Siglas e Definições

AD HOC - termo jurídico em latim que significa a nomeação de alguém para realização de determinado ato.

ANS – Agência Nacional de Saúde.

Auto Avaliação de Riscos e Controles (CSA – Control Self Assesment) - Consiste na avaliação anual, realizada pelos gestores responsáveis pelas áreas da Unimed Andradas, com intuito de identificar os riscos e avaliar o ambiente de controles. A avaliação do Grupo Controles Internos é revisada pelo Comitê de GRC, por meio de técnicas testes de aderência e/ou resultados de trabalhos sobre o ambiente de controles internos.

Cadeia de Valor - Consiste na forma como as atividades, processos e negócios da Unimed Andradas estão organizados, de modo a gerar valor às partes interessadas, como cooperados, fornecedores, colaboradores, órgãos reguladores e consumidor final.

Categoria de Risco - É a classificação do grupo de riscos determinados no "Dicionário de Riscos" da Unimed Andradas.

Comitê de GRC – órgão interno que atua como consultivo em torno dos assuntos relacionados à Governança, Riscos e Controles Internos, podendo englobar temas como controles internos, processos e similares, se necessário. O Comitê de GRC se reunirá com o objetivo de 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 Comitê.

Dicionário de riscos - Documento corporativo utilizado pela Unimed Andradas , 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, com base no patrimônio líquido da Unimed Andradas, extensão do desgaste/conservação da imagem institucional da Unimed Andradas, 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 Andradas, 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 cooperados, 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 Andradas.

RN 518 - Resolução Normativa da ANS divulgada em 2022 e, que atualiza a RN 443/2019, a qual 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 Crítico – Risco Inaceitável, expõe a Unimed Andradas a danos severos com impactos de difícil correção, impossibilitando o alcance dos objetivos estratégicos.

Risco Alto – Risco inaceitável, expõe a Unimed Andradas a danos graves, dificultando o alcance dos objetivos estratégicos.

Risco Médio – Risco aceitável, pode expor a Unimed Andradas a danos graves, o que dificultaria o alcance dos objetivos do processo.

Risco Baixo – Risco aceitável, pode expor a Unimed Andradas a danos de menor relevância, no entanto, não deve dificultar o alcance dos objetivos do processo.

Risco Irrelevante – Risco irrelevante, muito embora existente, não expõe a Unimed Andradas a perdas significativas

Objetivo

Estabelecer um conjunto de princípios, diretrizes, papéis e responsabilidades relacionados às práticas de Gestão de Riscos adotados pela Unimed Andradas, 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.

Abrangência

Todos os administradores (Diretores, Membros do Conselho de Administração, Conselho Fiscal e do Conselho Técnico Ético) e colaboradores da Unimed Andradas.

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 518, 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.

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 Andradas, 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 Andradas, 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, 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 Andradas, o qual está dividido de acordo com os grupos abaixo:

- Risco de Subscrição;
- Risco de Crédito e Mercado;
- Risco Legal e Operacional;
- Risco Estratégico;

Finalizada a identificação dos riscos, a estrutura de GRC deve ser responsável por associá-los aos processos alimentando a matriz de riscos e controles.

1.1. 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.

Os projetos que possuem maior complexidade em relação à sua execução e dependem de ações multidisciplinares, são coordenadas pela Gerência Administrativa e reportadas, no mínimo semestralmente, durante as reuniões do Conselho de Administração.

A gestão dos riscos estratégicos (positivos e negativos) é realizada por meio de reuniões bimestrais no mínimo, entre as áreas da Comitê de GRC e a Gerência Administrativa, mantendo o foco nos projetos considerados prioritários, de acordo com critérios estabelecidos e aprovados junto ao Conselho de Administração da empresa e projetos voltados para a cobertura dos riscos mais relevantes aos quais a empresa estão expostas.

1.2. 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: Impacto x Probabilidade.

