PROGRAMA
PROGRAMA DE COMPLIANCE

APRESENTAÇÃO

A Postal Saúde reafirma seu compromisso com a ética, a integridade, a transparência e o cumprimento das leis e regulamentos que regem suas atividades.

O Programa de Compliance constitui instrumento essencial para a sustentabilidade institucional, o fortalecimento da governança e a preservação da confiança dos nossos colaboradores, beneficiários, parceiros e da sociedade.

A Alta Administração acredita que a conformidade normativa e a conduta ética devem permear todas as decisões e relações institucionais. Por isso, apoia e incentiva a ampla divulgação deste Programa, bem como o engajamento de todos na consolidação de uma cultura organizacional pautada pela integridade.

Contamos com a participação ativa de cada colaborador e terceiro para o cumprimento das diretrizes aqui estabelecidas e para o contínuo aprimoramento do nosso ambiente de controle e governança.

1 DO OBJETIVO

1.1. O Programa de Compliance da Postal Saúde tem por objetivo estabelecer um conjunto estruturado de mecanismos de integridade, composto por diretrizes, políticas, procedimentos internos e ações baseadas em valores éticos, destinados à adequada gestão dos riscos de integridade, regulatórios e reputacionais, assegurando a conformidade com leis, regulamentos, normas internas e princípios aplicáveis.

1.2. O Programa visa prevenir, detectar e remediar atos ilícitos, promover a cultura de ética e integridade e assegurar a sustentabilidade institucional e a confiança dos públicos de relacionamento.

2 DA ABRANGÊNCIA

2.1. Aplica-se a todos os colaboradores da Operadora, sejam eles próprios, cedidos, estagiários ou menores aprendizes, de todas as unidades intervenientes, independente de cargo ou função exercidos, bem como os Administradores da Operadora, compreendidos aqui os membros da Diretoria Executiva e os membros do Conselho Fiscal e Deliberativo.

3 DOS PRINCÍPIOS

3.1. O Programa de Compliance fundamenta-se nos seguintes princípios:

3.1.1. **Boa-fé**: obrigação de se agir com lealdade, sinceridade, respeito e transparência, por todas as partes interessadas;

3.1.2. **Comprometimento**: consiste no envolvimento e responsabilização da Alta Administração, dos gestores e de todos os colaboradores com a implementação da presente política e com o aperfeiçoamento contínuo das sanções aplicáveis;

3.1.3. **Conformidade**: cumprimento da legislação e regulamentação aplicáveis, bem como das normas e políticas internas da Operadora;

3.1.4. **Eficiência**: oferecer o melhor serviço possível preservando os recursos disponíveis;

3.1.5. **Equidade**: igualdade de direitos, julgamento justo e imparcial;

3.1.6. **Ética**: observância de valores e princípios que orientam comportamentos responsáveis e íntegros;

3.1.7. **Impessoalidade**: utilização de critérios técnicos e objetivos, sem discriminações, privilégios ou emprego de subjetividade tendenciosa associada a aspectos de cunho pessoal.

3.1.8. **Integridade**: atuação pautada pela honestidade, probidade e retidão na condução das atividades profissionais;

3.1.9. **Prestação de contas (accountability)**: obrigação de gestores e colaboradores de assumir responsabilidade por suas decisões e ações, assegurando a adequada justificativa e rastreabilidade dos atos praticados;

3.1.10. **Proporcionalidade**: orienta a adoção de medidas de prevenção, detecção e resposta a irregularidades de forma equilibrada, evitando excessos e garantindo que os recursos sejam empregados de maneira eficiente e racional;

3.1.11. **Responsabilidade**: reconhecimento de que todos os colaboradores são responsáveis pela observância das normas de compliance e pela condução ética de suas atividades;

3.1.12. **Transparência**: disponibilização de informações claras, completas e atualizadas. A Operadora compromete-se com a divulgação transparente de informações institucionais relevantes por meio de seu Portal de Governança.

