METODOLOGIA DE GESTÃO DE RISCOS

**MINISTÉRIO DA SAÚDE**

Esplanada dos Ministérios, Bloco G, Edifício Sede, Brasília – DF 70058-900 **-** Brasília-DF

**Equipe**

**Diretoria de Integridade – DINTEG/MS**

Carolina Palhares Lima - Diretora de Integridade

Nilton Carlos Jacintho Pereira - Assessor da Diretoria deIntegridade

**Coordenação-Geral de Controle Interno –CGCIN/DINTEG/MS**

Aline Ribeiro - Coordenadora-Geral de Controle interno

**Coordenação de Gestão de Riscos – COGER/CGCIN/DINTEG/MS**

Francisco José Ribeiro Facchinetti - Coordenador de Gestão deRiscos

**SUMÁRIO**

[**1.** **INTRODUÇÃO** 5](#_Toc67810486)

[**2.** **Estrutura da Governança da Gestão de Riscos no MS** 5](#_Toc67810487)

[**2.1** **Comitê Interno de Governança - CIG** 5](#_Toc67810488)

[**2.2** **Comitê de Gestão de Riscos - CGR** 6](#_Toc67810489)

[**2.3** **Unidade de Gestão de Riscos e Integridade - UGRI** 7](#_Toc67810490)

[**2.4** **Gestor de Processo - GP** 8](#_Toc67810491)

[**2.5** **Diretoria de Integridade - DINTEG** 9](#_Toc67810492)

[**3.** **MÉTODO DE PRIORIZAÇÃO DE PROCESSOS** 10](#_Toc67810493)

[**4.** **PLANO DE GESTÃO DE RISCOS** 13](#_Toc67810494)

[**5.** **PROCESSO DE GERENCIAMENTO DE RISCOS** 15](#_Toc67810495)

[**5.1** **Entendimento do Contexto** 16](#_Toc67810496)

[**5.2** **Identificação e análise dos Riscos** 17](#_Toc67810497)

[**5.3** **Avaliação dos Riscos** 20](#_Toc67810498)

[**5.4** **Resposta aos Riscos** 24](#_Toc67810499)

[**5.5** **Monitoramento e Análise Crítica** 26](#_Toc67810500)

[**5.6** **Registro e Comunicação** 27](#_Toc67810501)

[**6.** **CONSIDERAÇÕES FINAIS** 28](#_Toc67810502)

[**REFERÊNCIAS BIBLIOGRÁFICAS** 29](#_Toc67810503)

[ANEXO I – GERENCIAMENTO DE RISCOS 30](#_Toc67810504)

[ANEXO II – FLUXOGRAMA: GESTÃO DE RISCOS 39](#_Toc67810505)

 [39](#_Toc67810506)

[ANEXO III – ATRIBUIÇÕES E COMPETÊNCIAS DOS ATORES 40](#_Toc67810507)

 [40](#_Toc67810508)

# **INTRODUÇÃO**

A proposta desta metodologia é apresentar os principais referenciaisque norteiam o Ministério da Saúde sua estrutura de governança, gestão de riscos, método de priorização dos processos e nas etapas do seu gerenciamento. Os riscos considerados estratégicos assumem uma importância maior pelo efeito que podem provocar na organização, merecendo, dessa forma, especial atenção dos gestores que formulam e aprovam as estratégias.

Esta metodologia foi elaborada a partir da Política de Gestão de Riscos-PGR e representa um instrumento importante para sua implementação.Ela não tem o objetivo de esgotar o assunto e informações.

# **Estrutura da Governança da Gestão de Riscos no MS**

A Governança da Gestão de Riscos prescinde de clareza dos papéis e das responsabilidades, a fim de trazer segurança processual, suporta os processos de gestão de riscos, assegurar a qualidade das informações e o reporte tempestivo.

# **Comitê Interno de Governança - CIG**

Composto pelo SecretárioExecutivo e pelos titulares das Secretarias do Ministério da Saúde e criado no termo da Portaria GM/MS nº 347, de 5 março de 2021.

O CIG auxilia a alta administração na implementação e na manutenção de processos, estruturas e mecanismos adequados à incorporação dos princípios e das diretrizes de governança, conforme abaixo:

I – assegurar o alinhamento da gestão de riscos com os objetivos do planejamento estratégico institucional;

II – aprovar a Política, a Metodologia e o Plano de Gestão de Riscos;

III – definir o apetite ao risco e deliberar sobre as propostas de alteração dos níveis de exposição a riscos que possam impactar o alcance dos objetivos institucionais;

IV – assegurar que as informações relevantes sobre a gestão de riscos estejam disponíveis para subsidiar a tomada de decisão;

V – assegurar a utilização de mecanismos de comunicação e de institucionalização da gestão de riscos;

VI – deliberar sobre o resultado da avaliação de desempenho institucional da gestão de riscos;

VII – assegurar a realização de ações que incentivem e promovam a cultura e a capacitação na gestão de riscos; e

VII – assegurar alocação dos recursos necessários à gestão de riscos.

Em resumo, compete ao CIG assegurar a estrutura de governança de gestão de riscos do Ministério da Saúde.

# **Comitê de Gestão de Riscos - CGR**

Composto por representantes das Secretarias, indicados pelos Secretários das pastas, com cargo de Direção e Assessoramento Superior (DAS) 5 ou equivalente, que tenha conhecimento em gestão de riscos e autonomia para tomada de decisão, deverão:

I – promover o alinhamento da gestão de riscos com os objetivos do planejamento estratégico institucional;

II – avaliar as propostas de Política e de Metodologia de Gestão de Riscos para submetê-las ao CIG;

III – avaliar o Plano de Gestão de Riscos consolidado pela DINTEG e definir quais processos serão sugeridos ao CIG para integrar ao mesmo;

IV – manifestar sobre o apetite ao risco e sobre as propostas de alteração dos níveis de exposição a riscos recebidos das UGRI’s, para submetê-los aos CIG;

V – comunicar, ao CIG, informações relevantes sobre a gestão de riscos para subsidiar o processo de tomada de decisão;

VI - aprovar mecanismos de comunicação da gestão de riscos;

VII- aprovar os Planos de Respostas aos Riscos;

VIII - analisar o relatório de avaliação de desempenho institucional da gestão de riscos e submetê-lo ao CIG; e

IX– apoiar as ações que incentivem e promovam a cultura e a capacitação em gestão de riscos.

O CGR é responsável por receber e avaliar políticas, normas, metodologias, planos e outros documentos propostos, manifestar-se e encaminhar ao CIG para aprovação.

# **Unidade de Gestão de Riscos e Integridade - UGRI**

Composta, em cada Secretaria e Superintendência Estadual do Ministério da Saúde (SEMS), por profissionais com conhecimento em gestão de riscos e vinculados, hierarquicamente, às Unidades Organizacionais e, tecnicamente, à Diretoria de Integridade (DINTEG).

