GRUPO IAG SAÚDE

Política de Gestão de Riscos

POLÍTICA DE GESTÃO DE RISCOS

1. OBJETIVO

O objetivo da Gestão de Risco é contribuir para implementação de ações que permitam um sistemático reconhecimento, identificação, avaliação, controle e gerenciamento de riscos de compliance e de segurança da informação, relacionados às obrigações de compliance, às atividades, produtos, serviços e aspectos pertinentes às operações, assim como riscos relacionados ao Compliance, Estratégicos, Financeiros, Imagem, Ocupacionais, Operacionais, e Segurança da Informação, à confidencialidade, integridade e disponibilidade das informações, entre outros presentes nos processos do Grupo IAG Saúde.

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).

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. Exemplo de ambiente interno: missão, valores, estratégias, políticas e procedimentos, cultura de compliance, relações com as partes interessadas e ambiente externo: social, cultural, político, legal, regulatório, financeiro, tecnológico, internacional, nacional ou local (adaptado da 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, individualmente ou combinado, tem o potencial para dar origem ao risco, podendo ser, por exemplo pessoas, processos, sistemas, infraestrutura física ou organizacional, tecnologia de produto ou de produção ou eventos externos (não-gerenciáveis). (ANS, 2018).

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

Impacto ou dano: resultado de um evento que afeta os objetivos.

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

Probabilidade: chance de algo ocorrer / o quanto ocorre no contexto analisado.

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

4. DIRETRIZES

A metodologia utilizada pelo Grupo IAG Saúde para gerenciar riscos abrange todos os itens e requisitos do Processo de Gestão de Riscos definido no referencial normativo NBR ISO 31000:2018, conforme Figura 1 – Processo de Gestão de Riscos.

O gerenciamento de riscos de compliance e de segurança da informação, estão, portanto, incorporados à cultura de compliance e aos pilares fundamentais da segurança da informação: confidencialidade – envolve os esforços empregados para garantir que os dados sejam mantidos em segredo ou privados; integridade – garante que os dados sejam corretos, autênticos e confiáveis, ou seja, que os dados

não foram adulterados e, portanto, podem ser confiáveis e disponibilidade – garante que sistemas, aplicativos e dados estejam disponíveis e acessíveis para usuários autorizados quando eles precisarem.

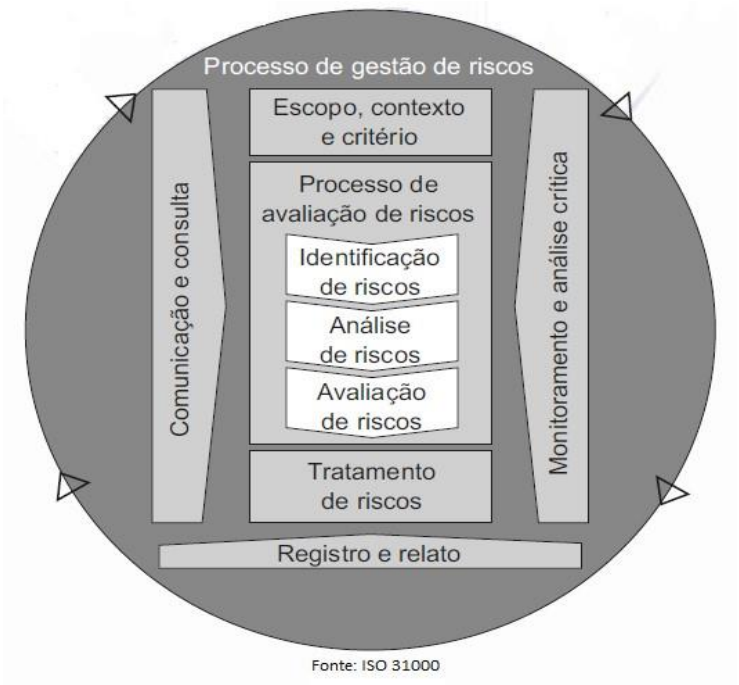

Figura 1 – Processo de Gestão de Riscos.

- **Comunicação e Consulta:** A comunicação procura promover a conscientização e o entendimento do risco a todos os funcionários do Grupo IAG Saúde, enquanto a consulta envolve ações para obter retorno e informação para auxiliar a tomada de decisão.
- **Escopo, contexto e critérios:** A prática de gestão de riscos é parte integrante de todos os processos do Grupo IAG Saúde, uma vez que a identificação dos riscos é realizada através do desdobramento dos processos críticos em atividades críticas e na análise de contexto, tendo como resultado a definição dos objetivos de compliance e de segurança da informação.

