

ASSOCIAÇÃO DE ASSISTÊNCIA A SAÚDE DOS EMPREGADOS DA COPASA



Política de Gestão de Riscos

ÍNDICE

1. OBJETIVO	5
2. REFERÊNCIAS.....	5
3. RESPONSABILIDADES	5
3.1. Conselho de Gestão.....	5
3.2. Superintendência Executiva	6
3.3. Assessoria de Governança, Risco e Estratégia	6
3.4. Auditoria Interna	7
3.5. Colaboradores e Coordenadores/Assessores	8
4. DEFINIÇÕES	8
4.1. Apetite a riscos:	8
4.2. Cadeia de Valor:.....	8
4.3. Classificação do Risco:	9
4.4. Controle de Risco:.....	9
4.5. COSO - The Comitee of Sponsoring Organizations:	9
4.6. Efeito do Risco:	9
4.7. Evento de Risco:	9
4.8. Fator de Risco (Causas):.....	9
4.9. Gestão de Riscos:	9
4.10. Gerenciamento de Riscos:.....	10
4.11. Identificação de Eventos de Risco:	10
4.12. Impacto do Risco:.....	10
4.13. Incerteza:	10
4.14. Indicador de Risco:.....	10

4.15.	Key Risks Indicators (KRIs):.....	10
4.16.	Mapa de Risco:	10
4.17.	Materialidade:.....	11
4.18.	Matriz de Risco:	11
4.19.	Modelo das Três Linhas:	11
4.20.	Nível de Risco:	11
4.21.	Parâmetros de Medição de Riscos:.....	11
4.22.	Plano de ação:	11
4.23.	Probabilidade:	11
4.24.	Priorização dos Riscos:.....	12
4.25.	Resposta ao risco:.....	12
4.26.	Revisão dos Riscos:.....	12
4.27.	Risco:	12
4.28.	Risco Corporativo:.....	12
4.29.	Risco de Processo:	12
4.30.	Risco de Crédito:.....	12
4.31.	Risco de Gestão:.....	13
4.32.	Risco de Mercado:	13
4.33.	Risco de Subscrição:.....	13
4.34.	Risco Estratégico:	13
4.35.	Risco Inerente:	13
4.36.	Risco Legal:	13
4.37.	Risco Operacional:.....	14

4.38.	Risco Residual:	14
4.39.	Ritos de Monitoramento da Gestão de Riscos:	14
4.40.	Tratamento:.....	14
4.41.	Três linhas:.....	14
4.42.	Matriz R.A.C.I.:.....	14
5.	PRINCÍPIOS	15
5.1.	Declaração de Appetite a Riscos.....	15
5.2.	Adoção de boas práticas de governança corporativa.....	15
5.3.	Utilização de padrões e metodologias reconhecidos pelo mercado	15
5.4.	Envolvimento dos órgãos de governança.....	16
5.5.	Processo de tomada de decisão	16
5.6.	Estabelecimento e manutenção da infraestrutura necessária para a gestão integrada de riscos	16
5.7.	Integração da gestão de riscos aos processos organizacionais.....	16
5.8.	Análise periódica da gestão de riscos	16
5.9.	Adoção do modelo das Três Linhas	16
5.10.	Matriz R.A.C.I.....	17
6.	DIRETRIZES.....	18
6.1.	Identificação dos riscos	18
6.2.	Avaliação dos riscos.....	18
6.3.	Tratamento dos riscos	18
6.4.	Monitoramento dos riscos	19
6.5.	Comunicação dos riscos	19
7.	DISPOSIÇÕES FINAIS.....	20

1. OBJETIVO

Esta Política de Gestão de Riscos tem como objetivo estabelecer os princípios, diretrizes, conceitos e responsabilidades a serem constatados nos processos de gerenciamento de riscos e de controles internos no âmbito corporativo e de processo, de forma a possibilitar o planejamento, identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos e de controles internos, em conformidade com as regulamentações aplicáveis, como também a propagação da cultura e de boas práticas de governança.

