GRUPO IAG SAÚDE

Política de Gestão de Riscos

POLÍTICA INSTITUCIONAL - PADRÃO: POI IAG 007

POLÍTICA DE GESTÃO DE RISCOS

Versão: 05

Aprovação: Alta Direção

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, relacionados às obrigações de compliance às atividades, produtos, serviços e aspectos pertinentes às operações, assim como riscos relacionados à saúde ocupacional, imagem, mercado, financeiro, entre outros presentes nos processos do Grupo IAG Saúde.

O gerenciamento dos riscos visa estimular a adoção de práticas de gestão de risco em diferentes níveis e dentro dos contextos específicos da organização, permitir que as informações sobre riscos provenientes desse processo sejam adequadamente reportadas e utilizadas como base para tomada de decisões e a responsabilização em todos os níveis organizacionais aplicáveis. Para organizações, um único meio viável para controlá-los é através de uma abordagem de sistemas de gestão, sendo de responsabilidade dos gestores sua aplicabilidade.

2. ABRANGÊNCIA

Todos os setores do Grupo IAG Saúde.

3. SIGLAS E DEFINIÇÕES

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

Controle: Medida que está modificando o risco. Ação que bloqueia a continuidade da falha (ISO 31000/2018).

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.

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.

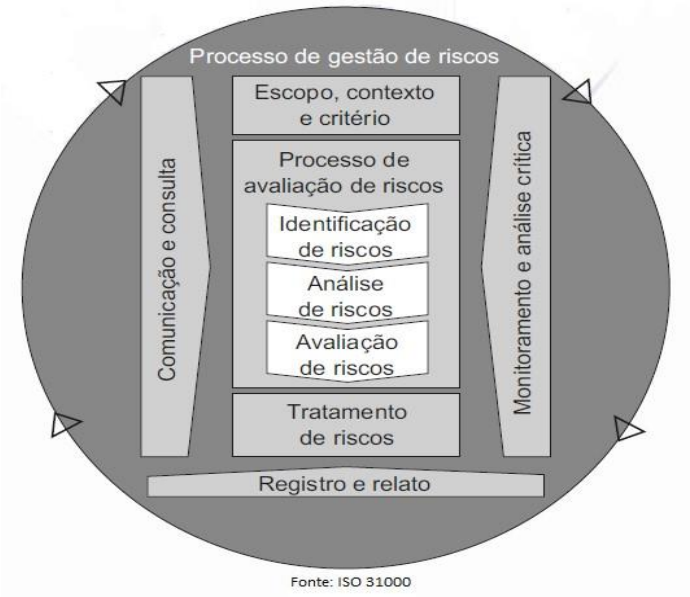
ISO: International Organization for Standardization (Organização Internacional de Normalização)

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.



Fonte: ISO 31000

- **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 desempenhadas por cada setor conforme matriz de gestão de risco.

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.

Ocupacional	Possibilidade de o funcionário ter sua saúde acometida pelos riscos ocupacionais (químicos, físicos e/ou ergonômicos) ou pelas condições de trabalho. Refere-se também a possibilidade de ocorrência de acidente no local de trabalho ou de trajeto.
Imagem	Quando houver probabilidade do produto ou serviço gerar insatisfação do cliente interno ou externo. Refere-se também a probabilidade de dano a reputação conquistada pelo IAG Saúde no mercado.
Compliance	Refere-se ao descumprimento de obrigações e a não conformidade na execução em relação a regulamentos internos e externos, políticas e/ou procedimentos.
Desabastecimento	Probabilidade de faltar consultor (mão de obra), equipamentos, sistema e outros meios necessários à realização e/ou entrega do serviço/ produto.
Financeiro	Custos, despesas, perda de receita que possam afetar a saúde financeira do negócio.
Mercado	Perdas que podem ser ocasionadas por mudanças no comportamento do mercado de atuação da organização. Pode ser definido também pelo risco de perda de clientes devido a propostas concorrentes mais atrativas de produtos ou serviços.

Os setores devem elaborar a Matriz 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.

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 dos processos críticos definidos nos mapas de

processos e no desdobramento deste processo em atividades críticas. Para identificação dos riscos de cada categoria são utilizadas técnicas de brainstorming entre os envolvidos no processo e a expertise dos gestores do setor. Os riscos podem ser identificados a partir do descumprimento de rotinas estabelecidas em documentos internos, descumprimento de leis e outras normas externas, descumprimento de requisitos da Cadeia Cliente Fornecedor, não conformidades de auditoria interna e/ou auditoria externa, resultados de indicadores e durante a implantação de mudanças que possam afetar o sistema de gestão.