3.1.13. **Cultura de Integridade:** promoção contínua de comportamentos éticos por meio de ações estruturadas de engajamento, comunicação e incentivo à conduta responsável em todos os níveis da organização.

4 DAS COMPETÊNCIAS

4.1. O Programa de *Compliance* está sob gestão da Unidade de *Compliance* e Riscos, que tem as atribuições elencadas na Matriz de Atribuições da Operadora.

4.1.1. Unidade de *Compliance* e Riscos

4.1.1.1. Estruturar, implementar e manter o Programa.

4.1.1.2. Identificar e monitorar riscos.

4.1.1.3. Elaborar e revisar políticas e normas internas de Compliance.

4.1.1.4. Promover treinamentos e ações de conscientização.

4.1.1.5. Monitorar o Canal de Denúncias.

4.1.1.6. Reportar informações relevantes à Alta Administração.

4.1.1.7. Atuar com autonomia técnica e independência, com acesso irrestrito às informações necessárias para o desempenho de suas atribuições.

4.2 Para o cumprimento das suas atribuições, a Unidade de *Compliance* atua de forma integrada com outras áreas, com destaque para:

4.2.1. Alta Administração

4.2.1.1. aprovar formalmente o Programa de *Compliance.*

4.2.1.2. apoiar sua implementação e aperfeiçoamento contínuo.

4.2.1.3. promover a disseminação de valores éticos e de *Compliance.*

4.2.1.4. incentivar práticas de gestão baseadas em gerenciamento de riscos.

4.2.1.5. estimular o uso responsável do Canal de Denúncias.

4.2.1.6. assegurar recursos necessários à manutenção do Programa.

4.2.1.7. adotar medidas adequadas diante de violações às normas internas ou à legislação.

4.2.2 Comitê de Ética e Disciplina

4.2.2.1. orientar a Operadora sobre questões relacionadas à ética e à conduta.

4.2.2.2. supervisionar o funcionamento do Canal de Denúncias.

4.2.2.3. acompanhar investigações internas decorrentes de denúncias ou indícios de irregularidades.

4.2.2.4. propor medidas disciplinares quando constatadas violações.

4.2.2.5. apoiar a Alta Administração na tomada de decisões relacionadas à integridade e à disciplina institucional.

4.2.3 Unidades Administrativas Gestoras

4.2.3.1. Ter conhecimento das diretrizes previstas do Programa de *Compliance.*

4.2.3.2. Cumprir e disseminar normas de *Compliance.*

4.2.3.3. Reportar riscos e irregularidades à Unidade de Compliance e Riscos.

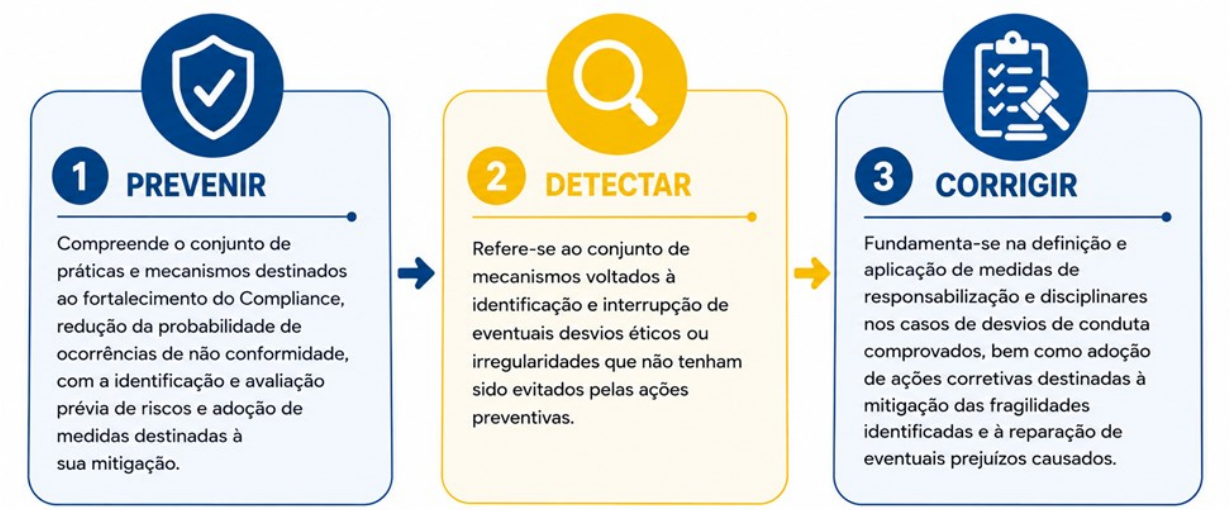
5 DA ESTRUTURA DO PROGRAMA DE COMPLIANCE