2. REFERÊNCIAS

- COSO ERM 2017 (*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*).
- Modelo das Três Linhas do IIA 2020 – uma atualização das Três Linhas - Institute of Internal Auditors) (2020);
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;
- Norma ABNT ISO GUIA 73:2009 – Gestão de Riscos: Vocabulário;
- Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa – IBGC, 6ª edição, 2023;
- RN nº 518 de 2022, da ANS e suas alterações;
- Estatuto Social da Copass Saúde;
- Código de Conduta Ética da Copass Saúde.

3. RESPONSABILIDADES

3.1. Conselho de Gestão

- I. Avaliar e aprovar a Política de Gestão de Riscos;
- II. Acompanhar os resultados da implementação de controles e os indicadores provenientes da Gestão de Riscos por meio de relatórios gerenciais.

3.2. Superintendência Executiva

- I. Estabelecer diretrizes gerais e promover a integração das práticas de gestão de riscos e controles internos ao processo decisório;
- II. Garantir a execução das ações previstas na Política de Gestão de Riscos;
- III. Avaliar e aprovar a Matriz de riscos, bem como as diretrizes gerais para estabelecimento dos limites aceitáveis de exposição aos riscos (Apetite a Riscos).
- IV. Aprovar os Planos de Resposta aos Riscos com níveis de criticidade acima do limite do tolerável;
- V. Promover as condições necessárias para a implementação dos Planos de Resposta de todos os riscos corporativos e riscos de processo;
- VI. Recomendar para aprovação do Conselho de Gestão, os indicadores dos riscos classificados como críticos;
- VII. Ser responsável por identificar, monitorar e mitigar os riscos corporativos e riscos de processo;
- VIII. Compor equipe ou contratar terceiros responsáveis pela articulação das ações de Revisão dos Riscos, como organização de reuniões e dinâmicas, mediação das discussões e compilação das conclusões;
- IX. Participar e contribuir nos debates e validar as definições provenientes das etapas de Revisão dos Riscos;
- X. Incentivar a participação dos Colaboradores e do Conselho de Gestão nas etapas de Revisão dos Riscos.

3.3. Assessoria de Governança, Risco e Estratégia

- I. Incentivar a aplicação dos princípios e diretrizes desta Política, bem como a aderência quanto à eficácia da gestão de riscos e dos procedimentos de controles internos;

- II. Participar do processo de aplicação da metodologia para a definição dos riscos;
- III. Participar do fortalecimento da cultura no que se refere a gestão de riscos, garantindo a participação dos Colaboradores e do Conselho de Gestão nas etapas de Revisão dos Riscos;
- IV. Opinar sobre a definição dos indicadores e apetite aos riscos, submetendo-a à aprovação da Superintendência Executiva;
- V. Coordenar, de maneira contínua, a avaliação e monitoramento dos riscos corporativos e riscos de processo da Associação;
- VI. Realizar a análise dos riscos residuais, submetendo-a à aprovação da Superintendência Executiva;
- VII. Revisar a metodologia de avaliação de risco corporativo e de processo, submetendo-a à aprovação da Superintendência Executiva;
- VIII. Contribuir com os Coordenadores na elaboração e implementação dos Planos de Resposta aos Riscos;
- IX. Acompanhar a elaboração, implementação e a execução dos Planos de Resposta aos Riscos, e dar ciência à Superintendência Executiva e ao Conselho de Gestão;
- X. Supervisionar a implementação de controles e o acompanhamento dos indicadores provenientes da Gestão de Riscos por meio das diretrizes definidas nesta Política;
- XI. Coordenar o processo de elaboração de Planos de Continuidade dos Negócios ou de Planos de Contingência, quando necessário, relativos aos riscos corporativos e riscos de processo.

