Sumário

1. OBJETIVO

Definir diretrizes, princípios, papéis e responsabilidades para o processo de Gerenciamento de Riscos e Controles Internos, estabelecendo subsídios para identificar, mensurar, monitorar, controlar, mitigar e gerenciá-los, aprimorando assim os processos decisórios e vislumbrando oportunidades de melhorias nos controles internos da Elosaúde.

2. ABRANGÊNCIA

Esta política aplica-se a todos os administradores (Diretores, membros do Conselho Deliberativo e Conselho Fiscal), colaboradores da Elosaúde, bem como, por todos os seus respectivos participantes e prepostos a eles vinculados e terceiros, considerando suas necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas. O cumprimento desta Política também é obrigatório a todos os terceiros e prestadores de serviços.

3. DEFINIÇÕES

Ambiente Interno: Fornece a base pela qual os riscos são identificados e abordados pelo responsável do processo.

ANS: A Agência Nacional de Saúde Suplementar é o órgão responsável pela normalização, controle, regulação e fiscalização das atividades relativas à assistência privada à saúde.

Apetite ao Risco: Quantidade total de riscos que uma organização está disposta a aceitar na busca de sua missão.

Atividade de Controle: Medida que mantém e/ou modifica o risco.

Compliance: estar em conformidade com a legislação, as regulamentações, as normas e procedimentos, externos e internos, e com os princípios de nossa Instituição que garantem as melhores práticas de mercado e de Governança Corporativa.

Coso (The Comitee of Sponsoring Organizations): Organização dedicada à melhoria dos relatórios financeiros, sobretudo pela aplicação da ética e efetividade na aplicação e cumprimento dos controles internos.

Fator de Risco: Descrição detalhada ou causa que contribui para a materialização do risco no processo.

Gestão do Risco: Atividades coordenadas pelos responsáveis dos processos para evitar que a organização seja afetada negativamente e assim, impactando nos seus objetivos.

Gerenciamento do Risco: Processo conduzido pela área de Governança Corporativa e Compliance com a anuência da Alta Administração que possibilita tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor, auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais.

IIA (Institute of Internal Auditors): Instituto de Auditores Internos.

ISO 31000:2018 (International Organization for Standardization): Norma desenvolvida que estabelece os princípios e orientações genéricas sobre gestão de riscos.

Governança Corporativa e Compliance: Estrutura que compõe, mas não se limite a Governança, Risco e Compliance.

Linhas de Defesa: Conjunto de diretrizes elaboradas para organizar as responsabilidades, designando os papéis das áreas de modo que as ações ocorram de forma sistemática e complementar, buscando a otimização dos resultados e a mitigação dos riscos.

Matriz de Riscos: Ferramenta utilizada para apoiar a gestão de riscos, quanto: identificação, mapeamento, classificação, testes, tratamento e monitoramento dos riscos.

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.

Risco: Possibilidade de um evento ocorrer e ter impacto nos objetivos da organização, sendo medido em termos de consequências e probabilidades.

Risco Inerente: Nível de risco antes da consideração de qualquer ação de mitigação.

Risco Residual: Nível de risco depois da consideração das ações adotadas pela gestão para reduzir inerente.

Risco Tolerável: Nível de risco aceitável para o que está sendo avaliado.

Tratamento de Riscos: Processo de implementar respostas a risco selecionadas.

4. DIRETRIZES

Esta política visa proporcionar o gerenciamento de riscos integrado e eficaz, tendo como base a metodologia dos componentes e princípios do COSO, ISO 31000-2018 e Ressoluções Normativas da ANS (RN), bem como suas respectivas alterações, em linha com as melhores práticas utilizadas no mercado nacional e internacional, para a proposição e implementação do modelo corporativo de gestão de riscos e controles internos.

5. GESTÃO DE RISCOS

A ISO 31000 define Gestão de Riscos como “atividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco”. A ANS traz que gestão de riscos é "o conjunto de ações direcionadas ao desenvolvimento, disseminação e implantação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da ANS”. Ou seja, gestão de riscos implica em agir de forma a prevenir que as falhas ocorram, demanda conhecer os riscos, ou seja, identificá-los e mensurá-los. Só é possível gerenciar o que se tem conhecimento e o que se tem algum nível de controle.