5.1. Postal Saúde reconhece que a atuação ética, responsável e em conformidade com a legislação e regulamentação aplicáveis é essencial para a sustentabilidade institucional, a geração de valor e a preservação de sua reputação.

5.2. O Programa de *Compliance* está alinhado ao plano estratégico da Operadora, contribuindo para a sustentabilidade institucional, a mitigação de riscos e o atendimento às exigências regulatórias.

5.3. O Programa de *Compliance* fundamenta-se em três eixos estruturantes:

Figura 1 - Eixos estruturantes



Fonte: PRESI/GECRI

5.3.1. **Prevenir**: Para o desenvolvimento do presente eixo, definem-se as seguintes práticas:

a) Comprometimento e apoio da Alta Administração;

b) Instância responsável pelo Programa de *Compliance*;

c) Gestão de Riscos;

d) Regras e instrumentos de *Compliance*;

e) *Due Diligence* de Integridade; e

f) Comunicação e Treinamento.

a) Comprometimento e apoio da Alta Administração

A Alta Administração da Postal Saúde é composta pelo Conselho Deliberativo, Conselho Fiscal e pela Diretoria Executiva, sendo estes responsáveis por assegurar a efetividade do Programa de *Compliance*, conforme atribuições previstas no Estatuto Social e seus respectivos regimentos.

Os órgãos de governança reafirmam seu compromisso com a ética, a integridade, a transparência e a conformidade nas relações mantidas com os diversos públicos de relacionamento da Operadora, adotando postura de tolerância zero em relação a práticas de corrupção, fraude, suborno, conflitos de interesse e quaisquer desvios de conduta.

Além disso, os membros da Alta Administração devem acompanhar periodicamente as ações do Programa de *Compliance*, bem como declarar ostensivamente a importância dos valores da Operadora e das políticas que compõem o Programa, por intermédio de manifestações públicas explícitas, internas e externas.

b) Instância responsável pelo Programa de *Compliance*

A Unidade de *Compliance* e Riscos é a instância responsável pela gestão do Programa, competindo-lhe o acompanhamento, monitoramento e condução das ações e medidas necessárias à sua implementação, manutenção e aprimoramento.

Encontra-se subordinada administrativamente ao Diretor-Presidente, sem prejuízo de sua independência funcional, o que assegura alinhamento institucional e suporte à execução de suas atividades.

Possui acesso direto à Alta Administração, garantindo a adequada comunicação de informações relevantes, inclusive situações de risco, não conformidades e resultados de atividades de monitoramento.

A função de *Compliance* é independente das atividades operacionais e de gestão de riscos, atuando de forma autônoma na supervisão da conformidade normativa, no monitoramento de controles e no reporte à Alta Administração, sem prejuízo da atuação coordenada com a gestão de riscos corporativos.