POLÍTICA DE GESTÃO DE RISCOS

O Grupo IAG Saúde definiu os domínios de risco que serão monitorados pelos setores, conforme quadro abaixo:

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.

Os setores devem elaborar a Matriz de Gestão de Risco e atualizar as informações sempre que necessário. A revisão da ferramenta acontecerá anualmente, e o acompanhamento será feito através de indicador específico em que os setores

deverão analisar as ocorrências das falhas e propor novas situações e ações frente aos riscos.

As orientações para a gestão de riscos estão especificadas no *REG IAG 211 Matriz de Gestão de Riscos*.

4.1 PROCESSO DE AVALIAÇÃO DE RISCOS

4.1.1 IDENTIFICAÇÃO DO RISCO

As fontes de risco, áreas de impacto, eventos e suas causas e consequências potenciais são identificados através das atividades críticas dos processos definidos nos mapas de processos e no histórico de informações provindas da análise do contexto em que o Grupo IAG Saúde está inserido. Para identificação dos riscos de cada categoria podem ser utilizadas técnicas de *brainstorming* entre os envolvidos no processo e a *expertise* dos gestores do setor. Os riscos podem ser identificados a partir dos objetivos de compliance, na execução de rotinas estabelecidas em documentos internos, no cumprimento de leis e outras normas externas, no cumprimento de requisitos da Cadeia Cliente Fornecedor, nas auditorias interna e/ou externa, nos resultados de indicadores e durante a implantação de mudanças que possam afetar o sistema de gestão de compliance e de segurança da informação.

As informações obtidas são traduzidas no *REG IAG 211 Matriz de Gestão de Riscos*, que é composta por:

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 em que o Grupo IAG Saúde está inserido.

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.

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.

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:

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

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. Nomear a forma de monitoramento da probabilidade – indicador, registro/controle, ou a combinação de ambos.

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 Atual: define a escala de gradação dos riscos a partir do resultado da multiplicação entre os níveis de gravidade e probabilidade. Deve-se ainda, identificar o *Nível de Risco Anterior* nas análises subsequentes e registrar na Matriz. Ver os critérios estabelecidos na *Tabela 3 – Nível de Risco*.

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. Dessa forma avalia a necessidade de tratamento e estabelece as ações e a apreciação das causas e fontes de risco, consequências positivas ou negativas etc..

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.

POLÍTICA DE GESTÃO DE RISCOS

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

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.

POLÍTICA DE GESTÃO DE RISCOS

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

POLÍTICA DE GESTÃO DE RISCOS

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 mantém o risco.

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).

A Diretoria define a estratégia a ser adotada, seja ela – aceitar, reduzir, compartilhar ou transferir ou evitar – em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecidos em confronto com a avaliação que se fez do risco.

Se for identificada disparidade entre os níveis de risco avaliados e aqueles percebidos pelo gestor do processo, é realizada uma investigação para determinação da situação que melhor represente a realidade.

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

3.6 Tipo de resposta ao risco:

Aceitar: os controles são implantados e uma modificação pode acarretar um investimento desproporcional ao benefício. Manter o controle implementado e monitorado de forma a garantir que seu nível de risco está dentro do que foi pré-estabelecido.

Reduzir: agir tanto sobre as causas como sobre as consequências do risco e avaliar se os controles são suficientes para mitigar os riscos, ou seja, reduzir a probabilidade ou o impacto de uma ameaça, tornando-a um risco menor.

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. A transferência do risco implica também na transferência das respostas ao risco. Mas atenção: transferir o risco não o elimina. A transferência dos riscos deve ser comunicada e gerenciada em outro processo.

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

Após a definição destes parâmetros o software 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, respectivamente.

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.

4.3 MONITORAMENTO DO RISCO E EVIDÊNCIA DA OCORRÊNCIA DE FALHAS

O monitoramento de ocorrência das falhas pode ser definido de diferentes formas: indicador, registro, não conformidade, expertise. Mensalmente todos os setores da instituição monitoram o indicador "Percentual de ocorrência do risco", cujo

propósito do monitoramento e análise crítica é melhorar e assegurar a qualidade e eficácia do gerenciamento de riscos.

A área da Qualidade e Compliance realiza, trimestralmente, 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.

5 REGISTROS

REG IAG 211 Matriz de 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.