AsUGRI’ssão os pontos focais da gestão de riscos nas Unidades e deverão:

I – coordenar o gerenciamento de riscos dos processos de sua Unidade Organizacional;

II – assegurar o alinhamento do processo de gerenciamento de riscos da sua Unidade Organizacional com os objetivos do planejamento estratégico institucional;

III – apoiar e monitorar o processo de gerenciamento de riscos da sua Unidade Organizacional;

IV – consolidar as informações apresentadas pelos Gestores de Processos-GP e propor os processos prioritários de sua Unidade Organizacional para compor o Plano de Gestão de Riscos;

V – assegurar o cumprimento do apetite ao risco definido e submeter as propostas de alteração dos níveis de exposição a riscos ao titular da Unidade Organizacional;

VI – comunicar, ao titular da Unidade Organizacional, as informações relevantes sobre a gestão de riscos para subsidiar o processo de tomada de decisão;

VII – avaliar os Planos de Respostas aos Riscos elaborados pelos Gestores de Processos, submetê-los ao titular da Unidade Organizacional para aprovação e encaminhá-los à DINTEG;

VIII – analisar e emitir opinião sobre os Relatórios de Gestão de Riscos elaborados pelos Gestores de Processos, submetê-los ao titular da Unidade Organizacional e encaminhá-los à DINTEG;

IX – apoiar a cultura e as ações de capacitação em gestão de riscos; e

X – atuar na articulação com os Gestores de Processos e com as demais Unidades responsáveis pela gestão de riscos no MS.

Ou seja, a UGRI é responsável por avaliar os resultados dos trabalhos de gestão de riscos, manifestar-se e encaminhar ao titular da Pasta para aprovação e posterior envio à DINTEG.

# **Gestor de Processo - GP**

Responsável direto por determinado processo, inclusive pelo seu gerenciamento de riscos. Tem a competência direta pela aplicação de métodos e metodologias para o gerenciamento dos riscos dos processos sob a sua gestão, em cumprimento às orientações, normas e políticas afetas ao tema, devendo:

I – alinhar o processo de gerenciamento de riscos com os objetivos do planejamento estratégico institucional;

II – aplicar a Metodologia e utilizar as ferramentas da gestão de riscos nos processos sob sua responsabilidade;

III – selecionar os processos sob sua responsabilidade que devam ter os riscos gerenciados e tratados com prioridade e propor sua inclusão no Plano de Gestão de Riscos;

IV – observar o apetite ao risco definido e propor alterações  dos níveis de exposição a riscos, quando for o caso;

V – gerar e comunicar, à UGRI, informações relevantes sobre a gestão de riscos para subsidiar o processo de tomada de decisão;

VI – elaborar o Plano de Resposta aos Riscos dos processos sob sua responsabilidade;

VII – avaliar os resultados da execução dos Planos de Resposta aos Riscos;

VIII – elaborar os Relatórios de Gestão de Riscos dos processos sob sua responsabilidade e encaminhar à UGRI para análise;

IX – estimular a cultura e a capacitação em gestão de riscos; e

X – averiguar, ao longo do tempo, se os riscos de seus processos estão em níveis aceitáveis, considerando os controles implementados.

Ou seja, é responsável pelo monitoramento, elaboração e envio de informações sobre o processo de gerenciamento de riscos sob a sua gestão, de acordo com as orientações disponíveis.

# **Diretoria de Integridade - DINTEG**

Composta por agentes públicos com capacitação em temas afetos à gestão de integridade, de riscos e de controles internos da gestão, a DINTEG deverá:

I – supervisionar o alinhamento da gestão de riscos com os objetivos do planejamento estratégico institucional;

II – propor Política, Metodologia e normas para a gestão de riscos;

III – apoiar e assessorar as UGRI’s no processo de gerenciamento de riscos das suas Unidades Organizacionais;

IV – consolidar as informações apresentadas pelas UGRI’s para subsidiar a elaboração da proposta do Plano de Gestão de Riscos e sugerir ajustes, se for o caso;

V – contribuir com a definição de apetite ao risco e monitorar as propostas de alteração dos níveis de exposição a riscos das Unidades Organizacionais;

VI – propor mecanismos de comunicação e de institucionalização da gestão de riscos;

VII – consolidar e comunicar, ao CGR e ao CIG, as informações relevantes sobre a gestão de riscos para subsidiar o processo de tomada de decisão;

VIII – manifestar sobre os Planos de Respostas aos Riscos das Unidades Organizacionais, encaminhando ao CGR para análise e aprovação;

IX – acompanhar a implementação dos Planos de Respostas aos Riscos e comunicar o seu estágio de execução ao CGR;

X – elaborar, anualmente, o relatório de avaliação de desempenho institucional da gestão de riscos e submetê-lo ao CGR;

XI – promover a cultura e as ações de capacitação em gestão de riscos;

XII – acompanhar o resultado da gestão de riscos e propor os encaminhamentos necessários;

XIII – apoiar a implantação e melhoria contínua do processo de gerenciamento de riscos; e

XIV – assessorar tecnicamente o Comitê Interno de Governança e o Comitê de Gestão de Riscos.

A DINTEG é responsável por assessorar tecnicamente o CIG, o CGR e as UGRI’s no processo de gestão de riscos e, como segunda linha de defesa (IIA, 2020), deve acompanhar e monitorar o gerenciamento de riscos no Ministério da Saúde.

# **MÉTODO DE PRIORIZAÇÃO DE PROCESSOS-MPP**

O Método de Priorização de Processos-MPP é uma ferramenta adaptadaaoMinistério da Saúde e contribui para o estabelecimento de processos prioritários para gerenciamento de riscos, uma vez que é possível classificá-los pela Cadeia de Valorem prioridades**Alta**, **Média** e **Baixa**, em função do seu grau de exposição a riscos.

O MPP deverá ser utilizado pelas Unidades para auxiliar na classificação dos processos prioritários (estratégicos) sob a sua gestão, cujo resultado será analisado pela UGRI e incluído no Plano de Gestão de Riscos da Unidade. Após aprovação do titular da Pasta, a UGRIdeve encaminhar a classificação à DINTEG para compor o Plano de Gestão de Riscos do Ministério. A seguir, de forma detalhada, o método será explicado.

**GUIA DE ORIENTAÇÕES PARA PREENCHIMENTO**

**Método de Priorização de Processos - MPP**



Figura 1 – Esquema lógico de priorização de processos

Fonte: própria do Ministério da Saúde

1. Definição de Pesos

Para definição de pesos será utilizada ferramenta baseada na *AnalyticHierarchyProcess* – AHP.