3.4. Auditoria Interna

- I. Prover o Conselho de Gestão e a Superintendência Executiva com avaliação e assessoria independentes, objetivas, imparciais e tempestivas sobre a adequação, eficácia da governança, do gerenciamento de riscos e controles

internos, para apoiar o atingimento dos objetivos organizacionais, promover e facilitar a melhoria contínua.

- II. Aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança e a confiabilidade do processo de coleta, mensuração, classificação, acumulação, registro e divulgação de eventos e transações;

3.5. Colaboradores e Coordenadores/Assessores

- I. Participar e contribuir nos debates das etapas de Revisão dos Riscos;
- II. Identificar e avaliar os riscos corporativos, de processos, de projetos e outros de sua responsabilidade;
- III. Definir, estruturar e monitorar os indicadores, implementando ações para o atingimento das metas estabelecidas;
- IV. Elaborar, implementar e monitorar os controles internos e o Planos de Resposta aos Riscos;
- V. Executar as ações de implementação de controles e o acompanhamento dos indicadores sob suas respectivas lideranças;
- VI. Reportar a evolução da implementação dos controles e o desempenho dos indicadores por meio de relatórios gerenciais.

4. DEFINIÇÕES

4.1. Appetite a riscos:

Níveis de exposição a riscos que a Copass Saúde está disposta a aceitar em busca de atingir os objetivos estratégicos e criar valor para as partes interessadas relevantes.

4.2. Cadeia de Valor:

É a representação do conjunto de processos realizados pela Copass Saúde, incluindo processos de suporte e de gestão e os suportes finalísticos (relacionados à entrega final de serviços pela organização).

4.3. Classificação do Risco:

É a etapa que trata da avaliação cada evento de risco com o objetivo de hierarquizá-los com relação a sua importância, o que permitirá o tratamento prioritário dos riscos mais críticos. Os riscos são classificados quanto à Probabilidade e Impacto.

4.4. Controle de Risco:

É qualquer medida que modifica o risco. Os controles incluem qualquer processo, política, dispositivo ou prática adotada que visa mitigar a probabilidade de um evento de risco ocorrer ou alterar o impacto decorrente de um risco. Os controles podem ser classificados como: preditivo, preventivo, corretivo e mitigatório.

4.5. COSO - The Committee of Sponsoring Organizations:

Organização privada, sem fins lucrativos, dedicada a estabelecer diretrizes visando proteger a organização dos riscos. Suas recomendações são consideradas um referencial para a implantação dos sistemas de controle interno das organizações, aumentando a confiabilidade dos relatórios financeiros, por meio da ética, efetividade dos controles internos e governança corporativa.

4.6. Efeito do Risco:

É o impacto ou consequência causados por um evento de risco. Pode ser notado como perdas financeiras, prejuízos de imagem ou credibilidade, entre outros.

4.7. Evento de Risco:

É um evento provável que gera alguma consequência ou perda aos objetivos da organização ou à execução de um processo.

4.8. Fator de Risco (Causas):

É a origem, causa-raiz ou gatilho que proporciona a ocorrência do evento de risco, quando não controladas efetivamente. Pode ser relacionado a um problema ou vulnerabilidade existente no processo.

4.9. Gestão de Riscos:

O conjunto de ações direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a

alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos.

4.10. Gerenciamento de Riscos:

Processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar, positiva ou negativamente, os objetivos, processos de trabalho e projetos nos níveis estratégico, tático e operacional.

4.11. Identificação de Eventos de Risco:

Corresponde ao conjunto de análises realizadas a fim de avaliar os eventos de risco existentes na organização. Esta etapa inclui a avaliação de riscos já identificados (determinando se ainda são riscos enfrentados pela organização) e análise para identificação de novos riscos, não considerados anteriormente.

4.12. Impacto do Risco:

É a mensuração do grau de criticidade de um risco caso ele aconteça. É a medida de relevância das consequências que ele gera. Podendo ser mensurado de forma qualitativa e/ou quantitativa.

