Atividade: Política de Gestão de Riscos e Controles Internos

Responsável: Gestor de Riscos e Controles Internos

Controle Histórico		
Revisão	**Data**	**Motivo / Alteração**
00	27/10/2020	Emissão inicial
00	27/10/2020	Aprovado por Diretoria Executiva

Siglas e Definições

Agente de Qualidade: 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 Gestão de Riscos e Controles Internos.

Auto Avaliação de Riscos e Controles (CSA – *Control Self Assesment*): consiste na avaliação, realizada pelos gestores responsáveis pelas áreas da Unimed Nordeste Paulista, com intuito de identificar os riscos e avaliar o ambiente de controles. A avaliação dos gestores é revisada pela Área de Gestão de Riscos e Controles Internos, por meio de técnicas como *walkthrough*, testes de aderência e/ou resultados de trabalhos sobre o ambiente de controles internos, como por exemplo, processos de fiscalização de Órgãos Reguladores, trabalhos das auditorias internas e externas, perdas operacionais, entre outros.

Cadeia de Valor: consiste na forma como as atividades, processos e negócios da Unimed Nordeste Paulista estão organizados, de modo a gerar valor às partes interessadas.

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

Categoria de Risco: é a classificação do grupo de riscos determinados no “Dicionário de Riscos” da Unimed Nordeste Paulista e também pode ser identificado como “Domínios de Risco”.

Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação: reunião que tem por objetivo garantir a transparência e a ética na Unimed Nordeste Paulista, zelando pela efetiva adoção das melhores práticas de Governança, assim como avaliar os riscos inerentes aos seus negócios, incluindo avaliação qualitativa e quantitativa, de forma a assegurar a boa gestão dos recursos, a proteção e a valorização do seu patrimônio. A estrutura, composição, competências e regras de funcionamento estão previstas no Regimento Interno do Comitê.

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 atividade. Esses controles mitigam diretamente o risco para uma elevada percentagem das transações ou valores processados.

Controle compensatório: controle não considerado chave, mas que na falha 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 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 de ambiente de controles (ausência de controle, ausência de evidência, ausência de política, deficiência no desenho, etc.).

Dicionário de riscos: documento corporativo utilizado pela Unimed Nordeste Paulista, também conhecido como "Domínios de Riscos", com o objetivo de padronizar em uma linguagem comum e definir conceitualmente os tipos de riscos mapeados.

Frequência: número de eventos ocorridos em um determinado período de tempo.

Impacto: é o volume do prejuízo/ganho financeiro, extensão do desgaste/conservação da imagem institucional da Unimed Nordeste Paulista, provocados por um determinado evento, demandas regulatórias e/ou dos objetivos estratégicos.

Indicador de risco: métrica baseada em aspectos quantitativos ou qualitativos. Medida ao longo do tempo que 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 generalistas sobre gestão de riscos. Possuí 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 Nordeste Paulista, que tem por objetivo apresentar o resultado da avaliação dos riscos identificados, mensurando critérios que auxiliarão no estabelecimento das prioridades com relação ao tratamento.

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

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 ou em um processo de *control self assessment* (CSA).

Política de Gestão de Riscos e Controles Internos: declaração das intenções e diretrizes gerais de uma organização, relacionadas ao gerenciamento dos riscos.

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.

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

Resposta ao Risco: decisão que será tomada após a identificação do risco original ou avaliação do ambiente de controle dos riscos residuais, com objetivo de promover discussões que assegurem a eficiência do ambiente de controles internos da Unimed Nordeste Paulista, podendo ser as seguintes: eliminar, transferir, mitigar e aceitar.

Risco negativo: medida da incerteza a respeito de um evento ao qual a Unimed Nordeste Paulista 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 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 Unimed Nordeste Paulista 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.