A AHP é um método multicritério que permite definir uma hierarquia para calcular prioridades e avaliar um conjunto de alternativas, originalmente desenvolvido pelo Prof. Thomas L. Saaty.

O método também permite "traduzir" opiniões subjetivas, tais como preferências ou percepções, em relações numéricas mensuráveis, nisso AHP ajuda a tomada de decisões de uma forma mais racional, transparente e melhor compreensível.

Com base na ferramenta AHP, disponível em Excel, será possível calcular os pesos a serem utilizados nos critérios da avaliação quantitativa e qualitativa do MPP, com base em julgamento/comparações de pares, os participantes da reunião determinarão a importância relativa de uma alternativa com relação à outra.

1. Quantitativa X Qualitativa – 1º Julgamento dos Participantes

Utilize a planilha QUANTI X QUALI e compare a importância da Avaliação Quantitativa em **relação** à Avaliação Qualitativa e preencha a tabela. Qual elemento é mais importante, A ou B. Em seguida atribua valor entre 1 a 9, conforme escala para determinar a importância relativa de uma alternativa com relação a outra, conforme apresentado na tabela específica, ao final.

$$CF=\frac{XX\% \left(avaliação quantitativa\right)+ XX\% (avaliação qualitativa)}{100}$$

|  |  |  |
| --- | --- | --- |
| **Critérios** | **Maisimportante** | **Escala** |
| **A** | **B** | **Aou B** | **(1-9)** |
| AvaliaçãoQuantitativa | AvaliaçãoQualitativa |  |  |

1. Qualitativa – 2º Julgamento dos Participantes

Utilize a planilha QUALI e compare a importância dos fatores definidos para Avaliação Qualitativae preencha a tabela. Qual elemento é mais importante, A ou B. Em seguida atribua valor entre 1 a 9 para determinar a importância relativa de uma alternativa com relação a outra, conforme apresentado na tabela específica, ao final.

| **Critérios** | **Maisimportante** | **Escala** |
| --- | --- | --- |
| **A** | **B** | **Aou B** | **(1-9)** |
| RelevânciaEstratégica do Processo | Demandas do TCU/CGU/MPU |  |  |
|  | Demanda Judicial emSaúde |  |  |
| Recursos Humanos |  |  |
| RecursosTecnológicos |  |  |
|  | EstruturaOrganizacional |  |  |
| Demandas do TCU/CGU/MPU | Demanda Judicial emSaúde |  |  |
|  | Recursos Humanos |  |  |
| RecursosTecnológicos |  |  |
| EstruturaOrganizacional |  |  |
| Demanda Judicial emSaúde | Recursos Humanos |  |  |
|  | RecursosTecnológicos |  |  |
| EstruturaOrganizacional |  |  |
| Recursos Humanos | RecursosTecnológicos |  |  |
|  | EstruturaOrganizacional |  |  |
| RecursosTecnológicos | EstruturaOrganizacional |  |  |

A escala de intensidade sugerida vai de 1 a 9, com 1 significando a indiferença de importância de um critério em relação ao outro, e 9 significando a extrema importância de um critério sobre outro.

Tabela de Importância:

|  |  |  |
| --- | --- | --- |
| **Intensidade** | **Definição** | **Explicação** |
| 1 | Igualimportância | Os elementos contribuem igualmente para o objetivo |
| 3 | Moderadaimportância | De acordo com a experiência e julgamento, um elemento favorece ligeiramente sobre o outro |
| 5 | Grande importância | De acordo com a experiência e julgamento um elemento favorece grandemente sobre outro |
| 7 | Superimportância | Um elemento é altamente favorecido sobre outro, a dominância é verificada na prática |
| 9 | Extrema importância | E possível afirmar que um elemento favorece de forma extrema sobre o outro |
| 2, 4, 6 e 8 | Podem ser usados ​​valores expressos intermediários |

A Coordenação de Gestão de Riscos-COGER disponibilizará a planilha AHP a todas as unidades, que deverão solicitar pelo e-Mail: coger@saude.gov.br.

# **PLANO DE GESTÃO DE RISCOS**

O Plano de Gestão de Riscos é um documento que orienta a operacionalização do gerenciamento de riscos, em cumprimento aos princípios e diretrizes da Política de Gestão de Riscos-PGRe a declaração de apetite ao risco do Ministério da Saúde.

Dessa forma, o Plano de Gestão de Riscos apresentará por Unidade (Secretarias, Departamentos, Coordenações) os processos que terão prioridade no gerenciamento, bem como o cronograma de sistematização das respostas aos riscos.Outro ponto importante, que as unidades devem observar, antes de adentrar no gerenciamento dos riscos, é que o Plano deve sempre estar balizado pelos seguintes pontos:

* Planejamento estratégico, tático e operacional;
* Documentos diversos acerca do processo;
* Especificações e resultados pretendidos;
* Cronograma de execução (físico e financeiro);
* Normas, leis e regulamentos;
* Notícias e informes públicos;
* Livros, artigos e material de pesquisa;
* Registros históricos;
* Projetos, planos e ações.

 Fonte: Adaptado do livro: Como combater o desperdício no setor público (SOUZA, 2019).

O Plano de Gestão de Riscos aprovado será objeto de cumprimento pelas Unidades responsáveis pela sua execução, cujo cumprimento deverá ser monitorado pelo Gestor de Processos, pela UGRI e de forma segregada pela DINTEG, conforme orientações disponíbilizadas.

A estrutura física do Plano de Gestão de Riscos para o desenvolvimento das atividades e tarefas de ações mitigadoras poderá ser estruturado em word, excel ou até mesmo em plataforma computacional, desde que tenha a seguinte configuração mínima:

* Unidade (UGRI);
* Responsável pela Unidade;
* Ponto focal da Unidade;
* Macroprocesso/processo/projeto;
* Custo previsto (caso tenha);
* Data prevista para início da implementação;
* Data prevista para término da implementação;
* Riscos, nível dos riscos, categorias dos riscos, recomendações;
* Plano de resposta, definir tratamento, controles e avaliar resultados;
* Cronograma detalhado por atividades e tarefas;
* Sistemática de monitoramento e comunicação;
* Relatórios parciais de indicadores de resultados.

Nota: essa estrutura é sugestiva e modelos de planilhas e de relatórios poderão ser solicitados à Coordenação de Gestão de Riscos-COGER, pelo e-Mail: coger@saude.gov.br.

O objetivo do Plano de Gestão de Riscos é de iniciar o processo de gerenciamento dos riscos, assim, faz-se necessário o seu alinhamento aos objetivos estratégicos do Ministério e, principalmente, o engajamento das partes interessadas (os donos do negócio) acerca dos macroprocessos, processos ou projetos. O que se pretende é desenvolver planos ágeis de ações, por meio de um processo interrogativo como:

* O que pode dar errado?
* Como e onde podemos falhar?
* Em que somos vulneráreis?
* Quais ativos devemos proteger?
* Como sabemos se nossos objetivos e metas (PPA/PNS) foram alcançados?
* Onde alocamos mais recursos financeiros, orçamentário, humano, materiais, outros?
* Quais atividades são mais complexas e merecem maior atenção?
* Quais são nossas maiores exposições aos riscos de integridade?
* Quais decisões nossas requerem mais atenção, análise e cuidado?

