Política de Gestão de Riscos e Controles Internos

Postal Saúde
Sua vida, nossa existência

POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS	
Unidade Administrativa Gestora (UAG) do Instrumento Normativo	• Presidência **(PRESI)** • Gerência de Compliance e Riscos **(GECRI)**
Unidade Administrativa Gestora (UAG) pela Análise Técnica Administrativa e Padronização do Instrumento Normativo	• Presidência **(PRESI)** • Gerência de Compliance e Riscos **(GECRI))**
Unidade Administrativa Gestora (UAG) pela Conformidade Legal do Instrumento Normativo	• Presidência **(PRESI)** • Gerência Jurídica **(GEJUR)**
Numeração	**POL 011**
Versão	002
Macroprocesso	Gerenciar a Estratégia e Governança Corporativa
Data da Apreciação pela DIREX	DIREX Nº 404 de 18 de setembro de 2024
Data da Aprovação CODEL	CODEL Nº 225 de 25 de setembro de 2024
Data de Publicação	**09/10/2024**
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

LISTA DE FIGURAS

CAPÍTULO 1 - DO OBJETIVO

1.1. Estabelecer diretrizes para orientar a Gestão de Riscos e Controles Internos da Postal Saúde, disseminando a cultura da gestão de riscos e o ambiente de controle, fortalecendo a governança corporativa e fornecendo subsídios para o tratamento adequado dos riscos e a tomada de decisões de forma segura.

CAPÍTULO 2 - DA ABRANGÊNCIA

2.1. Esta Política abrange todos os colaboradores da Postal Saúde, sejam eles próprios ou cedidos, além de pessoas e empresas com as quais a Postal Saúde tenha ou venha a ter relacionamento direto ou indireto, e aos que atuam a serviço ou em seu nome, tais como prestadores de serviços, fornecedores e parceiros dentre outros.

CAPÍTULO 3 - DOS CONCEITOS E DEFINIÇÕES

Ambiente de controle: conjunto de normas, processos e estruturas-base para a governança da Postal Saúde, incluindo a condução da gestão de riscos e de controles internos.

Apetite a risco: nível de risco que a Postal Saúde está disposta a aceitar para alcançar sua missão e visão, e gerar valor às partes interessadas.

Cadeia de Valor: instrumento indicativo da forma como as atividades, processos e negócios estão organizados no âmbito da Postal Saúde, de modo a gerar valor às partes interessadas, tais como, mas não apenas, fornecedores, colaboradores, órgãos reguladores e beneficiários.

Controles internos: conjunto de medidas adotadas pela Postal Saúde no âmbito de suas operações para salvaguardar suas atividades em prol do cumprimento das atividades necessárias para o alcance de seus objetivos e satisfação de suas obrigações em todos os níveis.

***Committee of Sponsoring Organizations of the Treadway Commission* - COSO**: entidade sem fins lucrativos dedicada à melhoria contínua da confiabilidade dos dados apresentados nas demonstrações financeiras, por meio da ética, efetividade dos controles internos e governança corporativa, que desenvolveu, em 1992, o *framework* "*Internal Control - Integrated Framework*", posteriormente revisado e relançado no ano de 2013, o qual se tornou referência mundial para o estudo e a aplicação de controles internos efetivos.

Dono do risco: gestor responsável primariamente pelo processo operacional, atividade, departamento, projeto ou entidade que deve gerenciar os riscos de forma disciplinada e integrada, em conformidade com a Política de Riscos da Postal Saúde.

Fator de risco: evento interno e/ou externo que pode causar a materialização do risco, normalmente com atração de consequências prejudiciais para a Postal Saúde.

Gestão de riscos: conjunto de atividades proativas, integradas e estruturadas para análise, avaliação, priorização, tratamento e monitoramento de riscos que podem impactar a capacidade de a Postal Saúde alcançar seus objetivos, sejam eles estratégicos, corporativos e/ou operacionais.

Impacto: resultado ou efeito da materialização do risco que pode afetar adversamente a capacidade de a Postal Saúde alcançar seus objetivos estratégicos, corporativos e/ou operacionais. Os impactos (ou as consequências) podem ser expressos qualitativa e/ou quantitativamente, em dimensões financeira, de imagem entre outras.

Matriz de Controle: documento que relaciona os atributos (objetivo, ação e descrição, evidência e periodicidade) dos controles internos existentes em um processo.

Matriz de Riscos: instrumento de gestão que visa expor de forma explícita e de fácil acesso os riscos e os fatores de riscos do objeto avaliado, em prol de permitir a avaliação da respectiva magnitude, com base nas métricas de probabilidade e de impacto, com vistas à identificação do melhor tratamento para manutenção de sua extensão dentro dos níveis aceitáveis de risco da entidade, à luz do apetite a riscos pré-definido.

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.

