Ministério do Planejamento,
Desenvolvimento e Gestão - MP

Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão

Assessoria Especial de Controles Internos - AECI

Ministro do Ministério do Planejamento, Desenvolvimento e Gestão – MP
Dyogo Henrique de Oliveira

Esteves Pedro Colnago Júnior
Secretário Adjunto

Assessor Especial de Controle Interno
Rodrigo Fontenelle de Araújo Miranda

Elaboração:
Assessoria Especial de Controle Interno
Rodrigo Fontenelle de Araújo Miranda
Alexandre Quaresma Inácio Silveira
Aline Gonçalves dos Santos
Andrea Katherine de Souza Suguino
Dacy Bastos Ribeiro da Costa Claudino
Illana Pinheiro Bezerra
Mario Iwazaki
Maury Gonzaga Farias
Silvio Marques de Andrade
Vera Lúcia de Melo

Colaboração:
Comitê Técnico de Gestão de Integridade, Riscos e Controles Internos da Gestão
Secretaria Executiva do Ministério do Planejamento, Desenvolvimento e Gestão

Versão: 1.2 – 07/06/2017

APRESENTAÇÃO

O objetivo deste manual é apresentar a Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão, no contexto do Modelo em desenvolvimento no MP (Política, Instâncias de Supervisão, Metodologia e Solução Tecnológica).

A metodologia tem por finalidade orientar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos da unidade, a partir do Método de Priorização de Processos, bem como instruir sobre o monitoramento e reporte.

Neste manual estão descritas as premissas que embasaram sua elaboração, os procedimentos a serem utilizados na aplicação da metodologia, além de apresentar os conceitos utilizados, papéis e responsabilidade, taxonomia de eventos de riscos e lista de controles básicos.

Fornece, também, diretrizes básicas acerca de boas práticas, com objetivo de despertar os gestores para a importância da gestão de integridade, riscos e controles internos da gestão. Assim, é um ponto de partida que não esgota o tema, cujo aprofundamento pode ser adquirido em publicações especializadas, num processo de contínuo aprendizado.

Inicialmente, até que seja desenvolvido sistema específico para a gestão integridade, riscos e controles internos da gestão, a aplicação poderá ser realizada por meio de planilha Excel, denominada “Planilha Documentadora”, parte integrante deste Manual.

Sumário

Lista de Figuras

Lista de Tabelas

1. INTRODUÇÃO

A incerteza ou o risco é inerente a praticamente todas as atividades humanas. No mundo corporativo onde as empresas estão expostas a uma miríade de incertezas originadas de fatores econômicos, sociais, legais, tecnológicos e operacionais, a gestão de integridade, riscos e controles internos é crucial para que se alcance os objetivos estratégicos.

Uma das funções da gestão de integridade, riscos e controles internos da gestão é assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, o cumprimento de prazos, leis e regulamentos etc, e, implementar uma estratégia evitando o consumo intenso de recursos para solução de problemas quando estes surgem inesperadamente, bem como a melhoria contínua dos processos organizacionais.

No ambiente de trabalho, muitas vezes depara-se com fatores internos e externos que tornam incerto o êxito do atingimento dos objetivos do projeto ou da atividade que se encontra em desenvolvimento. Independentemente da área em que se atua, e até na vida pessoal, os riscos (ameaças ou oportunidades) podem afetar o andamento da ação, levando-a a uma direção completamente diferente daquela inicialmente planejada.

As responsabilidades e deveres do governo em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão. Neste contexto, a gestão de integridade, riscos e controles internos da gestão torna-se uma importante ferramenta para ajudar na tomada de decisões baseadas em metodologias e normas que geram, dentre outros benefícios, a redução ou a eliminação de retrabalhos.

O Ministério do Planejamento, Desenvolvimento e Gestão instituiu, por meio da Portaria nº 150, de 4 de maio de 2016, seu Programa de Integridade, baseado nos Guias de Integridade, publicados pelo Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU, que incentiva gestores e servidores a conhecer melhor o seu órgão, o planejamento estratégico, os processos e os eventos de riscos a que estão sujeitos.

O Programa de Integridade tem a finalidade de mitigar ocorrências de corrupção e desvios éticos a partir da mobilização e participação ativa dos gestores públicos. Objetiva estabelecer um conjunto de medidas que assegurem a entrega de resultados esperados pela sociedade, por meio do fortalecimento e aprimoramento da estrutura de governança, gestão de riscos e controles e procedimentos de integridade. É constituído de quatros pilares: ambiente de integridade; gestão de integridade, riscos e controles; procedimentos de integridade; e comunicação e monitoramento.

O Ambiente de Integridade é o 1º Pilar do Programa de Integridade e oferece as bases para que o Programa seja efetivo. É composto de ações de comprometimento e apoio da alta administração, de alinhamento ao planejamento estratégico e de instituições de instâncias tal

como o Comitê de Gestão Estratégica, cuja missão é acompanhar e fiscalizar o Programa, e a Comissão de Ética do Ministério.

A Gestão de Integridade, Riscos e Controles é o 2º Pilar do Programa de Integridade. A finalidade atribuída a este pilar diz respeito à definição de uma Política de Gestão de Riscos no âmbito do Ministério do Planejamento, Desenvolvimento e Gestão, à instituição do Subcomitê de Integridade, Riscos e Controles (SIRC) e à implementação do Gerenciamento de Riscos.

O 3º Pilar do Programa de Integridade diz respeito à instituição e *compliance* de Procedimentos de Integridade. A instituição de procedimentos de integridade envolve o desenvolvimento do código de conduta, do canal de denúncias e do plano de capacitação e educação continuada dos servidores. O *compliance* de procedimentos de integridade envolve ações que fomentem a declaração de bens e combatem o conflito de interesses e a presença de nepotismo, além da implementação eficiente da Lei de Acesso à Informação.

A Informação, Comunicação e o Monitoramento, 4º Pilar do Programa de Integridade, é um processo contínuo e permanente de disponibilização da informação a níveis adequados para as partes interessadas, de relacionamento entre as instâncias de supervisão e de monitoramento das ações do Programa de forma a avaliar a qualidade do sistema de controle interno ao longo do tempo.

2. NORMAS E REGULAMENTAÇÕES RELACIONADAS

No âmbito da Administração Pública Federal existe um conjunto de normas e regulamentações relacionadas à temática de gestão de integridade, riscos e controles, entre elas:

Programa de Integridade, Portaria Nº 150, de 4 de maio de 2016, institui o Programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão e Portaria Nº 425, de 30 de dezembro de 2016, que altera a Portaria MP nº 150, de 4 de maio de 2016, que instituiu o programa de Integridade e o Comitê de Gestão Estratégica do Ministério do Planejamento, Desenvolvimento e Gestão.

Instrução Normativa Conjunta CGU/MP Nº 1, de 10 de maio de 2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

Código de Conduta Ética, Portaria Nº 382, de 6 de dezembro de 2016, aprova o Código de Conduta Ética dos agentes públicos do Ministério do Planejamento, Desenvolvimento e Gestão.

Política de Gestão de Integridade, Riscos e Controles Internos da Gestão, Portaria Nº 426, de 30 de dezembro de 2016, dispõe sobre a instituição da Política de Gestão de Integridade, Riscos e Controles da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

O Planejamento Estratégico do MP para o período 2016-2019 destaca a missão, visão e os nove objetivos estratégicos do MP. Traz ainda, no painel de contribuição das suas diversas unidades, os objetivos que cada uma delas terá para o período mencionado, em consonância com aqueles definidos para o Ministério. Além disso, apresenta iniciativas e entregas destinadas à implantação da gestão de riscos em alguns macroprocessos selecionados.

