Política de Gestão de Riscos

Versão 10

POLÍTICA DE GESTÃO DE RISCOS

1. OBJETIVO

O objetivo da Gestão de Riscos é apoiar a implementação de ações que assegurem o reconhecimento, identificação, avaliação, controle e monitoramento sistemático dos riscos que possam impactar o Grupo IAG Saúde.

Esse processo contempla, de forma integrada, os riscos de compliance e de segurança e privacidade da informação, bem como riscos estratégicos, financeiros, de imagem, ocupacionais e operacionais, entre outros associados às atividades, produtos, serviços e obrigações do Grupo.

No âmbito da segurança e privacidade da informação, a gestão de riscos está alinhada aos princípios de confidencialidade, integridade e disponibilidade, garantindo que dados e sistemas sejam protegidos, confiáveis e acessíveis às partes autorizadas.

2. ABRANGÊNCIA

Esta política institucional se aplica-se a todos os colaboradores, fornecedores críticos, prestadores de serviços, parceiros comerciais e demais partes interessadas do Grupo IAG Saúde, que de alguma forma são impactadas pelas ações da organização.

3. SIGLAS E DEFINIÇÕES

Apetite ao risco: quantidade e tipo de riscos que uma organização está preparada para buscar ou reter (ISO 27005:2023). A Diretoria demonstra liderança e comprometimento ao estabelecer a quantidade e o tipo de risco que pode ou não ser assumido para orientar o desenvolvimento de critérios, assegurando que estes sejam comunicados à organização e às suas partes interessadas.

Consequência: resultado de um evento que afeta os objetivos (ISO 31000:2018).

Contexto: ambiente interno e/ou externo no qual a organização busca atingir seus objetivos. Exemplos: ambiente interno (missão, valores, estratégias, políticas, procedimentos, cultura de compliance, relações com as partes interessadas) e ambiente externo (político, econômico-financeiro, social, tecnológico, ambiental internacional, nacional ou local, legal, cultural, regulatório) (ISO 27005:2023).

Controle: medida que mantém e/ou modifica o risco. Controles incluem, mas não estão limitados a: processo, política, dispositivo, prática, ou outras condições e/ou ações que mantêm e/ou modificam o risco. (ISO 31000:2018). Os controles são destinados a enfrentar os riscos, de forma preventiva ou corretiva.

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias (ISO 31000:2018).

Fonte de risco: elemento que, isolado ou em conjunto, tem potencial para gerar risco, podendo incluir pessoas, processos, sistemas, infraestrutura física ou organizacional, tecnologia ou eventos externos (ISO 31000:2018).

Gestão de Risco: atividades coordenadas para dirigir e controlar uma organização no que se refere aos riscos (ISO 31000:2018).

ISO: International Organization for Standardization (Organização Internacional de Normalização)

Probabilidade: chance de algo acontecer (ISO 31000:2018).

Risco: efeito da incerteza nos objetivos (ISO 31000:2018).

Risco Inerente: nível de risco calculado (Probabilidade x Gravidade) na ausência de quaisquer controles ou desconsiderando a eficácia dos controles existentes. Representa o risco bruto (ISO 31000:2018 – Análise de Riscos)

Risco Residual: nível de risco calculado (Probabilidade x Gravidade) após a consideração da existência e eficácia dos controles em vigor (ISO 31000:2018 – Tratamento de Riscos). O risco remanescente após o tratamento de riscos. A organização deve decidir se o risco remanescente é aceitável e, se não for, realizar tratamento adicional.

4. DIRETRIZES

A metodologia adotada pelo Grupo IAG Saúde para o gerenciamento de riscos está estruturada em conformidade com todos os requisitos do Processo de Gestão de Riscos definido pela ABNT NBR ISO 31000:2018, conforme ilustrado na *Figura 1 – Processo de Gestão de Riscos*.

Os riscos de compliance e de segurança da informação são tratados de forma integrada e incorporados à cultura organizacional, alinhando-se às diretrizes das ABNT NBR ISO/IEC 37301:2021 – Sistema de Gestão de Compliance e ISO/IEC 27001:2022 – Sistema de Gestão de Segurança da Informação.