Materiais

Material de Escritório

Tarefas

1. OBJETIVO

Garantir que a política de Gestão de Riscos e Controles Internos da Unimed Nordeste Paulista esteja formalizada, atualizada e disponível para consulta de todos os colaboradores, de forma, que reconheçam suas funções e responsabilidades no processo. Assegurar que os controles internos sejam efetivos e consistentes com a natureza, complexidade e riscos das operações, bem como orientar os procedimentos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades, incorporando a visão de riscos à operação e tomada de decisões estratégicas, em conformidade com as melhores práticas de mercado.

2. APLICAÇÃO

As disposições desta “Política” se aplicam a Unimed Nordeste Paulista e também os serviços terceirizados com impacto direto na operação.

3. DESCRIÇÃO DAS DIRETRIZES E REGRAS

3.1 Papeis e responsabilidade

As responsabilidades no modelo de Gestão de Riscos e Controles Internos da Unimed Nordeste Paulista, 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 Gestão de Riscos e Controles, ocorre na 2ª linha de defesa, de maneira independente, mas não de forma isolada das áreas gestoras, conforme demonstrado:

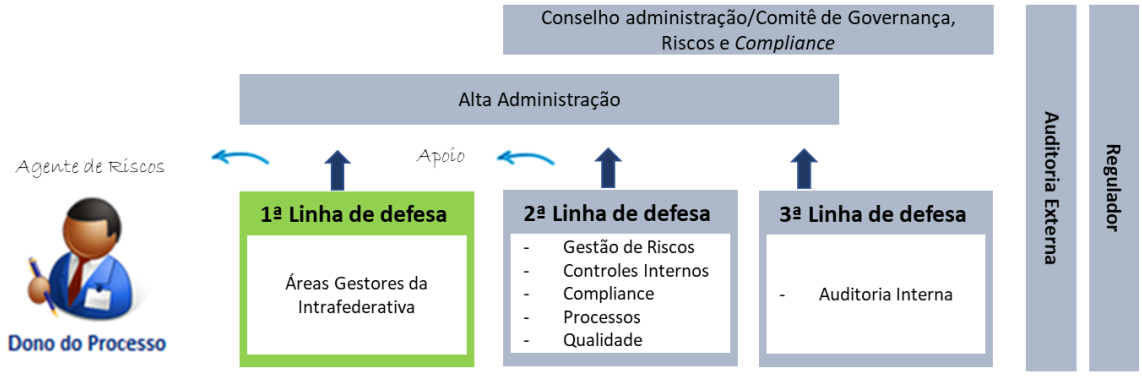


Figura 1 - Estrutura de camadas e níveis de reporte

1ª linha de defesa: responsável pelo gerenciamento, monitoramento e ações de respostas aos riscos, sendo a área responsável pelos processos/atividades, riscos 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 alta administração da organização e órgãos de governança, 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.

O processo de mapeamento de riscos e controles internos está alinhado as diretrizes e valores éticos definidos pelo Código de Conduta Ética, fazendo parte do Programa de Integridade da Unimed Nordeste Paulista.

3.2 Processo de Avaliação de Riscos e Controles Internos

O processo de Avaliação de Riscos e Controles Internos da Unimed Nordeste Paulista tem como base os componentes e princípios do COSO e ISO 31000:2018, que tem como objetivo propiciar uma gestão integrada e eficaz, em linha com as melhores práticas utilizadas no mercado nacional e internacional, para a proposição e implementação do modelo corporativo de gestão de riscos e controles internos.

