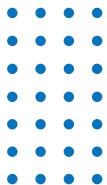




POLÍTICA DE
GESTÃO DE RISCOS
E CONTROLES INTERNOS

POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

Unidade Administrativa Gestora do normativo	Presidência (PRESI) Gerência de Compliance, Riscos e Controles Internos (GECRI)
Unidade Administrativa responsável pela análise normativa (interna) e padronização	Presidência (PRESI) Gerência de Estratégia e Inteligência Organizacional (GEORG) Coordenação de Estratégia e Inteligência Organizacional (COORG)
Unidade Administrativa responsável pela conformidade	Gerência Jurídica (GEJUR) Coordenação Consultiva e Regulatória (CONSU)
Numeração	011
Versão	001
Data da Apreciação pela Diretoria-Executiva	DIREX Nº 252, de 10 de junho 2021
Data da Aprovação do Conselho Deliberativo	CODEL Nº 148, de 30 de junho 2021
Data de Publicação	15/09/2021
Data da Vigência	16/09/2021
Advertência	Este normativo é de uso exclusivo da Postal Saúde. A divulgação não autorizada estará sujeita às penalidades cabíveis por lei. Toda e qualquer autorização para cópia, divulgação, apresentação ou qualquer outra finalidade deverá ser obtida junto à Postal Saúde.



Sumário

CAPÍTULO 1 - DO OBJETIVO	4
CAPÍTULO 2 - DA ABRANGÊNCIA	7
CAPÍTULO 3 - DAS DEFINIÇÕES	9
CAPÍTULO 4 - DOS PRINCÍPIOS	14
CAPÍTULO 5 - DAS DIRETRIZES	17
CAPÍTULO 6 - INSTÂNCIAS DE SUPERVISÃO	23
CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES	26
CAPÍTULO 8 - COMPROMISSOS E PENALIDADES	33
CAPÍTULO 9 - DAS DISPOSIÇÕES GERAIS	35
CAPÍTULO 10 - DOS DOCUMENTOS ASSOCIADOS	37





DO 01 OBJETIVO



CAPÍTULO 1 - DO OBJETIVO

- 1.1. A Política de Gestão de Riscos e Controles Internos tem o objetivo geral de estabelecer as diretrizes, os princípios, as competências e responsabilidades a serem observadas na gestão dos riscos corporativos, estratégicos, de processo e de projetos, bem como na gestão dos controles internos, de modo a fortalecer a governança corporativa da Postal Saúde, reduzir os impactos da incerteza na gestão (exposição aos riscos) e ampliar a possibilidade de alcance de resultados positivos, a partir do gerenciamento de oportunidades, buscando o pleno alcance dos Objetivos Estratégicos da Operadora e o cumprimento de sua Missão e Visão.
- 1.2. A Gestão de Riscos na Postal Saúde terá por objetivos específicos:
 - I. Uniformizar o conhecimento entre os gestores de riscos e administradores quanto aos principais riscos envolvidos em suas atividades;
 - II. Conduzir a tomada de decisão, a fim de que os atores de riscos tenham acesso tempestivo às informações suficientes para tal, auxiliando na alocação e utilização eficaz de recursos para o tratamento e monitoramento dos riscos e, consequentemente, aperfeiçoando os processos organizacionais e controles internos da operadora, e;
- 1.3. Por sua vez, a Gestão dos Controles Internos terá por objetivos específicos:
 - I. proporcionar garantia razoável do alcance dos objetivos estratégicos da Operadora, dando suporte ao cumprimento da Missão e Visão, à continuidade do negócio e à sustentabilidade institucional;
 - II. assegurar a confiabilidade e integridade das informações, dados e relatórios produzidos pela Operadora;
 - III. buscar a utilização eficiente dos recursos, com eficácia em sua execução;
- III. Garantir o cumprimento da Missão e Visão da Postal Saúde, sua continuidade e sustentabilidade alinhadas aos seus objetivos.

CAPÍTULO 1 - DO OBJETIVO

- IV. assegurar a conformidade da Operadora com a Lei e com as normas internas aplicáveis; e;
- V. assegurar a gestão da continuidade dos negócios da Operadora.





02

**DA
ABRANGÊNCIA**



CAPÍTULO 2 - DA ABRANGÊNCIA

- 2.1. A Política de Gestão de Riscos e Controles Internos da Postal Saúde abrangerá todos os empregados da Operadora — sejam eles próprios, cedidos, estagiários ou menores aprendizes —, de todas as Unidades Administrativas Gestoras (UAGs), Unidades e Núcleos de Representação Regionais (URRs e NARs), independentemente de cargo ou função exercidos, bem como os Administradores da Operadora, compreendidos aqui os membros da Diretoria Executiva e dos Conselhos Fiscal (COFIS) e Deliberativo (CODEL).
- 2.2. A Política se estende ainda a todos os terceiros com os quais a Postal Saúde tenha relacionamento direto ou indireto e aos que atuam a serviço ou em nome da Operadora, tais como prestadores de serviços, assistenciais ou não, fornecedores e/ou quaisquer partes interessadas, sua Mantenedora e Patrocinadores, Órgãos Reguladores e, não menos importante, aos Beneficiários dos Planos de Assistência à Saúde oferecidos pela Operadora.