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	Muito Baixo	- Aumento no custo/prazo até 5%; - Impacto Financeiro até R$ 5.000,00; - Interferência no escopo/procedimentos insignificante; - Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).
2	Baixo	- Aumento no custo/prazo entre 6% e 10%; - Impacto Financeiro:Entre R$ 5.001 a R$ 10.000; - Interferência no escopo/procedimentos: Pouca (atrasos de algumas horas); - Pequeno impacto nos objetivos.
3	Médio	- Aumento no custo/prazo entre 11% e 15%; - Impacto financeiro entre R$ 10.001 a R$ 50.000; - Interferência no escopo/procedimentos relevante (interrupção temporária/atrasos de até 2 dias); - Moderado impacto nos objetivos, porém recuperável;
4	Alto	- Aumento no custo/prazo entre 16% e 20%; - Impacto Financeiro entre R$ 50.001 a R$ 100.000; - Interferência no escopo/procedimentos muito relevante (interrupção temporária/atrasos de até 1 semana); - Significativo impacto nos objetivos, de difícil reversão; - Prejudicial à imagem da Unimed Andradas.

5	Muito Alto	- Aumeto no custo/prazo acima de 20%; - Impacto Financeiro acima de R$ 100.000,00; - Interferência no escopo/procedimentos Grave (descontinuidade das atividades por tempo indeterminado); - Catastrófico impacto nos objetivos, de forma irreversível; - De descumprimento às Normas da ANS ou Legislação Brasileira; - Prejudicial à imagem da Unimed Andradas.

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. A escala utilizada considera a quantidade de vezes que o risco possa se materializar e/ou o percentual de ocorrências que possa acontecer em relação ao total das atividades ao qual a empresa está exposta.

PROBABILIDADE		
Métricas		**Descrição**
1	Muito Baixa	Evento: Extraordinário, sem histórico de ocorrência. Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade. Possibilidade de ocorrência 1 (até 10% de ocorrências).
2	Baixa	Evento Casual, sem históriooco de ocorrência. Probabilidade: Rara, de forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. Possibilidade de ocorrência até 2 (entre 11% e 25%);
3	Média	Tipo de Evento: Esperado, de pouca frequência, com histórico de ocorrência parcialmente conhecido; Probabilidade: Possível, de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade; Possibilidade de Ocorrência até 6 (entre 26% a 75%).
4	Alta	Tipo de Evento: Esperado, com histórico de ocorrência amplamente conhecido; Probabilidade: Provável, de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade; Possibilidade de Ocorrência até 12 (entre 76% e 90%).
5	Muito Alta	Tipo de Evento: Repetitivo e constante; Probabilidade: Praticamente certa, de forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade; Possibilidade de Ocorrência acima de 12 (acima de 90%).

1.2.1. Matriz de Risco

Matriz de classificação do risco							Avaliação Nível do risco
Matriz de classificação do risco		Impacto					
		1 Muito baixo	2 Baixo	3 Médio	4 Alto	5 Muito Alto	Nível do risco
Probabilidade	5 Muito Alto	5	10	15	20	25	Crítico (16 a 25)
	4 Alto	4	8	12	16	20	Alto (10 a 15)
	3 Médio	3	6	9	12	15	Médio (5 a 9)
	2 Baixo	2	4	6	8	10	Baixo (2 a 4)
	1 Muito baixo	1	2	3	4	5	Irrelevante (1')

Nível 5, Risco Crítico = Nível de risco inaceitável, expõe a Unimed Andradas a danos severos com impactos de difícil correção, impossibilitando o alcance dos objetivos estratégicos;

Nível 4, Risco Alto = Nível de risco inaceitável, expõe a Unimed Andradas a danos graves, dificultando o alcance dos objetivos estratégicos;

Nível 3, Risco Médio = Nível de risco aceitável, pode expor a Unimed Andradas a danos graves, o que dificultaria o alcance dos objetivos do processo;

Nível 2, Risco Baixo = Nível de risco aceitável, pode expor a Unimed Andradas a danos de menor relevância, no entanto, não deve dificultar o alcance dos objetivos do processo;

Nível 1, Risco Irrelevante = Nível de risco irrelevante, embora existente, não expõe a Unimed Andradas a perdas significativas.