A ISO 31000 e ANS são as metodologias seguidas de forma que expõe em suas orientações que o “Gerenciamento de Riscos Corporativos – Estrutura Integrada” visa o aperfeiçoamento das organizações e de suas atuações, otimizando processos, abrindo oportunidades, diminuindo prejuízos e conscientizando-as sobre as suas responsabilidades.

5.1 PRINCÍPIOS DA GESTÃO DE RISCOS

- Incentivar o comprometimento e envolvimento de todos os colaboradores, essencialmente dos gestores, quanto a identificação, gerenciamento e mitigação dos riscos;
- Cultivar a clareza e transparência na identificação dos riscos e sua devida gestão e tratamento;
- Buscar constantemente a melhoria dos processos da Elosaúde;
- Manter a fidedignidade dos dados, informações e relatórios produzidos pela Operadora;
- Subsidiar a tomada de decisões;
- Disseminar a cultura de prevenção a riscos.

5.2 GERENCIAMENTO DO RISCO

O Gerenciamento do Risco ocorre para que se possa tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor, auxiliar a tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais, ocorrendo de acordo com

as seguintes etapas:

a) IDENTIFICAÇÃO

O principal objetivo dessa atividade é identificar através de um processo interativo, envolvendo a Assessoria de Governança e Compliance e o gestor responsável pelo risco, os eventos que possam afetar o alcance dos objetivos da Elosaúde, bem como o ambiente de controle necessário para gerir estes eventos.

b) CLASSIFICAÇÃO

Este processo ocorre após a identificação dos riscos e são categorizados de acordo com o Dicionário de Riscos da Elosaúde, no qual divide-se em qualitativos e quantitativos, de acordo com a definição abaixo:

Qualitativo - Na avaliação do risco qualitativo, o foco é na percepção sobre a probabilidade deste risco ocorrer e seu impacto nos aspectos organizacionais pertinentes. Esta percepção é representada em escalas como “baixa – média – alta”, que são utilizadas para definir o nível final do risco.
Este processo prioriza os riscos de acordo com os seus efeitos potenciais nos objetivos da Instituição. Sendo assim, um risco com nível crítico, sua importância pode ser ampliada.

Quantitativo - A análise quantitativa de riscos tem como objetivo levantar dados mensuráveis, numericamente, dos riscos envolvidos na organização. Com isso, a Instituição terá um domínio maior das variáveis envolvidas no processo, ganhando mais controle sobre os seus objetivos estratégicos.

O mais comum é que ambos sejam adotados de forma complementar. Primeiro, deve ser feita uma análise qualitativa, no qual o processo é examinado para que os riscos sejam identificados, classifica-se o impacto de cada risco e, então, as prioridades são definidas. Depois, é feita a análise quantitativa sobre cada risco, por meio da aplicação de ferramentas que transformam essas informações em números.

5.3 TIPOS DE RISCOS

Risco Operacional - Definido como a possibilidade de eventuais situações de perdas ocasionadas por falhas, deficiência ou inadequação de processos internos, pessoas e sistemas, além de eventos externos. Dentre os eventos de riscos operacionais, podem ser considerados: falha humana, interrupção das atividades, segurança da informação, fraude interna/externa, integridade das informações, concentração de atividades, não conformidade, dependência de pessoal, capacitação de pessoal, ineficiência, falha na comunicação interna, inefetividade, descumprimento contratual, segurança patrimonial, infraestrutura, falha sistêmica, entre outros.

Risco Estratégico - Relacionado a perdas resultantes de falhas, deficiências ou inadequação de processos relacionados aos objetivos de alto nível que dão suporte à missão institucional. Dentre os eventos de riscos estratégicos, podem ser considerados: planejamento e orçamento, comunicação externa, imagem, indicadores e performance, investimento em projetos, insatisfação dos clientes, sustentabilidade, entre outros.