Processos Operacionais: conjunto de atividades integradas de forma lógica com o objetivo de transformar dados, informações, documentos, serviços em dados, informações, documentos e/ou serviços com valor agregado. Os processos possibilitam a condução das ações, decisões e recursos em direção aos objetivos estratégicos, corporativos e/ou operacionais.

Probabilidade: instituto indicativo de alta possibilidade de ocorrência de determinado evento. Pode ser expressa em termos quantitativos, como percentagem, frequência de ocorrência ou outra métrica numérica, ou, ainda, em termos qualitativos.

Risco: elemento indicativo da possibilidade de ocorrência de determinado evento capaz de afetar negativamente o alcance dos objetivos estratégicos, corporativos e/ou operacionais da Postal Saúde.

Risco de integridade: elemento indicativo da possibilidade de ocorrência de determinado resultado relacionado com atos de violação do Código de Conduta, Ética e Integridade e, consequentemente, dos valores morais da Postal Saúde. A violação pode estar associada a ação ou omissão, a exemplo de assédio, fraude, corrupção, suborno e outros correlatos.

Risco de mercado: elemento indicativo da possibilidade de ocorrência de determinado resultado associado a incerteza ligada à exposição a perdas decorrentes da volatilidade dos preços de ativos, tais como cotações de moedas e de ações mobiliárias, taxas de juros e preços de imóveis dentre outros.

Risco estratégico: elemento indicativo da possibilidade de ocorrência de determinado resultado diretamente coligado com os objetivos estratégicos da Postal Saúde, assim entendidos aqueles constantes do planejamento estratégico em vigor.

Risco financeiro: elemento indicativo da possibilidade de ocorrência de determinado resultado em decorrência de transações financeiras e operações de investimentos, sejam os agentes pessoa física ou jurídica.

Risco legal: elemento indicativo da possibilidade de ocorrência de determinado resultado proveniente do não-cumprimento de leis, normas, regulamentações, acordos, práticas vigentes ou padrões éticos aplicáveis, considerando, inclusive, o risco de que a natureza do produto/serviço prestado possa tornar a Postal Saúde particularmente vulnerável a litígios judiciais e a insolvabilidade.

Risco operacional: elemento indicativo da possibilidade de ocorrência de determinado resultado relacionado com os procedimentos internos da Postal Saúde, tais como perda resultante de inadequações ou falhas em processos internos, falhas causadas por pessoas e/ou por sistemas dentre outras.

Risco residual: elemento indicativo da possibilidade de ocorrência de determinado resultado que remanesça após a adoção de ações de tratamento do risco bruto.

Segregação de responsabilidade: consiste na separação das funções de autorização, aprovação, supervisão, execução, controle e contabilização. Isso para que ninguém tenha sob sua responsabilidade todas as fases essenciais de um processo operacional.

Tolerância ao risco: margem de riscos que a empresa está disposta a aceitar para além do apetite ao risco pré-definido.

Teste de controle: ação realizada para confirmar se o controle é confiável em relação a eficiência e eficácia, de forma que possa ser depositada confiança de que ele seja suficiente para manter o fator de risco dentro dos níveis de risco aceitáveis na organização.

CAPÍTULO 4 - DOS PRINCÍPIOS

4.1. Esta Política está pautada nos princípios estabelecidos no Programa de Integridade da Postal Saúde, acessível na *intranet*.

CAPÍTULO 5 - DAS DIRETRIZES

5.1 Diretrizes gerais da Gestão de Riscos e Controles internos

5.1.1 A Gestão de Riscos e Controles Internos no âmbito da Postal Saúde devem ser direcionadas a:

a) consecução do propósito, missão, visão e objetivos estratégicos da Postal Saúde;

b) salvaguarda dos interesses, reputação, marca e subsistência das atividades;

c) agregação de valor e proteção do ambiente interno;

d) integração e aperfeiçoamento contínuo dos processos organizacionais e operacionais;

e) segurança substancial e subsistente das tomadas de decisão;

f) informatização e sistematização da estrutura, infraestrutura e processos para identificar e aproveitar as oportunidades de melhoria e aperfeiçoamento dos processos, em busca dos objetivos estratégicos;

g) disseminação de informações amplas e confiáveis;

h) consideração adequada dos fatores humanos e culturais;

i) transparência, inclusão e observância das boas práticas ambientais, sociais e de governança – ESG;

j) dinamicidade, interatividade, resiliência e capacidade de reação rápida e eficaz em cenários de mudanças;

k) ampliação da adesão aos preceitos básicos de integridade e de valores éticos;

l) inovação;

m) utilização da gestão de riscos e controles internos para apoio à melhoria contínua dos processos organizacionais;

n) utilização responsável e eficiente dos recursos, com atenção à legislação e às normas dos órgãos regulatórios aplicáveis à Postal Saúde.

5.1.2 **Das diretrizes específicas de Gestão de Riscos**

5.1.2.1 A Gestão de Riscos na Postal Saúde deve ser realizada de maneira dinâmica e padronizada, permitindo que os gestores possam monitorar os aspectos relacionados aos riscos dos respectivos processos e as atividades sob sua responsabilidade.