03

DAS DEFINIÇÕES



Administradores ou Alta Administração: Gestores integrantes do nível executivo, eleitos ou designados e nomeados para os cargos de Diretor, ou Conselheiro, com autoridade para estabelecer políticas, objetivos e conduzir a implementação da estratégia da organização.

Apetite a risco: Expressão ampla para definição de quanto risco a Operadora está disposta a enfrentar para implementar a estratégia, alcançar objetivos e agregar valor aos interessados no cumprimento de sua missão.

Atores de Riscos: Todos aqueles envolvidos na Gestão de Riscos: Diretoria-Executiva, Conselhos Fiscal e Deliberativo, diretores de Riscos e gestores de Riscos.

Checagem: Consiste em verificar, por meio de avaliação e testes, se os controles apresentados e as ações adotadas para tratamento dos riscos apresentaram efetividade.

Conformidade: Cumprimento e/ou observância de normas, legislações, regramentos e boas práticas estabelecidas.

Controles internos: Conjunto de métodos e medidas coordenados e aplicados em uma empresa na forma de procedi-

mentos, atividades, normas e objetivos que, se efetivos, proporcionam maior confiança nas informações e na proteção de seus valores.

Efetividade: Está relacionada à análise do controle realizado com o alcance do resultado pretendido. Trata-se de verificação da mitigação dos riscos frente aos controles executados.

Eficácia: É a capacidade da Operadora em cumprir as metas, os prazos e os objetivos planejados, independentemente do custo aplicado.

Eficiência: É a relação entre o serviço ofertado e os custos dos insumos empregados, ou seja, executar processos com qualidade, investindo o mínimo de insumos possível.

Gerenciamento de Risco: Processo cíclico, sistêmico e contínuo, que possibilita a identificação, a avaliação, o planejamento do tratamento e o monitoramento de riscos, no sentido de fornecer segurança razoável ao atingimento dos objetivos da Operadora.

CAPÍTULO 3 - DAS DEFINIÇÕES

Gestão de Risco: Conjunto de ações conduzidas pelos atores de riscos e que visam à redução da probabilidade de ocorrência e/ou impactos de riscos identificados e à maximização de oportunidades, objetivando o alcance dos objetivos estratégicos, a eficiência nas operações e a melhoria de desempenho dos processos, da governança e da reputação.

Gestor de riscos: Profissional responsável pelo gerenciamento de riscos de um processo de trabalho, projeto, produtos e/ou serviços em seus respectivos âmbitos e escopos de atuação. Gestores de riscos são responsáveis e têm propriedade na gestão dos riscos sobre processos de sua titularidade. É sua função atuar na identificação, avaliação e classificação dos riscos de seus processos e estabelecer as ações a serem implementadas para o tratamento e o controle do risco.

Governança: Conjunto de procedimentos e direcionadores para definir responsabilidades e criar diretrizes que orientam, monitoram e avaliam as pessoas e os processos organizacionais. Apoiada pela alta administração, demonstra às partes interessadas como a empresa deve ser dirigida e administrada.

Impacto: Efeito resultante da ocorrência de um evento de risco.

KRI – Key Risk Indicator (Indicadores Chave de Riscos): medidas ou métricas utilizadas para verificação do potencial de exposição a determinado risco.

Matriz de Riscos: Ferramenta de gerenciamento que apresenta os riscos identificados e seus respectivos níveis de acordo com o avaliado na escala de probabilidade e impacto, permitindo ampliar a visibilidade dos gestores na mensuração e priorização dos riscos que podem afetar o alcance dos objetivos estratégicos.

Método: Modelo de aplicação de procedimentos sistemáticos composto por técnicas, normas e operações predefinidas de acordo com um planejamento para alcançar um objetivo.

Monitoramento: Ação periódica e contínua realizada para acompanhamento dos riscos e seus planos de tratamentos. Consiste ainda em verificar periodicamente o cumprimento das ações adotadas para o tratamento dos riscos e comunicar aos órgãos colegiados sobre o andamento das atividades.

CAPÍTULO 3 - DAS DEFINIÇÕES

Nível de Risco: Classificação da magnitude de um risco, resultante da combinação de sua probabilidade e impacto.

Órgãos Colegiados: Diretoria-Executiva, Conselho Fiscal e Conselho Deliberativo.

Plano de tratamento: Descrição detalhada das ações e atividades a serem realizadas para implementação de melhorias no processo visando ao tratamento do risco. Deve ser formalizado, apresentando as etapas, os responsáveis e os prazos para implementação.

Primeira linha: Atuam na primeira linha de defesa os responsáveis por identificar, avaliar, controlar e mitigar os riscos em sua operação, assim como implementar as ações corretivas para resolver deficiências em processos e controles.