Risco Legal - Engloba todas as ameaças que a instituição está vulnerável em decorrência do não cumprimento de leis, regras, regulamentações, acordos, práticas vigentes ou padrões éticos aplicáveis, acompanhado da interpretação errônea de dispositivos legais, desorganização das obrigações e transações fraudulentas que são algumas das possíveis causas de prejuízos financeiros decorrente do risco legal. Dentre os eventos de riscos legal, podem ser considerados: Tributário/Fiscal, Civil, Penal, Trabalhista, Regulatório, Contábil, *Compliance*, entre outros.

Risco de Crédito - Perdas relacionadas à probabilidade da contraparte de uma operação, ou de um emissor de dívida, não honrar total ou parcialmente seus compromissos financeiros. Dentre os eventos de riscos de crédito, podem ser considerados: inadimplência, aceitação de clientes, garantias contratuais, fluxo de caixa, entre outros.

Risco de Mercado - Relacionado à incerteza dos retornos esperados de seus ativos e passivos, em decorrência de variações em fatores como taxas de juros, taxas de câmbio, índices de inflação, preços de imóveis e cotações de ações. Dentre os eventos de riscos de mercado, podem ser considerados: taxa de juros desfavorável, participações, situação política adversa, concorrência e mercado, entre outros.

Risco de Subscrição - Relacionado ao processo de precificação indevida, ou na estimativa incorreta das provisões técnicas, além da probabilidade dos eventos a serem pagos pela Elosaúde em um período futuro, ultrapassarem o montante de contraprestações a ser recebidos. Dentre os eventos de riscos de subscrição, podem ser considerados: provisão técnica, precificação, alçada de desconto, alçada de checagem, despesas assistenciais, conferência de pagamentos, entre outros.

5.4 AVALIAÇÃO DO RISCO

Mensuração de impacto e probabilidade relacionados aos riscos identificados essa etapa consiste em avaliar os eventos sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas. Os riscos devem ser avaliados quanto à sua condição de inerentes e residuais.

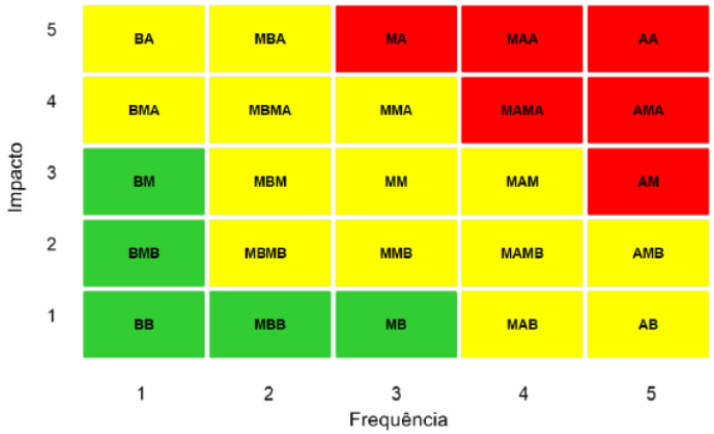
5.5 MATRIZ DE RISCO E MAPA DE CALOR

Após a avaliação, os riscos serão graduados por meio da Matriz de Risco e o modelo de gerenciamento de riscos é consolidado com o mapa de calor que contempla áreas conforme nível do risco.

Metodologia da Matriz de Riscos

F. *RI - Risco Inerente*

GRÁFICO 1
AVALIAÇÃO DO RISCO INERENTE



$$RI = \text{Probabilidade de Ocorrência} \times \text{Impacto}$$

5.6 RESPOSTA AO RISCO

Após as etapas anteriores, a decisão sobre a estratégia adotada para tratar cada risco depende principalmente do grau de apetite ao risco da empresa, previamente aprovado pela Diretoria Executiva.

5.7 APETITE AO RISCO

Refere-se aos riscos que a Elosaúde está disposta a aceitar para atingir os objetivos estabelecidos, no qual a alta administração escolhe a resposta aos riscos, desenvolvendo uma série de medidas para alinhar a tolerância e o apetite.