5.1.2.2 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.

5.1.2.3 Deverão ser consideradas na execução do gerenciamento de riscos a análise de mudanças internas e externas, e avaliação de fragilidades que impactem os objetivos estratégicos da Postal Saúde para o desenvolvimento das atividades de controle.

5.1.2.4 Deverá ser assegurado o desenvolvimento contínuo de todos os atores envolvidos no gerenciamento de riscos e controles internos, de modo a qualificar suas atividades e resultados.

5.1.2.5 A atuação da Gestão de Riscos deverá ser independente e autônoma, fomentado pela Alta Administração, de modo a buscar a imparcialidade nas operações.

5.2 Metodologia para avaliação dos riscos

5.2.1 Para o desenvolvimento das atividades de gerenciamento de riscos deverá ser adotado o método estabelecido nesta Política em conjunto com o Manual de Gerenciamento de Riscos e Controles Internos.

5.2.2 A metodologia para avaliação de riscos pressupõe corpo de regras e diligências estabelecidas para realizar determinada pesquisa em prol de (i) identificar, (ii) avaliar/mensurar, (iii) tratar e (iv) monitorar os riscos a que a Postal Saúde possa estar exposta e que sejam, ou possam vir a ser, empecilho para o alcance dos seus objetivos.

5.2.3 A definição de metodologia de avaliação de riscos está diretamente relacionada com a sustentabilidade e sucesso da Postal Saúde, e visa permitir o mapeamento e tratamento dos riscos de forma sistemática, objetivando subsidiar a tomada de decisões mais assertivas e eficientes em relação aos seus objetivos.

5.3 Identificação dos Riscos

5.3.1 A identificação de riscos é fase contemplada pelo processo de gestão de riscos e pressupõe a detecção de elemento abstrato indicativo da possibilidade de ocorrência de determinado evento capaz de afetar negativamente o alcance dos objetivos da Postal Saúde. Deve-se, nessa fase, identificar os respectivos fatores de riscos, ou seja, fatos geradores dos riscos, os quais devem compor a Matriz de Riscos institucional, para serem analisados e tratados com o intuito de serem mitigados, e então monitorados.

5.3.2 A fase de identificação de riscos visa, dentre outros pontos, refinar o objeto que será avaliado. Esse objeto pode se relacionar com os objetivos estratégicos da Postal Saúde, com uma diretriz corporativa ou com um processo operacional. Nesse momento é imprescindível se obter o máximo de informações acerca do objeto.

5.3.3 Os riscos são identificados com base nos objetivos obtidos por meio de entrevista com a área gestora ou por meio do mapeamento de processos. Deve-se, nessa etapa, identificar e relacionar os riscos inerentes à própria atividade da Postal Saúde, em seus diversos níveis, e correlacionar os fatores de risco, a probabilidade de ocorrência, os impactos previstos e os responsáveis por cada risco.

5.3.4 Para cada risco identificado, o dono do risco deve apontar as respectivas causas (fatores de risco). Pode haver mais de uma causa, ou seja, fator de risco, para cada risco. Por isso, o avaliador, seja o dono do risco ou o profissional da área de gerenciamento de riscos, deve ser crítico e criterioso.

5.3.5 A identificação dos riscos pode acontecer de forma global, a partir da análise geral dos processos internos diante dos objetivos estratégicos da Postal Saúde, ou de forma isolada, a

partir de eventos ocorridos que indiquem pré-disposição a constituição de novos fatores de riscos com potencialidade de materialização de riscos.

5.3.6 As categorias que compõem o processo de gestão de riscos no âmbito da Postal Saúde são, essencialmente:

a. Riscos estratégicos
b. Riscos corporativos
c. Riscos operacionais (processos)
d. Riscos legais (conformidade/integridade)
e. Riscos de mercado
f. Riscos financeiro
g. Riscos de imagem

5.4 Avaliação dos Riscos

5.4.1 Após a identificação dos riscos e dos fatores de riscos, torna-se necessário analisá-los qualitativa e quantitativamente, utilizando as métricas de probabilidade e de impacto aprovadas pela Alta Administração. Trata-se da segunda etapa do processo de gerenciamento de riscos.

5.4.2 Essa atividade requer que o responsável pelo risco determine a frequência possível do evento, utilizando base de informações históricas da Postal Saúde ou do mercado, e que indique o hipotético impacto para as correspondentes dimensões definidas na Matriz de Riscos.

5.4.3 A partir da análise e dimensionamento do risco bruto, contrapor-se-á ao apetite a riscos aprovado para a Postal Saúde, de forma a estabelecer os melhores parâmetros para o consequente tratamento.