Probabilidade: Possibilidade de ocorrência de um evento de risco.

Processo: Conjunto de atividades ou tarefas logicamente relacionadas que, usando os recursos necessários, produzem resultados reais, adicionando valor a cada etapa executada.

Proprietário de Riscos: Ator a quem recai a responsabilidade máxima pelo gerenciamento de riscos. É responsável por liderar, supervisionar e conduzir os gestores de Riscos na definição dos riscos prioritários, bem como na definição dos planos de tratamento de riscos.

Risco ou evento de risco: Fato que pode influenciar no alcance dos objetivos estratégicos de modo positivo, negativo ou ambos.

Riscos Prioritários: Eventos de riscos mapeados na fase de Contextualização e Identificação de Riscos, que devem ser considerados para evolução nas fases de gerenciamento de riscos.

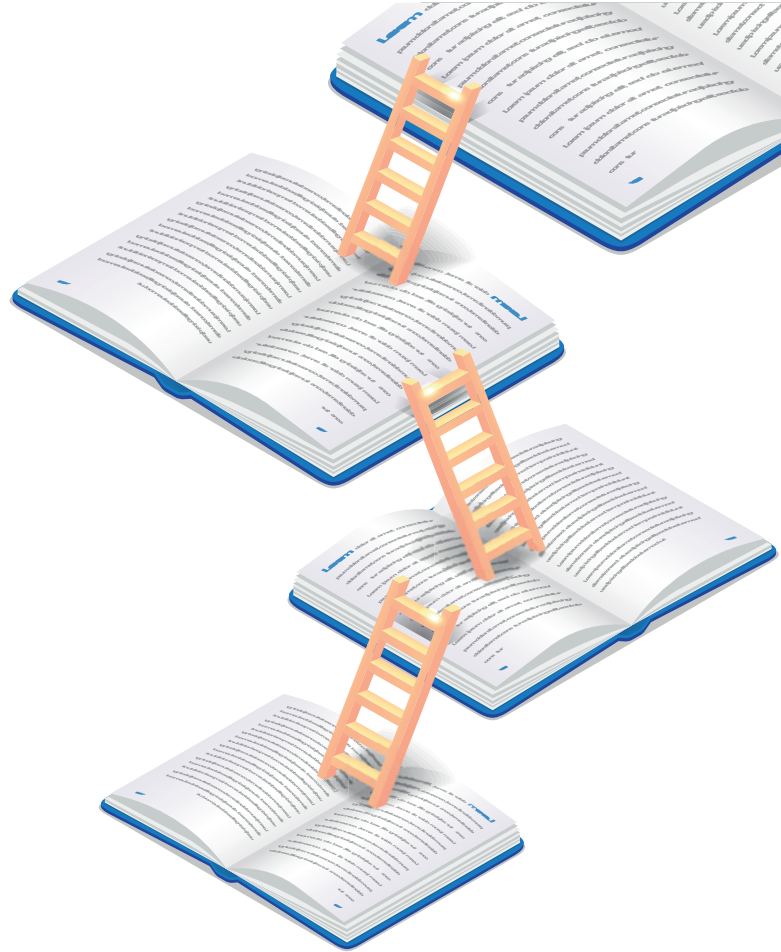
Segunda linha: Atua na segunda linha de defesa o órgão, a pessoa ou a gerência que tem o objetivo de apoiar os envolvidos na Gestão de Riscos para que cumpram com suas responsabilidades de primeira linha, fornecendo de forma íntegra e imparcial o conhecimento e os instrumentos necessários para a Gestão de Riscos e implementação de Controles Internos, além de ser responsável pela implementação da metodologia de Gestão de Riscos e supervisão da conformidade e efetividade dos controles.

CAPÍTULO 3 - DAS DEFINIÇÕES

Terceira linha: Na terceira linha de defesa atua a Auditoria Interna, realizando avaliações mais abrangentes e objetivas sobre a forma como a primeira e segunda linhas de defesa alcançam seus objetivos, atuando com maior nível de independência e reportando-se diretamente aos órgãos colegiados.

Tolerância a risco: Nível de variação suportado no desempenho em relação à meta para o cumprimento de um objetivo específico

Unidade de Riscos: Atores da Gestão de Riscos responsáveis por auxiliar os diretores e gestores de Riscos no processo de gerenciamento desses, atuando como facilitadores, promovendo e acompanhando todas as fases definidas.