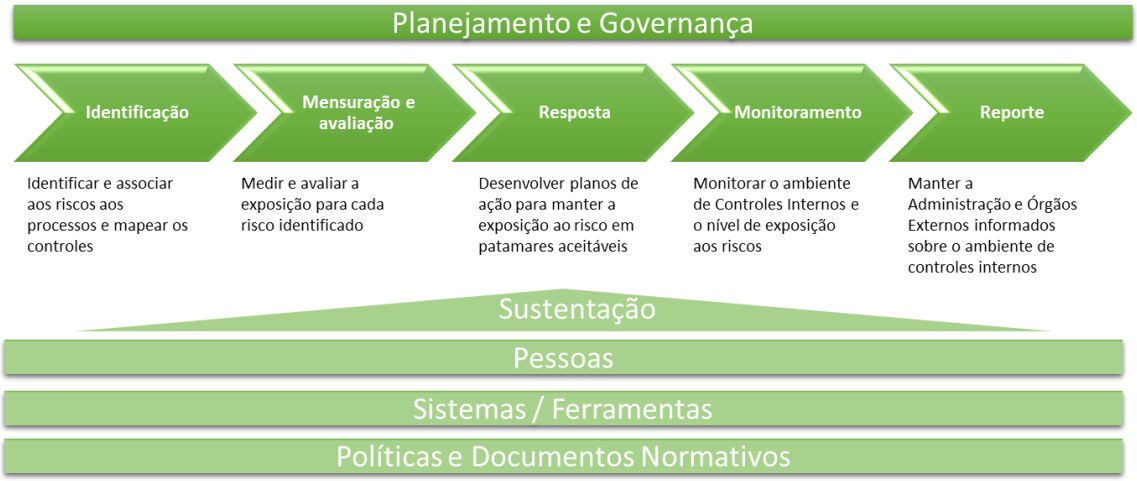


Figura 2 – Processo de Gestão de Riscos

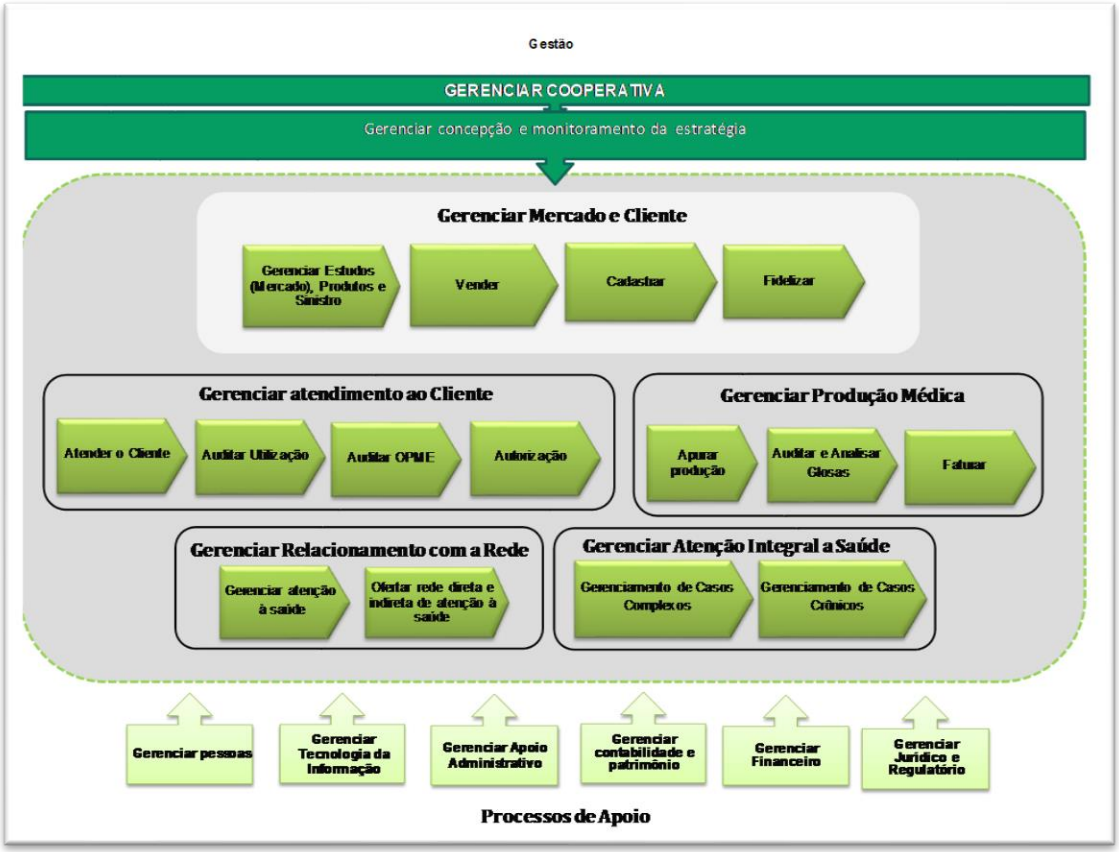
Destacamos a seguir as principais etapas do processo.