Fonte: Adaptado do livro: Como combater o desperdício no setor público (SOUZA, 2019).

# **PROCESSO DE GERENCIAMENTO DE RISCOS**

O método elaborado para o gerenciamento de riscos no Ministério da Saúde considera as orientações da Política de Gestão de Riscos do MS, dos *frameworks* disponíveis, em especial a Norma ABNT NBR ISO 31000:2018 e o COSO ERM 2017, além de boas práticas aplicáveis à administração pública.

A adoção de um método para gerenciar riscos é de extrema importância e contribuirá para a padronização do processo. Dessa forma, esta metodologia orientará na sistematização da discussão do entendimento do contexto, no processo de avaliação dos riscos, nas respostas a esses, no monitoramento e análise crítica, no registro e relato, e na comunicação e consulta.

Esta metodologia deverá ser aplicada pelas Unidades e tem o objetivo principal de gerenciar os riscos dos macroprocessos e processos finalísticos da Cadeia de Valor do Ministério da Saúde, priorizados pelo Método de Priorização de Processos e registrados no Plano de Gestão de Riscos de cada Unidade.

Ressalta-se que, os processos priorizados para o gerenciamento de riscos deverão ser também mapeados (fluxogramados) pelos seus gestores para em seguida aplicar as cinco grandes etapas, conforme demonstrado na figura seguinte:



Figura 2 – Etapas do Gerenciamento de Riscos

Fonte: Adaptado dos guias de boas práticas CGU, TCU, COSO e ISO

# **Entendimento do Contexto**

Consiste em compreender o ambiente externo e interno noqual osprocessos, cujos riscos serão gerenciados, encontram-se inseridos. Nesta etapa devem ser obtidas pelo menosas seguintes informações do processo objeto do gerenciamento:

* Mapeamento do processo (fluxogramação e descrição, detalhando as principais e grandes etapas do processo e os intervenientes– partes relacionadas);
* Objetivos gerais e específicos ou resultados a serem alcançados: descrição que permita a identificação dos riscos que possam impactar o cumprimento desses objetivos;
* Leis, regulamentos e normas aplicáveis: para permitir a verificação de conformidade e auxiliar na adoção de ações de controle;
* Políticas, objetivos, diretrizes e estratégias;
* UGRI e gestoresresponsáveis pelos processos, que possuem a competência principal pela sua execução e o gerenciamento dos seus riscos (dono do risco);
* Sistemas utilizados na operacionalização dos processos; e
* Cenários considerando oportunidades e ameaças, bem como forças e fraquezas.

Recomenda-se a utilização de ferramentas de extração de dados e informações, que possam ser aplicadas dentro do tempo e espaço.A exemplo no Anexo I – Gerenciamento de Riscos apresentamos de forma detalhada as informações citadas acima, a Matriz SWOT e disponibilizamos também um formulário modelo para lançar as informações sobre os ambientes.

# **Identificação e análise dos Riscos**

Compreende encontrar, reconhecer e descrever riscos que podem impedir o alcance dos objetivos/resultados de um processo objeto do gerenciamento deriscos. A análise dos riscos considera as incertezas,as causas (fontes ou origem do risco)e as consequências. Um risco pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos, ou seja, elementos que, individualmente ou combinados, têm o potencial intrínseco de dar origem ao risco e os possíveis efeitos (impacto),caso o risco se materialize.

**Causas**: condições que dão origem à possibilidade de um risco ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

**Consequências**: o efeito de um risco sobre os objetivos (estratégicos, operacionais, comunicação, conformidade, outros).

**Incerteza**: circunstâncias que ocorrem devido a mudanças ambientais ou ocorrências de fatos que diminuem ou tiram a segurança processual.

**Fonte ou origem do risco**: elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco.

No processo de identificação de riscos, deve-se buscar a participação depessoas que conheçam bem o objeto de gerenciamento.Antes de iniciar a identificação dos riscos, deve-se ter bem claro e descritoo objetivo do processo que se deseja alcançar (pode fixá-lo na parede para ser a todo instante consultado).

Abaixo, listamos aspectos importantes a serem considerados no momento de identificar, reconhecer e descrever um risco:

* responder a seguinte pergunta-chave: o que pode atrapalhar ou até impedir o alcance do objetivo/resultado do processo objeto da análise;
* os riscos representam uma possibilidade, portanto, deverão ser descritas as falhas e inadequações que poderão ocorrer e, não somente, aquelas que já ocorreram;
* atentar, também, para as falhas que implicam em descumprimento de normas internas e externas e que geram ou podem gerar penalidades (ex.: advertências, impedimentos, outros) e/ou sanções (ex.: multas) para a organização;
* considere as principais fontes de riscos: infraestrutura, pessoal, processos, tecnologia, entre outros;
* registre os riscos significativos e relevantes que impeçam o alcance dos objetivos; e
* descarte os riscos irrelevantes para a organização, que na prática só implicam em um aumento do custo com a adoção de controles.

Devem ser utilizadas técnicas/ferramentas que permitam a identificação/reconhecimento do risco, tais como: questionários e *checklist*; *whorkshop* e reuniões (*Brainstorming*); Gravata-borboleta (*Bow-tie*);entrevistas; eoutras. Dentre as principais técnicas e de fácil aplicação, destacam-se:

**Reuniões (*Brainstorming*):** tem por objetivo estimular e incentivar o livre fluxo de geração de ideias possíveis sobre determinado assunto. Neste método, os principais atores envolvidos no processo reúnem-se para apresentar suas ideias, tendo por objetivo contribuir na identificação de falhas potenciais e osriscos associados.

**Entrevistas:** consiste em realizar uma entrevista com os principais agentes envolvidos no processo e especialistas da área buscando assim identificar osriscos.

**Gravata Borboleta (*Bow-tie)*:** nesta técnica, identifica-se o risco e em seguida suas possíveis causas e consequências. A identificação e registro das possíveis causas e consequências contribuirão com a forma de prevenir a ocorrência do risco (controles preventivos) e/ou com as formas de atenuar as consequênciascasooriscosematerialize(controlesdeatenuaçãoerecuperação).

 Os riscos identificados, reconhecidos e registrados devem ser revisados com vistas a serem reformulados, reorganizados de maneira que a sua descrição seja clara o suficiente para ser compreendido e tratado.