4.13. Incerteza:

É o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

4.14. Indicador de Risco:

São demonstrações quantitativas e/ou qualitativas utilizadas para medir a ocorrência ou a proximidade de ocorrência de um determinado evento de risco. É a medição que, conjugada com a avaliação do contexto, é utilizada para avaliar como o risco se comporta e fornecer alertas quanto à exposição ou ao seu potencial de perda futura.

4.15. Key Risks Indicators (KRIs):

Indicadores que sinalizam possível exposição do risco monitorado e propiciam que as ações corretivas sejam realizadas de forma preventiva.

4.16. Mapa de Risco:

Ferramenta de registro e compilação dos Riscos da organização e das principais informações que os detalham, como fatores, efeitos, classificações, indicador e controles.

4.17. Materialidade:

Um risco é denominado material quando o apetite a riscos definido é alcançado ou superado.

4.18. Matriz de Risco:

Conjunto dos eventos de risco identificados pela empresa, descritos e classificados em pilares e categorias.

4.19. Modelo das Três Linhas:

Conjunto de princípios e diretrizes, elaborado e divulgado pelo IIA Global, The Institute of Internal Auditors, que visa esclarecer e organizar as responsabilidades e papéis dos profissionais da organização no gerenciamento de riscos e controles.

4.20. Nível de Risco:

É o valor numérico que representa a criticidade de um risco. É composto pela combinação dos valores de Probabilidade e Impacto.

4.21. Parâmetros de Medição de Riscos:

As informações quantitativas ou qualitativas, obtidas direta ou indiretamente, que permitam avaliar as dimensões dos riscos identificados a partir da probabilidade de sua ocorrência e das consequências possíveis.

4.22. Plano de ação:

Conjunto de atividades necessárias para assegurar as respostas aos riscos, após a definição do tratamento a ser dado. Possuem início e fim definidos.

4.23. Probabilidade:

É a chance de algo acontecer, não importando se definida, medida, determinada, objetiva ou subjetivamente, qualitativa ou quantitativamente.

4.24. Priorização dos Riscos:

Corresponde à etapa de seleção dos riscos que deverão ser monitorados e tratados por meio da implementação de novos controles. A seleção é realizada com base na hierarquização obtida com as classificações de Impacto e Probabilidade.

4.25. Resposta ao risco:

Ação para reduzir, manter ou evitar a exposição da empresa ao risco, atuando na probabilidade e/ou no impacto, incluindo, mas não se limitando a controles internos.

4.26. Revisão dos Riscos:

Conjunto de atividades realizadas periodicamente, com o objetivo de identificar, avaliar e definir tratamentos para os Riscos da organização.

4.27. Risco:

Fatores ou eventos que, caso ocorram, podem causar impactos negativos ou danos, dificultando ou impossibilitando o cumprimento dos objetivos da COPASS SAÚDE, bem como podem subsidiar o processo de tomada de decisão, representando uma oportunidade ou ameaça.

4.28. Risco Corporativo:

São riscos que afetam, de alguma forma, o cumprimento dos objetivos de uma empresa, interferindo, positiva ou negativamente sua habilidade de gerar valor. Estão associados ao negócio como um todo, e geralmente, relacionam-se a oportunidades, ameaças, pontos fortes ou fracos da organização.

4.29. Risco de Processo:

São riscos críticos identificados a partir de um processo já mapeado pela empresa. São caracterizados pelos eventos que impactam nos resultados operacionais, seja de processos de gestão, da operação e/ou de apoio.

4.30. Risco de Crédito:

São riscos relacionados à probabilidade da contraparte de uma operação, ou de um emissor de dívida, não honrar, total ou parcialmente, seus compromissos financeiros, ou de ter alterada sua classificação de risco de crédito.

4.31.Risco de Gestão:

Definido como a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos relacionados aos objetivos orçamentários, financeiros, patrimonial, desenvolvimento institucional, incluindo a capacidade de crescimento e aprendizagem.