3.3 Mapeamento dos Processos

O mapeamento possibilita uma visão detalhada dos processos e atividades da Unimed Nordeste Paulista, 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 chaves que atuam nos processos do negócio.

Os principais objetivos do mapeamento de processos estão relacionados a entender as atividades de negócio, suporte ou gestão, considerando o escopo definido, identificar os eventos e fatores de risco, bem como os controles do processo ou atividade crítica. A etapa de mapeamento de processos é fundamental para o funcionamento dos controles internos, uma vez que constitui a fase de entendimento sobre o ambiente de negócios e estrutura de controles.

Os processos de negócio, apoio e gestão da Unimed Nordeste Paulista estão documentados na Cadeia de Valor, conforme descrito abaixo:



3.4 Identificação dos Riscos

Uma vez mapeados os processos e atividades, é preciso identificar quais são os eventos de riscos que podem afetar o alcance dos objetivos da Unimed Nordeste Paulista, bem como o ambiente de controles necessário para gerir estes eventos. Sendo assim, o principal objetivo é identificar os riscos dos processos/atividades, bem como seus respectivos fatores, impactos e probabilidades de ocorrência.

Caso o processo/atividade a ser avaliado não esteja mapeado e disponível na Cadeia de Valor da Unimed Nordeste Paulista, ele deve ser providenciado, possibilitando a identificação e associação dos riscos referente às atividades mapeadas.

Para auxiliar o levantamento dos riscos, a área de Gestão de Riscos e Controles Internos deve realizar o seguinte exercício:

• Por que o risco pode se materializar?

• O que pode causar a materialização do risco?

• Quais são os agentes causadores?

• O que ocorre caso o fator de risco se materialize?

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

• Risco de Crédito

• Risco de Liquidez

• Risco de Mercado

• Risco Estratégico

• Risco de Subscrição

• Risco de Imagem

• Risco Operacional

• Risco Legal

• Risco Ambiental

• Risco Assistencial

• Risco Civil

• Risco de Desabastecimento

• Risco Financeiro

• Risco Ocupacional

• Risco Sanitário

Finalizada a identificação dos riscos, a Área Gestão de Riscos e Controles Internos, deve garantir o correto monitoramento, atualização das matrizes de riscos.

3.5 Identificação dos Controles

Paralelamente ao mapeamento/identificação dos riscos, a Área de Gestão de Riscos e Controles Internos, deve identificar com apoio dos gestores os controles existentes na estrutura da Unimed Nordeste Paulista, os quais possuem o objetivo de mitigar a exposição aos riscos identificados.

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

3.6 Mensuração do Impacto e Probabilidade

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:

Impacto (gravidade), que significa o valor financeiro ou não, oriundo da materialização dos riscos negativos ou positivos, além de impactos reputacionais e nos objetivos estratégicos da Unimed Nordeste Paulista.

Tabelas de Mensuração de Impactos/Gravidade

IMPACTO/GRAVIDADE		
NÍVEL	CLASSIFICAÇÃO	DESCRIÇÃO
1	Leve	A falha quando ocorre gera danos leves e reversíveis. Exemplos: perda do prazo de entrega da lista de presença em treinamentos; falha atualização de cadastros.
2	Moderada	A falha quando ocorre gera danos moderados e reversíveis. Exemplos: danos gerados por erros no cadastro do beneficiário; avaliação incorreta da produção para faturamento; atraso na auditoria de contas.
3	Grave	A falha quando ocorre gera danos graves, não sendo completamente reversíveis podendo até mesmo ser fatais (óbito no caso de paciente; insolvência, no caso da organização). Exemplos: falha na avaliação dos riscos dos participantes do programa de gerenciamento de doenças crônicas; falha no gerenciamento da qualificação de rede; ausência/ falha na referência para assitência pré-hospitalar.