5.5 Tratamento dos Riscos

5.5.1 O tratamento do risco é etapa crucial do gerenciamento de riscos da Postal Saúde, e componente principal da terceira fase do processo. É no contexto do tratamento que se decide sobre as ações que recairão sobre os fatores de riscos com base nas probabilidades de ocorrência e/ou de impacto, com o objetivo de prevenir a probabilidade de ocorrência ou, pelo menos, de minimizar o impacto, acaso o risco venha a se materializar.

5.5.2 O tratamento dos riscos no âmbito da Postal Saúde admite quatro possibilidades básicas, quais sejam:

5.5.2.1 **Aceitar os riscos**, hipótese que se desdobra em outras duas possibilidades: a primeira se relaciona à magnitude do risco diretamente atrelado ao apetite a riscos pré-definido; a segunda se vincula ao custo do tratamento do risco, que pode vir a ser maior do que o impacto que a materialização do risco pode trazer, se ocorrer.

5.5.2.2 **Compartilhamento e/ou transferência**, que consiste na divisão ou repasse de responsabilidade do impacto do evento, acaso materializado, com outra instituição. Essa hipótese é utilizada quando não existe a possibilidade de mitigação da probabilidade do risco ou quando o impacto, após o tratamento de mitigação, continua elevado. O compartilhamento e/ou transferência do risco pode ser verificado a partir de contratos de seguro, de *hedge* e afins.

5.5.2.3 **Evitar**, cuja medida perpassa por ações capazes de eliminar a exposição da Postal Saúde aos fatores de riscos. Se trata de decisão estratégica que pode envolver, por exemplo, o cancelamento de projetos, saída do mercado, encerramento de atividades, venda de operações entre outras.

5.5.2.4 **Mitigar**, cuja ação é o tratamento mais presente nas organizações de forma geral. Consiste na implementação de uma ou mais ações de controle com o objetivo de diminuir a probabilidade de o evento de risco se materializar.

5.6 Monitoramento dos Riscos

5.6.1 A fase de monitoramento dos riscos é a quarta fase do processo de gerenciamento de riscos, e visa o aprimoramento contínuo da gestão de riscos e de fatores de riscos. Nela estão incluídas as atividades de acompanhamento do desempenho dos indicadores de gestão, supervisão da implantação e manutenção dos planos de ação correlatos, verificação do alcance das metas estabelecidas e avaliação da eficácia do tratamento conferido.

5.6.2 Os resultados da identificação e avaliação dos riscos devem ser informados à unidade administrativa responsável pela gestão de riscos, que os registrará e reportará à Alta Administração da Postal Saúde.

5.7 Apetite a Riscos

5.7.1 Periodicamente, ou sempre que necessário, os Órgãos Colegiados da Postal Saúde devem analisar e estabelecer, conforme competências, o apetite e a tolerância a riscos a que a organização deve/pode estar submetida na busca de seus objetivos estratégicos.

5.7.2 Os estudos para subsidiar a definição do apetite e da tolerância a riscos deverão ser conduzidos pela unidade administrativa responsável pelo gerenciamento de riscos e controles internos e aprovados pela Diretoria-Executiva e pelo Conselho Deliberativo. Essa aprovação deve ser amplamente divulgada no âmbito da Postal Saúde.

5.7.3 A definição dos níveis de tolerância e do apetite a riscos deverá estar alinhada às estratégias institucionais da Postal Saúde e servirão de suporte à tomada de decisão.

5.8 Das diretrizes específicas dos Controles Internos

5.8.1 Gerenciamento dos Controles Internos

5.8.1.1 Os controles internos permitem o monitoramento contínuo dos processos operacionais, bem como dos riscos de não conformidade, de acordo com as políticas e outras normas estabelecedoras de limites impostos pelos Órgãos Colegiados. Esses controles visam garantir a sustentabilidade, continuidade e solvabilidade da Postal Saúde.

5.8.1.2 As atividades de controle devem ser avaliadas regularmente, com base nas melhores práticas de Governança Corporativa estabelecidas pelos padrões e metodologias do COSO IC, normativos internos e externos.

5.9 Estrutura de Controles Internos

5.9.1 A estrutura de controles internos deve assegurar a mitigação dos fatores de riscos decorrentes de todas as atividades operacionais e identificados na Matriz de Riscos que possam afetar adversamente a realização dos objetivos do processo, projeto ou da Postal Saúde.

5.9.2 Deve-se garantir que os objetivos estabelecidos pela Alta Administração estejam alinhados com a estrutura de controles internos. As descrições dos controles internos devem ser acessíveis a todos os funcionários e compreender ações contínuas relativas às suas atividades, operações e níveis hierárquicos, prevendo, no mínimo:

a) a definição dos objetivos dos controles e das responsabilidades inerentes, de forma a evitar conflito de interesses nos processos internos;

b) os meios de identificação e avaliação das fragilidades que possam ameaçar sua eficiência e eficácia;

c) canais de comunicação que assegurem aos colaboradores acesso às informações relevantes para a execução de suas tarefas e responsabilidades, bem como o encaminhamento de contribuições para seu aperfeiçoamento;

d) existência de testes de segurança e conciliação para os sistemas de informações, em especial aqueles mantidos em meio eletrônico;

e) ações ou planos de contingência, quando necessários.