4.32.Risco de Mercado:

São riscos relacionados à exposição a perdas decorrentes da volatilidade dos preços de ativos, tais como cotações de ações, taxas de juros, taxas cambiais, preços de commodities e preços de imóveis.

4.33.Risco de Subscrição:

São riscos relacionados a uma situação econômica adversa que contraria as expectativas da operadora no momento da elaboração de sua política de subscrição quanto às incertezas existentes na estimativa das provisões técnicas e relativas à precificação.

4.34.Risco Estratégico:

Definido como a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos relacionados aos objetivos de alto nível, assim entendidos, os que dão suporte e estejam alinhados à missão institucional.

4.35.Risco Inerente:

É o nível de risco ao qual se estaria exposto caso não houvesse nenhum controle implantado.

4.36.Risco Legal:

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

4.37. Risco Operacional:

É a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

4.38. Risco Residual:

O nível de risco existente considerando os controles.

4.39. Ritos de Monitoramento da Gestão de Riscos:

Conjunto de atividades realizadas com o objetivo de acompanhar os riscos da organização, por meio dos seus Indicadores que apontarão cenários de maior ou menor criticidade e acompanhar a implementação dos novos Controles de Riscos, estabelecidos para o tratamento dos riscos mais críticos identificados na Revisão.

4.40. Tratamento:

Decisão que deverá ser tomada frente ao nível de exposição a um risco, compreendendo uma análise custo-benefício em relação ao apetite a risco definido pela Associação.

4.41. Três linhas:

É um modelo elaborado e divulgado pelo Institute of Internal Auditors - IIA Global, que auxilia na comunicação do gerenciamento de riscos e controles internos, por meio do esclarecimento dos papéis e responsabilidades essenciais, conforme abaixo descrito:

- I. **Primeira linha** - alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio;
- II. **Segunda linha** - fornecem assistência no gerenciamento de riscos e podem se concentrar em objetivos específicos do gerenciamento de riscos;
- III. **Terceira linha** - presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos.

4.42. Matriz R.A.C.I.:

Também conhecida como matriz de responsabilidades ou tabela RACI, a matriz RACI Consiste em um modelo simplificado de tabela que esclarece visualmente a divisão de responsabilidades, permitindo o acompanhamento das ações ao longo do

processo. Portanto é uma excelente ferramenta de gestão. Quando esses papéis são efetivamente distribuídos e bem definidos, as decisões são feitas rapidamente, a prestação de contas é mais transparente e a sequência de atividades fica mais organizada e corresponde à sigla para Responsible, Accountable, Consulted e Informed (Responsável, Aprovador, Consultado e Informado).

5. PRINCÍPIOS

5.1. Declaração de Appetite a Riscos

O apetite a Riscos da Copass Saúde é definido a partir da missão de promover cuidado integral, garantir a sustentabilidade da Associação e entregar valor em saúde.

A Copass Saúde não tolera decisões que possam comprometer:

- a sustentabilidade da Associação;
- aos padrões éticos e de *compliance*;
- a jornada assistencial dos seus beneficiários;
- a segurança operacional de seus processos;
- a saúde e segurança de seus beneficiários e colaboradores.

5.2. Adoção de boas práticas de governança corporativa

A Copass Saúde adota as melhores práticas de governança corporativa, no que tange à gestão de riscos e a políticas e práticas antifraude e anticorrupção, de forma sistemática, estruturada e oportuna, com o intuito de aprimorar e manter a transparência e a qualidade das suas informações, divulgadas interna e externamente, buscando melhor reputação perante o mercado e um diferencial na geração de valor para os seus beneficiários, mantenedora, patrocinadoras e demais partes interessadas.

5.3. Utilização de padrões e metodologias reconhecidos pelo mercado

Com um modelo baseado em metodologias e padrões formalizados e reconhecidos pelo mercado, a gestão integrada de riscos está alinhada às estratégias, iniciativas e estrutura organizacional, além de atender às exigências setoriais e dos órgãos reguladores e fiscalizadores.