3. Referencial Teórico

Embora exista uma grande quantidade de metodologias e estruturas de gestão de riscos mundialmente reconhecidas, tais como ISO 31000, Orange Book, do Tesouro Britânico, dentre outras, esse manual foi baseado na estrutura do COSO ERM, considerando que é o framework definido pela Portaria nº 426/2016, que aprovou a política de gestão de integridade, riscos e controles internos da gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

COSO (*Committee of Sponsoring Organizations)* é o Comitê das Organizações Patrocinadoras, da Comissão Nacional sobre Fraudes em Relatórios Financeiros. Criada em 1985, é uma entidade do setor privado – ou seja, foi uma iniciativa do setor privado, independente –, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros, principalmente para estudar as causas da ocorrência de fraudes em relatórios financeiros. Cabe ressaltar que a origem do modelo COSO está relacionada a um grande número de escândalos financeiros, na década de 70, nos Estados Unidos, que colocaram em dúvida a confiabilidade dos relatórios corporativos.

De acordo com o Comitê, **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. (COSO, 2013)

Em 2004, o COSO divulgou o trabalho **"Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO ERM)"**, com um foco mais voltado para o gerenciamento de riscos corporativos, que definiu gerenciamento de riscos corporativos da seguinte forma:

> É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO ERM, 2004)

De acordo com o COSO ERM, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização.

Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em **quatro categorias**:

1 - **Estratégicos** – metas gerais, alinhadas com sua missão.

2 - **Operações** – utilização eficaz e eficiente dos recursos.

3 - **Comunicação** – confiabilidade de relatórios.

4 - **Conformidade** – cumprimento de leis e regulamentos aplicáveis.

O COSO ERM definiu oito componentes em sua estrutura, quais sejam: ambiente de Controle, fixação de Objetivos, identificação de Eventos, avaliação de Riscos, resposta a Risco, atividades de Controle, informações e comunicações; e monitoramento.

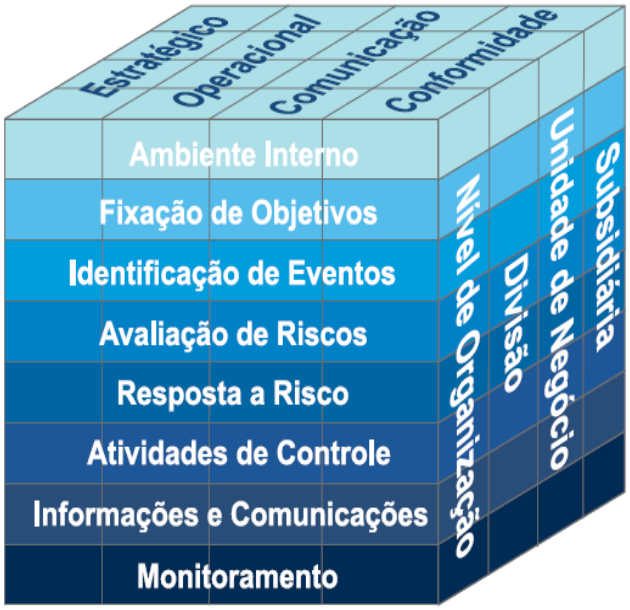

Figura 1 - Cubo do Coso (COSO ERM, 2004)

AMBIENTE DE CONTROLE

Este componente está relacionado ao núcleo de qualquer Organização, o pessoal (Recursos Humanos) – atributos individuais, principalmente integridade, valores éticos e competência, e o ambiente no qual operam. Ele provê uma atmosfera na qual as pessoas conduzem suas atividades e cumprem suas responsabilidades de controle, servindo de base para os demais componentes, retrata a "*consciência e a cultura de controle*" e é afetado fortemente pelo histórico e cultura da organização.

Segundo o Instituto de Auditores Internos (IIA), o Ambiente de Controle representa "*as atitudes e ações do Conselho e da Administração em relação à importância dos controles dentro da organização, definindo o tom da organização*".

O Ambiente de Controle está intrinsicamente relacionado aos controles informais, que estão fortemente relacionados com os valores das pessoas da organização e são igualmente

importantes para gerar um ambiente de controle saudável. Entretanto, não são detectados pelas abordagens e ferramentas tradicionais de auditoria, requerendo técnicas não tão comumente utilizadas, para que se obtenham evidências suficientes sobre a existência deste componente, tais como a observação do ambiente.

O ambiente de controle deve demonstrar o grau e comprometimento em todos os níveis da administração, com a qualidade do controle interno em seu conjunto. É o principal componente e os fatores relacionados ao ambiente de controle incluem, dentre outros:

- Integridade e valores éticos
- Competência das pessoas da entidade
- Estilo operacional da organização
- Aspectos relacionados com a gestão
- Forma de atribuição da autoridade e responsabilidade.

FIXAÇÃO DE OBJETIVOS

Definidos pela alta administração, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam influenciar na consecução dos objetivos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

IDENTIFICAÇÃO DE EVENTOS

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

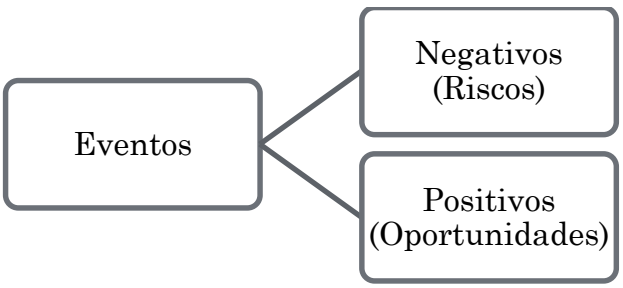

Figura 2 – Identificação de Eventos

Por meio da identificação de eventos, pode-se planejar o tratamento adequado para as oportunidades e para os riscos, que devem ser entendidos como parte de um contexto, e não de forma isolada.

Isso porque, muitas vezes, um risco que parece trazer grande impacto pode ser minimizado pela existência conjunta de uma oportunidade.

Após a identificação de eventos, separando-se as oportunidades dos riscos, vamos atuar sobre esses últimos, por meio da avaliação de riscos, quando determinaremos a forma de tratamento para cada risco identificado, e qual o tipo de resposta a ser dada a esse risco.

AVALIAÇÃO DE RISCO

A organização deve estar consciente dos riscos relevantes que envolvem o negócio, bem como deve gerenciar esses riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Assim, é pré-requisito o estabelecimento, pela Organização, de objetivos estratégicos alinhados a sua Missão e Visão, para que ela opere de forma conjunta e organizada.

A gestão de riscos (identificação e avaliação de riscos e definição de respostas, dentre elas controles) interage com o Planejamento Estratégico, na medida em que a organização ao identificar e tratar os riscos e implementar controles internos focados nesses riscos, estará aumentando a probabilidade de alcance dos objetivos definidos, ou seja, a gestão de riscos é considerada uma boa prática de Governança da organização, ao incluir aspectos relacionados a *accountability* (prestação de contas, no sentido de que a gestão está alinhada às diretrizes estratégicas), transparência (que é um pré requisito para uma adequada prestação de contas), dentre outros.

RESPOSTA A RISCOS

Para cada risco identificado, será prevista uma resposta, que pode ser de 4 tipos: **evitar**, **aceitar**, **compartilhar** ou **reduzir**.

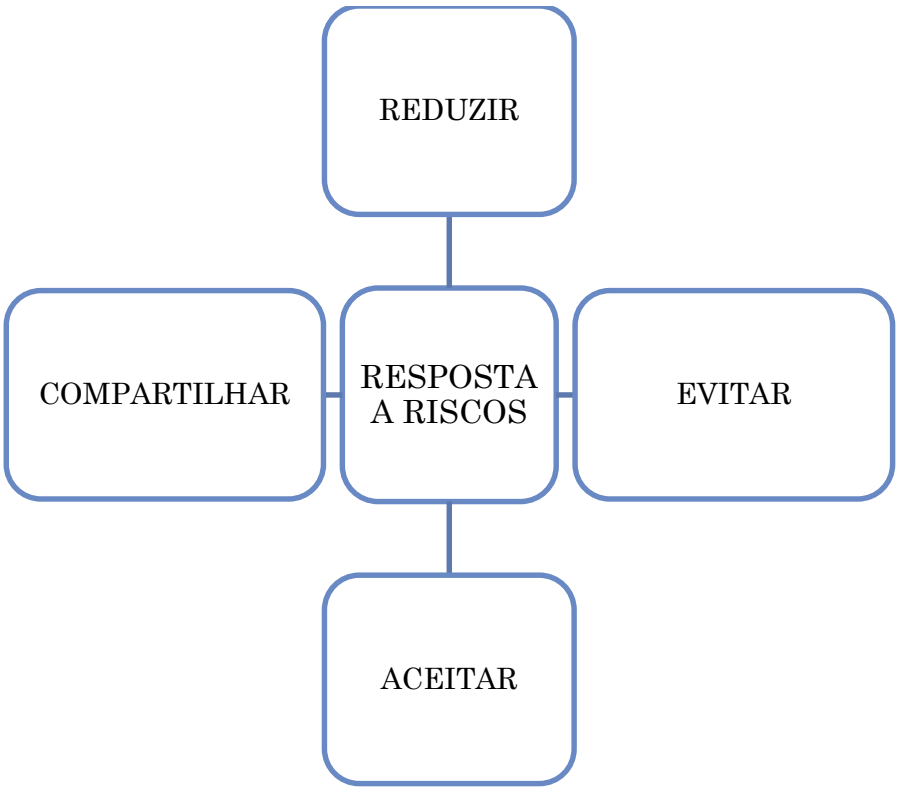

Figura 3 – Resposta a riscos

Em relação a riscos é importante apresentar dois conceitos.