5.9.3 A partir da identificação dos controles existentes nos processos e subprocessos, deve-se associá-los aos respectivos riscos identificados na Matriz correspondente.

5.9.4 Os controles devem ser executados em conformidade com a periodicidade definida no plano de trabalho da área responsável pela gestão dos controles internos. O responsável pelo processo de onde advém o controle interno deve monitorar e supervisionar a execução desses controles e, se necessário, propor ajuste e melhoria, sempre comunicando a área gestora do processo de controles internos.

5.9.5 A área de gestão de riscos e controles deverá, periodicamente, avaliar a eficiência do controle, por meio de testes práticos realizados nos ambientes utilizados pela área gestora do processo de onde advém o controle, independentemente de agendamento prévio.

5.9.6 A auditoria interna, conforme definido em seu plano anual de auditoria, deverá realizar exames e testes para validar a eficácia do controle interno.

5.9.7 Os controles internos devem ser avaliados segundo a métrica para avaliação das características do controle, de forma a determinar o risco do controle e, com isso, se calcular o risco residual.

5.10 Fases da gestão de Controles Internos

5.10.1 A estrutura de gestão dos controles internos na Postal Saúde compreenderá cinco componentes/fases essenciais e inter-relacionados, a saber:

5.10.2 **Disponibilização de Ambiente de Controle adequado:** a Alta Administração deve promover cultura de controle interno, demonstrando compromisso com a integridade e com a ética no âmbito da organização e proporcionando, assim, um ambiente adequado para a execução das atividades gerenciais correlacionadas. O ambiente de controle fortalecido pela Alta Administração é pilar primordial para a efetividade dos controles internos e sem o qual não é possível se realizar as demais atividades de gerenciamento de controle de forma producente.

5.10.3 **Avaliação de Riscos e identificação de Controles:** a organização deve identificar e avaliar os riscos significativos que possam afetar a realização dos seus objetivos, assim como os controles instituídos, ou que possam vir a ser, em prol da mitigação dos riscos e dos fatores de riscos.

5.10.4 **Realização de testes e/ou implementação de atividades de Controle:** procedimentos específicos devem ser estabelecidos, testados e implementados para mitigar os riscos identificados. Basicamente, são controles que devem ser integrados às operações diárias da organização, com a função de diminuir as probabilidades de riscos e/ou dos impactos em potencial.

5.10.5 **Prestação de informações e comunicação institucional:** informações relevantes devem ser identificadas e prestadas aos gestores dos riscos e dos controles inerentes, bem como à Alta Administração, e disseminadas com os demais colaboradores envolvidos, para que compreendam suas responsabilidades porventura relacionadas aos controles internos.

5.10.6 **Monitoramento:** desempenho dos controles internos deve ser monitorado regularmente por meio de rotina periódica de testes e pode ser objeto de auditorias e outras avaliações. As deficiências identificadas devem ser comunicadas à Alta Administração e ações corretivas devem ser propostas e implementadas prontamente pela área gestora do processo de onde advém o risco e controle, com o apoio do setor responsável pelo gerenciamento de controles internos.

5.11 Documentação de Controles Internos

5.11.1 A documentação dos controles internos deve ser formalizada através de uma Matriz de Controles Internos, a qual deve ser estruturada de forma a garantir a acessibilidade das informações necessárias à avaliação e entendimento de cada caso.

5.11.2 A Matriz de Controles Internos deve conter, pelo menos, as seguintes informações: (i) macroprocesso, (ii) processo, (iii) subprocesso, (iv) objetivo do controle, (v) ação de controle, (vi) descrição da ação de controle, (vii) nome da evidência, (viii) local de localização da evidência, (ix) periodicidade da realização do controle, (x) característica do controle executado, (xi) risco(s) atrelado(s) ao controle, conforme métrica aprovada, (xii)dono do risco e do controle e (xiii) periodicidade de teste recomendada.

5.11.3 Os registros na Matriz de Controles Internos devem ser atualizados pelo gestor responsável, revisados e validados pela área de gestão de riscos e controles internos.

5.11.4 Os Controles Internos devem estar identificados no fluxograma do processo, de forma a certificar o entendimento compreensivo de todo o sistema de controle interno da organização.

5.11.5 Os procedimentos e normativos institucionais devem orientar a forma e execução das atividades de controle. Toda e qualquer atualização no sistema de controle deve resultar na atualização dos procedimentos e normativos correlatos.