5.4. Envolvimento dos órgãos de governança

A atuação do Conselho de Gestão, do Conselho Fiscal, da Superintendência Executiva e da Assessoria de Governança, Risco e Estratégia assume papel primordial para o sucesso do processo de gestão de riscos, uma vez que são estes os principais envolvidos nas tomadas de decisão sobre questões estratégicas da Associação.

5.5. Processo de tomada de decisão

Garantir a priorização nas decisões, de modo que os riscos mais críticos possam ser tratados com maior foco e que as iniciativas propostas sejam viáveis e relevantes para efetiva mitigação dos riscos, com o intuito de garantir que eles sejam identificados, analisados, avaliados, tratados, monitorados e testados de forma eficiente e eficaz.

5.6. Estabelecimento e manutenção da infraestrutura necessária para a gestão integrada de riscos

Para gerenciar os riscos de forma eficiente, a Copass Saúde devem possuir uma infraestrutura adequada e integrada de processos, pessoas e tecnologia, estabelecendo mecanismos de comunicação claros e objetivos, sempre prezando pela transparência.

5.7. Integração da gestão de riscos aos processos organizacionais

A gestão integrada de riscos deve permear todas as práticas e processos organizacionais, de forma a garantir a identificação de eventos de riscos inerentes e residuais a todas as suas áreas de negócio, sejam eles com abrangência individual ou corporativa.

5.8. Análise periódica da gestão de riscos

A Assessoria de governança, risco e estratégia deve assegurar a eficácia do gerenciamento de riscos por meio de revisões frequentes dos seus processos e indicadores e maturidade, favorecendo o cumprimento de seus objetivos.

5.9. Adoção do modelo das Três Linhas

A Copass Saúde adota modelo de gestão de riscos baseado nos conceitos das Três Linhas (conceituadas como “Três Linhas”), elaborado e divulgado pelo Institute of Internal Auditors - IIA Global sendo:

- Primeira Linha: Núcleos e Assessorias, além dos gestores de projetos e de processos. Esta linha é responsável pela provisão de produtos/serviços aos clientes; e por gerenciar riscos, são os executores dos processos operacionais.
- Segunda Linha: Assessoria de Governança, Risco e Estratégia. Esta linha possui a *expertise* do processo de gestão de risco e é responsável por apoiar, monitorar e questionar questões relacionadas a riscos.
- Terceira Linha: Auditoria Interna. Esta linha realiza avaliação e assessoria independentes e objetivas sobre questões relativas ao atingimento dos objetivos.

5.10. Matriz R.A.C.I.

Matriz R.A.C.I. das principais atividades do processo de Gestão de Riscos considerando as Três Linhas:

ATIVIDADE	Proprietário do Risco	ASGRE	Auditoria Interna
	1ª Linha	2ª Linha	3ª Linha
Definir Plano de Gestão de Riscos	R	A	C
Analisar o Contexto	R	I	I
Selecionar os Processos Críticos	R	A	I
Identificar os Riscos Inerentes	R	I	I
Avaliar os Riscos Inerentes	R	I	I
Priorizar os Riscos Inerentes Críticos	R	A	I
Identificar e avaliar os Controles dos Riscos Inerentes Críticos	R	A	I
Avaliar os Riscos Residuais	R	A	I
Definir a(s) Resposta(s) dos Riscos	R	A	I
Validar a Matriz de Riscos	R	R	R
Tratar os Riscos Críticos Residuais	R	I	I
Monitorar os Riscos Críticos Residuais	R	I	I

Legenda:

R - Responsável para executar (Responsible): É efetivamente quem trabalha na atividade

A - Autoridade para aprovar (Accountable): É o papel do aprovador ou responsável pelo aceite formal da tarefa ou produto entregue. Este pode delegar a função para outros profissionais, entretanto ele é quem se responsabiliza pelo recebimento do trabalho.

