**INSTRUÇÕES PARA O PREENCHIMENTO DA MATRIZ E DOCUMENTAÇÃO DA ANÁLISE DE RISCOS**

(*Texto compilado e adaptado conforme o caso do Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão, do Ministério do Planejamento, Desenvolvimento e Gestão)*[[1]](#footnote-1)

**1. ESTABELECIMENTO DO CONTEXTO**

1. Informações sobre o órgão/unidade:
* Sobre o Ambiente Interno: inclui verificar, entre outros elementos: 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 integridade, riscos e controles internos da gestão.
* Sobre a Fixação de Objetivos: inclui verificar, em todos os níveis da unidade (departamentos, divisões, processos e atividades), se os objetivos foram fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução.

As informações poderão ser obtidas por meio de pesquisas em regimento interno, planejamento estratégico, projetos, orçamento, relatórios gerenciais, relatórios dos órgãos de fiscalização e controle, entre outros e, são diretamente relacionadas ao órgão/unidade.

b) Informações sobre o macroprocesso/processo:

Deve-se registrar o objetivo geral do macroprocesso/processo, as leis e regulamentos e os sistemas utilizados na sua execução.

c) Análise de *SWOT*

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 macroprocesso/processo quanto a oportunidades e ameaças (pontos fortes e pontos fracos).

**2. IDENTIFICAÇÃO DOS RISCOS DE INTEGRIDADE**

É apresentado um dicionário de riscos de integridade com a relação de fatores de riscos (causas) que podem favorecer a materialização dos riscos (eventos). Novos fatores de riscos e/ou novos eventos de riscos podem ser acrescidos, caso sejam identificados pela Instituição, além de poderem ser eliminados os riscos sugeridos, caso não sejam identificados no processo sob análise.

O processo de identificação de riscos requer a participação de servidores com conhecimento do processo, visão holística dos serviços da unidade nos seus diferentes níveis. É importante estabelecer iniciativas que permitam o conhecimento prévio dos conceitos e métodos relacionados com a gestão dos riscos de integridade.

O risco de integridade (evento) deve ser relacionado ao processo que está associado e em que atividade deste foi identificado. Utilize o dicionário de riscos de integridade como referência. Além disso, deve ser relacionada a causa (fator) que pode levar a materialização do risco de integridade.

**3. AVALIAÇÃO DOS RISCOS DE INTEGRIDADE**

A avaliação dos riscos de integridade é feita com base num modelo matricial que envolve probabilidade de ocorrer o risco e o impacto de sua ocorrência.

O risco de integridade identificado e avaliado nesta etapa é denominado RISCO INERENTE, que é aquele que existe independentemente da existência de qualquer ação para sua prevenção ou mitigação; é o risco potencial.

Os parâmetros para a determinação da probabilidade e impacto estão relacionados na aba “Escalas” e também estão automatizados na planilha de documentação (colunas E, F, G, H), que fará cálculo do risco inerente.

A determinação da probabilidade deve levar em conta o histórico de ocorrência do risco de integridade identificado na organização. Para tanto, podem ser utilizados registros, processos tramitados e/ou em tramitação, histórico de ocorrência das situações identificadas. O impacto ou consequência do risco deve ser avaliado (com base na escala sugerida) em função do comprometimento que poderá causar em processos e atividades prioritárias.

**4. IDENTIFICAÇÃO E AVALIAÇÃO DOS CONTROLES INTERNOS**

Segundo o COSO, “Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.” Neste sentido, diversas ações devem ser estabelecidas, por meio de políticas e procedimentos, que podem incluir uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio.

Deve ser identificada a existência de eventual atividade de controle que previna ou mitigue o risco de integridade identificado e a referida atividade deve ser avaliada conforme parâmetros descritos na aba “Avaliação de Controles”, que determinará o fator de avaliação a ser aplicado na determinação do risco residual.

Deve ser descrito o objetivo do controle e a atividade de controle relacionada, destacando todos os seus atributos: preventivo, detectivo ou corretivo, automático ou manual, sistemas e funções utilizadas, frequência de realização, quem realiza, relatórios gerados (se for planilha eletrônica identifique o nome e o local de armazenamento) e todas demais informações que permitam identificar e avaliar o controle.

Os parâmetros de avaliação dos controles (Coluna M) e o fator de avaliação estão automatizados na planilha para seleção pelo avaliador.

**5. DETERMINAÇÃO DO RISCO RESIDUAL**

O RISCO RESIDUAL (RR) é aquele que remanesce após a adoção de medidas de prevenção e/ou de mitigação do risco potencial e é sobre ele que deve avaliada a necessidade de aplicar novas medidas de tratamento.

O risco residual será apurado automaticamente pela planilha após a avaliação do risco inerente (RI) e da determinação do Fator de Avaliação do Controle Interno (FA).

Então:

RR = RI x FA

**6. MEDIDAS DE TRATAMENTO DOS RISCOS DE INTEGRIDADE**

As ações para responder os riscos residuais devem ser coerentes com o apetite ao risco (vide aba “Escalas”) e deve considerar se a resposta ao risco irá interferir na probabilidade de ocorrência ou no impacto desta.

Os planos de ação para tratamento dos riscos podem documentados na aba “Plano de Respostas” e devem considerar o modelo 5W2H, que envolve determinar expressamente:

- O que fazer

- Porque fazer

- Quem faz

- Onde

- Quando

- Como

- Quanto custa

1. https://repositorio.cgu.gov.br/handle/1/41827 [↑](#footnote-ref-1)