somente poderá ser feita pela Diretoria Executiva.

4.13. AVALIAÇÃO DO AMBIENTE DE CONTROLE

Após mensurar o impacto e probabilidade dos riscos associados ao processo, as áreas deverão avaliar os controles mapeados para mitigação dos riscos, por meio da técnica CSA (Autoavaliação de Controles - *Control Self Assessment*). Em seguida, logo depois da autoavaliação dos controles pelas áreas, eles serão avaliados pelo setor de Governança, Riscos e *Compliance* ou agentes de conformidade, por meio de *walkthrough* ou teste de controle.

***Walkthrough* e Testes de Controles**

São atividades sob responsabilidade da área de Governança, Riscos e *Compliance*, podendo ser executadas por agentes de conformidade. Essas atividades têm como objetivo avaliar a eficácia e eficiência dos controles existentes e associados aos riscos inerentes aos processos da Unimed Teresina. A avaliação por meio do *walkthrough* e dos testes de controles é um mecanismo que assegura a existência e revisão periódica dos processos, riscos e controles da Cooperativa, e deverá ser executada de acordo com o impacto do risco, conforme tabela abaixo:

Tabela 5 – Classificação do Risco Residual

	CLASSIFICAÇÃO DO RISCO RESIDUAL		
	Baixo	Médio	Alto
Tipo de Avaliação	<i>Walkthrough</i>	<i>Walkthrough</i>	Teste de Controle

Walkthrough

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Consiste na revisão do fluxo de atividades de um determinado processo e considera a avaliação do desenho dos controles para mitigação dos riscos, com o objetivo de:

- Confirmar o entendimento sobre o processo e o fluxo de transações;
- Validar a eficácia do desenho de controles identificados;
- Confirmar se os controles estão em operação; e
- Revisar os riscos dos processos e identificar novos riscos.

A realização do *walkthrough* nos controles deve fornecer as evidências necessárias para avaliar a eficácia do desenho do controle. Após conclusão dessa tarefa, os resultados devem ser registrados com o preenchimento das atividades realizadas, das evidências geradas e da conclusão do *walkthrough* (resultado efetivo ou inefetivo).

Nota: Para os controles considerados inefetivos, a área de Governança, Riscos e *Compliance* deverá registrar as deficiências de controles (*gaps*) para que os setores envolvidos elaborem planos de ação corretivos, conforme detalhado na etapa de Mitigação e Controle desta Política.

Teste de Controle

Consiste em avaliar a efetividade do funcionamento/operação dos controles, considerando as seguintes diretrizes:

- Avaliar se o controle é executado corretamente, de acordo com o seu desenho;
- Avaliar se o controle é executado de acordo com a frequência esperada;
- Verificar se o controle é aplicado a todas as operações contempladas pelo fluxo operacional; e
- Revisar se os desvios estão suportados por controles compensatórios.

Os testes de controles deverão ser realizados por meio de seleção de amostras aleatórias, feita para garantir a confiabilidade da base. O tamanho da amostra deve ser definido de acordo com a frequência do controle.

Para a execução dos testes de efetividade dos controles devem ser utilizadas as seguintes técnicas:

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

Indagação: entrevistas detalhadas para obtenção de evidências quanto à eficácia dos controles. Essa técnica deve ser realizada, obrigatoriamente, em conjunto com outros métodos de execução de testes (exemplo: análise de evidência documental), para corroborar a informação obtida na indagação.

Observação: consiste em observar a execução de uma atividade de controle, o que normalmente fornece evidência substancial sobre sua eficácia. Apesar disso, por si só, a observação não fornece material suficiente para concluir sobre o êxito da atividade de controle. A ausência de erros nos itens observados não fornece evidência conclusiva de que a atividade de controle é eficaz sem a supervisão.

Análise de documentação: é a obtenção de evidências quanto à eficácia do controle por meio de análise da documentação. O grau de segurança que se obtém com essa técnica é considerado alto para a grande maioria dos controles, porém pode haver a necessidade dessa etapa ser complementada com outro tipo de técnica.

“Reperformance”: consiste na reexecução independente do controle. O resultado confere alta segurança quanto à efetividade do controle para a amostra selecionada. Essa técnica tem como ponto desfavorável o seu alto custo e tempo para execução.

Por fim, da mesma maneira que no *walkthrough*, a área de Governança, Riscos e *Compliance* deve registrar os *gaps* (deficiências) e direcioná-los aos setores internos da empresa para a elaboração de planos de ação que mitiguem as deficiências apontadas.