- ✓ **Risco inerente** é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos.
- ✓ **Risco residual** é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes.

De acordo com o COSO, "Evitar" sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. "Reduzir" ou "Compartilhar" reduzem o risco residual a um nível compatível com as tolerâncias desejadas ao risco, enquanto "Aceitar" indica que o risco inerente já esteja dentro das tolerâncias ao risco.

É importante observarmos que aceitar o risco é uma forma de responder ao risco. Ou seja, se eu "não fizer nada" em relação ao risco, eu ainda assim estou respondendo a ele, desde que esse "não fazer nada" seja consciente. Isso pode vir a ocorrer quando o custo de implementação de uma medida qualquer para responder a determinado risco fique muito alto, maior até do que os benefícios que a resposta traria para a organização.

ATIVIDADES DE CONTROLE

As Atividades de Controle geralmente estão expressas em políticas e procedimentos de controle, que devem ser estabelecidos e aplicados para auxiliar e assegurar que ações identificadas pela Administração, como necessárias para tratar os riscos relacionados ao cumprimento dos objetivos da Organização, sejam realizadas de forma eficaz. As atividades de controle estão comumente voltadas para três categorias de riscos: de processo ou operacionais; de registros; e de conformidade. Assim, as atividades de controle contribuem para assegurar que:

- ✓ Os objetivos sejam alcançados.
- ✓ As diretrizes administrativas sejam cumpridas.
- ✓ As ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da entidade estejam sendo implementadas**.**

As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, podem vir a prevenir ou administrar os riscos inerentes ou em potencial da entidade. Não são exclusividade de determinada área da organização, sendo realizadas em todos os níveis. São exemplos de tipologias de atividades de controle:

- ✓ Atribuição de autoridade e limites de alçada
- ✓ Revisões da Alta Administração
- ✓ Revisão de superiores
- ✓ Normatização Interna
- ✓ Autorizações e Aprovações
- ✓ Controles Físicos
- ✓ Segregação de Funções
- ✓ Capacitação e Treinamento
- ✓ Verificações
- ✓ Conciliações
- ✓ Indicadores de Desempenho
- ✓ Revisão de Desempenho Operacional
- ✓ Programas de Contingência e Planos de Continuidade dos Negócios

INFORMAÇÃO E COMUNICAÇÃO

Abrangem informações e sistemas de comunicação, permitindo que as pessoas da Organização coletem e troquem informações necessárias para conduzir, gerenciar e controlar suas operações. Importante que toda a informação relevante, relacionada aos objetivos – riscos - controles, sejam capturadas e comunicadas por toda a Organização.

A Organização também deve possuir mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir externamente aquelas que sejam relevantes aos *stakeholders*, inclusive à sociedade, que, no caso das organizações públicas, pode ser considerada a principal parte interessada.

A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, econômicos, operacionais e estratégicos. Deve ser entendida como um canal que movimenta as informações em todas as direções – dos superiores aos subordinados, e vice-versa – pois determinados assuntos são mais bem visualizados pelos integrantes dos níveis mais subordinados.

MONITORAMENTO

Compreende o acompanhamento da qualidade do controle interno, visando assegurar a sua adequação aos objetivos, ao ambiente, aos recursos e aos riscos. Pressupõe uma atividade desenvolvida ao longo do tempo.

O processo completo de riscos e controles deve ser monitorado e modificações devem ser feitas para o seu aprimoramento. Assim, a estrutura de controle interno pode "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem. O monitoramento pode ser realizado por meio de:

- ✓ Atividades contínuas;
- ✓ Avaliações independentes (por exemplo, auditorias internas e externas); e
- ✓ Auto avaliações.

As atividades contínuas são incorporadas as demais atividades normais da Organização e as avaliações independentes garantem a eficácia do gerenciamento dos riscos ao longo do tempo. Modernamente também são utilizadas as autoavaliações, processo que pode ter um grande auxilio dos auditores.

O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerão basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento.

Diferentemente das Atividades de Controle, que são concebidas para dar cumprimento aos processos e políticas da Organização e visam tratar os riscos, as de monitoramento objetivam identificar fragilidades e possibilidades de melhorias. Lembrando que riscos e oportunidades mudam ao longo do tempo e devem ser monitoradas para que a organização possa realizar os ajustes necessários.

4. Escopo de Aplicação e Abrangência

Conforme já mencionado, o MP e a CGU publicaram a Instrução Conjunta MP/CGU nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Governo federal e determina aos órgãos e entidades do Poder Executivo federal a adoção de diversas medidas com vistas à sistematização de práticas relacionadas à gestão de riscos e controles internos.

Desde sua publicação o Ministério do Planejamento vem adotando medidas para o cumprimento dessa norma. Em 3 de janeiro de 2017 publicou a Portaria nº 426, de 30 de dezembro de 2016, que dispõe sobre a instituição da Política de Gestão de Integridade, Riscos e Controles da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

Desenvolveu também o Método de Priorização de Processos com o objetivo de estabelecer prioridades e definir prazos para gerenciamento de riscos, cujo escopo são os processos organizacionais.

A abrangência de aplicação deste manual de gestão de integridade, riscos e controles é sobre os órgãos específicos singulares do Ministério do Planejamento, Desenvolvimento e Gestão cujas naturezas, características e objetivos apresentam variações na eficaz gestão de riscos, independentemente do nível de maturidade em gestão de riscos em que se encontra.

5. Modelo de Gestão de Integridade, Riscos e Controles Internos da Gestão do MP

O Modelo de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão deve ser entendido como um conjunto de instrumentos institucionais que assegurem o alcance dos objetivos estratégicos, subsidiando a tomada de decisão, contribuindo para o aprimoramento dos processos e, mitigando a ocorrência de possíveis desvios por meio de uma gestão de integridade, riscos e controles internos da gestão eficaz.

Os instrumentos institucionais, por sua vez, viabilizam a implementação do gerenciamento de integridade, riscos e controles internos da gestão no âmbito do Ministério do Planejamento, Desenvolvimento e Gestão.