Identificados e registrados os riscos e os seus componentes (causas e consequências), deve-se indicar a sua Categoria. No Ministério da Saúde adotam-se as seguintes:

**Estratégico**: risco associado à possibilidade de perda resultante do insucesso das estratégias adotadas, levando-se em conta a dinâmica da atuação (sociedade, fornecedores e orçamento) e as alterações políticas e econômicas no País e fora dele, ou seja, qualquer incerteza que afeta a realização das diretrizes estratégicas.

A gestão dos riscos estratégicos passa a ser elemento-chave para o sucesso e a sobrevivência das organizações; é essencial que os riscos estratégicos sejam identificados, avaliados e monitorados, e que a organização esteja preparada para mitigá-los.

**Operacional**: risco associado a possibilidade de perdas diretas ou indiretas resultantes de processos internos inadequados ou falhos, da existência de recursos humanos insuficientes ou inadequados, sistemas ou eventos externos.

**Legal/Conformidade (Regulatório)**: risco associado à possibilidade de violações ou do não cumprimento de leis, normas, regulamentos, contratos, códigos de conduta e integridade, políticas e normas internas ou princípios éticos.

**Reputação**/**Imagem**: risco associado à possibilidade de uma percepção negativa da imagem pública da organização, fundamentada ou não, por parte de reguladores, clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral.

**Integridade**: risco associado à corrupção, fraudes, irregularidades, desvios éticos e de conduta que podem comprometer os valores e padrões preconizados.

**Financeiro/Orçamentário:**eventos que podem comprometer a capacidade do Ministério de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades.

# **Avaliação dos Riscos**

Envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é necessária ação de resposta ao risco. A avaliação é realizada utilizando-se a matriz de probabilidade x impacto.

Identificados, reconhecidos e registrados os riscos, suas causas e consequências, devem ser avaliados sob a perspectiva do impacto e da probabilidade. Normalmente, as causas se relacionam à probabilidade de o riscoocorrer e as consequências ao impacto, caso o riscose materialize.

A Matriz de Riscos é uma ferramenta que permite aos gestores mensurar, avaliar e ordenar os riscos de acordo com o seu nível de risco. Ela foi elaborada considerando a escala de probabilidade e impacto (matriz 5x5) e está distribuída em quatro níveis, que representam os níveis de riscos dimensionados em função do apetite a risco definido pelo Ministério da Saúde.

A probabilidade representa a possibilidade de um determinado risco ocorrer. Poderá ser determinada de forma objetiva ou subjetiva, qualitativa ou quantitativa.

Via de regra, as estimativas de probabilidade de riscos são conduzidas/atribuídas utilizando-se dados de eventos passados observáveis, os quais fornecem uma base mais objetiva do que as estimativas inteiramente subjetivas. Entretanto, o julgamento dos gestores, embasados na experiência, é relevante para a definição do peso atribuído à probabilidade, porém, deve-sereconhecer as limitações inerentes.

Os pesos a serem atribuídos à PROBABILIDADE na matriz de riscos são:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Muito Baixa | Baixa | Média | Alta | Muito Alta |
| 1 | **2** | **3** | **4** | **5** |
| Improvável. Pode ocorrer emcircunstâncias excepcionais. | **Rara** possibilidade de ocorrer. | **Possível.** Poderá ocorrer**.** As circunstâncias apontam uma possibilidade moderada. | **Provável.** Deve ocorrer em algum momento. Aqui as circunstâncias apontam fortemente para essa possibilidade. | **Praticamente Certo.** Em algum momento ocorrerá orisco. |

Figura 3 – Pesos Probabilidade

Os pesos a serem atribuídos ao IMPACTO na matriz de riscos são:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Muito Baixa | Baixa | Média | Alta | Muito Alta |
| 1 | **2** | **3** | **4** | **5** |
| Mínimo impacto nos objetivos. | **Pequeno** impactonos objetivos. | **Moderado** impactonos objetivos, porém recuperáveis. | **Significativo** impactonos objetivos e de difícil reversão. | **Os impactos serão trágicos eirreversíveis.** |

Figura 4 – Pesos Impacto

Avaliado o risco, com a aplicação da Matriz de Riscos (atribuição de pesos ao impacto e a probabilidade), obtém-se os níveis de riscos dimensionados em função do apetite a risco.

|  |
| --- |
| **Classificação** |
| *Níveis de Riscos* | *Faixas* | *Respostas* |
| **RE** | **Risco Extremo** | 20 - 25 | **Evitar** |
| **RA** | **Risco Alto** | 12 - 19,99 | **Mitigar** |
| **RM** | **Risco Médio** | 4 - 11,99 | **Compartilhar** |
| **RB** | **Risco Baixo** | 0 - 3,99 | **Aceitar**  |

Figura 5 – Classificação dos níveis de riscos

Fonte: Manual de Metodologia de Gestão de Riscos da CGU

Dessa forma a matriz de riscos apresenta:



Figura 6– Matrix de Riscos Impacto x Probabilidade (5x5)

Fonte: Manual de Metodologia de Gestão de Riscos da CGU

Assim, o nível de risco é expresso pelo resultado da multiplicação do peso atribuídoao IMPACTO e à PROBABILIDADE, considerado as faixas atribuídas. Desta forma, os níveis de risco serão classificados em: **Extremo, Alto, Médio e Baixo**.



Figura 7 – Classificação dos riscos

Fonte: Manual de Metodologia de Gestão de Riscos da CGU

O risco deve ser avaliado quanto à suacondição de inerente, residual ou a conjugação de ambos.

A Análise do**risco inerente**é realizada aplicando-se a matriz de riscos (probabilidade ximpacto), em um primeiro momento sem considerar quaisquer controles que reduzem ou poderiam reduzir a probabilidade da sua ocorrência ou atenuar o impacto, caso se materialize.

Depois, é necessário identificar os controles existentes e avaliar a sua eficácia em relação ao cumprimentos dos objetivos do processo objeto do gerenciamento de riscos, verificando se esses respondem de fato os riscos identificados, de acordo com o apetite e a tolerância a risco.

As atividades de controle são as ações estabelecidas, sejam por meio de políticas,procedimentos e tarefas, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a assegurar o cumprimento das diretrizes determinadas pela Administração para mitigar os riscos que possam impedir ou dificultar o cumprimento dos objetivos institucionais.

Dessa forma, deve-se avaliar os controles existentes em relação à sua eficácia na mitigação do risco em análise, identificando e reconhecendo seus resultados mitigadores.

Identificados, reconhecidos e registrados os controles devem ser avaliados e classificados em relação ao seu Nível de Confiança (NC). Cada um (NC) corresponde a um Fator de Avaliação dos Controles (FAC). Para essa classificação, considere:



Figura 8– Classificação conforme o nível de confiança

Fonte: Manual de Metodologia de Gestão de Riscos da CGU

O Risco Residualé o resultado da multiplicaçãoentreo valor do *Risco Inerente e o FatordeAvaliação dosControles (FAC).* O **Risco Residual**é oqueaindapermanece depois de considerado o efeito das medidas adotadas pela gestão para responder a probabilidade e o impacto dos riscos, incluindo controles internos e outrasações.