Nota: essa fase de avaliação, por meio de *walkthrough* e testes de controles, poderá ser realizada por agentes de conformidade.

Quality Assurance

Caso o processo de *walkthrough* seja realizado por agentes de conformidade, será necessário avaliar os

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

resultados alcançados, de modo a assegurar que o padrão de qualidade de execução seja cumprido pelas equipes designadas. Assim, o *Quality Assurance* consiste em:

- Verificar a coerência da avaliação realizada por meio de *walkthrough*;
- Avaliar a capacidade de mitigação dos planos de ação, para os casos aplicáveis; e
- Verificar a existência de evidências que suportam os resultados alcançados.

4.14. EFETIVIDADE DO CONTROLE

Com o término do ciclo de avaliação por meio de *walkthrough*, a área de Governança, Riscos e Compliance deverá concluir sua avaliação sobre o ambiente de controles internos da Unimed Teresina. Neste momento, a avaliação é realizada de forma qualitativa e deve levar em consideração não apenas os resultados alcançados no *walkthrough*, mas também a probabilidade de ocorrência da materializaçãodo risco, do histórico de falhas, dos apontamentos de fiscalização, de auditorias, entre outros.

Apresentamos, a seguir, os conceitos a serem considerados para auxiliar a avaliação:

Tabela 6 - Efetividade do Controle

Inefetivo	Efetivo	Inexistente
Os controles internos apresentam falta de confiabilidade e as ações corretivas são implementadas somente após a materialização dos riscos.	Os controles internos apresentam confiabilidade, não necessitando de ações corretivas. Além disso, existem políticas, normas e procedimentos formalizados.	Os controles internos não foram definidos e aplicados, elevando a classificação do risco por conta de sua exposição.

4.15. PLANOS DE AÇÃO

Para os riscos que as áreas de negócios (1ª linha de defesa) não optarem por “Evitar” ou “Aceitar”, deverão ser definidos planos de ação para correção/melhoria do ambiente de controle, visando a mitigação do risco. Os planos de ação podem ser originários de aderência a novos normativos e/ou regulamentações ou derivados de análises de autoavaliação, *walkthrough*, testes de controles ou auditorias. Para cada plano de ação deve ser definido também um prazo para implementação.

Para os controles associados aos riscos residuais “moderados” e “altos”, testados e considerados

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

inexistentes ou inefetivos, se torna obrigatória a necessidade de planos de ação e controles compensatórios, visando a diminuição da possível materialização do risco, assim como há a necessidade de testar esses controles compensatórios até a implementação do plano de ação definitivo.

Segue abaixo tabela para aplicação dos planos de ação, de acordo com o resultado da efetividade do controle e risco residual:

Tabela 7 – Efetividade do Controle e Risco Residual

Efetividade do controle	RISCO RESIDUAL		
	Baixo	Moderado	Alto
Inexistente/ Inefetivo	Plano de Ação	Plano de ação + controle compensatório	Plano de ação + controle compensatório

4.15.1. Monitoramento dos Planos de Ação

O acompanhamento da implementação dos planos de ação deve ser realizado pela área de Governança, Riscos e *Compliance*, para posterior encerramento da atividade. Caso o prazo de implementação ultrapasse o que definido inicialmente, a referida área deve solicitar a reavaliação do setor responsável pelo processo (1ª linha de defesa) e a respectiva alteração.

Finalizado o plano de ação pela área proprietária (1ª linha de defesa), o setor de Governança, Riscos e *Compliance* deverá avaliar a efetividade dos planos de ação por meio de *walkthrough* e/ou teste no controle, para posterior encerramento da deficiência.

4.16. REGISTRO E REPORTE

A etapa de reporte contempla a responsabilidade da área de Governança, Riscos e *Compliance* em relação ao reporte do processo de Avaliação de Riscos e Controles à alta administração da Unimed Teresina. Também deve ser considerado o reporte independente realizado pela Auditoria Interna (3ª linha de defesa).

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

O reporte da avaliação de riscos e controles deverá ser realizado junto aos gestores responsáveis pelos processos avaliados ao final de cada ciclo de avaliação e, posteriormente, ao Comitê de Governança, Riscos e *Compliance*.

Apresentamos, a seguir, exemplos de assuntos a serem abordados:

- Resultado dos riscos identificados;
- Resultado da avaliação do ambiente de controles;
- Monitoramento de planos de ação; e
- Opinião conclusiva sobre o ambiente de controles internos.