São instrumentos do Modelo:

- Política de Gestão de Integridade, Riscos e Controles Internos da Gestão
- Instâncias de Supervisão
- Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão
- Solução Tecnológica

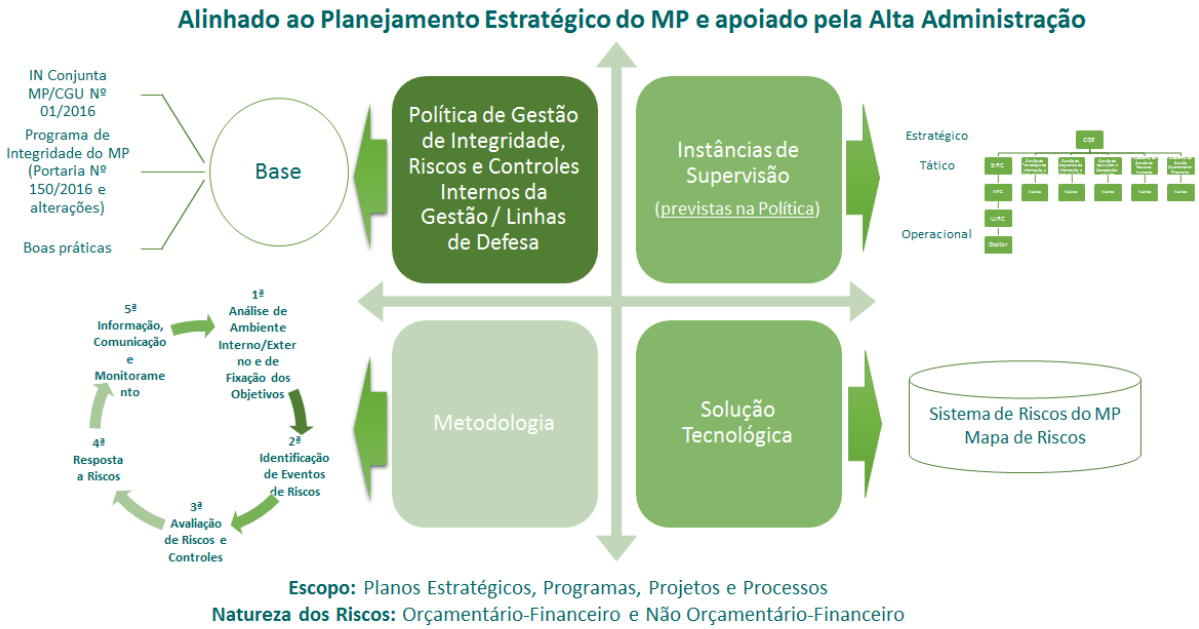

Figura 4 - Modelo de Gestão de Integridade, Riscos e Controles Internos da Gestão

5.1. Política de Gestão de integridade, Riscos e Controles Internos da Gestão - PGIRC

A Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, em seu art. 17, orienta as entidades do Poder Executivo federal sobre a instituição de Política de Gestão de Riscos.

A PGIRC, no âmbito do Ministério do Planejamento, foi instituída por meio da Portaria nº 426, de 30 de dezembro de 2016, e tem por finalidade estabelecer os princípios, diretrizes e responsabilidades a serem observados e seguidos na gestão de integridade, riscos e controles internos da gestão.

A Política aplica-se aos órgãos de assistência direta e imediata ao Ministro de Estado e aos órgãos específicos singulares do MP, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades no MP.

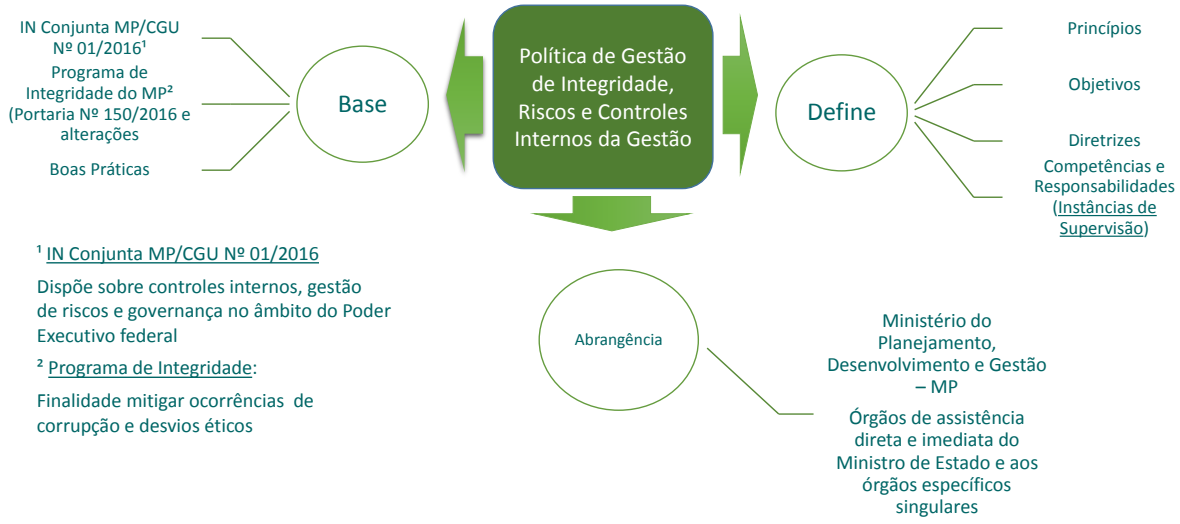

Figura 5 - PGIRC

5.2. Instâncias de Supervisão / Linhas de Defesa

As instâncias de supervisão têm a finalidade de assessorar o Ministro de Estado na definição e implementação de diretrizes, políticas, normas e procedimentos para Gestão de Integridade, Riscos e Controles Internos da Gestão.

São Instâncias de Supervisão:

- Comitê de Gestão Estratégica – CGE - composto pelo Ministro de Estado do Planejamento e pelos dirigentes titulares dos órgãos de assistência direta e imediata do Ministro e dos órgãos específicos singulares;
- Subcomitê de Gestão de Integridade, Riscos e Controles Internos da Gestão – SIRC - composto por servidores dos órgãos de assistência direta e imediata do Ministro de Estado do Planejamento e dos órgãos específicos e singulares do Ministro do Estado do Planejamento, indicados por seus respectivos dirigentes titulares;
- Núcleo de Gestão de Integridade, Riscos e Controles Internos da Gestão – NIRC - composto por servidores com capacitação em temas afetos à gestão de integridade, de riscos e de controles internos da gestão, vinculados à Assessoria Especial de Controle Internos do Gabinete do Ministro;
- Unidade de Gestão de Integridade, Riscos e Controles Internos da Gestão – UIRC - composta, em cada Secretaria do Ministério do Planejamento, Desenvolvimento e Gestão, pelo dirigente máximo e por servidores com capacitação nos temas afetos à gestão de integridade, riscos e controles internos da gestão; e
- Gestor de Processos de Gestão - a todo e qualquer responsável pela execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos.

As instâncias de supervisão e as competências para a gestão de integridade, riscos e controles internos da gestão estão definidas na PGIRC. As responsabilidades de cada instância de supervisão estão resumidas na Matriz de Responsabilidades do MP no Anexo II.

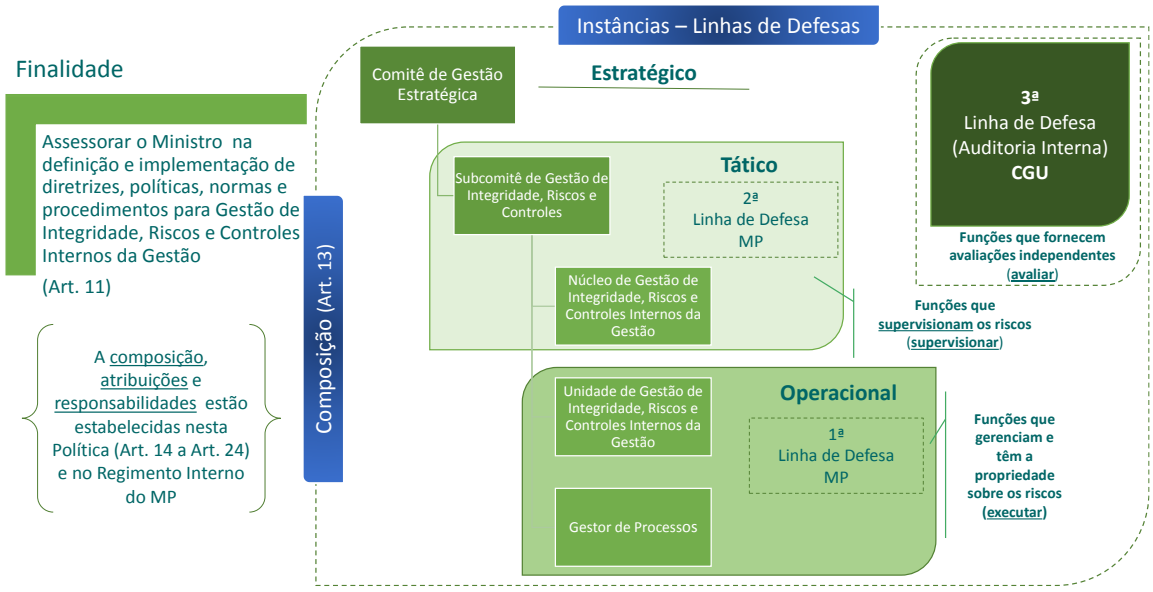

Figura 6 - Instâncias de Supervisão / Linhas de Defesa

Os órgãos/unidades têm, coletivamente, a responsabilidade e o dever de prestação de contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançar

esses objetivos e o estabelecimento de estruturas e processos de governança para melhor gerenciar os riscos durante a realização desses objetivos.