CAPÍTULO 6 - DAS INSTÂNCIA DE SUPERVISÃO

6.1. As Instâncias de Supervisão têm como função essencial apoiar e dar suporte aos diversos níveis hierárquicos da Postal Saúde e de 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 processo, conforme representação a seguir:

Figura 1 – Modelo de três linhas

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

6.3. A primeira linha é composta por todos os colaboradores da Postal Saúde que possuem parcela de responsabilidade sobre a Gestão de Riscos e Controles Internos, bem como os Líderes de Riscos e os Gestores dos Riscos, os quais são os responsáveis primários pelo gerenciamento de um processo de trabalho, projeto ou produto em seus respectivos âmbitos e escopos de atuação, de onde se extraia riscos e controles, e que têm propriedade sobre os riscos e controles correlatos.

6.4. A segunda linha é composta pela unidade administrativa gestora dos Riscos e Controles Internos no âmbito da organização como um todo, que tem em seu escopo de atuação o objetivo precípuo de apoiar a 1ª linha e a responsabilidade de auxiliar na implantação de métodos de gerenciamento de riscos e de controles internos segundo as diretrizes da Alta Administração.

6.5. A terceira linha é composta pela Auditoria Interna, de forma independente.

6.5.1. 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.

6.6. Os Órgãos Colegiados da Postal Saúde, quais sejam, Conselho Fiscal, Conselho Deliberativo e Diretoria Executiva são os órgãos de governança, aos quais as três linhas se reportam direta ou indiretamente e os responsáveis primários por estabelecer diretrizes e fortalecer a cultura de gestão de riscos, controles e integridade.

CAPÍTULO 7 - DAS ATRIBUIÇÕES E RESPONSABILIDADES

7.1 Conselho Deliberativo

a) estabelecer diretrizes gerais e promover a integração das práticas de gestão de riscos e controles internos relativas ao processo decisório;
b) incentivar e patrocinar a conscientização e de desenvolvimento de cultura organizacional pautada na importância do gerenciamento de riscos e controles internos para a efetividade e fortalecimento da governança corporativa;
c) aprovar a Política de Gestão de Riscos e Controles Internos, assim como as suas revisões;
d) aprovar as métricas de riscos a serem utilizadas para avaliação da probabilidade e impacto;

e) aprovar o apetite a riscos da Postal Saúde, bem como a priorização dos riscos, segundo os objetivos estratégicos da organização;
f) zelar pela perenidade e sustentabilidade da Postal Saúde, incorporando os aspectos de ordem econômica, social, ambiental e de boas práticas de governança corporativa na definição dos negócios e operações;
g) conhecer do relatório de gestão de riscos e controles internos submetidos pela Diretoria-Executiva e sobre ele deliberar;
h) patrocinar a implantação e manutenção da rotina de gestão de riscos e controles internos no âmbito da Postal Saúde.

7.2 Conselho Fiscal

a) fiscalizar os atos dos administradores, verificando o cumprimento dos deveres legais e estatutário, incluindo o acompanhamento dos riscos e controles institucionais;
b) examinar as demonstrações financeiras do exercício social e dar seu parecer sempre que solicitado;
c) denunciar formalmente à Diretoria Executiva e/ou ao Conselho Deliberativo e, se for o caso à Mantenedora e Patrocinadoras, os erros, fraudes ou crimes que vier a constatar na gestão de riscos e controles internos da Postal Saúde.

7.3 Diretoria Executiva

a) garantir a aplicação dos princípios e diretrizes desta Política de Riscos, bem como a aderência dos abrangidos em prol de proporcionar efetividade ao processo de gestão de riscos;
b) disseminar a cultura de gestão de riscos na Posta Saúde e fortalecer os papéis dos gestores em relação à sua responsabilidade no gerenciamento dos riscos das atividades e processos sob sua responsabilidade;
c) patrocinar a implantação da gestão de riscos e controles internos no âmbito de sua respectiva atuação;
d) submeter ao Conselho Deliberativo da Postal Saúde a Matriz de Riscos e as diretrizes gerais para o estabelecimento do apetite a risco, com proposta de nível aceitável de risco para a organização;
e) definir, em conjunto com a área responsável pelo processo de gerenciamento de riscos, a priorização dos riscos a serem tratados, e submeter a escala de priorização ao Conselho Deliberativo, para análise e aprovação;
f) apoiar e monitorar os gestores de riscos no estabelecimento das ações de tratamento e na definição dos mecanismos de controles para os riscos e fatores de riscos;
g) avaliar a adequação do processo de gestão de riscos, discutindo e validando, em sede colegiada ou por diretoria, as avaliações apresentadas pelos gestores/donos dos riscos e o tratamento definido para os riscos, de acordo com o apetite a risco aprovado pelo Conselho Deliberativo;
h) analisar e aprovar os relatórios de gestão de riscos submetidos ao colegiado pelo Diretor-Presidente;
i) submeter os relatórios de gestão de riscos e controles internos ao Conselho Deliberativo (CODEL) e ao Conselho fiscal (COFIS), para conhecimento e considerações;
j) proporcionar os insumos e recursos necessários à implementação e manutenção adequada da gestão de riscos e controles internos no âmbito da Postal Saúde;
k) monitorar a materialização de riscos estratégicos e reportar sua ocorrência ao Conselho Deliberativo.