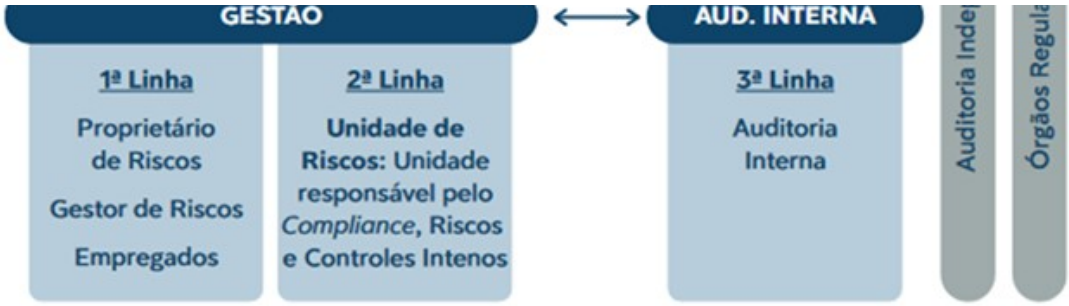
A atuação da Unidade de *Compliance* e Riscos deve ocorrer de forma isenta, imparcial e livre de conflito de interesse, assegurando a credibilidade e a efetividade do Programa.

c) Gestão de Riscos

Compete à Unidade de *Compliance* e Riscos apoiar as Unidades Administrativas Gestoras, assegurando que os riscos corporativos sejam identificados, avaliados, tratados, monitorados e reportados de forma sistemática. Essa atuação inclui a verificação da execução e efetividade dos controles internos, bem como a recomendação de ações corretivas ou preventivas, quando necessário, de modo a garantir níveis aceitáveis de exposição ao risco e alinhamento aos objetivos estratégicos da Operadora.

A Postal Saúde segue as diretrizes da ABNT NBR ISO 31000 como referência metodológica, Resolução Normativa ANS nº 518/2022; e 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 2 - Modelo de três linhas



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

I) 1ª Linha de Defesa – Gestão Operacional: Composta pelas áreas de negócio e operacionais, responsáveis pela identificação, avaliação, mitigação e monitoramento dos riscos inerentes às suas atividades, bem como pela implementação e execução dos controles internos. Compete ainda à primeira linha manter evidências dos controles executados, comunicar tempestivamente falhas identificadas e apoiar a realização de testes de efetividade dos controles.

II) 2ª Linha de Defesa – *Compliance* e Gestão de Riscos: Representada pela Unidade de *Compliance* e Riscos, responsável por estabelecer diretrizes, metodologias e ferramentas de gestão de riscos, apoiar e supervisionar a atuação da primeira linha, além de monitorar os planos de ação (gestão do *follow up*).

III) 3ª Linha de Defesa – Auditoria Interna: Responsável por avaliar de forma independente a eficácia da governança, da gestão de riscos e dos controles internos, emitindo recomendações para aprimoramento contínuo.

As três linhas de defesa devem atuar de forma coordenada e complementar, assegurando a efetividade do sistema de controles internos e a adequada gestão dos riscos da Operadora.

A metodologia de gestão de riscos deve ser aplicada a todos os processos priorizados pela Alta Administração e contempla as seguintes etapas:

- Identificação dos fatores de risco considerando cenários internos e externos;
- Mapeamento dos controles internos existentes e avaliação de sua efetividade;
- Definição de planos de ação para tratamento das lacunas identificadas, com responsáveis e prazos definidos;
- Estabelecimento de cronograma de implantação, garantindo acompanhamento contínuo e reporte estruturado.
- Monitoramento e reporte periódico à Alta Administração.

A Operadora deverá manter monitoramento contínuo dos riscos identificados, a revisão periódica da efetividade dos controles internos e o acompanhamento de indicadores-chave de risco (KRIs), de forma a possibilitar a identificação tempestiva de vulnerabilidades, a adoção de medidas preventivas e o suporte à tomada de decisão pela Alta Administração.

