Sumário

1. OBJETIVO

Estabelecer um conjunto de princípios, diretrizes, papéis e responsabilidades relacionados às práticas de Gestão de Riscos adotados pela Unimed Fesp, considerando aspectos como:

- Transmitir conhecimento entre todos colaboradores quanto aos principais riscos das suas atividades em especial aqueles relacionados aos riscos de subscrição, de crédito, de mercado, legais e operacionais.
- Alinhamento do Apetite ao Risco, definido pela empresa, com seu planejamento e estratégia de negócios, a fim de auxiliá-los no processo de decisão.
- Incorporação de uma abordagem consistente, integrada e abrangente para o Gerenciamento de Riscos, considerando o papel de todos os colaboradores.
- Estabelecimento de instrumentos para identificação, avaliação, medição, tratamentos de ocorrência e respostas, bem como a comunicação dos riscos, relacionados as 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.

2. ABRANGÊNCIA

Todos os administradores (Diretores Estatutários, Membros do Conselho de Administração, Conselho Fiscal, Comitês de assessoramento do Conselho de Administração) e colaboradores da Unimed Fesp, Fespart Participações S.A e empresas sócias e coligadas, bem como, por todos os seus respectivos administradores, colaboradores e prepostos a eles vinculados.

3. CONCEITOS E SIGLAS

ANS – Agência Nacional de Saúde

Agente de Compliance - Colaborador interno designado para apoiar as áreas operacionais no gerenciamento dos riscos relacionados à execução das atividades cotidianas, servindo como suporte e facilitador da estrutura de GRC.

Auto Avaliação de Riscos e Controles (CSA – Control Self Assesment) - Consiste na avaliação semestral, realizada pelos gestores responsáveis pelas áreas da Unimed Fesp e empresas ligadas e/ou controlas por esta, 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 por exemplo, processos de fiscalização de Órgãos Reguladores, trabalhos das auditorias internas e externas, perdas catalogadas na base de dados de perdas operacionais entre outros.

Cadeia de Valor - Consiste na forma como as atividades, processos e negócios da Unimed Fesp e empresas ligadas e/ou controlas por esta estão organizados, de modo a gerar valor às partes interessadas, como acionistas, fornecedores, colaboradores, órgãos reguladores e consumidor final.

Categoria de Risco - É a classificação do grupo de riscos determinados no “Dicionário de Riscos” da Unimed Fesp e empresas ligadas e/ou controlas por esta.

Comitê de GRC - órgão externo que atua como consultivo em torno dos assuntos relacionados à Governança, Riscos e Compliance, podendo englobar temas como controles internos, processos e similares, se necessário.

Dicionário de riscos - Documento corporativo utilizado pela a Unimed Fesp e empresas ligadas e/ou controladas por esta, 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.

Formulário de Risco Assumido: Documento corporativo utilizado pela a Unimed Fesp e empresas ligadas e/ou controladas por esta, com objetivo de formalizar o aceite do risco classificado como Alto

GRC – estrutura que compõe, mas não se limite a Governança, Risco e Compliance, tendo ainda como setor interno Qualidade & Controles internos.

Impacto - É o volume do prejuízo/ganho financeiro, com base no patrimônio líquido da Unimed Fesp e empresas ligadas e/ou controlas por esta, extensão do desgaste/conservação da imagem institucional da Unimed Fesp e empresas ligadas e/ou controlas por esta, provocados por um determinado evento, descumprimento de demandas regulatórias e/ou não atendimento 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 genéricas 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.

Matriz de Riscos - Demonstração gráfica dos riscos associados às atividades da Unimed Fesp e empresas ligadas e/ou controlas por esta, que tem por objetivo apresentar o resultado da avaliação dos riscos identificados, mensurando critérios que auxiliarão no estabelecimento das prioridades com relação ao tratamento.

Núcleo de GRC - Reunião que tem por objetivo garantir a transparência e a ética, 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 Núcleo.

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.

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.

Política de Gestão de Riscos - Declaração das intenções e diretrizes gerais de uma organização, relacionadas à gestão de riscos.