O modelo de Três Linhas de Defesa, constante na Declaração de Posicionamento do Instituto dos Auditores Internos do Brasil – IIA, será melhor implementado com o apoio ativo e a orientação do Comitê de Gestão Estratégica.

Ressalta-se que com a aprovação da PGIRC, pelo CGE, as linhas de defesas ficam bem definidas no âmbito do Ministério do Planejamento, Desenvolvimento e Gestão, a saber:

Na 1ª Linha de Defesa, gestão operacional, estão as funções que gerenciam e têm propriedade sobre os riscos, são responsáveis por implementar ações corretivas para resolver deficiências em processos e controles. Também tem a atribuição de identificar, avaliar, controlar e reduzir os riscos guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos. No âmbito do MP, estas funções são de responsabilidade do nível operacional, representados pelo gestor do processo e pela UIRC.

Na 2ª Linha de Defesa, gerenciamento de riscos e conformidade, estão as funções que supervisionam os riscos, são responsáveis por: (i) ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa; (ii) apoiar as políticas de gestão, definir papéis e responsabilidades e estabelecer metas para implementação; (iii) auxiliar no desenvolvimento de processos e controles para gerenciar riscos; (iv) fornecer orientações e treinamento sobre processos de gerenciamento de riscos; (v) facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos por parte da gerencia operacional - 1ª linha de Defesa; (vi) Monitorar a adequação e a eficácia do controle interno, a precisão e a integridade do reporte, a conformidade com leis e regulamentos e a resolução oportuna de deficiências. No âmbito do MP estas funções são de responsabilidade do nível tático, representados pelo NIRC, vinculado à AECI, e pelo SIRC.

Na 3ª Linha de Defesa, auditoria interna, está a função de avaliações abrangentes, independentes e objetivas sobre a eficácia da governança, do gerenciamento de riscos e controle. E, ainda, como a primeira e a segunda linha de defesa alcançam os objetivos de gerenciamento de riscos e controles. No âmbito do Administração Pública federal esta função é de responsabilidade do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – CGU.

5.3. Metodologia de Gerenciamento de Integridade, Riscos e Controles internos da Gestão

Gerenciar riscos contribui para assegurar a comunicação eficaz, cumprir leis e regulamentos, evitar danos à reputação, mitigar possíveis riscos de corrupção e desvios éticos e, por fim, auxilia a unidade atingir seus objetivos.

Para a elaboração da metodologia de gestão de integridade, riscos e controles internos da gestão – MGIRC do MP considerou-se, especialmente, as seguintes orientações:

- Programa de Integridade do MP/Portaria Nº 150, de 06 de maio de 2016;
- Instrução Normativa Conjunta MP/CGU Nº 01, de 10 de maio de 2016;
- Política de Gestão de Integridade, Riscos e Controles Internos da Gestão/Portaria 426, de 30 dezembro de 2017;
- Committee of Sponsoring Organizations of the Treadway Commission – COSO II, e
- Boas práticas sobre o assunto.

Primeiramente, o ideal é que a Cadeia de Valor / Base de Processos e os processos da unidade estejam mapeados. A Cadeia de Valor é a representação de modelo que permite a visão lógica dos processos organizacionais, enquanto que os Processos de Trabalho representam detalhadamente as atividades, o processamento, as entradas e saídas de cada processo. Ambos são essenciais para que a aplicação da metodologia de gerenciamento de integridade, riscos e controles internos da gestão tenha maior efetividade.

Dessa forma, a base para o gerenciamento de integridade, riscos e controles internos da gestão são os processos de trabalho e o escopo para aplicação da metodologia poderá ser definido com a aplicação do Método de Priorização de Processos, que pode ser consultado no manual específico a ser disponibilizado pela Assessoria Especial de Controle Interno (AECI).

Após a priorização dos processos, a metodologia de gestão de integridades, riscos e controles poderá ser aplicada. A metodologia é composta por cinco etapas, conforme ilustrado de forma resumida na Figura 7. Mais detalhes da metodologia serão apresentados na seção 6.

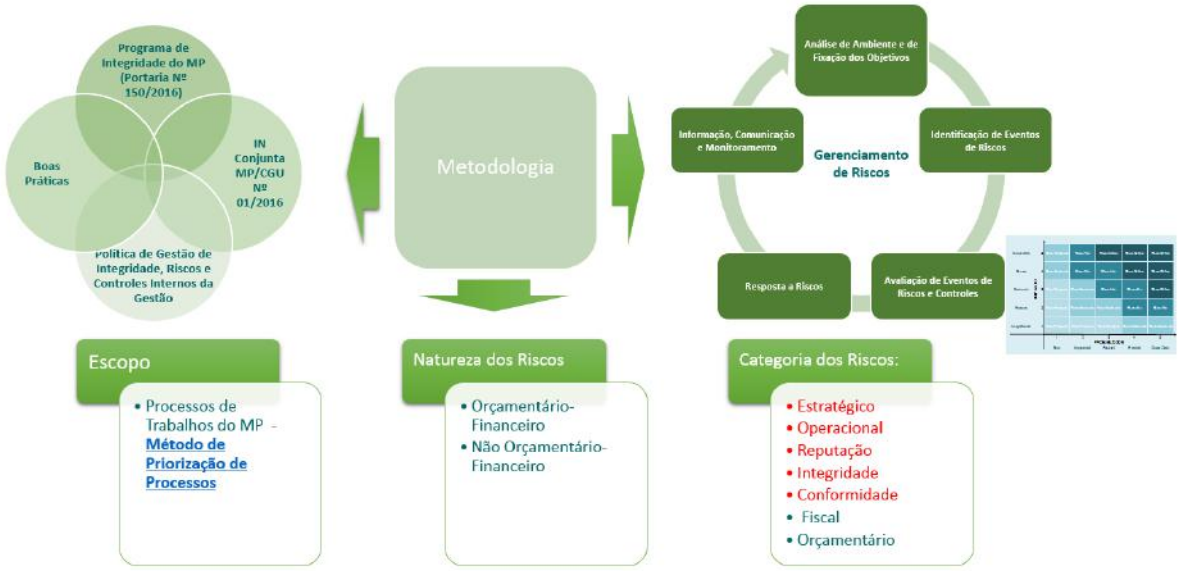

Figura 7 - Síntese da Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão

5.4. SOLUÇÃO TECNOLÓGICA

A solução tecnológica caracteriza-se como um instrumento de apoio a aplicação da metodologia de gerenciamento de integridade, riscos e controles internos da gestão.