C - Precisa ser consultado (Consulted): Consultado, alguém cuja entrada agrega valor e/ou é essencial para a implementação final. A comunicação é de duas vias (consulta <=> resposta).

I - Precisa ser informado (Informed): Informado, a pessoa ou grupos de pessoas que precisam ser notificados de resultados ou ações tomadas, mas não precisam estar envolvidos no processo de tomada de decisão. A comunicação é apenas num sentido =>.

6. DIRETRIZES

A gestão de riscos deve ser um processo contínuo, que busca envolver toda a organização tratando os eventos e as áreas de forma conjunta.

Visando alcançar os objetivos desta política, deve-se executar as etapas do processo de gestão de riscos, descritas a seguir:

6.1. Identificação dos riscos

- I. Os riscos devem ser considerados em todas as decisões e a sua gestão deve ser realizada de maneira integrada;
- II. Deve haver um alinhamento com as estratégias e com os interesses e benefícios para os Associados, Mantenedora e Patrocinadoras da Copass Saúde;
- III. Identificar as incertezas relacionadas ao negócio da Associação e permitir atuação de forma preventiva aos eventuais efeitos negativos de tais incertezas.
- IV. Aproveitar as oportunidades e antever as ameaças internas e externas que possam afetar os objetivos da Copass Saúde.

6.2. Avaliação dos riscos

- I. Classificar os riscos conforme sua natureza, categoria e seu nível de criticidade.
- II. Identificar os fatores de riscos e os seus respectivos controles de forma a assegurar que a probabilidade e impactos possam ser eliminados, retidos, mitigados, explorados e/ou compartilhados.

6.3. Tratamento dos riscos

- I. As ações de resposta devem considerar as possíveis consequências dos riscos e priorizadas de acordo com a criação ou proteção de valor da

Associação, e com as necessidades e expectativas das partes interessadas;

- II. Planejar as respostas aos riscos, analisando cenários, benefícios, aspectos negativos, riscos inter-relacionados e mensurando a relação entre impacto e mitigação.

6.4. Monitoramento dos riscos

- I. Os mecanismos de monitoramento devem ser eficientes e garantir o cumprimento dos planos e limites estabelecidos, visando aprimorar a sinergia entre as três linhas, assegurando as responsabilidades de todos envolvidos;
- II. Gerenciar, de forma proativa e abrangente, os riscos associados aos processos estratégicos, de negócio e de suporte priorizados, de forma a mantê-los em um nível tolerável de magnitude;
- III. Assegurar o monitoramento e a análise crítica do próprio gerenciamento de riscos como parte integrante de um processo contínuo de melhoria da governança corporativa.

6.5. Comunicação dos riscos

- I. A comunicação dos riscos deve fortalecer a gestão de riscos de forma dinâmica, interativa e de caráter proativo quanto aos eventos internos e externos capazes de modificar o contexto e o posicionamento da Copass Saúde;
- II. Fortalecer a gestão de riscos como parte da cultura da Associação;
- III. Garantir a administradores, mantenedora, patrocinadoras e demais partes interessadas um fluxo contínuo, transparente e adequado de informações associadas aos principais riscos e seu processo de gestão, respeitando o grau de sigilo das informações, bem como os procedimentos corporativos, políticas, diretrizes e demais normas internas de segurança da informação;

7. DISPOSIÇÕES FINAIS

Esta Política está alinhada às demais Políticas da Copass Saúde.

O descumprimento a qualquer dispositivo desta Política sujeitará o infrator as penalidades previstas nos Normativos da Associação.

Informações de Controle:

Versão 0 - Aprovada pelo Conselho de Gestão em 02/07/2020 – PRC nº 021/2020

Versão 1 - Aprovada pelo Conselho de Gestão em 19/06/2024 – PRC nº 047/2024

Responsável pelo documento: Assessoria de Governança, Risco e Estratégia - ASGRE

Instância de revisão: Superintendência Executiva

Instância de aprovação: Conselho de Gestão