7.4 Unidade Administrativa Gestora do Processo de Riscos e Controles Internos

a) apoiar as unidades Gestoras da Postal Saúde nas tarefas relacionadas ao gerenciamento de riscos e controles internos, em conformidade com as melhores práticas de gestão, atuando como facilitador do processo e acompanhando todas as fases definidas nesta Política e no Manual de Gestão de Riscos;

b) coordenar a implantação das diretrizes, políticas, metodologias e práticas de gerenciamento de riscos corporativos e controles internos na Postal Saúde;
c) instrumentalizar a gestão sobre o processo, implementar ferramentas adequadas para o gerenciamento de riscos e controles internos e coordenar sua utilização nos diversos níveis da Postal Saúde;
d) zelar pela efetiva disseminação e adequada aplicação das políticas e metodologias.
e) monitorar as ações de manutenção do processo de gerenciamento de riscos, como também o tratamento e os mecanismos de controles para os riscos identificados;
e) revisar e aperfeiçoar o processo de gerenciamento de riscos, periodicamente ou sempre que for necessário, implementando melhorias e novas formas de fortalecer a capacidade de a Postal Saúde alcançar seus objetivos;
f) mapear os riscos e fatores de risco da Postal Saúde e criar mecanismos de monitoramento e gerenciamento, segundo as diretrizes da diretoria executiva e do conselho deliberativo;
g) instruir e apoiar o gestor do risco e dos controles na implementação das ações voltadas à contenção dos fatores de risco;
h) elaborar relatórios de riscos e controles internos e submeter à Diretoria Executiva e ao Conselho Deliberativo da Postal Saúde em periodicidade não superior a um ano, ou sempre que requisitado;
i) realizar a capacitação dos gestores e demais colaboradores da Postal Saúde em Gestão de Riscos e Controles Internos, de forma continuada;
j) assegurar que as informações e orientações correlatas ao gerenciamento de riscos e controles internos estejam disponíveis e acessíveis a todos os colaboradores da Postal Saúde;
k) disseminar a cultura de gestão de riscos e controles internos, no que couber, no âmbito da Postal Saúde;
l) criar, analisar e propor mecanismos de controles internos advindos do gerenciamento de riscos, visando reduzir conflitos de informação e interesses, otimizar recursos e auxiliar eficientemente a tomada de decisão.

7.5 Auditoria Interna

a) avaliar a efetividade do processo de gestão de riscos e controles internos em todos os níveis da Postal Saúde e em conformidade com o plano anual de auditoria, aprovado pelo Conselho Deliberativo;
b) avaliar a adequação das ações de tratamento e mecanismos de controles internos, recomendando, quando necessário, implementação de planos de ação voltados para a melhoria dos processos.

7.6 Dono do Risco

a) assegurar que o processo de gerenciamento de riscos e controles internos seja compreendido e observado por todos os membros de sua equipe, e que eles estejam cientes e engajados quanto às ações necessárias ao fortalecimento da governança corporativa no âmbito da Postal Saúde;
b) identificar os riscos e fatores de riscos associados aso processos de sua responsabilidade, as causas de riscos e os seus impactos para a Postal Saúde e tratá-los forma contemporânea e eficaz;
c) instituir, monitorar e adequar as ações de tratamento de riscos e os controles internos de seus processos, de modo que estejam adequados e suficientes para a mitigação de riscos e de fatos de riscos no contexto de sua área de atuação;
d) realizar as revisões de processos, em conjunto com a unidade administrativa gestora de processos, sempre que alguma rotina tiver que sofrer alteração;
e) reportar, seguindo a metodologia e os padrões definidos institucionalmente, todos os riscos e fatores de riscos associados aos processos de sua incumbência, assim como os controles internos instituídos, à unidade administrativa responsável pelo processo de Gestão de Riscos e Controles Internos;
f) dar acesso irrestrito de seus processos e procedimentos à área de Gestão de Riscos e Controles Internos sempre que requisitado, para o fim de realização de testes;

g) atender às recomendações da área responsável pela Gestão de Riscos e Controles Internos, bem como às solicitações de reuniões, entrevistas, subsídios e afins.

CAPÍTULO 8 - DO COMPROMISSO E PENALIDADES

8.1 Todos os abrangidos por esta Política deverão assinar o Termo de Ciência e Compromisso com o Programa de Integridade da Postal Saúde.

8.2 O descumprimento desta Política por seus abrangidos é considerado infração disciplinar e poderá acarretar a aplicação de sanções, segundo o Código de Conduta, Ética e Integridade e Política de Consequências.

CAPÍTULO 9 - DAS DISPOSIÇÕES GERAIS

9.1 Caso haja alguma dúvida relacionada às diretrizes e condutas a serem adotadas nesta Política, deve-se consultar a unidade responsável pela Gestão de Riscos e Controles Internos 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.