Inicialmente, a solução será disponibilizada em uma planilha dotada das configurações necessárias para aplicação da metodologia. Posteriormente, de forma a garantir uma maior padronização e salvaguarda dos dados, um sistema será disponibilizado e terá os requisitos desejáveis a seguir:

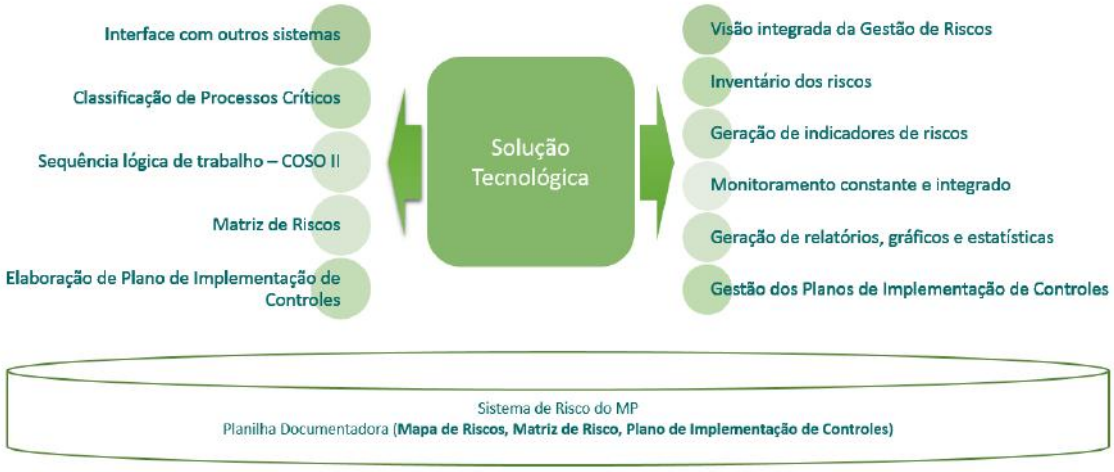

Figura 8 - Visão da Solução Tecnológica

6. METODOLOGIA DE GERENCIAMENTO DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS DA GESTÃO DO MP

Para aplicação da metodologia, faz-se necessário que os macroprocessos/processos das unidades estejam claramente definidos e priorizados. O Método de Priorização de Processos – MPP é uma ferramenta que objetiva a classificação dos processos de uma unidade/órgão, com vista a estabelecer processos prioritários e seus respectivos prazos para o tratamento de possíveis inconsistências/fragilidades/falhas. O manual específico para aplicação do MPP será disponibilizado pela AECI.

Após a definição do processo a ser trabalhado, seja escolhido por necessidade da unidade ou por meio do MPP, a metodologia desenvolvida, baseada no COSO ERM, poderá ser aplicada. Tal metodologia foi dividida em cinco etapas e pode ser vista sucintamente na Figura 9, sendo melhor explicitada no decorrer das sessões, de maneira a auxiliar a implementação de cada etapa no processo selecionado.

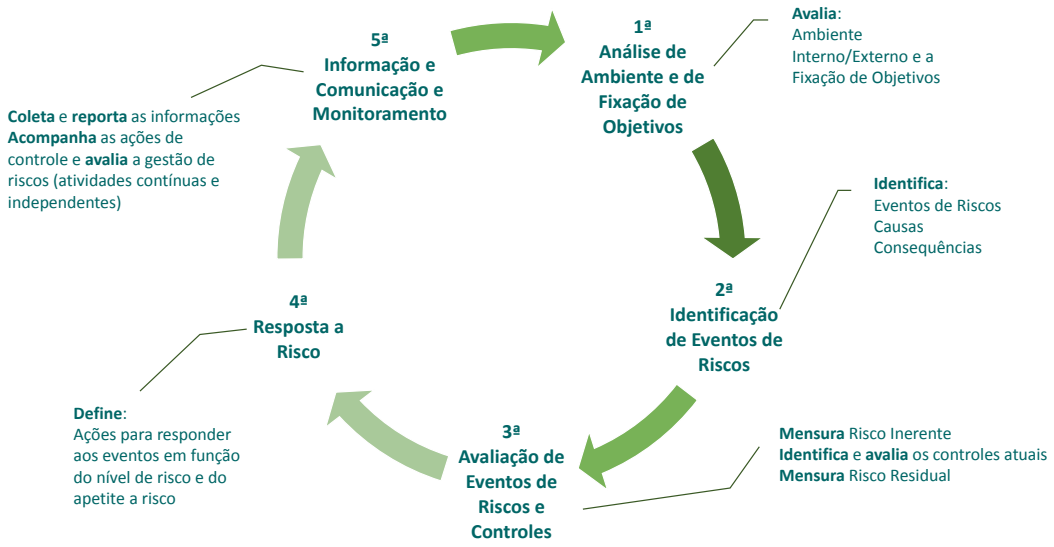

Figura 9 – Etapas da Metodologia de Gerenciamento de Integridade, Riscos e Controles Internos da Gestão

Assim, a partir de um plano de atuação elaborado com base na aplicação do Método de Priorização de Processos (classificação de processos e respectivos prazos), da definição da equipe responsável com seus papéis e responsabilidades, da identificação das partes intervenientes/interessadas no processo, são realizadas as etapas a seguir.

6.1 ETAPAS DO GERENCIAMENTO DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS DA GESTÃO

6.1.1 Etapa 1 - Análise de Ambiente e de Fixação de Objetivos

O ambiente de controle está relacionado aos controles informais, que estão vinculados aos valores das pessoas da organização e são igualmente importantes para gerar um ambiente de controle saudável. A análise do ambiente tem a finalidade de colher informações para apoiar a identificação de eventos de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo.

Definidos pela alta administração, os objetivos devem ser divulgados a todos os componentes da organização, antes da identificação dos eventos que possam influenciar nos seus atingimentos. Eles devem estar alinhados à missão da entidade e devem ser compatíveis com o apetite a riscos.

Para iniciar o preenchimento da ferramenta Planilha Documentadora, considere as informações a seguir:

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.

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.

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), sugere-se a utilização da ferramenta **Análise de SWOT[1]:**

Figura 10 – Análise de SWOT MP

Para registrar as informações coletadas nesta etapa, utilize a **aba Ambiente e Fixação de objetivos** da ferramenta disponibilizada pela AECI, como mostra o formulário abaixo.

[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.

Formulário de Levantamento de Informações sobre Ambiente e sobre a Fixação de Objetivos		
Órgão / Unidade		
Diretoria / Coordenação		
Informações sobre o Ambiente Interno - existência de:	**Sim**	**Não**
Código de Ética / Normas de Conduta	( )	( )
Estrutura Organizacional	( )	( )
Política de Recursos Humanos (compromisso com a competência e desenvolvimento)	( )	( )
Atribuição de Alçadas e Responsabilidades	( )	( )
Normas Internas	( )	( )
Informações sobre a Fixação de Objetivos - existência de:	**Sim**	**Não**
Missão	( )	( )
Visão	( )	( )
Objetivos	( )	( )

Este fornulário tem a finalidade de avaliar aspectos dos dois primeiros componentes do COSO GRC (Ambiente Interno e Fixação de Objetivos) e contribui para identificar também a existencia de aspectos relacionados à integridade.

Informações sobre o Macroprocesso/Processo	
Macroprocesso/Processo	
Objetivo Geral	
Leis e Regulamentos:	
Sistemas:	

Análise de SWOT

A análise de SWOT é realizada com foco no macroprocesso/processo e visa obter informaçõespara apoiar a identificação de eventos de riscos, bem como escolher as ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo, da unidade e do MP.

Análise do Ambiente Interno	
Forças (Pontos Fortes)	1.
	2.
	3.
	4.
	5.
	6.
Fraquezas (Pontos Fracos	1.
	2.
	3.
	4.
	5.
	6.
Análise do Ambiente Externo	
Oportunidades (Pontos Fortes)	1.
	2.
	3.
	4.
	5.
	6.
Ameaças (Pontos Fracos)	1.
	2.
	3.
	4.
	5.
	6.

Figura 11 - Análise de Ambiente e Fixação de Objetivos

As informações coletadas, 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 integridade, riscos e controles internos da gestão.

Pontos de Atenção

1. Macroprocesso/Objetivo do Macroprocesso: essas informações deverão ser coletadas da Cadeia de Valor ou do mapeamento do processo.

2. Leis e Regulamentos: listar todas as leis, regulamentos e normas que afetam ou influenciam o macroprocesso/processo. Essas informações são importantes para verificar se há riscos e descumprimento de leis, regulamentos e normas, bem como auxilia na adoção de ações de controle.

3. Sistemas: listar os sistemas e outras ferramentas (ex: planilhas) que operacionalizam o processo. Essas informações são importantes para verificar se os controles são manuais ou eletrônicos.