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 Fesp e empresas ligadas e/ou controlas por esta.

RN 443 - Resolução Normativa da ANS divulgada em 2019 e, que dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de planos de assistência à saúde.

Risco negativo - 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 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 empresa 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.

Sistema de Gestão de Riscos - Software que sustenta o gerenciamento de riscos e controles da Unimed Fesp e empresas ligadas e/ou controlas por esta, auxiliando na identificação e monitoramento dos riscos, avaliação do ambiente de controle, deficiências e planos de ação.

4. DIRETRIZES

O processo de Avaliação de Riscos e Controles da empresa tem como base os componentes e princípios do COSO, ISO 31000:2018 e RN 443, bem como suas respectivas alterações, 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. Destacamos a seguir as principais etapas do processo:

- Mapeamento dos processos;
- Escopo;
- Contexto interno e externo;
- Identificação dos riscos;
- Gerenciamento dos Riscos Estratégicos;
- Identificação dos controles;
- Identificação das deficiências;
- Autoavaliação de riscos e controles, pelos gestores;
- Mensuração do impacto e probabilidade;
- Classificação do risco;
- Resposta ao risco;
- Monitoramento e avaliação do ambiente de controles;
- Registro e reporte;
- Análise crítica.

4.1 Identificação dos Riscos

Uma vez mapeados os processos e subprocessos, é preciso identificar quais são os eventos de riscos que podem afetar o alcance dos objetivos da Unimed Fesp e empresas ligadas e/ou controlas por esta, bem como o ambiente de controles necessário para gerir estes eventos. Sendo assim, o principal objetivo dessa atividade é identificar os riscos dos processos, bem como seus respectivos fatores, impactos e probabilidades de ocorrência.

Caso o subprocesso a ser avaliado não esteja mapeado e disponível na Cadeia de Valor da Unimed Fesp e empresas ligadas e/ou controlas por esta, caberá a estrutura de GRC executar suas atividades sem esta documentação, possibilitando a realização de seus trabalhos. Neste caso, devem alertar a área de Qualidade & Controles Internos, para que possa apoiar a respectiva área no mapeamento do subprocesso, possibilitando a

associação dos riscos e fatores de risco às atividades e, posteriormente, realizar o mapeamento do subprocesso, conforme o padrão adotado pela empresa.

Para auxiliar o levantamento dos riscos e fatores de riscos, a estrutura de GRC deve-se 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 fatores de riscos, seus impactos e probabilidades de ocorrência, estes devem ser classificados de acordo com o Dicionário de Riscos da Unimed Fesp e empresas ligadas e/ou controlas por esta, o qual está dividido de acordo com os grupos abaixo e disposto no Anexo I desta Política.

- Risco de Subscrição;
- Risco de Crédito e Mercado;
- Risco Legal e Operacional;
- Risco Estratégico;
- Risco de Imagem;
- Risco Ambiental.

Finalizada a identificação dos riscos, a estrutura de GRC deve ser responsável por associá-los aos processos e cadastrá-los no sistema de Gestão de Riscos, alimentando ainda a matriz de riscos e controles.

4.2 Gerenciamento de Risco Estratégico

Após análise dos ambientes interno e externo, durante os ciclos de elaboração e revisão da estratégia, define-se os objetivos estratégicos. O alcance desses objetivos deve ser suportado por ações e projetos, os quais estão vinculados a cada objetivo do mapa estratégico da empresa.

As ações representam iniciativa da empresa que não são consideradas projetos, pois caso o fossem deveriam ser submetidas e monitoradas, mensalmente, durante as reuniões do Grupo Executivo - GE.

Os projetos que possuem maior complexidade em relação à sua execução e dependem de ações multidisciplinares, são coordenadas pelo Escritório de Projetos da empresa e reportadas, mensalmente, durante as reuniões do Grupo Executivo.