Os impactos (gravidade) também são classificados conforme o grau de comprometimento financeiro dos riscos, conforme a seguir:

1 – Leve: Comprometimento em nível operacional, sem gerar perdas financeiras à Operadora.

2 – Moderado: Comprometimento operacional que gerar prejuízos financeiros à operadora, como juros, multas por atraso ou descumprimento de contratos. O risco é considerado moderado se o impacto for igual ou inferior a R$ 50.000,00 (cinquenta mil reais).

3 – Grave: O impacto financeiro para classificação do risco como grave deve superar o montante de R$ 50.000,00 (cinquenta mil reais).

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.

PROBABILIDADE		
NÍVEL	CLASSIFICAÇÃO	DESCRIÇÃO
1	Baixa	A falha ocorre em baixa frequência. Se indicador: o desempenho está na meta ou melhor que a meta. Se observação: falha nunca ou raramente ocorre.
2	Média	A falha ocorre um pouco mais frequente. Se indicador: o desempenho está até 10% fora da meta (para o lado indesejado). Se observação: falha ocorre muito pouco.
3	Alta	A falha pode ocorrer de forma mais frequente. Se indicador: o desempenho está mais do que 10% pior que a meta desejada. Se observação: falha ocorre com frequência.

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

Matriz de Riscos

NÍVEL DE RISCO				
Gravidade x Probabilidade		GRAVIDADE		
		1	2	3
PROBABILIDADE	3	3	6	9
	2	2	4	6
	1	1	2	3

Área III (Vermelha) - são os riscos com alta significância. 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. Os riscos classificados nessa área devem ser monitorados de forma rotineira e sistemática, podendo exigir também a implementação das estratégias de proteção e prevenção (ação corretiva)

Área I (Verde) - são os riscos com baixa significância. Esses riscos somente devem ser gerenciados e administrados, pois estão com “exposição aceitável”.

3.7 Cálculo do Risco

O Risco leva em consideração as métricas de impacto/gravidade e probabilidade. O seu valor é resultado da multiplicação dessas duas variáveis:

Risco = Impacto x Probabilidade

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

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.

3.8 Resposta ao Risco

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 criação de controles e melhorias em processos ou atividades, 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 (exemplo: terceirização de atividades);

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 deve ser seguida e formalmente documentada, para assunção de Risco:

Alçada	Risco Residual		
	Baixo	Moderado	Alto
Coordenadores	X		
Diretoria		X	X

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

Preferencialmente, deve ser realizado em reuniões executivas como no Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação, onde a assunção será formalizada em atas de reunião com a aprovação do corpo diretivo.

Os riscos classificados como “baixo” são de natureza operacional e com possibilidade de correção/reversão dos danos.

3.9 Avaliação do Ambiente de Controle

Após mensurar o impacto e probabilidade dos riscos associados aos processos e atividades, as áreas deverão avaliar os controles mapeados para mitigação dos riscos, por meio da técnica CSA (*Control Self Assesment*). Após a autoavaliação dos controles pelas áreas, os mesmos serão avaliados pela área de Gestão de Riscos e Controles Internos, por meio de *walkthrough* ou teste de controle.