A área de Governança, Riscos e *Compliance* deverá elaborar o relatório de Avaliação do Ambiente de Controles Internos, semestralmente, que deverá permanecer arquivado na área por, no mínimo, 5 (cinco) anos, estando ainda à disposição da Agência Nacional de Saúde Suplementar (ANS), das auditorias, da Diretoria Executiva e do Conselho de Administração, caso solicitado.

Além das definições descritas acima, quaisquer casos não previstos e/ou em desacordo com a presente Política deverão ser submetidos ao Comitê de Governança, Riscos e *Compliance*, dado que este é o fórum competente para reporte e acompanhamento das disposições previstas neste documento.

4.17. ANÁLISE CRÍTICA

A etapa de análise crítica da gestão de risco deve ser realizada semestralmente. A análise crítica deve incluir:

- O resultado das auditorias de Gerenciamento de Riscos (internas e externas);
- As ações de aculturação para reforço da mentalidade de riscos; e
- O resultado da avaliação dos controles internos.

Esta política entrará em vigor na data de sua aprovação.

	POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	Código: SUT.POL.GO.01.01
		Publicação: xx/xx/xxxx

5 DOCUMENTOS E REGISTROS ASSOCIADOS

- Política de Conduta Profissional;
- Política de Segurança da Informação;
- Política de Gestão da Continuidade dos Negócios;
- Código de Conduta Ética; e
- Regimento Comitê de Governança, Riscos e *Compliance*.

6. HISTÓRICO DAS REVISÕES

Revisão	Data	Descrição da Alteração	Elaborado / Revisado por:	Aprovador
-	-	Emissão da versão inicial da Política de Gestão de Riscos e Controles Internos.	-	-

7. DICIONÁRIO DE RISCOS

Categoria	Subcategoria	Descrição
Risco Operacional	Risco de Inadequação ao Sistema da Qualidade	Possibilidade de não aderência aos requisitos da ISO 9001:2015
	Risco de Falha Humana (Erro na execução, entrega ou gestão das atividades do negócio)	Possibilidade de perda associada às ações não intencionais de pessoas envolvidas em negócios da Unimed Teresina. Exemplos: - equívocos; - omissão; - distração; - negligência; - falta de qualificação profissional.

		POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS		Código: SUT.POL.GO.01.01
				Publicação: xx/xx/xxxx
Risco Operacional		Risco de Fraude Interna	Possibilidade de perda ocasionada por comportamento resultante de dolo ou má fé para auferir benefícios. Exemplos: - adulteração de controles; - descumprimento Intencional de normas da Unimed Teresina; - desvio de valores financeiros; - divulgação proposital de informações erradas.	
		Risco de Fraude Externa	Possibilidade de perda ocasionada por comportamento resultante de dolo ou má fé das contrapartes (segurados, clientes, corretores, fornecedores etc..) para auferir benefícios.	
		Risco de Fraude a Licitações Públicas e Contratos Administrativos	Possibilidade de perda financeira ou reputacional decorrente de: a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório; b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público; c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo; d) fraudar licitação pública ou contrato dela decorrente; e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo; f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou de prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.	
		Inadequação de Processos	Possibilidade de perda ocasionada por inadequação dos processos internos. Exemplos: - Falta de manutenção dos processos; - Falha na comunicação ou formalização dos processos da Unimed Teresina.	
		Risco de Indisponibilidade de Pessoal Especializado	Possibilidade de perda ocasionada por remoção ou perda inesperada de pessoa chave de uma posição ou responsabilidade sem substituto imediato.	
		Risco de Infraestrutura/Dano a Ativo Físico	Possibilidade de perda causada pela inadequação da: - estrutura física; - estrutura logística; - estrutura tecnológica; - estrutura de pessoal.	
		Interrupção do Negócio ou Falha de Sistemas	Possibilidade de perdas associadas às falhas em aspectos lógicos de tecnologia da informação.	

		POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS		Código: SUT.POL.GO.01.01
				Publicação: xx/xx/xxxx
	Risco de Segurança da Informação	Possibilidade de perda decorrente de: - quebra de confidencialidade das informações; - ausência de integridade das informações; - falha na autenticidade das informações; - ações criminosas com origem fora da empresa, por falhas na segurança dos sistemas.		
	Risco de Lavagem de Dinheiro	Possibilidade dos produtos comercializados pela Unimed Teresina serem utilizados para a transformação de recursos ganhos de forma ilegal em ativos com uma origem aparentemente legal.		
Risco Operacional	Risco de Eventos Externos ou Catástrofes	Possibilidade de perdas relacionadas à: - catástrofes naturais; - atentados; - vandalismos; - greves; - paralisações; - epidemias ou pandemias; - outros eventos independentes da vontade ou das condições da Unimed Teresina.		
	Risco de Não Conformidade	Possibilidade de perda ocasionada pela: - inobservância das normas e instruções internas; - violação das normas e instruções internas; - Interpretação indevida das normas e instruções internas; - inobservância, violação ou interpretação indevida das leis e normas externas, tais como comerciais, cíveis, tributárias, trabalhistas e as editadas pela ANS.		
	Risco de Corrupção de Agentes Públicos	Possibilidade de algum colaborador ou funcionário terceirizado da Unimed Teresina prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a terceira pessoa a ele relacionada.		
	Práticas Trabalhistas ou Segurança no Trabalho	Possibilidade de perda decorrente de decisões judiciais ou extrajudiciais desfavoráveis, por práticas incompatíveis com leis e/ou acordos referentes a relações trabalhistas.		
	Risco de Provento e/ou Qualidade	Possibilidade de perdas decorrentes de situações em que o prestador não entregue os serviços contratados ou entregue fora do prazo acordado ou ainda situações em que os serviços prestados não atinjam os requisitos de qualidade contratados e esperados.		
Risco Legal	Risco Contratual	Possibilidade de perda relacionada à: - inadequação formal do contrato; - interpretação de cláusulas contratuais; - não conformidade com a legislação pertinente.		
	Risco de Contencioso	Possibilidade de perda decorrente de decisões judiciais contrárias aos interesses da Unimed Teresina ou a possibilidade de um terceiro acionar a Cooperativa junto ao judiciário.		

		POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS		Código: SUT.POL.GO.01.01
				Publicação: xx/xx/xxxx
Risco de Crédito	Risco de Contraparte/ Inadimplência	Possibilidade de perda na falha da contraparte no cumprimento de obrigações contratuais ou degradação da qualidade de crédito.		
	Risco de Concentração	Possibilidade de perda decorrente da excessiva concentração em operações com contrapartes.		
Risco de Liquidez	Risco de Incapacidade de Pagamento	Possibilidade de perda decorrente da inexistência de recursos suficientes para o cumprimento, nas datas previstas, dos compromissos assumidos ou venda forçada de ativos a preços inferiores ao de mercado.		
	Risco de Descasamento	Possibilidade de perda decorrente de variações temporais nos fluxos de caixa de curto e longo prazo.		
Risco Estratégico	Risco de Conjuntura	Possibilidade de perda decorrente de movimentos externos a empresa, que possam causar perda de participação no mercado, em virtude de mudanças que tornam a empresa ou produto menos competitivo.		
	Risco de Planejamento	Possibilidade de perda decorrente de estratégias equivocadas.		
Risco de Subscrição	Risco de Aceitação e Precificação	Possibilidade de perda provocada pela aceitação inadequada ou falha no estabelecimento das tarifas aos riscos cobertos.		
	Risco de Provisões Técnicas	Possibilidade de perda provocada pela inadequação do cálculo das provisões técnicas.		
	Risco da Concorrência	Possibilidade de perda provocada por taxas mais competitivas praticadas por outras Operadoras.		
Risco de Mercado	Risco de Oscilação de Preços	Possibilidade de perda no valor da carteira em função de mudanças adversas nos preços, taxas de juros, de câmbio, índices e derivados.		
	Risco de Concentração de Investimentos	Possibilidade de agravamento das perdas no valor da carteira, causado pela não diversificação dos investimentos.		
Risco de Imagem / Risco Reputacional	Risco de Imagem / Risco Reputacional	Possibilidade de perdas decorrentes a danos na imagem e reputação da Unimed Teresina.		
Risco Ambiental	Agentes Físicos	Ruídos, vibrações, pressões anormais, temperaturas extremas, radiações etc.		
	Agentes Químicos	Poeiras, fumos, névoas, neblinas, gases, e/ou vapores que podem ser absorvidos por via respiratória ou através da pele etc.		
	Agentes Biológicos	Bactérias, fungos, bacilos, parasitas, protozoários, vírus, entre outros.		
	Acidentes	Arranjo físico inadequado, máquinas e equipamentos sem proteção, ferramentas inadequadas ou defeituosas, iluminação inapropriada, eletricidade e armazenamento inadequados, animais peçonhentos, entre outras situações de risco que poderão contribuir para a ocorrência de acidentes.		
	Ergonômicos	Esforço físico intenso, levantamento e transporte manual de peso, exigência de postura inadequada, controle rígido de produtividade, imposição de ritmos excessivos, jornadas de trabalho prolongadas, monotonia e repetitividade, além de outras situações causadoras de estresse físico e/ou psíquico.		