As estratégias adotadas para responder aos **riscos residuais** são: **EVITAR** (risco extremo), **MITIGAR** (risco alto), **COMPARTILHAR** (risco médio) e **ACEITAR** (risco baixo). A fim de melhor exemplificar e detalhar os passos para a execução da avaliação de riscos, no Anexo I e II – Gerenciamento de Riscos, deixamos para o usuário explicações, modelos de planilhas e informações mais específicas que poderão auxilá-lo no processo de avaliação dos riscos (os modelos atualizados e abertos das planilhas documentadoras poderãos ser solicitados à Coordenação de Gestão de Riscos-COGER pelo email: coger@saude.gov.br.

# **Resposta aos Riscos**

A resposta aos riscos deve ser realizada com a participação de pessoas que conheçam o processo objeto do gerenciamento de riscos, devendo também ter a participação do gestor do processo.

Obtido o risco residual, que em potencial pode afetar negativamente o cumprimento dos objetivos institucionais, adote uma das estratégias de respostas, definidas em função do nível de risco.

Cada risco residual está relacionado a uma opção de resposta, nisso os Gestores de Processos, responsáveis pelo gerenciamento de riscos, deverão adotar as ações de controles, conforme apresentado no quadro abaixo:



Figura 9 – Classificação de respostas conforme o nível de risco

Fonte: Manual de Metodologia de Gestão de Riscos da CGU

As atividades de controles devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão, bem como a preparação prévia de plano de ações para responder aos riscos.

As respostas aos ricos podem ter natureza preventiva ou detectiva e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio. A segregação é uma das atividades de controle inseridasno desenvolvimento do processo.

São pontos importantes que facilitam a proposição de ações para responder aos riscos:

* que medidas poderiam ser adotadas para reduzir a probabilidade de ocorrência do risco, aqui vale ter uma atenção especial para as causas que deram origem ao risco registradasna etapa de identificação.
* que medidas poderiam ser adotadas para reduzir o impacto do risco no alcance dos objetivos/resultados, que atenção especial deverá ser dada neste momento e vale voltar nas possíveis consequências registradas na etapa de identificação do risco.
* considerar os benefícios potenciais relativos ao alcance dos objetivos, face aos custos, esforço ou desvantagens da implementação, especificando as ações para responder os riscos, de maneira que sejam compreendidas pelos envolvidos eque auxilia na sua implementação e, ainda, que permita o seu monitoramento.

A decisão quanto à implementação de medidas para responder os riscos deve considerar a quantidade e o nível de riscos mitigados por cada medida proposta. As medidas para respondê-los podem envolver, por exemplo, a adoção de um novo controle, aprimorar um controle existente, o redesenho de um processo, a realocação de pessoas, a realização de ações de capacitação, o desenvolvimento ou aperfeiçoamento de soluções de tecnologia da informação, o aprimoramento das normas internas, e a adequação da estrutura organizacional, entre outros.

Para permitir o gerenciamento e monitoramento das medidas para responder os riscos, é importante a elaboração de um plano de respostas, que deverá conter, minimamente:

* informações da Unidade, processo, responsáveis e o período em que a análise foi realizada.
* os riscos residuais, sua classificação, sua categoria, tipo de resposta aprovada.
* as ações propostas, como serão implementadas, os responsáveis e partes relacionadas (intervenientes), datas de início e fim.

O Plano de Tratamento será individualizado por unidade e deverá ser avaliado e aprovado pelo seu dirigente máximo. Após a aprovação, deverá ser encaminhadoà Diretoria de Integridade para consolidação e monitoramento, cujo resultado será submetidoao Comitê de Gestão de Riscos-CGR e ao Comitê Interno de Governança-CIG.

Espera-se, com os resultados do tratamento, com a implementação de ações de controles propostas para responder ao risco residual, fique abaixo do limite de exposição definido na declaração de apetite e tolerância a riscos, aprovada por meio daMatriz de Riscos.

O modelo de planilha documentadora e de relatório poderão ser solicitados a Coordenação de Gestão de Riscos-COGER pelo e-Mail: coger@saude.gov.br.

# **Monitoramento e Análise Crítica**

O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e a eficácia da concepção, implementação e resultados do processo de gerenciamento de riscos, com responsabilidades claramente estabelecidas.

O processo do monitoramento compreende a verificação do desempenho ou da situação do gerenciamento de riscos, abrangendoo cumprimento da Política de Gestão de Riscos, do Plano de Gestão de Riscos e do Plano de Respostas aos Riscos.

O monitoramento e a análise crítica caberãoa cada instância, ou seja, ao Gestor do Processo-GP, à Unidade de Gestão de Riscos e Integridade-UGRI e à Diretoria de Integridade-DINTEG e deverá ser realizado de forma contínua ou periódica, considerando o tempo previsto para o cumprimento dos prazos pactuados,junto aos respectivos responsáveis.

A partir do resultado do monitoramento e a análise crítica,caberá a Diretoria de Integridade-DINTEG a consolidação dos resultados, elaboração de relatório para análise do Comitê de Gestão de Riscos-CGR e apreciação do Comitê Interno de Governança-CIG.

# **Registro e Comunicação**

Registro e comunicação consistem em documentar e relatar o processo de gerenciamento e riscos e os seus resultados, com o intuito de fornecer informações à tomada de decisão, melhoria do processo, entre outros.

Segundo a Norma ABNT NBR ISO 31000:2018, o processo de gestão de riscos e seus resultados devem ser documentados e comunicados pormeio de mecanismos apropriados. A documentação e a comunicação visam: (a) comunicar atividades e resultados de gestão de riscos em toda a organização; (b) fornecer informações para a tomada de decisão; (c) melhorar as atividades de gestão de riscos; e (e) auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e comresponsabilização por atividades de gerenciamento deriscos.

O registro e comunicação devem ocorrer durante todas as etapas do processo de gerenciamento de riscos, atingir todas as partes interessadas e ocorrer de forma clara e objetiva. A comunicação, por meio de reporte, deverá ser parte integrante da governança, pois aprimora a troca de informações entre as unidades e as partes interessadas, apoia a alta administração e os órgãos de supervisão no cumprimento de suasresponsabilidades e nas tomadas de decisões.