***Walkthrough* e Testes de Controles:** tem como objetivo avaliar a eficácia e eficiência dos controles existentes e associados aos riscos inerentes aos processos e atividades da Unimed Nordeste Paulista. A avaliação por meio do *walkthrough* e testes de controles é um mecanismo que assegura a existência e revisão periódica dos processos, riscos e controles da Unimed Nordeste Paulista, e deverá ser executada de acordo com o impacto do risco, conforme tabela abaixo:

	CLASSIFICAÇÃO DO RISCO RESIDUAL		
	Baixo	**Médio**	**Alto**
Tipo de Avaliação	*Walkthrough*	*Walkthrough*	Teste de Controle

Walkthrough: 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 fluxo de transações;
- Validar a eficácia do desenho de controles identificados;
- Confirmar se os controles estão em operação;
- Revisar os riscos dos processos/atividades 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 do *walkthrough*, os resultados devem ser armazenados, com o preenchimento das etapas realizadas, evidências geradas e conclusão do *walkthrough* (resultado efetivo ou inefetivo).

Nota: Para os controles considerados inefetivos, a Área de Gestão de Riscos e Controles Internos, deverá registrar as deficiências de controles (*gaps*) conjuntamente com o plano de ação estabelecido com a área responsável. Os reportes de monitoramento dos planos de ação, devem ser mensais e de forma consolidada reportada no Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação.

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;
- Revisar se os desvios estão suportados por controles compensatórios.

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

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

Indagação: entrevistas detalhadas para obtenção de evidências quanto à eficácia dos controles. Esta técnica deve ser realizada, obrigatoriamente, em conjunto com outras técnicas 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, não fornece evidência suficiente para concluir sobre a eficácia 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: obtenção de evidências quanto à eficácia do controle por meio de análise da documentação. O grau de segurança que se obtém com esta técnica é considerado alto para a grande maioria dos controles, porém pode haver a necessidade de ser complementado com outro tipo de técnica.

Por fim, da mesma maneira que no *walkthrough*, a Área de Gestão de Riscos e Controles Internos deverá registrar as deficiências de controles (*gaps*) conjuntamente com o plano de ação estabelecido com a área responsável. Os reportes de monitoramento dos planos de ação, devem ser mensais e de forma consolidada reportada no Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação.

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

Quality Assurance: Caso o processo de *walkthrough* seja realizado por agentes de qualidade, será necessário avaliar os resultados alcançados, de modo a assegurar que o padrão de qualidade de execução seja cumprido pelas equipes designadas. 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;

- Verificar a existência de evidências que suportam os resultados alcançados.

3.10 Efetividade do Controle

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 materialização

do risco, histórico de falhas, apontamentos de fiscalização, auditorias, etc. Apresentamos a seguir os conceitos a serem considerados para auxiliar a avaliação:

Tabela de 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, procedimentos formalizados.	Os controles internos não foram definidos e aplicados, elevando a classificação do risco, por conta de sua exposição.

3.11 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 o prazo para implementação e o seu responsável.

Para os controles associados aos riscos residuais “moderados” e “altos”, testados e considerados inexistentes ou inefetivos, a necessidade de planos de ação e controles compensatórios se torna obrigatória, visando a diminuição da possível materialização do risco, assim como 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:

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

3.11.1 Monitoramento dos Planos de Ação

O acompanhamento da implementação dos planos de ação deve ser realizado pela Área de Gestão de Riscos e Controles Internos, que reportará mensalmente aos coordenadores das áreas os planos de ação, seus responsáveis e status. Desta forma, a área responsável deverá atualizar as informações e retornar para Gestão de Riscos e Controles.

Caso a conclusão do plano de ação, ocorra antes do previsto, à área responsável deve notificar Gestão de Riscos e Controles Internos.

4. Registro e Reporte

A etapa de reporte contempla a responsabilidade da Área Gestão de Riscos e Controles Internos em relação ao reporte do processo de Avaliação de Riscos e Controles à Alta Administração da Unimed Nordeste Paulista.

O reporte da avaliação de riscos e controles deverá ser realizado para os Coordenadores 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;
- Opinião conclusiva sobre o ambiente de controles internos.