A gestão dos riscos estratégicos (positivos e negativos) é realizada por meio de reuniões mensais, entre as áreas da estrutura de GRC e o Escritório de Projetos, mantendo o foco nos projetos considerados prioritários, de acordo com critérios estabelecidos e aprovados junto à Diretoria Executiva da empresa e projetos voltados para a cobertura dos riscos mais relevantes aos quais a empresa estão expostas.

4.3 Mensuração de 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:

O impacto causado pela materialização de um risco pode ou não significar o valor financeiro, oriundo da materialização dos riscos negativos ou positivos, conforme tabela abaixo.

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.

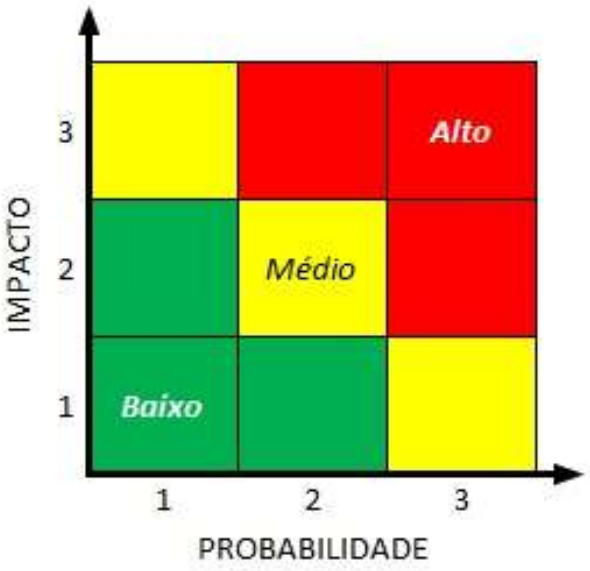
Obs.: A definição de impacto para os processos das camadas de apoio e gestão da cadeia de valor da empresa será a mesma adotada para a Unimed Fesp e CNU.

A probabilidade de ocorrência de um determinado evento de risco ocorre, quando se considera o contexto e a frequência de execução da atividade na qual está inserido.

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, monitoramento do subprocesso por meio de indicadores, relatos de não conformidade e 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, monitoramento do subprocesso por meio de indicadores, histórico de ocorrências, relatos de não conformidade e 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, monitoramento por meio de indicadores, histórico de ocorrências, relatos de não conformidade e relatórios gerenciais.

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

4.3.1. Matriz de Risco



Área III (Vermelha) - são os riscos com alta significância, podendo ser: com probabilidade frequente de ocorrência e com impacto alto, com probabilidade frequente e com impacto moderado ou com probabilidade eventual 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 ser: com probabilidade frequente de ocorrência e baixo impacto, com probabilidade eventual de ocorrência e impacto moderado ou com 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 ser: com probabilidade rara de ocorrência e baixo impacto, com probabilidade eventual de ocorrência e baixo impacto ou com probabilidade rara de ocorrência e impacto moderado. Esses riscos somente devem ser gerenciados e administrados, pois estão com “exposição aceitável”.

4.4 Cálculo do Risco

A tabela abaixo apresenta a pontuação e resultado obtido no cálculo do risco, a partir da metodologia do item acima voltado para matriz de risco.

SIGNIFICÂNCIA DO RISCO
Alto – 6 ou 9
Médio – 3 ou 5
Irrelevante – 1 ou 2

Obs.: 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.

4.5 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 subprocessos, por meio da formulação e implementação de planos de ação;

Transferir: Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma parcela de riscos (exemplos: resseguro e 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 no sistema de Gestão de Riscos, para assunção de Risco:

Alçada	Risco Residual		
	Baixo	Moderado	Alto
Gerência	X	X	
Superintendência e Diretoria			X

Obs.: A assunção dos riscos classificados como “Alto” somente poderá ser feita pela Diretoria Executiva. No entanto, os mesmo deverão ser reportado, previamente, na reunião

de superintendentes, para conhecimento e avaliação, se a decisão for em aceitar o risco, o responsável deverá preencher e assinar o formulário de risco assumido

4.6 Avaliação do Ambiente de Controle

Após mensurar o impacto e probabilidade dos riscos associados ao subprocesso, as áreas deverão avaliar os controles mapeados para mitigação dos riscos, por meio da técnica CSA (Auto Avaliação de Controles - Control Self Assesment).