6.1.2 Etapa 2 - Identificação de Eventos de Riscos

Esta etapa tem por finalidade identificar e registrar tanto os eventos de riscos que comprometem o alcance do objetivo do processo, assim como as causas e efeitos/consequências de cada um deles. Considere, neste momento, o resultado da **análise do Ambiente e de Fixação de Objetivos**, Etapa 1.

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades. Nessa metodologia, inicialmente, trataremos apenas sobre eventos negativos.

Por meio da identificação de eventos de riscos, pode-se planejar a forma de tratamento adequado e qual o tipo de resposta a ser dada a esse risco, destacando que os eventos de riscos devem ser entendidos como parte de um contexto, e não de forma isolada.

Componentes do Evento de Risco:

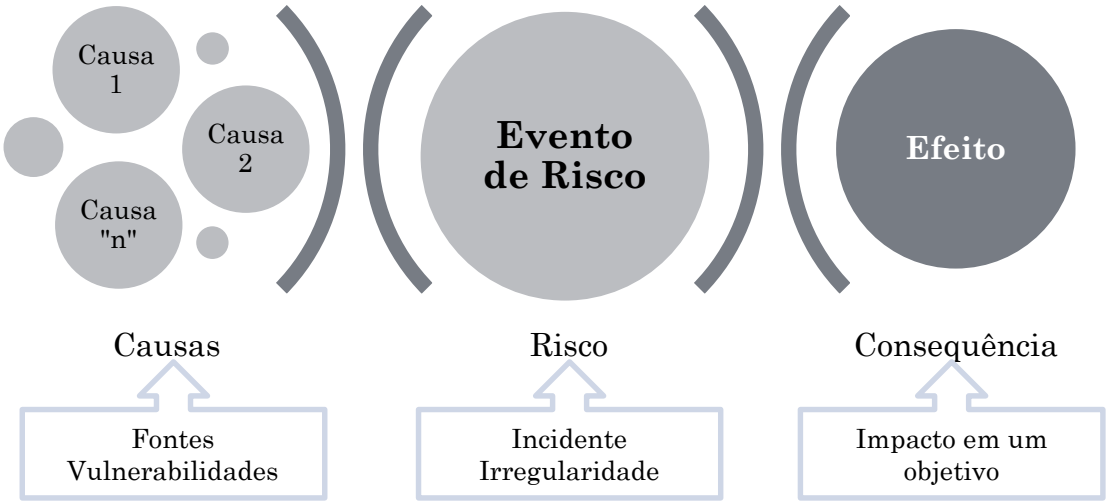

Figura 12 – Componentes do Evento de Risco

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

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Consequência: o resultado de um evento de risco sobre os objetivos do processo.

Como identificar os eventos de riscos?

O processo de identificação de riscos requer a participação de servidores com conhecimento do processo, visão holística dos negócios/serviços da unidade nos seus diferentes níveis. É importante também que tenham conhecimento da metodologia de gerenciamento de integridade, riscos e controles internos da gestão ou tenham recebido treinamento para aplicação da metodologia e uso da planilha documentadora.

A técnica a ser utilizada na identificação de eventos de risco deve ser a que melhor se adapta ao grupo. Dentre as principais técnicas estão: questionários e c*hecklist*; *whorkshop* e *brainstorming;* inspeções e auditorias, fluxogramas, diagrama de causa e efeito, *bow-tie*, etc.

De forma abreviada, o diagrama de causa e efeito, também conhecido como espinha de peixe ou diagrama de *ishikawa*, é uma técnica para identificação de uma possível causa raiz de um problema. No diagrama, cada espinha refere-se a uma causa e a cabeça refere-se ao problema que as causas levam. Esse método pode ser aplicado em *workshops* e *brainstorming*, partindo da identificação de um problema e em seguida as suas possíveis causas. Além disso, também

pode ser utilizado em conjunto com o método dos "cinco porquês", aumento o grau de profundidade de cada causa ou "espinha do peixe" ao se questionar o porquê das causas.

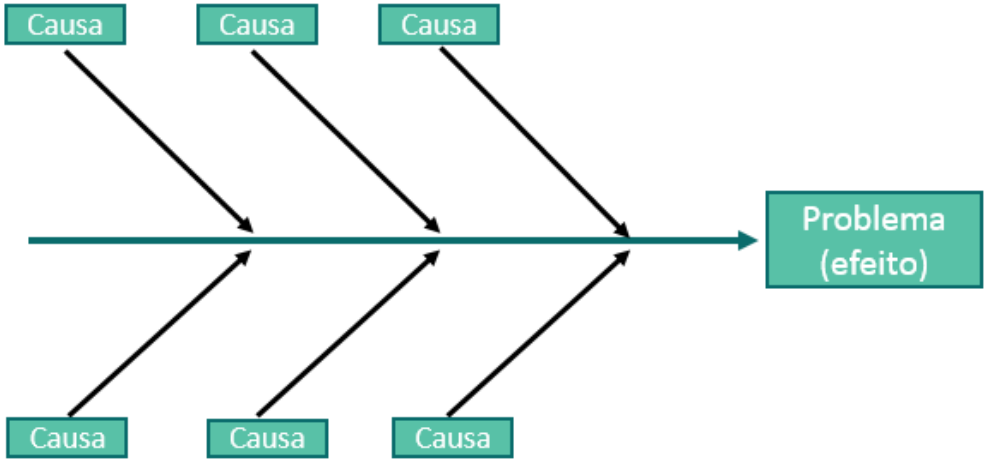

Figura 13 – Diagrama de Causa e Efeito

O método *bow-tie* ou gravata borboleta, considerado uma evolução do diagrama de causa e efeito, consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que um problema pode estar relacionado a diversas causas e consequências. Como no diagrama de causa e efeito, identifica-se o problema e em seguida suas possíveis causas e consequências. Para finalizar, identifique as formas de prevenir a ocorrência do risco e as formas de mitigar as consequências caso o risco se materialize. Veja a figura 14 para uma melhor compreensão.

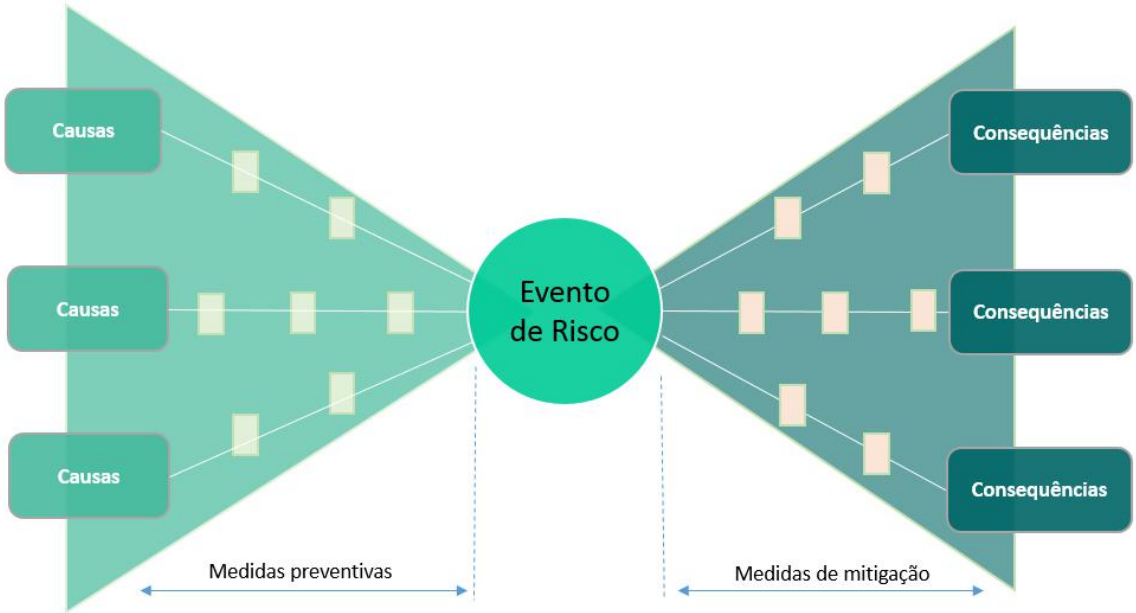

Figura 14 – Método Bow-Tie

A sintaxe a seguir para descrição de um evento risco poderá auxiliar no desenvolvimento desta etapa:

Devido a **<CAUSA/FONTE>**, poderá acontecer **<DESCRIÇÃO DO EVENTO DE RISCO>**, o que poderá levar a **<DESCRIÇÃO DO IMPACTO/EFEITO/CONSEQUÊNCIAS>** impactando no/na **<OBJETIVO DE PROCESSO >**.