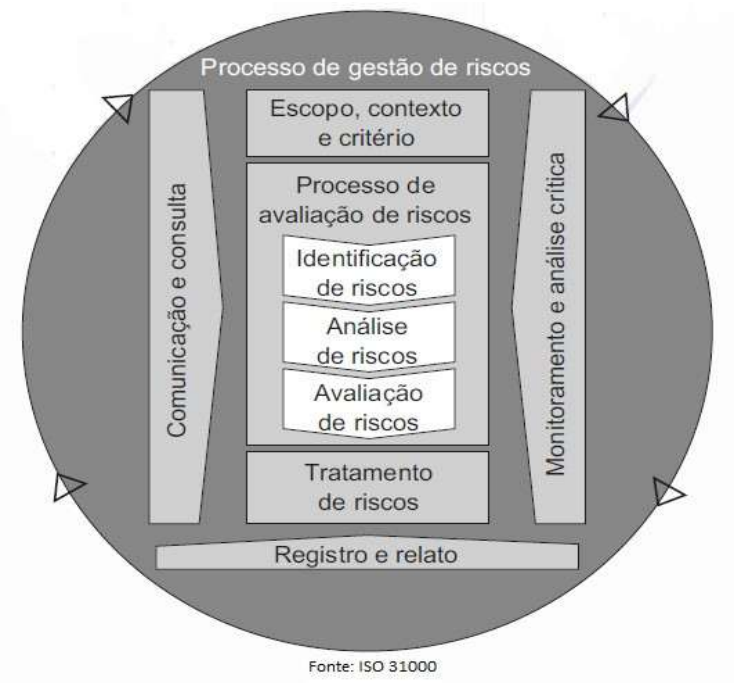
Nesse contexto, o gerenciamento de riscos em segurança da informação está fundamentado nos seus três pilares essenciais:

- Confidencialidade: assegurar que os dados sejam mantidos em sigilo e acessíveis apenas a pessoas autorizadas;
- Integridade: garantir que os dados permaneçam corretos, autênticos e confiáveis, preservando-os contra alterações não autorizadas;
- Disponibilidade: assegurar que sistemas, aplicativos e informações estejam acessíveis para os usuários autorizados sempre que necessário.

POLÍTICA DE GESTÃO DE RISCOS

Dessa forma, a gestão de riscos fortalece a cultura de compliance e garante a efetividade dos controles, promovendo a continuidade e a resiliência dos processos críticos do Grupo IAG Saúde.

Figura 1 – Processo de Gestão de Riscos.



Comunicação e Consulta: A comunicação visa promover a conscientização e o entendimento sobre os riscos, enquanto a consulta busca obter contribuições e informações que apoiem a tomada de decisão.

Escopo, Contexto e Critérios: A gestão de riscos é parte integrante de todos os processos. A identificação dos riscos ocorre a partir do desdobramento dos processos críticos, análise do contexto e definição dos objetivos de compliance e segurança da informação.

Esta política adota como referência a Declaração de Aplicabilidade (SoA) vigente, que consolida os controles de segurança da informação.

POLÍTICA DE GESTÃO DE RISCOS

Domínios de Risco Monitorados: O Grupo IAG Saúde monitora os seguintes domínios:

Ambiental	Probabilidade de ocorrência de eventos danosos ao meio ambiente em que se está inserido, decorrentes da ação de agentes físicos, químicos ou biológicos. Esses agentes podem gerar condições ambientais potencialmente perigosas, favorecendo sua persistência, disseminação e modificação no ambiente, com potencial para causar efeitos nocivos ou prejudiciais à saúde humana, tanto de forma individual quanto coletiva.
Compliance	Relacionados ao cumprimento de regulamentações internas e externas, leis e políticas e/ou procedimentos. Exemplos: não conformidade com normas ISO, questões fiscais, penalidades legais.
Estratégico	Relacionados às decisões estratégicas da empresa, como entrada em novos mercados, fusões e aquisições. Exemplos: mudanças no mercado, concorrência intensa, falha na execução da estratégia.
Financeiro	Relacionados à gestão financeira, incluindo fluxo de caixa, investimentos, dívidas e custos. Exemplos: flutuações cambiais, inadimplência, perdas de investimento.
Imagem	Relacionada à imagem e à reputação da empresa perante clientes, parceiros e público em geral, podendo levar a perda de mercado. Exemplos: escândalos, má conduta corporativa, crise de relações públicas, insatisfação do cliente interno ou externo.
Ocupacionais	Relacionados à saúde e segurança dos funcionários e clientes. Exemplos: acidentes de trabalho, doenças ocupacionais, ergonomia, ambiente físico, pandemias.
Operacionais	Relacionados às operações diárias da empresa, como processos, sistemas, pessoal e infraestrutura referentes ao atendimento aos clientes internos e externos, a partir da execução das políticas, procedimentos, regulamentações, leis. Exemplos: erros humanos, interrupções de serviços, atendimento falho ou parcialmente realizado junto ao cliente interno ou externo, falhas de equipamentos.
Segurança da Informação	Relacionados à proteção dos dados e sistemas da empresa. Exemplos: violações de dados, ataques cibernéticos, vazamento de informações confidenciais, danos à integridade da informação e disponibilidade de sistemas.