Após a autoavaliação dos controles incorporado junto as áreas, este devem avaliados pela estrutura de Governança, Riscos e Compliance através da área da Qualidade por meio de walkthrough ou teste de controle.

Além dos itens estabelecidos nesta Política relacionado aos controles internos, também deve ser considerado parte integrante desta, a Política de Controles Internos

4.6.1. Walkthrough e Testes de Controles

Atividades sob responsabilidade da estrutura de Governança, Riscos e Compliance, podendo ser executada por agentes de conformidade. Tem como objetivo avaliar a eficácia e eficiência dos controles existentes e associados aos riscos inerentes aos processos e subprocessos da empresa. 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 empresa, 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 subprocesso e considera a avaliação do desenho dos controles para mitigação dos riscos, com o objetivo de:

- Confirmar o entendimento sobre o subprocesso e fluxo de transações;
- Validar a eficácia do desenho de controles identificados;
- Confirmar se os controles estão em operação;

- Revisar os riscos dos subprocessos 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 registrados no sistema de Gestão de Riscos, com o preenchimento das atividades realizadas, evidências geradas e conclusão do walkthrough (resultado efetivo ou inefetivo).

Obs.: Para os controles considerados inefetivos, a estrutura de Governança, Riscos e Compliance deve registrar as deficiências de controles (gaps), abrindo o registro de deficiências no sistema de Gestão de Riscos, para que as áreas envolvidas 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;
- 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.

Reperformance: consiste na reexecução independente do controle. O resultado confere alta segurança quanto à efetividade do controle para a amostra selecionada. Esta 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) no sistema de Gestão de Riscos e direcioná-los às áreas internas para elaboração de planos de ação que mitiguem as deficiências apontadas.

Obs.: Esta 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 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.

5. PAPÉIS E RESPONSABILIDADES

As responsabilidades no modelo de Gestão de Riscos, Controles Internos e Compliance da Unimed Fesp e empresas ligadas e/ou controlas por esta 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 estrutura de GRC ocorre na 2ª linha de defesa, de maneira independente, mas não de forma isolada das áreas gestoras.

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

- É representada por todos os gestores das áreas de negócio e suporte, os quais devem assegurar a efetiva gestão de riscos dentro do escopo das suas responsabilidades organizacionais diretas.
- Gerir os riscos e controles dos processos de sua atribuição e das atividades terceirizadas relevantes sob sua coordenação, por meio de abordagens preventivas e detectivas.
- Implementar ações para mitigação e/ou monitoramento dos riscos.
- Comunicar prontamente a estrutura de Governança, Riscos e Compliance sempre que identificar riscos potenciais não previstos no desenvolvimento das atividades de controle ou alterações em relação às normas e regulamentações vigentes.
- Avaliar as normas externas e internas e verificar o impacto que estas podem ter nos seus processos e procedimentos e a necessidade de planos de ação para garantir sua aderência.
- Definir e implantar os planos de ação para endereçamento dos apontamentos efetuados pelas Auditorias, Reguladores, Riscos e Compliance.

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.

- É responsável pelo apoio à 1° linha de defesa no gerenciamento dos riscos corporativos e é representada pela estrutura de Governança, Riscos e Compliance - estrutura com

atuação consultiva junto às áreas executivas, porém com avaliação e reporte independentes sobre o gerenciamento dos riscos e ambiente de controle da empresa.