A Área de Governança, Riscos e *Compliance* deverá elaborar o relatório de Gestão de Riscos e Avaliação do Ambiente de Controles Internos, destacando em especial quanto a(o):

- Desenvolvimento e precificação de produtos;
- Comercialização e/ou disponibilização de seus produtos;
- Recebimento, processamento e pagamento de Eventos ou Sinistros, incluindo sua regulação;
- Contratação de outras operadoras, seguradoras ou resseguradoras como formas de mitigação riscos de suas atividades;
- Investimentos;
- Gestão de fluxos de recebimento e pagamento da operadora;
- Cálculo de provisões técnicas e Teste de Adequação do Passivo (TAP), conforme as premiss estabelecidas pela ANS;
- Acompanhamento de processos judiciais e suas estimativas de valores a partir de histórico perdas;
- Transações com partes relacionadas e adiantamentos;
- Relacionamento com prestadores e outros fornecedores;
- Gestão de Tecnologia da Informação;
- Gestão da continuidade dos contratos.

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 é o fórum competente para reporte e acompanhamento das disposições previstas neste documento.

Esta política entrará em vigor na data de sua aprovação.

Registros

Não se aplica.

Anexos

MAN.CPD.001 - Código de Conduta Ética; e
Política de Gestão da Continuidade dos Negócios

Dicionário de Riscos

Categoria	Sub-Categoria	Descrição
Risco Operacional	Risco de Inadequação ao Sistema da Qualidade	Possibilidade de não aderência aos requisitos da ISO 9001:2015
	Risco de Falha Humana (Falha na execução, entrega ou gestão das atividades do negócio)	Possibilidade de perda associada a ações não intencionais de pessoas envolvidas em negócios da Unimed Nordeste Paulista Nordeste Paulista. Exemplos: - equívocos; - omissão; - distração; - negligência; - falta de qualificação profissional.
	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 Nordeste Paulista; - 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 (clientes, corretores, fornecedores, etc..) para auferir benefícios.

	Risco de Fraude a Licitações Públicas e Contratos Administrativos	Possibilidade de perda, financeira ou reputacional, a decorrente de: a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório; b) impedir, pertubar 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 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 Companhia.
	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 Infra-Estrutura/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.

	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 Nordeste Paulista serem utilizados para a transformação de recursos ganhos de forma ilegal em ativos com uma origem aparentemente legal.
	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 Nordeste Paulista.
	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 SUSEP, ANS, PREVIC e CVM.
	Risco de Corrupção de Agentes Públicos	Possibilidade de algum colaborador ou terceirizado da Companhia 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 Terceirização	Risco de provimento 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 Nordeste Paulista ou a possibilidade de um terceiro acionar a Unimed Nordeste Paulista junto ao judiciário.
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 Cias Seguradoras.
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, taxas de câmbio, índices e derivativos.
	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 Companhia.
Risco Ambiental	Agentes Físicos	Ruídos, vibrações, pressões anormais, temperaturas extremas, radiações, etc.
	Agentes Químicos	Poeiras, fumos, névoas, neblinas, gases, 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 inadequada, eletricidade, armazenamento inadequado, 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 stress físico e/ou psíquico.
Risco Assistencial	Assistencial	Probabilidade de ocorrência de um evento adversos infeccioso e/ou não infeccioso em um paciente.
Risco Civil	Cível	Probabilidade de ato ilícito ou omissão, causar agravo a terceiros e/ou suas propriedades que, estabelecido culpa, dano e nexo causal, se traduz na obrigação de reparação indenizatória.

Risco de Desabastecimento	Desabastecimento	Probabilidade de faltar insumos, equipamentos e outros meios necessários a realização e/ou entrega do serviço.
Risco Financeiro	Financeiro	Custo, Despesas, perda de receita que possam afetar a saúde financeira do negócio,
Risco Ocupacional	Ocupacional	Probabilidade de agravo à saúde humana advindo de atividade laboral (ourelacionados ao trajeto), tanto sendo de origem, biológica, química, física, ergonômica, como de condição ou ato inseguro.
Risco Sanitário	Sanitário	Probabilidade que tem uma atividade, serviço ou substância, de produzir efeitos nocivos ou prejudiciais na saúde humana de maneira coletiva.

Referências Bibliográficas

Não se aplica.