Cada setor é responsável por elaborar e atualizar sua Matriz de Gestão de Riscos anualmente ou quando necessário. As diretrizes para elaboração e atualização da Matriz estão detalhadas no documento modelo *REG IAG 211 – Matriz de Gestão de Riscos*.

POLÍTICA DE GESTÃO DE RISCOS

4.1 PROCESSO DE AVALIAÇÃO DE RISCOS

4.1.1 IDENTIFICAÇÃO DO RISCO

A identificação de riscos envolve o reconhecimento sistemático das fontes de risco, áreas de impacto, eventos, causas e consequências potenciais. Tem como base as atividades críticas definidas nos Mapas de Processos setoriais, no histórico de informações obtido na análise de contexto, nas obrigações de compliance e nos controles do Anexo A da NBR ISO/IEC 27001.

O Grupo determina as questões externas e internas pertinentes para o seu propósito, incluindo se as mudanças climáticas são uma questão relevante que possa afetar a capacidade do SIGO em alcançar os resultados pretendidos.

Para apoiar a identificação de riscos em cada categoria, podem ser utilizadas técnicas de *brainstorming*, o conhecimento especializado dos gestores e demais metodologias participativas. Os riscos podem emergir de diferentes situações, como:

> objetivos de compliance; execução de rotinas estabelecidas em documentos internos; cumprimento de leis, normas externas e requisitos da Cadeia Cliente-Fornecedor; auditorias internas e/ou externas; resultados de indicadores de desempenho; implantação de mudanças que possam impactar o SIGO.

As informações coletadas são registradas no documento *MR [sigla do setor] 001 – Matriz de Gestão de Riscos*, contemplando os seguintes itens da Seção 1 (Identificação):

> **1.1. Atividades Críticas do Processo/Análise de Contexto**: iniciar pelas ações que ocorrem nos processos internos. Elas estão listadas no Mapa de Processos e no histórico de informações provindas da análise do contexto avaliada no Planejamento Estratégico.
>
> **1.1.1 Proprietário do Risco**: os riscos identificados devem possuir um proprietário claramente definido, que será responsável por acompanhar, tratar

e responder adequadamente ao risco, garantindo que as ações de mitigação sejam conduzidas com diligência e alinhadas aos objetivos organizacionais.

Na Matriz de Gestão de Riscos Sistêmica, o proprietário do risco será a diretoria ou o setor diretamente responsável pela gestão da falha ou risco.

Nas Matrizes de Gestão de Riscos Setoriais, o proprietário do risco é a diretoria do setor, não sendo necessário incluir este campo na Matriz.

1.2 Falha/Risco: identificar os riscos considerando dados históricos, análises teóricas e necessidades das partes interessadas, gerados quando do cumprimento dos requisitos de processos, da legislação, dos objetivos de compliance e de segurança da informação, das diretrizes institucionais, dos resultados de indicadores, na execução dos controles, entre outros.

1.3 Prevenção: especificar as rotinas padronizadas, políticas, diretrizes disponíveis, que contemplem ações para evitar que a falha ocorra, ou seja, são os controles.

1.4 Domínio/Natureza do Risco: identificar o domínio de risco imediato, relacionado à falha descrita, sendo estes: Compliance, Estratégicos, Financeiros, Operacionais, Reputacionais, Saúde e Segurança e Segurança da Informação.

Propriedade de SI (Confidencialidade, Integridade, Disponibilidade): Este item é exclusivo à Matriz de Gestão de Riscos Sistêmica, para os controles das seções 5 Organizacionais, 6 Pessoas, 7 Físicos e 8 Tecnológicos e são especificados conforme NBR ISO/IEC 27002.