DOS 04 PRINCÍPIOS



4.1. A Gestão de Riscos e Controles Internos da Postal Saúde será pautada pelos seguintes princípios:

I. Comprometimento e apoio da alta administração: patrocínio irrestrito, com o incentivo à cultura do gerenciamento de riscos e de controle interno;

II. Autonomia e independência: atuação autônoma e independente dos agentes de riscos, de modo a garantir imparcialidade em sua atuação;

III. Agregar e proteger valor: refletir os valores da Operadora e estar alinhado aos objetivos estratégicos, contribuindo para seu alcance, eficiência nas operações e melhoria de desempenho dos processos, governança e reputação;

IV. Ser parte integrante de todos os processos organizacionais: estar bem desenvolvida, entendida e apoiada por todos os abrangidos, sendo parte integrante dos processos;

V. Subsidiar a tomada de decisões: auxiliar os

tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas e alternativas de ação;

VI. Abordar explicitamente a incerteza: considerar todos os cenários que possam impactar ou oportunizar o alcance dos objetivos, buscando a transparência em todas as situações de riscos constatadas;

VII. Ser sistemática, estruturada e oportuna: possuir procedimentos bem definidos, sendo executada de forma tempestiva e continuada;

VIII. Basear-se nas melhores informações disponíveis: ter acesso a todas as informações do processo de forma irrestrita e basear-se em opiniões de especialistas sempre que necessário;

IX. Atuar sob medida: estar de acordo com a estrutura, cultura e valores da Postal Saúde, alinhada com o contexto interno e externo da Operadora e com o perfil do risco;

CAPÍTULO 4 - DOS PRINCÍPIOS

- X. Considerar fatores humanos e culturais:** reconhecer capacidades, percepções e intenções que possam influenciar no gerenciamento dos riscos;
- XI. Prezar pela transparência e inclusão:** dar publicidade aos riscos identificados e envolver apropriada e oportunamente as partes interessadas;
- XII. Ser dinâmica, interativa e capaz de reagir às mudanças:** continuamente perceber e reagir às mudanças de cenários, internos ou externos, que possam impactar os objetivos da Operadora;
- XIII. Apoiar a melhoria contínua:** auxiliar no desenvolvimento e implementação de estratégias para melhorar processos e elevar a maturidade da Operadora na Gestão de Riscos.





DAS 05
DIRETRIZES



5.1. Das Diretrizes Gerais

- 5.1.1. A Gestão de Riscos e Controles Internos da Postal Saúde deverá fortalecer a tomada de decisão, baseando-se em estudos técnicos, operacionais, jurídicos e econômico-financeiros, além de diagnósticos de fragilidades, a fim de prover aos gestores da Operadora dados corretos, confiáveis e imparciais;
- 5.1.2. A Gestão de Riscos e Controles Internos deverá estar integrada ao Planejamento Estratégico da Postal Saúde e deve estar contemplada em todos os projetos e processos da Operadora;
- 5.1.3. Os riscos identificados, bem como seus planos de tratamento, deverão ser monitorados pela Unidade responsável pela Gestão de Riscos e Controles Internos (GECRI) e reportados trimestralmente à Diretoria-Executiva e aos Conselhos da Postal Saúde.

5.2. Da Gestão de Riscos

- 5.2.1. A Gestão de Riscos na Postal Saúde deverá ser executada de forma dinâmica e padronizada, utilizando as definições trazidas na ISO 31.000 e suas atuali-

zações, e as ferramentas delineadas na ISO 31.010 e suas atualizações, lançando mão ainda de documentos que possam agregar valor ao procedimento, tal como o COSO ERM e os normativos publicados pelo Órgão Regulador (ANS).

- 5.2.2. A execução do Gerenciamento de Riscos deverá ser planejada anualmente, com definição das prioridades para mapeamento, e deve ser aprovado, nos Órgãos Colegiados, o Plano Anual de Atividades de Compliance, Riscos e Controles Internos (PAACRI);
- 5.2.3. A construção do PAACRI, no que tange ao planejamento das prioridades de atuação para o gerenciamento de riscos, deverá utilizar as ferramentas descritas na ISO 31.000;
- 5.2.4. O ciclo de Gerenciamento de Riscos deverá ser de, no máximo, dois anos em relação ao último executado;
- 5.2.5. A Gestão de Riscos deverá levar em consideração a definição dos limites de apetite e tolerância a riscos estabelecidos pelos órgãos competentes, que ditará as prioridades de tratamento aos riscos identificados;

CAPÍTULO 5 - DAS DIRETRIZES

- 5.2.6. As decisões a serem tomadas deverão, sempre que possível, ser pautadas por informações de riscos, de modo que as escolhas sejam conscientes;
- 5.2.7. Deverão ser obtidas informações úteis e adequadas à tomada de decisão, por meio de metodologias e ferramentas que possibilitem o alcance dos objetivos e processos organizacionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos pela operadora;
- 5.2.8. O desempenho da Gestão de Riscos deverá ser medido por intermédio do monitoramento contínuo dos indicadores chave de riscos (KRI);
- 5.2.9. A avaliação de mudanças, internas e externas, que contribuam para identificação e avaliação de fragilidades que impactam os objetivos estratégicos da Operadora para o desenvolvimento e a realização de atividades de controle deverão ser consideradas na execução do gerenciamento de riscos;
- 5.2.10. Adotar procedimentos de controles internos proporcionais aos riscos, fundamentados na relação custo-benefício e na agregação de valor à Operadora;
- 5.2.11. Deverá ser assegurado o desenvolvimento contínuo de todos os atores envolvidos no gerenciamento de riscos, de modo a qualificar a sua execução;
- 5.2.12. A atuação da Gestão de Riscos deverá ser independente e autônoma, fomentado pela Alta Administração, de modo a buscar a imparcialidade nas operações.
- ### 5.3. Do Gerenciamento de Riscos
- 5.3.1. Para o desenvolvimento das atividades de gerenciamento de riscos deverá ser adotado o método estabelecido no Manual de Gerenciamento de Riscos e Controles Internos, o qual possibilita a execução de todas as suas fases;
- 5.3.2. O Gerenciamento de Riscos será composta pelas seguintes fases:
- 1. Contextualizar e identificar os riscos:** fase em que o contexto do trabalho é estabelecido, a fim de direcionar a identificação dos riscos, suas causas, consequências e controles existentes, que também é executado nesta fase.