Os fatores a considerar para um bom reporte incluem, minimamente: (a) as diferentes partes interessadas e suas necessidades específicas de informação e requisitos, (c) custo, frequência e pontualidade do relato, (c) modelo de relato, e (d) pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

Cada Unidade de Gestão de Riscos e Integridade-UGRI deverá abrir um processo no Sistema Eletrônico de Informações-SEI/MS e apensar todos os atos provenientes do processo de gerenciamentode riscos, conforme determina a Portaria Nº 900, de 31 de março de 2017.

# **CONSIDERAÇÕES FINAIS**

Em linha com a Política de Gestão de Riscos-PGR, a Diretoria de Integridade-DINTEG é responsável por orientar e promover a aplicação dos princípios e diretrizes da gestão de riscos e, em articulação com as demais Unidades, deverá potencializar a identificação, a avaliação, as respostas, o monitoramento e análise crítica, o registro e a comunicação no âmbito do Ministério da Saúde.

# **REFERÊNCIAS BIBLIOGRÁFICAS**

BRASIL. Ministério da Saúde**.** Portaria nº 1.822, de 20 de julho de 2017, que institui a Política de Integridade, Riscos e Controles Internos da Gestão – PGIRC no âmbito do Ministério da Saúde.

BRASIL. Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. Metodologia de Gestão de Riscos. Disponível em [http://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf.](http://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf) Acesso em Maio de 2019.

BRASIL. Tribunal de Contas da União. Manual de Gestão de Riscos do TCU. Disponível em [https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/.](https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/) Acesso em Maio de 2019.

BRASIL. ABNT NBR ISO 31000:2018. Associação Brasileira de Normas Técnicas (ABNT). Gerenciamento de Riscos.

BRASIL. (2016) Instrução Normativa nº 01/2016. Ministério do Planejamento Orçamento e Gestão, Controladoria Geral da União, Brasília, DF.

BRASIL. (2017) Manual de gestão de integridade, riscos e controles internos da gestão – CIRC, 1.2 Ministério do Planejamento, Desenvolvimento e Gestão, Brasília, DF.

COSO (2004) Enterprise risk Management: Integrated Framework. 136

FORRISCO: gerenciamento de riscos em instituições públicas na prática/Paulo Henrique de Souza Bermejo et al. Brasília/DF: Editora Evobiz, 2019.

SOUZA, Kleberson Roberto de. Como combater o desperdício no setor público: gestão de riscos na prática / Kleberson Roberto de Souza, Franklin Brasil Santos. – Belo horizonte: Fórum, 2019.

# ANEXO I–GERENCIAMENTO DE RISCOS

**Entendimento do Contexto**

Esta etapa consiste em compreender o ambiente interno e externo no qual os processos, cujos riscos serão gerenciados, encontram-se inseridos e tem por finalidade colher informações para apoiar a identificação de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do processo e os institucionais da Unidade.

Informações sobre o órgão/Unidade:

**Sobre o ambiente interno**:

**Forças**: inclui identificar e registrar as forças existentes no ambiente interno, como: integridade, valores éticos, competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional, políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes, provendo disciplina e prontidão para a gestão de riscos.

**Fraquezas**:inclui identificar e registrar as franquezas no ambiente interno que oferecem risco à execução do processo e ao cumprimento dos seus objetivos.

As informações sobre o ambiente interno poderão ser obtidas por meio de pesquisas em: planejamento estratégico, políticas, normas, projetos, orçamento, relatórios gerenciais, relatórios dos órgãos de fiscalização e controle, entre outros e, são diretamente relacionadas ao órgão/unidade.A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de riscos que potencialmente impeçam sua consecução

**Sobre o ambiente externo**:

**Oportunidades:** inclui identificar e registrar as situações positivas do ambiente externo que permitem o cumprimento dos objetivos do processo/Unidade.

**Ameaças:**inclui identificar e registrar as situações externas, sobre as quais não se tem controle, que representam dificuldades ou ameaças e impactam negativamente o cumprimento dos objetivos dos processos/Unidade (por exemplo: instabilidade política, descrédito nas instituições). Assim, é importante pensar em estratégias prévias para minimizar seus efeitos.

Para a aplicação dessa análise, sugere-se a utilização da ferramenta ***SOWT*[[1]](#footnote-2)**no que se refere a identificação de forças e fraquezas (pontos fortes e pontos fracos), bem como para analisar e registrar as possíveis influências do ambiente externo sobre o processo, no que se refere a oportunidades e ameaças (pontos fortes e pontos fracos).

A análise SWOT é realizada no processo objeto do gerenciamento de riscos.

Análise de SWOT

Forças

(Características internas que representam uma facilidade para o alcance dos objetivos do processo/Unidade)

Oportunidades

(Situações positivas do ambiente externo que permitem o cumprimento dos objetivos do processo/Unidade)

Fraquezas

(Fatores internos que oferecem risco à execução do processo e ao cumprimento dos seus objetivos)

Ambiente Externo

Ambiente Interno

Ameaças

(Situações externas, sobre as quais se tem pouco controle, que representam dificuldades para o cumprimento dos objetivos dos processos/Unidade)

Quadro 1 – Matriz SWOT

Fonte: conceitos adaptados.

Além de colher as informações para compreender o contexto do ambiente interno e externo no qual os processos estão inseridos, é primordial que o processo esteja mapeado.

Utilize o formulário abaixo para registrar as informações do resultado da análise de SWOT:



Quadro 2 – Formulário para registrar informações dos ambientes

Fonte: Elaboração própria

As informações acima, em conjunto com as informações do processo (normas, fluxograma das atividades, descrição das tarefas, responsáveis), são fundamentais para a realização das demais etapas do gerenciamento de riscos (identificação e análise dos riscos, avaliação dos riscos, respostas aos riscos, monitoramento e análise crítica, e relato e comunicação).

Ajuda:

1. Processo/Objetivo Geral: essas informações deverão ser coletadas da cadeia de valor/base de processos ou do mapeamento do processo.
2. Leis e Regulamentos: listar todas as leis, regulamentos e normas que afetam ou influenciam o processo. Essas informações são importantes para verificar inclusive se há riscos e descumprimento de leis, regulamentos e normas, bem como ajuda na adoção de medidas de controle.
3. Sistemas: listar os sistemas e outras ferramentas (planilhas) que operacionalizam o processo. Essas informações são importantes para verificar se os controles são manuais ou estão nos sistemas.

**Avaliação de Riscos**

Esta etapa contempla a identificação de riscos, a análise e a avaliação desses(mensuração), e tem por finalidade registrar os que comprometem o alcance do objetivo do processo/Unidade. Considere, neste momento o resultado da análise da Etapa 1, Entendimento do Contexto.

Identificação **de riscos**: encontrar, reconhecer e descrever os riscos que possam ajudar ou impedir que uma organização alcance seus objetivos;

**Análise de riscos**: considera as incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um risco pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos; e

**Avaliação de riscos (mensuração)**: envolve a comparação dos resultados da análise de riscos com os critérios estabelecidos para determinar onde é necessária ação de resposta, realiza-se a mensuração utilizando-se a matriz de probabilidade x impacto.