- Coordenar as atividades de Gestão de Riscos e Controles Internos junto às áreas de negócio e suporte, sendo independente no exercício de suas funções.
- Desenvolver e disponibilizar as metodologias, ferramentas, sistemas, infraestrutura e governança necessários para suportar o gerenciamento de Riscos Corporativos e Controles Internos nas atividades da empresa.
- Apoiar a primeira linha de defesa na implementação de práticas eficazes de gestão dos riscos corporativos.
- Certificar a eficiência e a eficácia do ambiente de controle da primeira linha de defesa, através de monitoramento e testes de controles.
- Assegurar a governança dos temas de Gestão de Riscos e Controles Internos, por meio de reporte periódico nos fóruns competentes.
- Acompanhar o endereçamento dos apontamentos efetuados pelas Auditorias e Reguladores.
- Coordenar as atividades de gestão de crises e de elaboração e aplicação dos planos de continuidade de negócios.
- Atuar em conjunto com outras áreas de suporte da organização que, dentre suas atribuições, também possuem atividades de segunda linha de defesa, como: Prevenção a Fraudes, Segurança da Informação e Jurídico, dentre outras.

3ª linha de defesa: Responsável por fornecer, para alta administração da empresa 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.

- É representada pela Auditoria Interna, e tem como objetivo fornecer opiniões independentes à Alta Administração sobre o processo de gerenciamento de riscos, a efetividade dos controles internos e a governança corporativa.

Conselho de Administração

- Tomar ciência periodicamente as diretrizes, estratégias e políticas referentes ao gerenciamento de riscos da empresa.
- Assegurar a aderência da empresa às políticas e às estratégias de gerenciamento de riscos.
- Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos de forma independente, objetiva e efetiva.

Diretor-Presidente

Compete ao Diretor-Presidente, no âmbito das Políticas Institucionais de Governança, de Controles Internos e Gestão de Riscos:

- Assegurar a aplicação das diretrizes dessa Política;
- Assegurar que o processo de gerenciamento da estrutura de governança e dos controles internos e riscos corporativos irá identificar, mensurar, monitorar, controlar, mitigar e comunicar os riscos associados à empresa, às instâncias diretivas e aos órgãos reguladores;
- Atender ao órgão regulador, nos quesitos das recomendações e apontamentos que dispõem sobre governança, controles internos e os riscos corporativos.

Diretoria Executiva

Compete à Diretoria Colegiada, no âmbito das Políticas Institucionais de Governança, de Controles Internos e Gestão de Riscos e assegurar a aplicação das diretrizes das Políticas Institucionais da Unimed Fesp, além de:

- Deliberar sobre a revisão da política de gerenciamento de riscos e submeter à informação do Conselho de Administração - CA.
- Deliberar o nível de apetite ao risco na condução dos negócios.
- Deliberar a metodologia a ser utilizada para condução do processo de gerenciamento dos riscos corporativos.
- Autorizar, quando necessário, exceções às políticas e aos procedimentos.
- Promover a disseminação da cultura de gerenciamento de riscos na empresa.
- Acompanhar de forma periódica a gestão de riscos com o objetivo de garantir sua eficácia e o cumprimento de seus objetivos.

Colaboradores

Observar e zelar pelo cumprimento da presente Política, bem como das disposições do Código de Conduta e, quando assim se fizer necessário, acionar a Gestão de GRC para consulta sobre situações que conflitem com esta Política ou mediante a ocorrência de situações nela descritas.

Gestão de GRC

Monitorar o cumprimento das diretrizes estabelecidas nesta Política, mantê-la atualizada, refletir ao seu conteúdo quaisquer alterações no direcionamento da marca e suportar eventuais dúvidas relativas ao conteúdo e sua aplicação, assim como desenvolver o conteúdo e monitorar a realização do treinamento Anticorrupção.

Auditoria Interna

Aferir, de forma independente, as regras e os procedimentos estabelecidos nesta Política, mitigando os riscos quanto às gestões, aos controles e aos processos internos e apurar casos de denúncias e reportar à Diretoria Executiva e Núcleo de Ética.

Auditoria Externa

- Avaliar a qualidade e adequação do sistema de controles internos, inclusive sistemas de processamento eletrônico de dados e de gerenciamento de riscos.
- Reportar o descumprimento de dispositivos legais e regulamentares que tenham ou possam vir a ter reflexos relevantes nas demonstrações contábeis ou nas operações da empresa.

6 GESTÃO DE CONSEQUÊNCIAS

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

Internamente, o descumprimento das diretrizes desta Norma enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem conforme a respectiva gravidade do descumprimento.