- 2. Analisar e avaliar os riscos e controles:** fase em que os riscos identificados são analisados pelos gestores de riscos com base na probabilidade de ocorrência e seu impacto, assim como é executada a análise dos controles existentes quanto às suas características e efetividade inicial. Compreende ainda a etapa de avaliação dos riscos, onde seu nível residual é comparado ao apetite e tolerância a riscos da Operadora para subsidiar a tomada de decisão pela definição de prioridades de tratamento. Nesta fase é elaborada a Matriz de Riscos e Controles da tarefa executada, e atualizada a Matriz de Riscos e Controles Geral da Postal Saúde;
- 3. Tratar os riscos:** fase em que são definidos e estabelecidas as ações de tratamento para redução dos níveis de riscos identificados na fase de avaliação e/ou estabelecimento de ações de contingência e planos de continuidade de negócio; e
- 4. Monitorar riscos e controles:** Fase em que os riscos passam por monitoramento contínuo a fim de que haja o controle de sua materialização.

Nesta fase ocorre ainda o monitoramento dos planos de tratamento definidos para redução dos níveis de risco.

Figura 1 - Gerenciamento de Riscos da Postal Saúde



Fonte: COCRI/GECRI

CAPÍTULO 5 - DAS DIRETRIZES

5.3.3. As fases do gerenciamento de riscos ainda deverão ser permeadas por atividades de comunicação e de melhoria contínua.

5.4. Categorias de Riscos

5.4.1. As categorias adotadas pela Postal Saúde serão, minimamente, as descritas abaixo, aplicáveis conforme o cenário de cada trabalho:

- Riscos Corporativos
- Riscos Estratégicos
- Riscos Operacionais
- Riscos de Compliance
- Riscos Legais
- Riscos à Imagem
- Riscos à Integridade
- Riscos de Crédito
- Riscos Atuariais
- Riscos de Subscrição
- Riscos Econômico-Financeiros
- Riscos Socioambientais.

5.5. Appetite e Tolerância a Riscos

5.5.1. Os Órgãos Colegiados da Operadora, anualmente, devem analisar e estabelecer, conforme as competências descritas nos itens 7.1, 7.2 e 7.3, o apetite e a tolerância a riscos a que a Postal Saúde deve estar submetida na busca do alcance de seus objetivos estratégicos e cumprimento de sua missão e visão.

5.5.2. Os estudos para subsídio da definição do apetite e da tolerância a riscos deverão ser conduzidos pela Gerência de Compliance, Riscos e Controles Internos e aprovados pela Diretoria- Executiva e pelo Conselho Deliberativo, devendo ser declarado e amplamente divulgado após aprovação.

5.5.3. A definição dos níveis de tolerância e do apetite a riscos deverá estar alinhada às estratégias institucionais da Operadora e devem servir de suporte à tomada de decisão.

5.6. Gerenciamento dos Controles Internos

- 5.6.1. Os controles internos deverão ser executados de forma integrada às atividades e aos processos de trabalho, com a colaboração dos empregados e da Alta Administração da Postal Saúde;
- 5.6.2. Devem-se definir e operacionalizar os controles internos considerando a avaliação dos riscos identificados, internos e externos, que se pretende gerenciar, com base na redução da ocorrência de riscos e seus impactos sobre os objetivos da Operadora;
- 5.6.3. Deverão ser implementados controles internos efetivos e compatíveis com a estrutura, a natureza, a complexidade, o grau de importância e os riscos dos processos de trabalhos;
- 5.6.4. Os controles internos implementados precisam ser tangíveis e/ou mensuráveis, possibilitando a execução de avaliações periódicas;
- 5.6.5. Criar condições para a implementação de procedimentos efetivos de controles internos que se integrem às práticas de gerenciamento de riscos;
- 5.6.6. Adotar procedimentos de controles internos proporcionais aos riscos, baseados na relação custo-benefício e na agregação de valor à Operadora; e
- 5.6.7. Os Controles Internos deverão ser avaliados periodicamente com o objetivo de verificar a sua eficácia.