6. PRINCÍPIOS DA GESTÃO DE RISCOS

- Incentivar o comprometimento e envolvimento de todos os colaboradores, essencialmente dos gestores, quanto a identificação, gerenciamento e mitigação dos riscos;
- Cultivar a clareza e transparência na identificação dos riscos e sua devida gestão e
- tratamento;
- Buscar constantemente a melhoria dos processos da Elosaúde;
- Manter a fidedignidade dos dados, informações e relatórios produzidos pela Operadora;
- Subsidiar a tomada de decisões;
- Disseminar a cultura de prevenção a riscos.

7. CONTROLES INTERNOS

A ANS define na RN 518 que controles internos são “um conjunto de medidas adotadas para salvaguardar as atividades da Operadora, assegurando o cumprimento de seus objetivos e obrigações em todos os níveis da organização”

Conforme a COSO, Committee of Sponsoring Organizations of the Treadway Commission (Comitê das Organizações Patrocinadoras da Comissão Treadway), definiu controle interno como “um processo levado a cabo pelo Conselho de Administração, Direção e outros membros da organização a fim de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos: eficácia e eficiência dos recursos; fidedignidade da informação financeira; cumprimento das leis e normas estabelecidas.”

Os Controles Internos devem ser estruturados para oferecer segurança razoável ao alcance dos objetivos da organização. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos da gestão, devem congregar todas as atividades

materiais e formais implementadas pela gestão para assegurar que as respostas aos riscos sejam executadas com eficácia, possibilitando à organização o alcance dos objetivos estabelecidos da gestão baseiam-se no gerenciamento de riscos e integram o processo de gestão.

Os componentes dos controles internos e gerenciamento de riscos aplicam-se a todos os níveis da Elosaúde.

Os Controles Internos devem observar os seguintes objetivos:

I - dar suporte ao propósito, à continuidade e à sustentabilidade institucional, proporcionando garantia razoável ao atingimento dos objetivos estratégicos da Elosaúde;

II - proporcionar eficiência, eficácia e efetividade operacional, mediante execução ordenada, ética e econômica das operações;

III - assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisão, ao cumprimento de obrigações de transparência e à prestação de contas; e

IV - assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos, procedimentos e diretrizes internas da Elosaúde.

Os controles internos adotados visam garantir a confiabilidade das informações, dados e relatórios produzidos pela Operadora, buscando a utilização eficiente dos recursos, com eficácia em sua execução a fim de inclusive se manter aderente às regulamentações vigentes.

7.1 LINHAS DE DEFESA: PAPÉIS E RESPONSABILIDADES NA GESTÃO DE RISCOS E CONTROLES INTERNOS

A O modelo das Três Linhas de Defesa surgiu há mais de 20 anos e, desde então, se tornou amplamente reconhecido, principalmente no setor de serviços financeiros, onde foi criado e teve publicação em 21 de setembro de 2010 pelas FERMA e ECIIA no *Guidance on the 8th EU Company law* como recomendação da implementação dos requisitos da lei para o monitoramento da efetividade do sistema de controles internos, auditoria interna e gerenciamento de riscos. O modelo de Três Linhas de Defesa é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais de cada um na empresa. Ele ajuda a evitar confusões, lacunas e sobreposições ao atribuir as responsabilidades pelas atividades de gerenciamento de riscos e controle. Além de destacar a influência da auditoria externa e dos reguladores. É importante lembrar que este modelo é flexível a fim de se adaptar a cada organização. Em 2020 o IIA (*The Institute of Internal Auditors*) publicou uma atualização

significativa que moderniza a abordagem, adotando inclusive um novo nome para o modelo, que passou a ser apenas "Modelo das Três Linhas", prevendo exatamente a flexibilização da proposta em detrimento das particularidades de cada empresa.

Além disso, a revisão valida a visão de que o modelo não é mais puramente defensivo passando a assumir uma postura proativa. A gestão de riscos também está envolvida em encontrar oportunidades, criar valor e ao mesmo tempo protegê-lo.