As informações obtidas são traduzidas na Matriz de Gestão de Riscos, que é composta por:

- **Motivo (Classificação 6M's):** Identificação de 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).
- **Causa** (Descrição das causas da falha/erro): Breve descrição das causas.
- **Consequência** (Descrição da consequência imediata - impacto - se a falha/erro ocorrer): Descrição do impacto imediato caso a falha/erro ocorra.
- **Domínio** (Classificação do domínio do risco): Seleção de uma categoria de domínio do risco caso o evento ocorra.

4.2 ANÁLISE DO RISCO:

A análise dos riscos refere-se ao desenvolvimento da compreensão do risco. Ela fornece informações para que decida sobre o tratamento dos riscos e identifique as estratégias de tratamento mais adequadas.

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.

- **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: se a opção for "leve" a pontuação é 1; se "moderada" é 2; se "grave" é 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.

- **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 um a boa relação custo benefício. São 3 opções: baixa, média ou alta. Cada opção tem uma pontuação específica: se a opção for "baixa" a pontuação é 1; se "média" é 2; se "alta" é 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.

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

PONTUAÇÃO	NÍVEL DE RISCO	DESCRIÇÃO
6 a 9	ALTA	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.
3 e 4	MÉDIA	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.
1 e 2	BAIXA	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.

- **Controles existentes:** atividades realizadas e registros utilizados, que se executados corretamente previnem o risco, caracterizados

como mecanismos/barreiras, estes devem ser descritos nas rotinas (POP's) relacionados à atividade.

Nível do controle: Identifica a eficiência do controle e verifica o valor concebido pela falha/matriz de (Tipo de Controle + Capacidade de Bloqueio + Aplicação):

Tipo de controle:

- Automatizado = 3
- Misto = 2
- Manual = 1

Capacidade de bloqueio: Detectivo ou Preventivo;

- Detectivo = 1
- Preventivo = 2

Aplicação: Ausente, Parcial, Total;

- Parcial = 1
- Total = 2

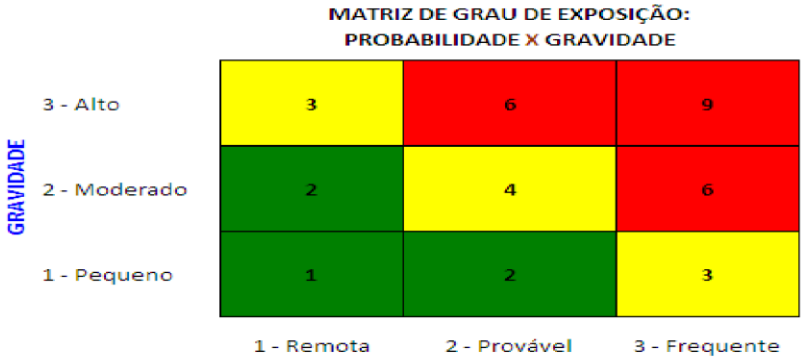
Após a definição destes parâmetros o software irá exibir a cor conforme as definições abaixo:

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

4.1. AVALIAÇÃO DO RISCO:

A avaliação de risco auxilia a tomada de decisões com base na análise dos riscos. A avaliação do risco envolve comparar a tendência do indicador que monitora o risco com a meta estabelecida, referencial externo (registros de observação) ou chances de ocorrência para definir sua probabilidade.

Após a definição da probabilidade e gravidade multiplica-se os resultados e identifica-se em qual quadrante o risco encontra-se (gradação/pontuação), conforme abaixo:



· **Referencial comparativo (Indicador ou observação relacionados):** Neste campo é descrito nome do indicador diretamente relacionado ao impacto do risco (deve monitorar se o mesmo ocorre), se houver. Se a opção é "observação", é informado o registro que acompanhará a ocorrência e tendência.

4.2 TRATAMENTO DO RISCO:

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

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.

- **Prevenção** (Documentos onde estão descritas ações de prevenção/barreira da ocorrência da falha/erro): é informada a identificação do procedimento descrito relacionado à prevenção (Ex: POP IAG XXX).
- **Correção** (Correção frente à falha/erro): é informada a ação imediata a ser tomada para mitigação da falha/erro, caso ocorra.
- **Contingência** (Contingência frente à falha/erro): descrição das ações a serem tomadas para impedir a descontinuidade da atividade crítica.
- **Ação Corretiva** (Plano de ação relacionado): é informado o nº do Plano de Ação elaborado para monitoramento do risco, se aplicável.

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.

5 REGISTROS

Não se aplica.

6 REFERÊNCIAS

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

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

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 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 Sistema de gestão de compliance – Requisitos com orientações para uso. ABNT, 2021.