06

INSTÂNCIAS DE SUPERVISÃO



CAPÍTULO 6 - INSTÂNCIAS DE SUPERVISÃO

6.1. As Instâncias de Supervisão têm como função essencial apoiar e dar suporte aos diversos níveis hierárquicos da Operadora e seus órgãos colegiados com o objetivo de integrar as atividades de Gestão de Riscos e Controles Internos nos processos e atividades organizacionais.

6.2. A Postal Saúde utiliza como base o modelo das três linhas do *Institute of Internal Auditors* (IIA) para operacionalizar sua estrutura de gerenciamento de riscos e controles, definidos conforme atuação e nível de responsabilidade dos envolvidos sobre cada o processo, representado da seguinte forma:



Fonte: COCRI/GECRI - Adaptado do Modelo das Três Linhas do IIA 2020 – uma atualização das três linhas de defesa.

CAPÍTULO 6 - INSTÂNCIAS DE SUSPENSÃO

- 6.3. A primeira linha é composta por todos os empregados da Operadora, os quais possuem parcela de responsabilidade sobre a Gestão de Riscos e Controles Internos, bem como os Proprietários de Riscos e os Gestores dos Riscos, sendo estes os responsáveis pelo gerenciamento de um processo de trabalho, projeto ou produto em seus respectivos âmbitos e escopos de atuação, portanto, tendo propriedade sobre os riscos identificados;
- 6.4. A segunda linha é composta pela unidade responsável pelo *Compliance*, Riscos e Controles Internos, caracterizada como unidade de riscos, e possui objetivo de apoiar a 1ª linha, tendo como principal responsabilidade a implantação do método de gerenciamento de riscos e controles;
- 6.5. A terceira linha é realizada pela Auditoria Interna (AUDIN), de forma independente;
- 6.6. A avaliação do processo de Gestão de Riscos e Controles Internos da Postal Saúde poderá ser matéria de avaliação pela terceira linha, bem como pela auditoria externa e/ou fiscalização de órgãos reguladores, fiscalizadores e de controle;
- 6.7. Os Órgãos Colegiados da Operadora, a saber: Conselho Fiscal, Conselho Deliberativo e Diretoria-Executiva são os órgãos de governança, aos quais as três linhas possuem reporte direto, sendo os responsáveis por estabelecer e apoiar a cultura voltada a riscos e à integridade.



07

ATRIBUIÇÕES E RESPONSABILIDADES



CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

7.1. Conselho Deliberativo (CODEL)

- 7.1.1. Aprovar a Política de Gestão de Riscos e Controles Internos da Postal Saúde;
- 7.1.2. Conhecer o relatório de Gestão de Riscos e Controles Internos submetido pela Diretoria- Executiva;
- 7.1.3. Aprovar e monitorar as diretrizes referentes ao apetite e à tolerância aos riscos da Postal Saúde;
- 7.1.4. Conhecer e acompanhar os riscos prioritários e que possuem maior impacto no alcance dos objetivos da Operadora;
- 7.1.5. Supervisionar os sistemas de Gestão de Riscos e Controles Internos estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a operadora, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude, nos termos do Estatuto Social da Operadora;
- 7.1.6. Emitir à Diretoria Executiva recomendações para o aprimoramento da Gestão de Riscos.

7.2. Conselho Fiscal (COFIS)

- 7.2.1. Conhecer e monitorar as diretrizes referentes ao apetite e à tolerância aos riscos da Postal Saúde;
- 7.2.2. Conhecer o relatório de Gestão de Riscos e Controles Internos submetido pela Diretoria Executiva;
- 7.2.3. Supervisionar os sistemas de Gestão de Riscos e Controles Internos estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a operadora, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados à ocorrência de corrupção e fraude, nos termos do Estatuto Social da Companhia;
- 7.2.4. Emitir à Diretoria Executiva recomendações para o aprimoramento da Gestão de Riscos.

7.3. Diretoria Executiva (DIREX)

- 7.3.1. Aprovar a Política de Riscos e Controles Internos e submetê-la para apreciação do Conselho Deliberativo;

CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

- 7.3.2. Aprovar o Manual de Gestão de Riscos e Controles Internos, bem como os demais normativos relacionados à temática de Gestão de Riscos e Controles;
- 7.3.3. Aprovar os indicadores de avaliação de desempenho da Gestão de Riscos;
- 7.3.4. Fomentar a implementação da Gestão de Riscos e controles internos, promovendo sua institucionalização na Operadora;
- 7.3.5. Estabelecer as diretrizes referentes ao apetite e à tolerância a riscos da Postal Saúde e submetê-las para apreciação do Conselho Deliberativo;
- 7.3.6. Conhecer e deliberar sobre o relatório de Gestão de Riscos e controles internos submetido pelo Diretor-Presidente e submetê-lo para conhecimento do Conselho Deliberativo e do Conselho Fiscal;
- 7.3.7. Assegurar os recursos necessários à implementação e execução do Sistema de Gestão de Riscos e Controles Internos da Postal Saúde;
- 7.3.8. Deliberar sobre a adequação, suficiência e eficácia da estrutura e processo de Gestão de Riscos e Controles Internos da Postal Saúde;
- 7.3.9. Assegurar o cumprimento dos objetivos estratégicos e da Política de Gestão de Riscos e Controles Internos;
- 7.3.10. Supervisionar o mapeamento e avaliação dos riscos que podem comprometer a realização dos objetivos estratégicos e a prestação de serviços de interesse público, reportando ao Conselho níveis de exposição a riscos aos quais a operadora está sujeita.
- 7.3.11. Estabelecer estruturas adequadas para o gerenciamento de integridade, riscos e controle internos em consonância com as diretrizes do Conselho Deliberativo;
- 7.3.12. Acolher as recomendações de aprimoramento da Gestão de Riscos emitidas pelos Conselhos Fiscal e Deliberativo, direcionar para os Agentes de Riscos e supervisionar o seu efetivo cumprimento; e
- 7.3.13. Emitir para os Agentes de Riscos recomendações para o aprimoramento da Gestão de Riscos.

CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

7.4. Unidade de Riscos

- 7.4.1. Apoiar a primeira linha no gerenciamento de riscos, atuando como facilitador do processo, promovendo e acompanhando todas as fases definidas nesta Política e no Manual de Gestão de Riscos e Controles Internos;
- 7.4.2. Apoiar o processo de Gestão de Riscos e controles internos na Postal Saúde, por meio da criação e disseminação de método para identificação, avaliação, tratamento e monitoramento de riscos;
- 7.4.3. Consolidar as informações levantadas durante a execução do trabalho de gerenciamento de riscos;
- 7.4.4. Emitir relatórios de Gestão de Riscos e controles internos e submeter à Presidência;
- 7.4.5. Apresentar o resultado do mapeamento de riscos ao Líder e ao Gestor de Riscos para que estes definam os riscos prioritários e respectivos planos de tratamento;
- 7.4.6. Apoiar a primeira linha no desenvolvimento de controles para gerenciar os riscos identificados;
- 7.4.7. Monitorar a execução das ações de tratamento de riscos prioritizados e a eficiência e eficácia dos controles;
- 7.4.8. Manter banco de informações de riscos atualizado a partir da aplicação do método de gerenciamento de riscos;
- 7.4.9. Avaliar as proposições de melhorias, recomendações emitidas e aprendizados no processo de Gestão de Riscos e realizar os ajustes necessários para o efetivo resultado da aplicação do modelo;
- 7.4.10. Monitorar os riscos ao longo do tempo, de modo a permitir que as respostas adotadas resultem na manutenção do risco em níveis adequados;
- 7.4.11. Assegurar que as informações adequadas sobre gerenciamento de riscos e controles internos estejam disponíveis em todos os níveis, no âmbito das unidades;
- 7.4.12. Disseminar a cultura do gerenciamento de riscos e de controles internos;

CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

7.4.13. Promover a melhoria das metodologias e instrumentos do gerenciamento de riscos e controles internos às melhores práticas;

7.4.14. Atuar de forma independente e autônoma no gerenciamento de riscos; e;

7.4.15. Recepcionar as recomendações de aprimoramento da Gestão de Riscos emitidas ou direcionadas pela Diretor-Executiva e implementá-las efetivamente.

7.5. Proprietários de Riscos

7.5.1. Assegurar que os riscos sejam gerenciados em conformidade com os princípios e diretrizes estabelecidas nesta Política, bem como com as regras estabelecidas no Manual de Gestão de Riscos e Controles Internos;

7.5.2. Supervisionar a institucionalização de estruturas adequadas de governança, Gestão de Riscos e controles internos no âmbito de sua gestão;

7.5.3. Supervisionar a promoção do desenvolvimento contínuo dos gestores de riscos e incentivar a adoção de

boas práticas de governança, de Gestão de Riscos e de controles internos;

7.5.4. Conhecer os riscos inerentes aos processos das gerências sob sua responsabilidade;

7.5.5. Gerir os riscos identificados nos processos sob sua gestão, com vistas à melhoria contínua dos processos;

7.5.6. Definir, com base nas diretrizes estabelecidas nesta Política e nos normativos associados, os riscos prioritários para tratamento prioritário;

7.5.7. Aprovar e garantir a implantação do plano de tratamento dos riscos estratégicos;

7.5.8. Patrocinar as iniciativas de gerenciamento dos riscos, de forma a disponibilizar os recursos necessários para seu tratamento;

7.5.9. Fomentar, junto aos Gestores de Riscos, que os níveis dos riscos dos processos sob sua gestão estejam adequados aos níveis de apetite e tolerância a riscos definidos pelos órgãos de governança;

CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

- 7.5.10. Atuar como instância superior para a tomada de decisões que extrapolem a alçada dos gestores de riscos, podendo submeter tais decisões ao crivo da Diretoria-Executiva; e
- 7.5.11. Liderar e supervisionar a institucionalização da Gestão de Riscos e dos Controles Internos, oferecendo suporte necessário para sua efetiva implementação nas unidades e processos sob sua gestão.
- 7.6. Gestores de Riscos**
- 7.6.1. Definir níveis adequados dos riscos identificados de acordo com a avaliação na escala de probabilidade e impacto;
- 7.6.2. Gerir os riscos dos processos dos quais é responsável;
- 7.6.3. Manter controles internos eficazes, encaminhando respostas aos riscos identificados, e propor, quando necessário, ações corretivas para resolver deficiências em processos e controles;
- 7.6.4. Elaborar os planos de tratamento e gerenciar suas ações, avaliando periodicamente os resultados;
- 7.6.5. Monitorar os processos sob sua responsabilidade, de modo a garantir que as respostas adotadas aos riscos estejam em conformidade ao modelo de gerenciamento de riscos aprovado pela Operadora;
- 7.6.6. Fomentar a implementação da Gestão de Riscos e Controles Internos junto aos empregados envolvidos no processo de sua responsabilidade, com base no modelo estabelecido;
- 7.6.7. Definir quais os riscos identificados no processo analisado deverão ser considerados riscos prioritários e submeter à avaliação do Diretor de Risco;
- 7.6.8. Definir e implementar planos de tratamento aos riscos que estejam acima do nível de risco tolerável, a fim de reduzir os riscos a níveis aceitáveis;
- 7.6.9. Manter controles internos eficazes, conduzindo procedimentos de resposta aos riscos;
- 7.6.10. Garantir a conformidade dos controles dos processos sob sua responsabilidade;

CAPÍTULO 7 - ATRIBUIÇÕES E RESPONSABILIDADES

- 7.6.11. Comunicar à Unidade de Riscos sobre alterações de processo em virtude de legislação, regulação ou qualquer outro evento que possa impactar na classificação do nível de risco avaliado, ou quando necessitar de apoio na priorização do mapeamento dos riscos do processo;
- 7.6.12. Atuar na primeira linha de defesa, com a implementação de ações corretivas para resolver deficiências em processos e controles; e
- 7.6.13. Gerar e reportar informações adequadas sobre o gerenciamento de riscos e controles internos à Unidade de Riscos.





08

COMPROMISSOS E PENALIDADES



CAPÍTULO 8 - COMPROMISSOS E PENALIDADES

- 8.1. Todos os abrangidos por esta Política deverão assinar o Termo de Ciência e Compromisso com o Programa de Integridade e instrumentos normativos, conforme o caso.
- 8.2. O descumprimento desta Política por seus abrangidos é considerado infração e poderá acarretar a aplicação de sanções previstas nos regramentos corporativos e dispositivos contratuais.
- 8.3. Esta Política de Gestão de Riscos e Controles internos, juntamente com o Programa de Integridade, Código de Conduta Ética e de Integridade e outros, compõem o conjunto de normativos da Postal Saúde que tratam de atitudes e comportamentos exigidos de todos aqueles por eles abrangidos, devendo ser rigorosamente observados.





09

DAS DISPOSIÇÕES GERAIS



CAPÍTULO 9 - DAS DISPOSIÇÕES GERAIS

- 9.1. Caso haja alguma dúvida relacionada às diretrizes e condutas a serem adotadas nesta Política, deverá ser consultada a unidade responsável pela Gestão de Riscos da Postal Saúde.
- 9.2. A ocorrência de qualquer violação ou suspeita de violação das disposições desta Política deverá ser comunicada por meio do Canal de Denúncias, que permite o tratamento adequado das comunicações de irregularidades identificadas de maneira segura e anônima.
- 9.3. A Postal Saúde manterá um plano de treinamento periódico e constante para os abrangidos com o intuito de divulgar e conscientizar sobre a importância do cumprimento das regras desta Política.
- 9.4. Os dados, as informações e os documentos produzidos no âmbito da Gestão de Riscos são documentos de caráter sigiloso, devendo ser mantidos apenas no âmbito da Operadora e sob conhecimento dos responsáveis.
 - 9.4.1 A divulgação de qualquer dado, informação e /ou documento de Gestão de Riscos deve ser autorizado pela Unidade de Riscos, que levará a questão para deliberação das instâncias superiores, quando necessário.



DOS 10 **DOCUMENTOS** **ASOCIADOS**



CAPÍTULO 10 - DOS DOCUMENTOS ASSOCIADOS

DOS DOCUMENTOS EXTERNOS

- ISO 31.000;
- ISO 31.010;
- RN ANS 443/2018;
- COSO ERM;
- Modelo das Três Linhas do IIA 2020 – uma atualização das três linhas de defesa;
- Instrução Normativa Conjunta MP/CGU 01/2016;
- Manual de Gestão de Riscos da Agência Nacional de Saúde Suplementar.

DOS DOCUMENTOS INTERNOS

- Manual de Gestão de Riscos e Controles Internos.



Caixa de Assistência e Saúde dos Empregados dos Correios

SBN, Quadra 1, Bloco F - 5º e 6º andares, Edifício Palácio da Agricultura

Asa Norte - Brasília/DF

CEP: 70040-908

ANS - nº 41913-3

www.postalsaude.com.br