1.5 Consequência: apontar o resultado/impacto de um evento que afeta os objetivos, seja ele positivo ou negativo.

1.6 Classificação 6Ms: identificar uma das categorias de causas de acordo com a ferramenta da qualidade Diagrama de Causa e Efeito (método, mão de obra, material, máquina, meio ambiente, medida).

1.7 Descrição das Causas da Falha: identificar os motivos que podem levar a ocorrência das falhas.

A seleção dos controles destinados à prevenção ou detecção de falhas é formalizada na Declaração de Aplicabilidade (SoA), em conformidade com os critérios da ABNT NBR ISO/IEC 27001.

4.2 ANÁLISE DO RISCO

A análise dos riscos visa desenvolver a compreensão do risco, fornecendo informações para a tomada de decisão sobre o tratamento, por meio dos seguintes parâmetros:

2.1 Fonte da Probabilidade: estimar a chance de ocorrência de um evento, por meio de análises qualitativas, quantitativas ou da combinação de ambas.

2.2 Indicador ou descrição da fonte de probabilidade: a probabilidade deve basear-se em dados quantitativos ou qualitativos ou da combinação de ambos, sempre que possível.

2.3 Probabilidade: é a chance da ocorrência de um evento, relacionada à falha identificada, cujos critérios estão estabelecidos na *Tabela 1 – Probabilidade*.

2.4 Gravidade: indica a intensidade do dano da consequência, caso a falha ocorra. Ver os critérios estabelecidos na *Tabela 2 – Gravidade*.

2.5 Nível de Risco Inerente: nível de risco bruto calculado (Probabilidade x Gravidade) na ausência de quaisquer controles ou desconsiderando a eficácia dos controles existentes. Este deve ser calculado para todos os riscos (novos e antigos) no ciclo atual. Ver critérios na *Tabela 3 – Nível de Risco*.

2.6 Nível de Risco Residual (Ciclo Anterior): Risco Líquido alcançado na rodada anterior. É o histórico de exposição. Serve para comparar os resultados da nova análise (item 3.8) com o desempenho do período anterior. Ex.: Se o item 3.8 for igual

ou maior que o 2.6, isso indica que o contexto (interno/externo) mudou ou o tratamento realizado no ciclo anterior foi ineficaz. Essa comparação direciona a avaliação da eficácia da estrutura de gestão de riscos.

Anualmente as áreas revisam a Matriz de Gestão de Risco, identificam a nova gradação de risco (probabilidade X gravidade) e comparam os resultados com o ano anterior, avaliando a necessidade de tratamento.

A *Tabela 1 Probabilidade*, especifica o nível de probabilidade, sua classificação e a descrição dos critérios para determinação da probabilidade.

Probabilidade: Chance de ocorrência. A probabilidade baseia-se em dados quantitativos sempre que possível, podendo ser evidenciada através de indicadores do processo ou registros. Estimativas subjetivas podem ser usadas quando não existir uma base de dados coletada ou quando a obtenção dos dados não apresentar uma boa relação custo-benefício. São 3 opções: baixa, média ou alta. Cada opção tem uma pontuação específica: "Baixa"= 1; "Média" = 2 e "Alta" = 3.

PROBABILIDADE		
NÍVEL	**CLASSIFICAÇÃO**	**DESCRIÇÃO**
1	**Baixa**	A falha ocorre em baixa frequência. Se indicador: o desempenho está na meta ou melhor que a meta. Se observação: falha nunca ou raramente ocorre.
2	**Média**	A falha ocorre um pouco mais frequente. Se indicador: o desempenho está até 10% fora da meta (para o lado indesejado). Se observação: falha ocorre muito pouco.
3	**Alta**	A falha pode ocorrer de forma mais frequente. Se indicador: o desempenho está mais do que 10% pior que a meta desejada. Se observação: falha ocorre com frequência.

Tabela 1 – Probabilidade

POLÍTICA DE GESTÃO DE RISCOS

A Tabela 2 Gravidade, especifica o nível da gravidade, sua classificação e a descrição dos critérios para determinação da gravidade.

Gravidade: é magnitude das consequências do evento, isto é, a intensidade do dano, se a falha/erro ocorrer: leve, moderada ou grave. Cada opção tem uma pontuação específica: "Leve" = 1; se "Moderada" = 2 e "Grave" = 3.

GRAVIDADE		
NÍVEL	**CLASSIFICAÇÃO**	**DESCRIÇÃO**
1	**Leve**	A falha quando ocorre gera danos leves e reversíveis. Exemplos: Atrasar a entrega de uma lista de presença ou ata de reunião, não estudar o cliente e as suas especificidades para iniciar o projeto, atraso na realização de um contato comercial.
2	**Moderada**	A falha quando ocorre gera danos moderados e reversíveis. Exemplos: não preenchimento da agenda do consultor; não disponibilização dos benefícios para os colaboradores, disponibilizar consultor que não possui competência técnica para o projeto.
3	**Grave**	A falha quando ocorre gera danos graves, não sendo completamente reversíveis podendo até comprometer a reputação da empresa no mercado. Exemplos: Vazamento de dados pessoais e outras informações confidenciais, perda de dados e informações, não comunicar os fechamentos de contrato, não cumprimento das obrigações contratuais e de legislações.

Tabela 2 – Gravidade

Nível do Risco (probabilidade X gravidade): a multiplicação da probabilidade e gravidade identifica o nível do risco do período de referência.

PONTUAÇÃO	NÍVEL DE RISCO	DESCRIÇÃO
1 e 2	**BAIXO**	A falha ocorre em baixa frequência e quando ocorre os danos causados podem ser leves e em alguns casos moderados. Ação: o setor responsável pela geração da falha deve acompanhar e desencadear ação quando julgar necessário.
3 e 4	**MÉDIO**	A falha ocorre um pouco mais frequente e quando ocorre os danos causados são moderados e totalmente reversíveis. Ação: o setor responsável pela geração da falha deve acompanhar através de análise crítica; é recomendável a implantação de um plano de ação.
6 a 9	**ALTO**	A falha pode ocorrer de forma mais frequente e/ou quando ocorre os danos causados são graves, não sendo completamente reversíveis podendo até comprometer a reputação da empresa no mercado. Ação: o setor responsável pela geração da falha/erro deve implantar plano de ação.

Tabela 3 – Nível de Risco.

4.3. AVALIAÇÃO DO RISCO

A avaliação do risco auxilia a tomada de decisões, envolvendo a comparação dos resultados da análise de riscos (3.8 – Nível de Risco Residual do Ciclo Atual) com os critérios de risco estabelecidos (3.9 Apetite ao Risco) para determinar onde é necessária ação adicional.

As etapas para avaliação de riscos consideram os seguintes itens:

3.1 Descrição do Controle: apontar qual controle é utilizado para a detecção ou prevenção da falha, que, ao ser executado, modifica ou mantém o risco, podendo ser: política, atividade prática estabelecida nos procedimentos, processo, dentre

outros. Os controles de segurança da informação descritos nesta etapa são fundamentados na Declaração de Aplicabilidade (SoA).

3.2 Tipo de Controle: Automatizado = 3; Misto = 2 e Manual = 1.

3.3 Capacidade de Bloqueio: Detectivo = 1 e Preventivo = 2.

3.4 Aplicação do controle: Parcial = 1 ou Total = 2.

3.5 Nível de Controle: indica a eficiência do controle, avaliado nos itens anteriores 'Tipo de Controle + Capacidade de Bloqueio + Aplicação'. Ver critérios na *Tabela 4*.

3.6 Probabilidade Residual: é a chance de ocorrência de um evento após a verificação da existência ou não da eficácia dos controles em vigor (Nível de Controle 3.5). Se os controles existentes (3.1 a 3.5) forem altamente eficazes, a pontuação de Probabilidade (conforme Tabela 1) deverá ser reduzida, refletindo a mitigação alcançada antes de qualquer novo Tratamento.

3.7 Gravidade Residual: indica a intensidade do dano da consequência após a verificação da existência ou não da eficácia dos controles em vigor (Nível de Controle 3.5). Se os controles existentes (3.1 a 3.5) forem eficazes na redução do impacto, a pontuação de Gravidade (conforme Tabela 2) deverá ser reduzida, refletindo o dano remanescente.

3.8 Nível de Risco Residual | Ciclo Atual: Risco Líquido do ciclo em atualização (3.6 Probabilidade *Residual* x 3.7 Gravidade *Residual*). Representa o risco que permanece após a verificação da existência ou não da eficácia dos controles existentes (3.5 Nível de Controle). Este valor é a base para as ações de Tratamento do ciclo (Item 4). Se este nível estiver acima do tolerável, ele deve ser tratado.

Após a definição destes parâmetros a célula do Excel irá exibir a cor conforme as definições abaixo:

NÍVEL DE CONTROLE		
FRACO	RAZOÁVEL	DESEJÁVEL
3	4 e 5	6 e 7

Tabela 4 – Nível de Controle

3.9 Apetite ao Risco – Declaração e Tolerância

A Alta Direção estabelece o apetite ao risco, que deve ser Baixo em domínios críticos que envolvem Compliance, Segurança da Informação, Imagem e Saúde/Segurança Ocupacional, e Alto para iniciativas de Pesquisa e Desenvolvimento e Experimentação (Provas de Conceito).

A **tolerância** ao Apetite ao Risco são os seguintes:

Baixo Apetite ao Risco (baixa tolerância): não se tolera riscos que possam afetar áreas críticas ou comprometer a conformidade. Situações típicas:

Segurança da Informação: riscos de vazamento de dados, indisponibilidade de sistemas, violação de CID.

Compliance: não conformidade com leis, normas, requisitos regulatórios ou contratuais.

Financeiro: perdas acima do limite pré-definido (>1% do faturamento anual).

Imagem e Reputação: riscos que possam gerar exposição negativa, perda de confiança no mercado.

Saúde e Segurança Ocupacional: acidentes graves, doenças ocupacionais, riscos à integridade física.

Riscos nesta categoria devem ser **evitados ou mitigados imediatamente**, mesmo que isso implique em custo elevado.

POLÍTICA DE GESTÃO DE RISCOS

Moderado Apetite ao Risco (tolerância calculada): A Alta Direção aceita riscos que envolvam inovação ou mudanças, desde que não comprometam a continuidade do negócio nem a conformidade legal. Situações típicas:

Projetos de inovação e melhorias: pilotos de novas tecnologias, automações em áreas de apoio.

Financeiro: perdas moderadas toleráveis (até 0,5% do faturamento anual).

Operacional: falhas que causem atrasos ou retrabalho, mas sejam reversíveis e com impacto limitado.

Imagem e Reputação: riscos de baixo alcance (ex.: insatisfação pontual de um cliente, sem repercussão pública).

Saúde e Segurança Ocupacional: situações de risco moderado (ex.: ergonomia, absenteísmo pontual).

Riscos nesta categoria **podem ser aceitos com monitoramento**, desde que haja plano de ação/contingência.

Alto Apetite ao Risco (posição ousada): aceita assumir riscos em cenários que favoreçam inovação, aprendizado ou ganho estratégico, desde que os impactos sejam mínimos e facilmente reversíveis.

Pesquisa e Desenvolvimento: experimentos, provas de conceito em ambiente controlado. Situações típicas:

Operações de baixa criticidade: áreas de suporte interno, sem impacto direto no cliente ou na conformidade.

Financeiro: pequenas perdas absorvíveis (abaixo de 0,1% do faturamento anual).

Imagem e Reputação: riscos de percepção interna (ex.: atrasos em relatórios internos sem visibilidade externa).

Tecnologia: adoção de novas ferramentas em caráter de teste, mesmo com possibilidade de falhas.

Riscos nesta categoria **podem ser assumidos** intencionalmente, servindo como aprendizado ou oportunidade de inovação.

3.10 Tipo de resposta ao risco:

A partir da comparação entre o 3.8 Nível de Risco Residual Ciclo Atual e o 3.9 Apetite ao Risco, define-se a resposta necessária, por meio dos parâmetros:

Aceitar: Os controles são implantados, e o nível de risco está dentro do que foi pré-estabelecido (Apetite ao Risco).

Reduzir: Agir tanto sobre as causas como sobre as consequências do risco e avaliar se os controles são suficientes para mitigar os riscos.

Compartilhar: Envolve alocar parte do risco para um terceiro (criando uma parceria) que tenha mais capacidade de concretizar a eliminação ou redução da ameaça.

Transferir: Tornar outro processo responsável pelo risco, o que implica na transferência das respostas ao risco, mas não o elimina, devendo ser comunicado e gerenciado em outro processo.

Evitar: Envolve alterar o plano de gerenciamento do risco para eliminar a ameaça, portanto, a sua causa.

Após a implementação das opções de tratamento de riscos, o Risco Residual é o risco que permanece. O setor deve decidir se o risco remanescente é aceitável e, se não for, realizar tratamento adicional, estabelecido na seção *4 – Tratamento do Risco*.

4.4 TRATAMENTO DO RISCO

O tratamento do risco será realizado quando o nível de risco – inerente (2.5) no primeiro ciclo de avaliação ou residual (3.8) nas atualizações – estiver acima do nível tolerável e será aplicado sobre as causas e os efeitos, de modo a reduzir a probabilidade e o impacto ajustados.

Envolve a identificação das diversas opções, a análise e avaliação dessas opções, e a implantação de planos de ação.

As opções para tratar o risco podem envolver:

> Aceitar o risco e reconhecer que ele existe e que não será aplicado tratamento adicional; Aceitar o risco residual ou aumentar esse risco, de maneira a perseguir uma oportunidade; Remover a fonte de risco; Mudar a probabilidade: agir sobre as causas para reduzir a chance de o evento ocorrer. Mudar as consequências: agir sobre os efeitos para reduzir o impacto (gravidade) caso o evento ocorra. Compartilhar o risco: alocar parte do risco para um terceiro, por exemplo, criar uma parceria ou contratar um seguro que tenha maior capacidade de eliminá-lo ou reduzi-lo; Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco.

O tratamento é onde se definem as ações, a serem registradas no documento *MR [sigla do setor] 001*:

4.1 Correção: ação imediata frente à falha/erro a ser tomada para mitigação.

4.2 Contingência: ação a ser tomada para assegurar a continuidade da atividade crítica.

4.3 Ação Corretiva: projeto ou controle a ser elaborado ou melhorado para eliminar a causa da falha/erro e para monitoramento do risco.

POLÍTICA DE GESTÃO DE RISCOS

4.5 MONITORAMENTO DO RISCO E EVIDÊNCIA DA OCORRÊNCIA DE FALHAS

O monitoramento pode ser definido por Indicador Base SigQuali, Indicador Outra Base, Registro/Controle ou uma combinação.

Mensalmente todos os setores monitoram o indicador "Percentual de ocorrência do risco", por meio do formulário "*MGR [sigla do setor] 001 - Monitoramento da Gestão de Riscos*".

O monitoramento deve incluir a reavaliação da eficácia do tratamento (4.3 Ação Corretiva) e a observação do Risco Residual.

A área da Qualidade e Compliance realiza, semestralmente, uma análise global dos riscos, para verificar a consistência entre os indicadores monitorados.

4.6. ADMINISTRAÇÃO DESTA POLÍTICA

Incentivamos os clientes, colaboradores, fornecedores e parceiros comerciais a comunicarem supostas violações destas diretrizes no Canal de Ouvidoria do Grupo IAG Saúde que se encontra na página de formulários de contato, no site do Grupo IAG Saúde: Contato e Ouvidoria - Grupo IAG Saúde

O Grupo IAG Saúde está comprometido em proteger de retaliação qualquer pessoa que, agindo de boa-fé, registre uma denúncia ou ajude em uma investigação, incluindo, mas não se limitando a: suspensão, assédio, ameaças, intimidação, coação, perda de benefícios, demissão ou qualquer outra forma de discriminação ou punição.

A ação ou a conivência que impliquem em desobediência ou inobservância das diretrizes desta política são consideradas infrações. As penalidades a que os infratores estão sujeitos são:

- Advertência

- Suspensão
- Demissão por justa causa
- Rescisão contratual

Declaramos que este documento é a cópia fiel da Política de Gestão de Riscos, aprovada pela Diretoria do Grupo IAG Saúde.

Quaisquer dúvidas sobre a aplicação desta Política deverão ser reportadas à área de Compliance, através do e-mail compliance@grupoiagsaude.com.br.

5. REGISTROS

MR [sigla do setor] 001 Matriz de Gestão de Riscos.

MGR [sigla do setor] 001 Monitoramento da Gestão de Riscos

6. REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO 31000:2018 – Gestão de riscos – Diretrizes ABNT, 2018

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2022 – Versão Corrigida: 2023 Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. ABNT, 2023.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002:2022 Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. ABNT, 2022.

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 37301:2021 Sistema de gestão de compliance – Requisitos com orientações para uso. ABNT, 2021.