A Operadora deverá estabelecer e revisar periodicamente o seu apetite a riscos, definindo níveis aceitáveis de exposição que orientem a tomada de decisão e a priorização de ações de mitigação.

d) Regras e instrumentos de *Compliance*

As regras e os instrumentos de Compliance refletem e reforçam as condutas esperadas das pessoas abrangidas pelo Programa de Compliance, estabelecendo princípios e diretrizes a serem observados nas rotinas diárias da Postal Saúde. Esses instrumentos orientam os envolvidos diante de situações de potenciais riscos, dúvidas e/ou conflitos, promovendo a atuação em conformidade com a missão, a visão e os valores da Operadora.

A Postal Saúde dispõe de um conjunto de políticas, normas e procedimentos que estabelecem diretrizes específicas, integradas e organizadas por temas, de forma coordenada entre si. Entre os principais instrumentos normativos, destacam-se:

- **Código de Conduta, Ética e Integridade**

Documento norteador e basilar, que estabelece os padrões de comportamento esperados e define direitos e deveres dos abrangidos pelo Programa de *Compliance.*

- **Política Anticorrupção**

Estabelece práticas de prevenção e combate à corrupção, lavagem de dinheiro, financiamento ao terrorismo, fraudes e demais ilícitos, inclusive nas interações com o setor público, e orienta temas como brindes, presentes e hospitalidades, conflitos de interesse e transparência nas relações.

- **Política de Diligências**

Estabelece diretrizes e critérios para a avaliação de Compliance de pessoas físicas e jurídicas, por meio de Due Diligence de Compliance (DDI) para empresas e de Background Check (BGC) para candidatos a contratação ou remanejamento de pessoal, com o objetivo de identificar e mitigar riscos à integridade, à imagem e à reputação da Postal Saúde.

- P**olítica de Privacidade e Proteção de Dados Pessoais**

Estabelece diretrizes para o tratamento de dados pessoais em conformidade com a legislação aplicável, incluindo controles, responsabilidades e respostas a incidentes de segurança.

- **Política de Consequências**

Define princípios, diretrizes **no** processo de aplicação de consequências quando do descumprimento dos princípios éticos previstos no Código de Conduta, Ética e Integridade da Postal Saúde, seus valores e regras de conduta, e demais instrumentos normativos.

- **Política de Governança Corporativa**

Define princípios, diretrizes e responsabilidades para a Governança Corporativa, visando à sustentabilidade do negócio no longo prazo.

- **Política de Prevenção à Lavagem de Dinheiro**

Estabelece diretrizes e práticas de prevenção, detecção, combate e comunicação de indícios de crimes de lavagem de dinheiro, aplicáveis às operações de cadastro, finanças, gestão de contratos e benefícios.

- **Política de Gestão de Riscos e Controles Internos**

Estabelece princípios, diretrizes e responsabilidades 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.

e) *Due Diligence* de Integridade

A Postal Saúde adota o processo de *Due Diligence* de Integridade (DDI) como medida preventiva essencial para mitigação de riscos de integridade relacionadas a terceiros e colaboradores.

A diligência compreende o conjunto de procedimentos destinados à identificação, avaliação, classificação, tratamento e monitoramento dos riscos de *Compliance*, previamente à contratação e durante todo o relacionamento com a Operadora, com o objetivo de mitigar riscos à integridade, à conformidade normativa e à reputação institucional.

Com base nos resultados da avaliação, o candidato e os terceiros são classificados conforme seu nível de risco, de acordo com critérios previamente definidos, possibilitando a adoção de controles e medidas proporcionais à natureza e à gravidade dos riscos identificados.

Os conceitos, diretrizes, responsabilidades e metodologia para avaliação do Grau de Risco de Integridade (GRI) estão

definidos na Política e no Manual de Diligências.