7. REFERÊNCIAS

- Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000:2018 - Gestão de riscos - Princípios e diretrizes
- Associação Brasileira de Normas Técnicas. NBR ISO 31010:2012 - Gestão de riscos — Técnicas para o processo de avaliação de riscos.
- COSO-ERM - Committee of Sponsoring Organizations of Treadway Commission (“COSO ERM”)
- Resolução Normativa 443 da ANS, que dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de planos de assistência à saúde, e suas respectivas alterações.

8. DOCUMENTAÇÃO COMPLEMENTAR

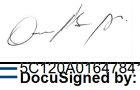
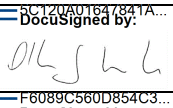
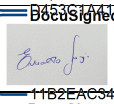
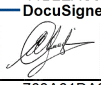
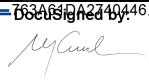
- Código de Conduta
- PLT Anticorrupção
- PLT Compliance
- PLT Controles Internos
- PLT Segurança da Informação
- Demais normas internas aprovadas pelas alçadas competentes e disponibilizadas a todos os colaboradores.

9. DISPOSIÇÕES GERAIS

É competência da Diretoria Executiva em conjunto com estrutura de GRC alterar esta Política sempre que se fizer necessário.

Esta Política entra em vigor na data de sua publicação e revoga quaisquer normas e procedimentos em contrário.

Identificação das Alterações		
Revisão	**Data da revisão**	**Alterações efetuadas**
00	16/11/2019	- Elaborado por Compliance e Gestão de Risco.

Áreas envolvidas	Validação	Data
Diretoria Executiva	Política aprovada em reunião pela Diretoria Executiva.	
Omar Abujamra Junior	DocuSigned by:  5C120A0164784 1A...	16/11/2019
Otto Cezar Barbosa Junior	DocuSigned by:  F6089C560D854C3...	16/11/2019
Reinaldo Antonio Monteiro Barbosa	DocuSigned by:  B453C1A41DA5465...	16/11/2019
Everaldo Gregio	DocuSigned by:  11B2EAC34FB94F1...	16/11/2019
Eduardo Ernesto Chinaglia	DocuSigned by:  763A61DA2740446...	16/11/2019
Marcos de Almeida Cunha	DocuSigned by:  59365A661A0D47A...	16/11/2019

ANEXOS

ANEXO I – DICIONÁRIO DE RISCOS

Dicionário de Riscos			
Tipo de Riscos	**ID**	**Categoria**	**Descrição**
Riscos Operacional	**R001**	Falha Humana	Falha na execução das atividades ocasionando retrabalhos
Risco Estratégico	**R073**	Terceirização	Não realizado de maneira consistente as regras da empresa
Risco Legal	**R087**	Corrupção/Fraudes	Atividades fraudulentas cometidas por empregados
Riscos de Mercado	**R025**	Publicidade inadequada	Pode causar mal entendido por parte dos clientes
Risco de Imagem	**R108**	Reputação	Exposição da Empresa a perda de consumidores e lucro
Risco de Crédito	**R106**	Variação Cambial	Volatilidade nas taxas de câmbio expõe a empresa a perdas
Risco de Subscrição	**R095**	Precificação	Falta de informação resultando em preços insatisfatório
Risco Ambiental	**R043**	Pandemia	Paralização das atividades pelo risco de contaminação

ANEXO II – FORMULÁRIOS DE RISCO ASSUMIDO

DADOS SOBRE O EMISSOR

Nome:	**Área:**	**Ramal:**
Cargo:	**Apoio:**	**Matrícula:**

Áreas Envolvidas:
Área responsável pela aceitação do Risco:

Este documento tem por objetivo reportar e documentar a aceitação de potenciais riscos que envolvem o ambiente de negócios – Risco Assumido

VISÃO GERAL SOBRE O RISCO

Classificação do Risco:
Risco:
Situação Atual:
Situação Proposta:

Comentários:

Responsável:	Data:	Aprovado por:	Data: