



Política de Gestão de Riscos

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 da informação, bem como riscos estratégicos, financeiros, de imagem, ocupacionais e operacionais, entre outros associados às atividades, produtos, serviços e obrigações da organização.

No âmbito da segurança 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

Todos os setores do Grupo IAG Saúde.

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

POLÍTICA DE GESTÃO DE RISCOS

ambiente externo (social, cultural, político, legal, regulatório, financeiro, tecnológico, internacional, nacional ou local) (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.

POLÍTICA DE GESTÃO DE RISCOS

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 tanto às diretrizes da ABNT NBR ISO/IEC 37301:2021 (Sistema de Gestão de Compliance) quanto da ABNT NBR ISO/IEC 27001:2022 (Sistema de Gestão de Segurança da Informação).

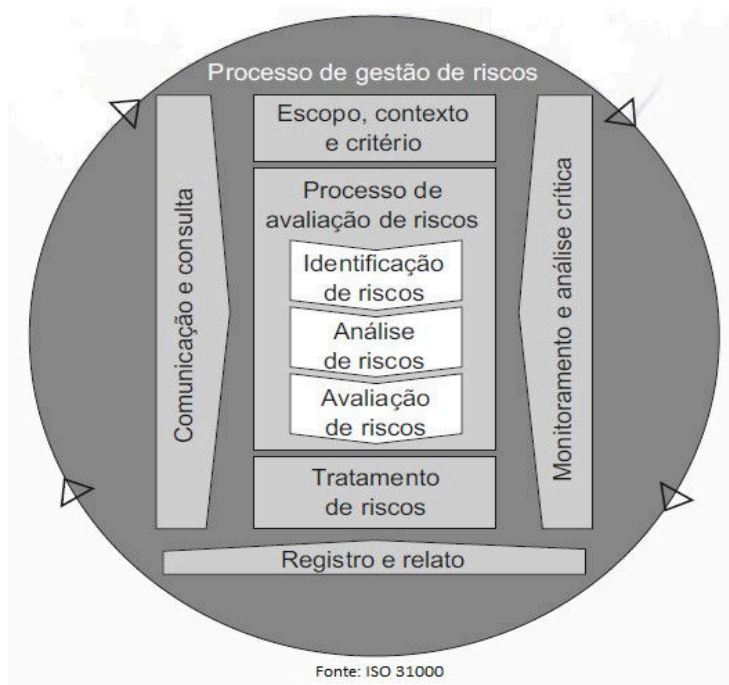
Nesse contexto, o gerenciamento de riscos em segurança da informação está fundamentado nos seus três pilares essenciais:

- **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.

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.

POLÍTICA DE GESTÃO DE RISCOS

Figura 1 – Processo de Gestão de Riscos.



Comunicação e Consulta: A comunicação tem como objetivo promover a conscientização e o entendimento sobre os riscos entre todos os colaboradores do Grupo IAG Saúde. Já a consulta busca obter contribuições e informações que apoiem a tomada de decisão, assegurando a participação ativa das partes interessadas.

Escopo, Contexto e Critérios: A gestão de riscos é parte integrante de todos os processos do Grupo IAG Saúde. A identificação dos riscos ocorre a partir do desdobramento dos processos críticos em atividades críticas e da análise do contexto organizacional, resultando na definição dos objetivos de compliance e de segurança da informação.

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

Domínios de Risco Monitorados: O Grupo IAG Saúde definiu os seguintes domínios de risco a serem monitorados pelos setores:

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

Ambiental	Possibilidade de ocorrência de eventos danosos ao meio ambiente que se está inserido decorrente da ação de agentes físicos, químicos ou biológicos, causadores de condições ambientais potencialmente perigosas que favoreçam a persistência, disseminação e modificação desses agentes no ambiente e/ou com potencial de produzir efeitos nocivos ou prejudiciais à saúde humana de maneira individual ou 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 sempre que necessário. A revisão formal ocorre anualmente, acompanhada por indicador específico que avalia a ocorrência de falhas e orienta a proposição de medidas preventivas ou corretivas.

As diretrizes para elaboração e atualização da Matriz estão detalhadas no *REG [sigla do setor] 001 – Matriz de Gestão de Riscos*.

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

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. Esse processo tem como base as atividades críticas mapeadas nos processos organizacionais, o histórico de informações obtido na análise de contexto em que o Grupo IAG Saúde está inserido, as obrigações de compliance e os controles do Anexo A da NBR ISO/IEC 27001.

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 sistema de gestão de compliance ou de segurança da informação.

As informações coletadas são registradas no *REG [sigla do setor] 001 – Matriz de Gestão de Riscos*, estruturada nos seguintes elementos:

1.1. Atividades Críticas do Processo/Análise de Contexto: iniciar pelas ações que ocorrem nos processos internos. Elas estão listadas no Mapa de Processos

POLÍTICA DE GESTÃO DE RISCOS

e no histórico de informações providas da análise do contexto em que o Grupo IAG Saúde está inserido.

1.1.1 Proprietário do Risco: Para assegurar a efetividade da gestão de riscos, cada risco identificado deve possuir um proprietário claramente definido. O proprietário do risco é o 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 descrito no item 1.1 da Matriz. A identificação deve ser precisa, refletindo a área com maior capacidade técnica e autoridade para conduzir as ações necessárias.

Nas Matrizes de Gestão de Riscos Setoriais, o proprietário do risco será a diretoria responsável pelo setor em questão. Cabe a essa diretoria liderar o processo de gestão de riscos, com o envolvimento ativo de sua equipe, assegurando que os riscos sejam tratados de forma integrada à rotina operacional.

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.

POLÍTICA DE GESTÃO DE RISCOS

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 aplicável somente à Matriz de Gestão de Riscos Sistêmica, para os controles das seções 5 Organizacionais, 6 Pessoas, 7 Físicos e 8 Tecnológicos.

Identificar o(s) valor(es) do(s) atributo(s) relacionado(s) ao controle pertinente – Confidencialidade, Integridade e Disponibilidade – conforme especificado na 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. Essa documentação assegura a rastreabilidade das decisões e fortalece a consistência dos controles implementados.

4.2 ANÁLISE DO RISCO

A análise dos riscos refere-se ao desenvolvimento da compreensão do risco. Ela fornece informações para tomada de decisão sobre o tratamento dos riscos e identificação das estratégias de tratamento mais adequadas. Portanto, para a compreensão do risco, analisam-se:

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

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*. (Baixa = 1, Média = 2, Alta = 3).

2.4 Gravidade: indica a intensidade do dano da consequência, caso a falha ocorra. Ver os critérios estabelecidos na *Tabela 2 – Gravidade*. (Leve = 1, Moderada = 2, Grave = 3).

2.5 Nível de Risco Inerente: nível de risco calculado (Probabilidade x Gravidade) na ausência de quaisquer controles ou desconsiderando a eficácia dos controles existentes. O resultado define o risco como Baixo (1 e 2), Médio (3 e 4) ou Alto (6 a 9). Este deve ser calculado para **todos** os riscos (novos e antigos) no ciclo atual. Representa o risco bruto, desconsiderando os controles. Serve para dimensionar a **importância estratégica** do risco. Não é a base para as ações do próximo ciclo, mas sim para entender a gravidade do *risco em potencial*.

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 2.7) com o desempenho do período anterior. Se o item 2.7 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.

2.7 Nível de Risco Residual (Ciclo em atualização): Risco Líquido em atualização. Este valor é a base para as ações de Tratamento do novo ciclo (Item 4). Representa

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

o risco atual com os controles existentes. Se este nível estiver acima do tolerável, ele deve ser tratado, e o plano de ação resultante (Seção 4.3) será o trabalho de mitigação a ser realizado no ciclo em atualização.

Anualmente a área revisa a Matriz de Gestão de Risco, identifica a nova gradação de risco (probabilidade X gravidade) e compara 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 (chance de algo ocorrer) baseia-se em dados quantitativos sempre que possível, podendo ser evidenciados 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

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

A Tabela 2 Gravidade, especifica os 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. São 3 opções: 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

POLÍTICA DE GESTÃO DE RISCOS

- **Nível do Risco (probabilidade X gravidade):** multiplicação da probabilidade e gravidade. Identifica o nível do risco no período de referência da Matriz de Gestão de Risco.

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.

4.1. AVALIAÇÃO DO RISCO

A avaliação do risco auxilia a tomada de decisões com base na análise dos riscos. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação adicional, que pode ser aceitar, reduzir, compartilhar, evitar.

As etapas para avaliação de riscos consideram os itens a seguir:

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

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

mantém o risco. Os controles de segurança da informação descritos nesta etapa são fundamentados na Declaração de Aplicabilidade (SoA), documento que registra a decisão sobre quais controles do Anexo A da ISO/IEC 27001 foram implementados e a justificativa para aqueles não adotados. Essa integração fortalece a transparência do processo decisório e a rastreabilidade das ações de mitigação.

3.2 Tipo de Controle: determina o tipo de controle e sua pontuação – Automatizado = 3; Misto = 2 e Manual = 1.

3.3 Capacidade de Bloqueio: determina a capacidade de bloqueio e sua pontuação – Detectivo = 1 e Preventivo = 2.

3.4 Aplicação do controle: determina a situação atual implantação do controle, com atribuição de pontuação – Parcial = 1 ou Total = 2.

3.5 Nível de Controle: indica a eficiência do controle e aponta o valor concebido pela falha, avaliado nos itens anteriores – Tipo de Controle + Capacidade de Bloqueio + Aplicação).

3.6 Apetite ao Risco e Risco Residual no Tratamento de Riscos

A Diretoria é responsável por definir a estratégia a ser adotada diante dos riscos mapeados e avaliados, categorizados da seguinte forma: aceitar, reduzir, compartilhar, transferir ou evitar. Essa decisão é orientada pela comparação entre o risco avaliado e o nível de exposição previamente estabelecido, o qual reflete o Apetite ao Risco da organização. Esse conceito estratégico representa o grau de risco que a organização está disposta a assumir para atingir seus objetivos, funcionando como um parâmetro essencial para decisões e prioridades no âmbito da gestão de riscos. Os critérios que norteiam o Apetite ao Risco são os seguintes:

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

POLÍTICA DE GESTÃO DE RISCOS

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 de um 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.

Moderado Apetite ao Risco (tolerância calculada). A Diretoria 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).

POLÍTICA DE GESTÃO DE RISCOS

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

Alto Apetite ao Risco (posição ousada). A Diretoria 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.

Após a implementação das opções de tratamento de riscos, o **Risco Residual** é o risco que permanece. A organização deve decidir se o risco remanescente é aceitável e, se não for, realizar tratamento adicional. Convém que os tomadores de decisão e outras partes interessadas estejam conscientes da natureza e extensão do risco remanescente (residual).

A partir da determinação do nível de controle, são definidos os tipos de resposta ao risco.

POLÍTICA DE GESTÃO DE RISCOS

3.7 Tipo de resposta ao risco:

- **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 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

4.2 TRATAMENTO DO RISCO

O tratamento do risco será realizado quando o nível de risco estiver acima do nível de risco tolerável e será aplicado sobre as causas e os efeitos, de modo a reduzir a probabilidade e o impacto ajustados.

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

O tratamento dos riscos envolve a identificação das diversas opções para tratar os riscos, a análise e a avaliação dessas opções, a preparação e a implementação de planos de ação.

As opções para tratar o risco podem envolver um ou mais dos seguintes itens e são validados pela Diretoria:

Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;

Assumir ou aumentar o risco de maneira a perseguir uma oportunidade;

Remover a fonte de risco;

Mudar a probabilidade;

Mudar as consequências;

Compartilhar o risco;

Reter o risco por decisão fundamentada.

Os riscos podem ser trabalhados em conjunto em reuniões setoriais, nos programas de treinamento e capacitação, planos de ação e relatos de não conformidade, independentemente da pontuação atingida.

4.1 Correção: é a ação frente à falha/erro a ser tomada para mitigação da falha/erro identificados.

4.2 Contingência: determinar a ação a ser tomada para assegurar a continuidade da atividade crítica, do processo, dos objetivos de compliance.

4.3 Ação Corretiva: especificar o plano de ação, projeto ou controle a ser elaborado ou melhorado para monitoramento do risco identificado.

POLÍTICA DE GESTÃO DE RISCOS

As ações são validadas pela Diretoria e podem envolver planos de ação, correções, contingências ou ações corretivas. Os controles implementados devem ser coerentes com aqueles documentados na SoA, assegurando eficácia e conformidade.

4.3 MONITORAMENTO DO RISCO E EVIDÊNCIA DA OCORRÊNCIA DE FALHAS

O monitoramento de ocorrência das falhas pode ser definido de diferentes formas:

Indicador Base SigQuali; Indicador Outra Base; Registro/Controle ou uma combinação entre Indicador e Registro. Mensalmente todos os setores da instituição monitoram o indicador "Percentual de ocorrência do risco", por meio do formulário "*MGR [sigla do setor] 001 - Monitoramento da Gestão de Riscos*", cujo propósito é melhorar e assegurar a qualidade e eficácia do gerenciamento de riscos.

A área da Qualidade e Compliance realiza, semestralmente, uma análise global dos riscos identificados pelos setores de forma a determinar se permanecem adequados para apoiar o alcance dos objetivos do Grupo IAG Saúde.

A consistência entre os indicadores monitorados e os controles descritos na SoA é verificada durante a análise global de riscos. Quaisquer alterações nos níveis de risco ou ocorrência de falhas relevantes podem demandar atualização da SoA, conforme evidenciado nos formulários e registros.

5. 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](#)

Este documento e seus anexos são públicos e suas informações podem ser divulgadas externamente. Se você o recebeu por engano, favor entrar em contato com o remetente imediatamente e apagá-lo de seus arquivos. Qualquer uso não autorizado, replicação ou disseminação deste documento ou parte dele é proibido. Antes de imprimir, pense no meio ambiente.

POLÍTICA DE GESTÃO DE RISCOS

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.

6. REGISTROS

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

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

7. REFERÊNCIAS

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

POLÍTICA DE GESTÃO DE RISCOS

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.