A Due Diligence de Integridade também deverá ser aplicada em processos de celebração de parcerias institucionais, contratos estratégicos e demais relações relevantes que possam expor a Operadora a riscos de integridade.

f) Comunicação e Treinamento

A conscientização sobre os temas relacionados à integridade deve ser amplamente promovida por meio de ações de comunicação interna e externa, bem como de treinamentos periódicos, utilizando-se todos os canais disponíveis.

A Operadora promoverá ações contínuas de fortalecimento da cultura de integridade, incluindo campanhas institucionais, engajamento da liderança e iniciativas de sensibilização.

No âmbito do Programa de Compliance, a comunicação deve ocorrer de forma clara, objetiva e acessível, assegurando que todos os abrangidos compreendam suas responsabilidades e conheçam as diretrizes voltadas à prevenção e ao combate de desvios éticos e legais.

Adicionalmente, com o objetivo de garantir a efetividade do Programa, serão realizados treinamentos periódicos e adequados aos diferentes públicos, abordando temas como ética, integridade, prevenção e combate à corrupção, fraude, lavagem de dinheiro, conflitos de interesses, entre outros assuntos relacionados à conformidade e à governança corporativa.

5.3.2. **Detectar**: Para desenvolvimento do eixo de detecção, definem-se as seguintes práticas:

a) Controles Internos;

b) Canal de Denúncias.

a) Controles Internos

A Postal Saúde adota um sistema de controles internos baseado no *framework* COSO, estruturado para fornecer segurança razoável e não absoluta, quanto ao alcance dos objetivos da Operadora, considerando limitações inerentes a qualquer sistema de controle, quanto à eficácia operacional, confiabilidade das informações e conformidade com leis e regulamentos.

O sistema de controles internos compreende o conjunto de políticas, procedimentos, atividades e responsabilidades destinados a prevenir, detectar e mitigar riscos que possam comprometer os objetivos estratégicos da Operadora.

A gestão de controles internos deve estar integrada ao processo de Gestão de Riscos Corporativos, assegurando que os riscos identificados e os seus fatores de riscos possuam controles associados, responsáveis formalmente definidos, mecanismos de monitoramento e periodicidade de avaliação compatíveis com as métricas de exposição ao risco da Operadora.

Os controles devem ser periodicamente avaliados quanto à sua eficácia, com realização de testes, revisões e aprimoramentos contínuos, seguindo as seguintes etapas:

I. Identificação e mapeamento de processos e riscos

II. Definição e implementação de controles

III. Testes periódicos de eficácia (design e operação)

IV. Registro e classificação de falhas

V. Elaboração e acompanhamento de planos de ação

VI. Reporte estruturado à Alta Administração

VII. Melhoria contínua.

b) Canal de Denúncias

O Canal de Denúncias é uma ferramenta institucional disponibilizada para colaboradores, beneficiários e demais partes interessadas, com o objetivo de possibilitar o relato de desvios de conduta ética, disciplinar ou legal praticados por pessoas

abrangidas pelo Programa de *Compliance* da Postal Saúde, de forma segura, confidencial e, caso desejado pelo denunciante, anônima.

A Postal Saúde incentiva o registro de denúncias realizadas de boa-fé relacionadas a possíveis irregularidades, infrações ou suspeitas de atos ilícitos que envolvam, direta ou indiretamente, a Operadora.

O Canal de Denúncias constitui um dos pilares fundamentais do Programa de *Compliance*, atuando como mecanismo de prevenção, identificação e tratamento de infrações legais, éticas ou disciplinares, tais como fraudes, atos de corrupção, assédio, discriminação e demais condutas que possam comprometer a reputação, a integridade e os interesses da Operadora.

As denúncias recebidas serão classificadas conforme seu potencial de ofensividade, sendo tratadas de acordo com prazos previamente definidos, garantindo rastreabilidade, registro auditável e monitoramento por indicadores.

O Canal de Denúncias é gerido pelo Comitê de Ética e Disciplina da Postal Saúde (COEDI), com apoio administrativo da Gerência de *Compliance* e Riscos (GECRI).

Ressalta-se que a Postal Saúde repudia qualquer forma de discriminação, retaliação ou ameaça contra denunciantes ou pessoas que colaborem com os processos de apuração garantindo a confidencialidade e a proteção das informações.

5.3.3. **Corrigir**: Para desenvolvimento do eixo de correção, definem-se as seguintes práticas:

a) Investigações Corporativas;

b) Monitoramento e melhoria contínua;

c) Gestão de Consequências.

a) Investigações Corporativas

As investigações internas seguem diretrizes estabelecidas no Manual de Investigações Corporativas, destinado a apurar fatos e responsabilidades por desvios de condutas éticas e/ou disciplinares, à luz do Programa de *Compliance* da Postal Saúde.

O Processo Ético Disciplinar pode ser instaurado:

- de ofício pelo Comitê de Ética e Disciplina (COEDI), quando constados indícios relevantes de autoria e materialidade para infrações éticas e / ou disciplinares;
- a partir de relatos registrados no Canal de Denúncias da Postal Saúde, inclusive de forma anônima;
- a pedido formal da Alta Administração;
- a pedido formal da Mantenedora ou de Patrocinadores; e
- a pedido formal das Unidades Administrativas Gestoras (UAGs).

As investigações deverão observar princípios de legalidade, proporcionalidade, ampla defesa e confidencialidade, garantindo tratamento justo e isonômico aos envolvidos.

O COEDI possui caráter consultivo e deliberativo em matérias disciplinares, cabendo às instâncias competentes a decisão final sobre as medidas disciplinares aplicáveis. A apuração e análise devem ocorrer de forma segregada, garantindo independência e imparcialidade.

b) Monitoramento e melhoria contínua (Gestão de *Follow up*)

Para verificar a efetividade e a conformidade do Programa de *Compliance*, é realizado o monitoramento contínuo das medidas e ações implementadas, por meio do Plano Anual de Atividades (PAACRI) e da emissão de relatórios periódicos submetidos à ciência dos órgãos colegiados, com o objetivo de identificar oportunidades de melhoria, bem como a necessidade de correções e aprimoramentos nos processos e controles adotados.

O Programa de *Compliance* poderá ser avaliado e revisado periodicamente, conforme prazos previstos em normativos internos ou sempre que houver mudanças relevantes no ambiente regulatório, no modelo de negócios ou no perfil de riscos

da Operadora, garantindo sua adequação e efetividade contínua.

Caso seja identificado descumprimento de regras ou a existência de falhas no processo, os relatórios de monitoramento elaborados darão subsídio à elaboração de planos de ação para melhoria e correção do Programa, a fim de que os objetivos sejam plenamente alcançados.

As ações de monitoramento incluem, entre outras:

- Acompanhamento de processos e controles relacionados a riscos, testes de controles e níveis de conformidade;
- Análise de indicadores;
- Verificação do cumprimento de políticas e procedimentos;
- Monitoramento de denúncias;
- Avaliação da implementação de planos de ação decorrentes de auditorias, apurações ou recomendações de órgãos de controle.

A gestão do *follow up*, no âmbito do Programa de *Compliance*, consiste no processo sistemático de acompanhamento das recomendações emitidas por auditorias internas, externas e demais órgãos de controle, assegurando que os planos de ação definidos pelas áreas responsáveis sejam implementados de forma adequada e dentro dos prazos estabelecidos. A 2ª linha de defesa atua como responsável por monitorar a evolução dessas ações, validar evidências, registrar avanços e identificar eventuais riscos decorrentes de atrasos ou insuficiências nas medidas adotadas, garantindo a efetividade das correções propostas.