**Fases da Avalição de Riscos**

1. **Identificação e análise de riscos**

A identificação de riscos requer a participação de colaboradores com conhecimento do processo, visão holística dos negócios/serviços da unidade nos seus diferentes níveis. É importante e desejável também que tenha conhecimento em gestão de riscos ou tenha recebido treinamento para aplicação da metodologia e uso das ferramentas disponibilizadas (sistema ou planilha Excel).São várias as técnicas de identificação de eventos de riscos: questionários e checklist; *whorkshop* e brainstorming; inspeções e auditorias, fluxos e análise de dependência. Escolha a técnica que favoreça a realização desta atividade e colete as informações.

Importante:

* Os riscos representam uma possibilidade, portanto, deverão ser descritas as falhas e inadequações que poderão ocorrer e não somente aquelas que já ocorreram;
* Atentar, também, para as falhas que implicam em descumprimento de normas externas e que geram ou podem gerar penalidades (ex.: advertências, impedimentos, outros) e/ou sanções (ex.: multas) para a Unidade;
* Envolve a identificação das causas e suas consequências/efeitos.

Como identificar os eventos de riscos?

Aqui, sugerimos a utilização da ferramenta *Bow-tie*(gravata borboleta)*,* considerando que é uma maneira simples de descrever e analisar causas, consequências e tratamentos implementados.

Nesta ferramenta, o risco é representado como o nó da gravata borboleta, sendo que à esquerda, ligadas por linhas ao nó, ficam as causas e à direita, também ligadas por linhas, ficam as consequências. Entre as causas e o nó, e as consequências e o nó são colocadas barreiras, representando os tratamentos e monitoramentos implantados, conforme demonstrado na figura a seguir:



Definições e termos:

**Causas de riscos**: (fontes de vulnerabilidades) condições que dão origem à possibilidade de um risco ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

**Consequência**: resultado de um risco sobre os objetivos (estratégicos, operacionais, comunicação, conformidade – COSO II).

**Fonte de riscos:** elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

**Risco**: possibilidade de ocorrência de um evento que poderá impactar o cumprimento dos objetivos institucionais.

**Vulnerabilidades**: implica em uma situação de risco (ocorrências de eventos ou mudanças) em um conjunto específico de circunstâncias (inexistência, inadequação e insuficiência).

Antes de iniciar a identificação de riscos é necessário obtero mapeamento do processo (fluxogramação e descrição, detalhando as principais e grandes etapas do processo e os intervenientes – partes relacionadas) e ter bem claro os objetivos gerais e específicos do processo objeto da identificação de riscos.

Os riscos identificados devem ser registrados no Mapa de Risco, que é o documento desenvolvido para documentar as etapas do gerenciamento, de forma a permitir a sua análise do ponto de vista das possíveis causas e consequências, para no momento seguinte permitir a avaliação (mensuração) quanto à probabilidade x impacto.



Uma vez identificado o risco, suas causas e consequências e registrados no Mapa de Risco, passa para a fase de avaliação dos riscos, ou seja, a mensuração.

1. **Avaliação de riscos (mensuração)**

Os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto. Normalmente as causas se relacionam à probabilidade do evento ocorrer e as consequências ao impacto, caso o evento se materialize.

A avaliação de riscos deve ser feita por meio de análises quantitativas e qualitativas ou da combinação de ambas e, ainda, quanto à sua condição de inerentes (risco bruto, sem considerar qualquer controle) e residuais (considerando os controles identificados e avaliados quando ao desenho e a sua execução).

Definições e termos(IN Conjunta MP/CGU Nº 01/2016):

**Risco inerente**: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais.

**Risco residual**: risco a que uma organização está exposta após a implementação de açõesgerenciaispara o tratamento do risco.

**Mensurar Risco Inerente**

Aplique a Matriz de Risco (impacto x probabilidade) para mensurar o risco inerente desconsiderando qualquer controle existente. A matriz de riscos desenvolvida é uma matriz 5X5 e classifica os riscos em 4 (quatro) níveis: Risco Extremo, Risco Alto, Risco Médio e Risco Baixo, conforme abaixo:



Para avaliar impacto considere:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Impacto |  |  |
| Muito Baixa | **Baixa** | **Média** | **Alta** | **Muito Alta** |
| 1 | **2** | **3** | **4** | **5** |
| Mínimo impacto nos objetivos. | **Pequeno impacto** nos objetivos. | **Moderado impacto** nos objetivos, porém recuperável. | **Significativo impacto** nos objetivos e de difícil reversão. | **Os impactos serão trágicos. Irreversíveis.** |

Para avaliar a probabilidade, considere:

|  |
| --- |
| Probabilidade |
| Muito Baixa | **Baixa** | **Média** | **Alta** | **Muito Alta** |
| 1 | **2** | **3** | **4** | **5** |
| Improvável. Pode ocorrer em circunstâncias excepcionais. | **Rara** possibilidade de ocorrer. | **Possível.** Poderá **ocorrer.** As circunstâncias apontam uma possibilidade moderada. | **Provável. Deve** ocorrer em **algum momento. Aqui as circunstâncias apontam fortemente para essa possibilidade.** | **Praticamente Certo.** Em algum momento ocorrerá orisco. |

**Identificar e Avaliar os Controles Existentes**

Para se obter o risco residual faz-se necessário identificar os controles existentes e avaliar o seu nível de confiança, aplicando-se o Fator de Avaliação do Controle-FAC ao valor total obtido na avaliação do risco inerente (impacto x probabilidade), conforme a seguir:





Após obtido o valor do risco inerente, impacto x probabilidade, identifique, registre e avalie os controles existentes para se chegar ao risco residual. Também nesta etapa identifique os controles existentes para cada evento e risco e realize a sua avaliação quanto ao desenho e à operação.

**Identificar e Avaliar os Controles**

Controles internos da gestão é o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade (Art. V, IN Conjunta MP/CGU Nº 01/2016).

**Mensurar Risco Residual**

Risco residual é o risco que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. (Art. XIV, IN Conjunta MP/CGU Nº 01/2016).Aplique novamente a Matriz de Risco (impacto x probabilidade) considerando, neste momento, os controles identificados e o resultado da sua avaliação.

# ANEXO II – FLUXOGRAMA: GESTÃO DE RISCOS

#

# ANEXO III – ATRIBUIÇÕES E COMPETÊNCIAS DOS ATORES

#

1. Análise SWOT é uma **ferramenta utilizada para fazer análise de cenário** (ou análise de ambiente). As informações obtidas sobre o ambiente interno e externo, contribuem na identificação dos riscos e na escolha das respostas aos riscos. [↑](#footnote-ref-2)