9.3 A Postal Saúde manterá um plano de treinamento periódico e constante para os abrangidos, com o intuito de divulgar e conscientizar a todos sobre a importância do cumprimento das regras desta Política.

9.4 Os dados, informações e documentos produzidos no âmbito da Gestão de Riscos e Controles Internos são documentos de caráter sigilosos, que devem ser mantidos sob domínio exclusivo da Postal Saúde.

9.5 A divulgação de qualquer dado, informação e /ou documento de Gestão de Riscos e Controles Internos deve ser autorizado pela unidade responsável pela Gestão de Riscos e Controles Internos, que poderá levar a questão para deliberação das instâncias superiores.

9.6 O presente documento deve ser lido conjuntamente com os demais instrumentos de governança e de procedimentos aplicáveis, especialmente daqueles relacionados a fraudes, corrupção, ética e disciplina.

9.7 Casos omissos devem ser submetidos à unidade responsável pela Gestão de Riscos e Controles Internos para apreciação e encaminhamentos pertinentes.

CAPÍTULO 10 - DOS DOCUMENTOS ASSOCIADOS

DOS DOCUMENTOS EXTERNOS

- Lei nº 12.846/2013 – Lei Anticorrupção. Que "Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências".
- Decreto nº 11.129/2022, que "Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira".
- Resolução Normativa – RN/ANS nº 518/2022, 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".

- COSO – ERM: 2017: Committee of Sponsoring Organizations od the Treadway Commission – Enterprise Risk Management – Integrated Framework.
- Norma ABNT Standard NBR ISO 31000:2018 – Gestão de Riscos: Diretrizes;
- Manual de Gestão de Riscos da Agência Nacional de Saúde Suplementar.

DOS DOCUMENTOS INTERNOS

- Estatuto Social da Postal Saúde.
- Matriz de Atribuição.
- Manual de Gestão de Riscos e Controles Internos.
- Código de Conduta, Ética e Integridade da Postal Saúde.

CAPÍTULO 11 - DO CONTROLE DAS REVISÕES

Versão	Data	Descrição da Revisão	Responsável
001	30/06/2021	**RES/DIREX 006/252 - Aprovação da Política de Gestão de Riscos e Controles Internos - VOTO PRESI 038/2021.** A Diretoria-Executiva apreciou o VOTO PRESI 038/2021, de 04 de junho de 2021, e, após apresentação do Sr. José Orlando Ribeiro Cardoso, Diretor-Presidente, em conjunto com a Sra. Clarice de Souza Coutinho de Moura Alves, Gerente de Compliance, Riscos e Controles Internos, por unanimidade, decidiu: a) aprovar a Política de Gestão de Riscos e Controles Internos nos termos do PTA GECRI 005/2021; b) encaminhar ao Conselho Deliberativo (CODEL) para deliberação; c) após aprovação do CODEL, encaminhar a matéria para a Gerência de Estratégia e Inteligência Organizacional (GEORG), para publicação. **RES/CODEL 01/148 - Aprovação da Política de Gestão de Riscos e Controles Internos - VOTO PRESI - 041/2021.** O Conselho Deliberativo apreciou o VOTO PRESI 041/2021, de 21 de junho de 2021, e, após apresentação e explanação da matéria realizada pelo Sr. José Orlando Ribeiro Cardoso, Diretor-Presidente, em conjunto com a Sra. Clarice de Sousa Coutinho de Moura Alves, Gerente de Compliance, Riscos e Controles Internos, por unanimidade, decidiu: aprovar a Política de Gestão de Riscos e Controles Internos nos termos do PTA PRESI/GECRI - 005/2021. **Vigência a partir de: 08/07/2021**	Clarice de Souza Coutinho de Moura Alves
001	15/09/2021	Revisão 1 - 15/09/2021 Conforme fragilidades apontadas pela Auditoria Interna, houve uma atualização da	Lucas Sampaio

		página nº2 quanto as datas e numeração das reuniões de apreciação da Diretoria-Executiva e Conselho Deliberativo.	
002	10/10/2024	**RES/DIREX 04/404 -** Política de Riscos e Controles Internos – A Diretoria-Executiva apreciou o VOTO DIREX/PRESI 038/2024, de 17 de setembro de 2024, dispensou a apresentação e aprovou, por unanimidade: a) as alterações propostas para a POL 011 – Política de Gestão de Riscos e Controles Internos **RES/CODEL 225/2024 -** O Conselho Deliberativo da Postal Saúde, no uso de suas atribuições estatutárias e fundamentado na RD-004/404/2024, de 17.09.2024, e na exposição feita pelo relator, RESOLVE: 1. Aprovar a Política de Gestão de Riscos e Controles Internos, nos moldes do VOTO DIREX/PRESI - 038 /2024, de 17/09/2024. **Vigência a partir de: 10/10/2024**	Verônica Conceição Martins

Postal Saúde

Sua vida, nossa existência

www.postalsaude.com.br