Esse monitoramento contínuo envolve o acompanhamento estruturado dos prazos e responsáveis, a verificação do cumprimento de políticas e controles e a avaliação da implementação das ações corretivas. As falhas identificadas são classificadas conforme sua criticidade, permitindo priorização e tratamento proporcional ao risco. As informações consolidadas pela 2ª linha subsidiam relatórios gerenciais e estratégicos, fortalecendo a governança e a transparência do Programa de *Compliance*.

c) Gestão de Consequências

A Gestão de Consequências tem como objetivo assegurar o tratamento adequado, proporcional e tempestivo das violações às normas internas, aos princípios éticos e à legislação aplicável.

As ocorrências identificadas por meio do Canal de Denúncias, auditorias, controles internos, monitoramentos, investigações ou outros mecanismos de detecção devem ser analisadas e tratadas de forma imparcial, confidencial e independente de cargo, função ou nível hierárquico, garantindo a isonomia e a integridade do processo de apuração.

Uma vez confirmadas irregularidades ou descumprimentos normativos, poderão ser aplicadas medidas disciplinares, corretivas e/ou administrativas compatíveis com a natureza e a gravidade da infração, observados os normativos internos e a legislação vigente.

As lições aprendidas decorrentes das apurações e tratativas realizadas devem contribuir para o aprimoramento contínuo do Programa de *Compliance,* fortalecendo os mecanismos de prevenção, detecção e resposta a riscos de integridade.

A Postal Saúde possui, em seu Código de Conduta e Integridade e em normativo específico, a definição das sanções aplicáveis nos casos de comprovado desvio de conduta. Dentre as medidas disciplinares, destacam-se:

- Advertência.
- Suspensão disciplinar não remunerada.
- Rescisão do contrato de trabalho por justa causa.
- Rescisão de contrato administrativo por justo motivo.
- Aplicação de multa punitiva.

6 DA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

6.1. A Postal Saúde realiza o tratamento de dados pessoais em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados- LGPD), demais normas aplicáveis à privacidade e proteção de dados, bem como de boas práticas utilizadas no mercado, a exemplo da ISO/IEC 27002/27001 – Código de Prática para a Gestão de Segurança da Informação/Sistema de Gestão da Segurança da Informação.

6.2. A gestão de proteção de dados pessoais integra o Programa de *Compliance* da Operadora, incluindo monitoramento de riscos correlacionados, gestão de incidentes de segurança da informação, e reporte à Alta Administração, dentre outros.

6.3. O tratamento de dados pessoais é realizado exclusivamente para finalidades legítimas, específicas e necessárias ao desempenho das atividades da Operadora, observando os princípios previstos na LGPD, em especial finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização.

6.4. A Postal Saúde também mantém formalmente designado Encarregado de Dados Pessoais (DPO), responsável por atuar como canal de comunicação entre a Operadora, os titulares de dados e a Agência Nacional de Proteção de Dados (ANPD).

7 DO RELATÓRIO

7.1. A Unidade de *Compliance* e Riscos reporta periodicamente à Alta Administração e, quando aplicável, aos órgãos de governança competentes, todas as ações relacionadas a efetividade do Programa de *Compliance*, permitindo a adoção de medidas corretivas e o aprimoramento contínuo da iniciativa.

8 DOS DOCUMENTOS ASSOCIADOS

8.1. DOCUMENTOS INTERNOS

- Código de Conduta, Ética e Integridade.
- Política Anticorrupção.
- Política de Governança Corporativa.
- Política de Consequências.
- Política de Diligências.
- Política de Privacidade e Proteção de Dados Pessoais.
- Política de Respostas a Incidentes.
- Política de Gestão de Riscos e Controles Internos.
- Política de Prevenção à Lavagem de Dinheiro.

8.2. DOCUMENTOS EXTERNOS

- Manual para Implementação de Programas de Compliance da CGU;
- NBR ISO 37001- Sistemas de gestão antissuborno - Requisitos com orientações para uso; e
- NBR ISO 37301 - Sistemas de Gestão de *Compliance*.