1.3. 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
Crítico – 16 a 25
Alto – 10 a 15
Médio – 5 a 9
Baixo - 2 a 4
Irrelevante – 1

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.

1.4. TRATAMENTO DE RISCO

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

Evitar: Um risco normalmente é evitado quando é classificado como “Crítico” ou “Alto”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a Unimed Andradas.

Na Unimed Andradas, evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pela Diretoria e pelo Comitê de Gestão de Riscos e Controles Internos.

Mitigar: Um risco normalmente é mitigado quando é classificado como “Crítico" ou “Alto". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na Unimed Andradas, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.

Compartilhar: Um risco normalmente é compartilhado quando é classificado como "Crítico" ou "Alto, mas a implementação de controles não apresenta um custo/benefício adequado. Na Unimed Andradas, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.

Aceitar: Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o 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 relatório efetuado pelo GRC, bem como na Matriz de Riscos, para assunção de Risco:

Alçada	Risco Residual		
	Baixo	Moderado	Alto
Gerência/GRC	X	X	
CA/Diretoria			X

Obs.: A assunção dos riscos classificados como "Alto" somente poderá ser feita pela Diretoria Executiva. No entanto, os mesmos deverão ser reportados, previamente, na reunião do Comitê GRC, para conhecimento e avaliação, se a decisão for em aceitar o risco, o responsável deverá preencher e assinar o formulário de risco assumido.

1.5. AVALIAÇÃO DO AMBIENTE DE CONTROLE

Nível	Eficácia	% de falhas identificadas	Descrição	Multiplicador no Risco Inerente (*)
Inexistente	Ineficiente	Acima de 75%	Ausência de controle efetivo para mitigar o risco. Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais	1

Fraco	Frágil	51 a 75%	O desenho do controle necessita de melhorias para mitigar o risco. Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Compensatório	26 a 50%	Controle manual desenhado adequadamente para mitigar o risco. No entanto, deve ser avaliado tempestivamente pois pode apresentar falhas. Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Satisfatório	1 a 25%	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Eficaz	0	Controle sistêmico avaliado pela área GRC que mitiga o risco do processo. Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

(*) Corresponde ao Fator de Avaliação dos Controles Internos-FACI

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, 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.

2. PAPÉIS E RESPONSABILIDADES

As responsabilidades no modelo de Gestão de Riscos e Controles Internos da Unimed Andradas 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 Controles Internos 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 Controles Internos.

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 Controles Internos - 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 a 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 Gestão de Riscos e Controles Internos da Unimed Andradas, 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 Executiva, 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 Andradas, 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.

Comitê de Gestão de Riscos e Controles Internos – GRC

Compete ao Comitê de Gestão de Riscos e Controles Internos, desempenhar as atribuições descritas no âmbito do seu Regimento, seguindo a política de Gestão de Riscos, levando a conhecimento do Conselho de Administração os monitoramentos efetuados, conforme as seguintes atribuições:

- 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.

- Propor, com periodicidade mínima anual, recomendações ao Conselho de Administração sobre os assuntos de que trata a esta;
- Avaliar os níveis de apetite por riscos fixados nesta Política e as estratégias para o seu gerenciamento;
- Supervisionar a atuação e o desempenho do diretor indicado para gerenciamento de riscos;
- Supervisionar a observância, pela Diretoria, conforme a esta Política;
- Avaliar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas estabelecidas; e
- Manter registros de suas deliberações e decisões.

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.

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.

3. DOCUMENTAÇÃO COMPLEMENTAR

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

4. 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.

Referências

ABNT NBR ISO 31000:2018 - Gestão de riscos - Princípios e diretrizes;

NBR ISO 31010:2012 - Gestão de riscos — Técnicas para o processo de avaliação de riscos;

COSO-ERM - Committee of Sponsoring Organizations of Treadway Commission;

Resolução Normativa 518 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.

Indicadores de Efetividade

Não se aplica.

Fluxo

Não se aplica.