7.2 COMPOSIÇÃO DAS LINHAS DE DEFESA

- **1ª Linha:** é composta pela GESTÃO OPERACIONAL e sua equipe, são os responsáveis primários por identificar, avaliar, tratar, controlar e reportar os riscos de suas áreas, de forma alinhada às diretrizes internas, regulamentações, políticas e procedimentos aplicáveis. A 1ª linha conta com pessoas que estão ligadas diretamente à rotina de negócio, são os executores dos processos, e por isso, são os que possuem maior domínio das atividades, assuntos e consequentemente maior conhecimento dos riscos.
- **2ª linha:** é composta por áreas independentes da 1ª linha, atuam como facilitadoras e têm como objetivo apoiar a gestão para que cumpram com suas responsabilidades de 1ª linha. A 2ª linha é responsável também por testar e avaliar a aderência à regulamentação, políticas e procedimentos. Nesta linha se encontram Controles Internos, Gestão de Riscos, Processos, Compliance, Qualidade e outras atividades de apoio.
- **3ª linha:** se resume na atividade de auditoria interna a qual tem como objetivo uma avaliação objetiva e independente da gestão dos riscos, controles e governança da organização. O resultado é a comunicação e efetivação das oportunidades de melhoria identificadas. Tem o papel de fornecer à Alta Administração e Conselhos avaliações abrangentes, independentes e objetivas relativas aos riscos a que estamos expostos, inclusive, evidenciando possíveis materializações.

O modelo das linhas de defesa demonstra de maneira clara os papéis e responsabilidades relacionados à gestão de riscos. É dever de todos a que se aplicam esta Política ter ciência de sua frente de atuação, tendo essencialmente, um olhar atento a fim de conhecer os riscos, evitá-los por meio de controles implementados e ainda, buscar oportunidades de melhorias.

8. PLANO DE AÇÃO

Para os riscos identificados nas áreas da Elosaúde que necessitem de controles para mitiga-los, serão abertos planos de ação que deverão conter, no mínimo, as seguintes informações:

I. Descrição da falha identificada;

II. Indicação da área responsável pelo risco;

III. Descrição do plano de ação elaborado pela área responsável pela ocorrência;

IV. Prazo para implementação do plano; e

V. Responsável pela implementação.

Os planos de ação deverão ser criados com base nos critérios de apetite ao risco definidos pela Alta Administração.
A área de Governança e Compliance acompanhará a implementação das ações definidas.
Caso não haja viabilidade de implementar os planos de ação dentro dos prazos exigidos, o responsavel imediato deve definir um controle compensatório de forma a reduzir a exposição ao risco, ou requisitar o seu aceite temporário.

9. GESTÃO DAS CONSEQUÊNCIAS

Todas as partes relacionadas devem agir de acordo com às diretrizes que regem a Instituição, evitando condutas antiéticas e possíveis sanções para si ou para a Elosaúde.
O descumprimento das diretrizes estabelecidas nesta política será tratado em conformidade com o Estatuto Social, Regimentos, Código de Ética e Conduta, Programa de Compliance e Integridade da Elosaúde.
Os indícios de irregularidades ou práticas de atos ilícitos devem ser registrados por meio do canal de denúncias, disponibilizado no site institucional.

10. COMUNICAÇÃO E TREINAMENTO

O setor de Governança Corporativa e Compliance, enquanto gestora do processo de Gestão de Riscos e Controles Internos, é responsável por recomendar os temas e a periodicidade dos treinamentos adequados aos diversos níveis da estrutura organizacional que ampliem a consciência sobre temas éticos e riscos à integridade.

11. DISPOSIÇÕES GERAIS

É competência da estrutura de GRC, em conjunto com a Superintendência da Elosaúde, alterar esta Política, sempre que necessário.
Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e Conselho Deliberativo e revoga quaisquer normas e procedimentos em contrário.

12. REFERÊNCIAS

- Resolução Normativa 518 e 507 – ANS
- OS 10 PILARES DO PROGRAMA DE COMPLIANCE. Disponível em: https://lec.com.br/os-10-pilares-de-um-programa-de-compliance/
- Código de Ética e Conduta Elosaúd
- Política de Governança Corporativa
- Política de Compliance e Integridade Elosaúde

13. ANEXOS

Não aplicável

14. HISTÓRICO DE REVISÕES

Identificação das Alterações		
Revisão	**Data da revisão**	**Alterações efetuadas**
00	01/12/2022	Implementação

Áreas envolvidas	Validação	Data
Conselho Deliberativo	Política aprovada em reunião pela Conselho Deliberativo	19/12/2022