Escolha a técnica que favoreça a realização desta atividade e colete as seguintes informações de acordo com **a aba Mapa de Riscos**:

Processo / Atividade	Identificação de Eventos de Riscos				
	Eventos de Risco	Causas	Efeitos / Consequências	Categoria do Risco	Natureza do Risco
Subprocesso/ Atividade 1	Evento 1	C 1	E/C 1	Reputação	Não Orçamentétio Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso/ Atividade 2	Evento 1	C 1	E/C 1	Operacional	Não Orçamentétio Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso/ Atividade 3	Evento 1	C 1	E/C 1	Reputação	Orçamentário Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso/ Atividade 4	Evento 1	C 1	E/C 1	Fiscal	Orçamentário Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso / Atividade 5	Evento 1	C 1	E/C 1	Operacional	Não Orçamentétio Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso / Atividade 6	Evento 1	C 1	E/C 1	Integridade	Orçamentário Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso / Atividade 7	Evento 1	C 1	E/C 1	Estratégico	Não Orçamentétio Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso/ Atividade 8	Evento 1	C 1	E/C 1	Orçamentário	Orçamentário Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		
Subprocesso/ Atividade 9	Evento 1	C 1	E/C 1	Fiscal	Orçamentário Financeiro
	Evento 2	C 2	E/C 2		
	Evento 3	C n	E/C n		

Figura 15 - Mapa de Riscos

Os eventos de riscos identificados devem ser registrados de forma a permitir o levantamento das possíveis causas e consequências e a sua classificação quanto à categoria e natureza, bem como a sua avaliação quanto à probabilidade x impacto.

Orientações:

1) Subprocesso/atividade: indique o nível em que se realizará a identificação dos eventos de riscos do macroprocesso/processo escolhido para a análise.
2) Evento de Risco: descreva os eventos de riscos identificados, a partir da utilização da técnica escolhida para essa atividade.
3) Causas: descreva as possíveis causas, condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

4) Efeitos/consequências: descreva os possíveis efeitos/consequências de um possível evento de risco sobre os objetivos do processo.
5) Categoria dos Riscos: sabendo-se que a categorização de riscos não é consensual na literatura, cabe a cada organização o desenvolvimento de suas categorias de acordo com suas peculiaridades. O MP, com auxílio do Comitê Técnico de Riscos, qualificou as categorias de risco conforme abaixo:
    a. Estratégico: eventos que possam impactar na missão, nas metas ou nos objetivos estratégicos da unidade/órgão, caso venham ocorrer.
    b. Operacional: eventos que podem comprometer as atividades da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão quanto à eficácia e a eficiência dos processos organizacionais.
    c. Orçamentário: eventos que podem comprometer a capacidade do MP de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.
    d. Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade do MP em cumprir sua missão institucional, interferem diretamente na imagem do órgão.
    e. Integridade: eventos que podem afetar a probidade da gestão dos recursos públicos e das atividades da organização, causados pela falta de honestidade e desvios éticos.
    f. Fiscal: eventos que podem afetar negativamente o equilíbrio das contas públicas.
    g. Conformidade: eventos que podem afetar o cumprimento de leis e regulamentos aplicáveis.

6) Natureza dos Riscos: está relacionada à categoria de risco escolhida. Se a categoria de risco for fiscal ou orçamentária, a natureza do risco será orçamentário-financeiro. Se a categoria do risco for estratégica, operacional, reputacional, integridade ou conformidade, a natureza do risco será não orçamentário-financeira.

Ponto de Atenção

1. Cada unidade deve considerar as categorias aplicáveis à sua realidade.

6.1.3 Etapa 3 - Avaliação de Eventos de Riscos e Controles

Esta etapa tem por finalidade avaliar os eventos de riscos identificados considerando os seus componentes (causas e consequências). Os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto. Normalmente as causas se relacionam à probabilidade de o 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 quanto ao desenho e a sua execução).

Risco inerente *é o risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.* (Art. 2º, XIV, IN Conjunta MP/CGU Nº 01/2016).

Risco residual*: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;* (Art. 2º, XV, IN Conjunta MP/CGU Nº 01/2016).

Controles internos da gestão**:** *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. 2º, V, IN Conjunta MP/CGU Nº 01/2016).

A realização desta etapa ocorrerá em três sub-etapas, sendo todas elas utilizando a ferramenta Planilha Documentadora com auxílio do guia Matriz de Risco.

1. Na aba **Cálculo do Risco Inerente**, faça a mensuração do **risco inerente** de acordo com o impacto e a probabilidade de ocorrência de cada evento.
2. Uma vez mensurado o risco inerente é necessário identificar e avaliar os controles que respondam aos eventos de riscos identificados, quanto ao seu desenho e quanto à sua operação. Na aba Mapa de Riscos, insira a descrição do controle atual e, utilizando as informações dos quadros abaixo, proceda com a avaliação quanto ao desenho e quanto à operação do controle.

a. Quanto ao desenho: são verificadas as seguintes informações:

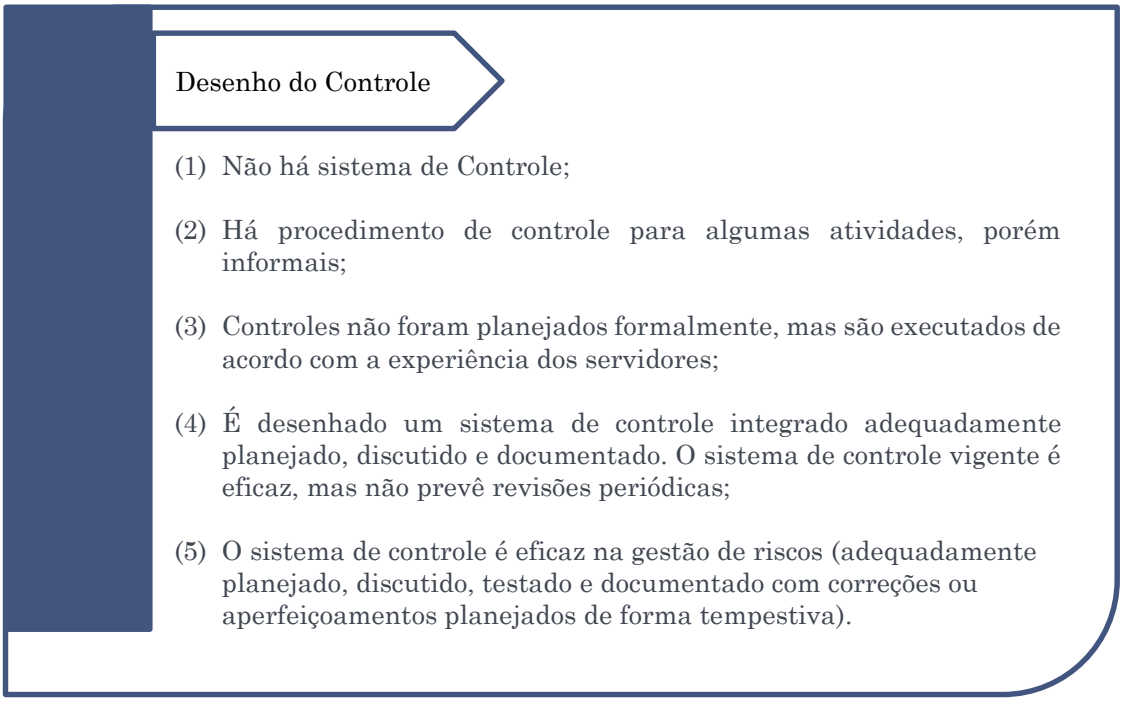

Figura 16- Desenho do Controle

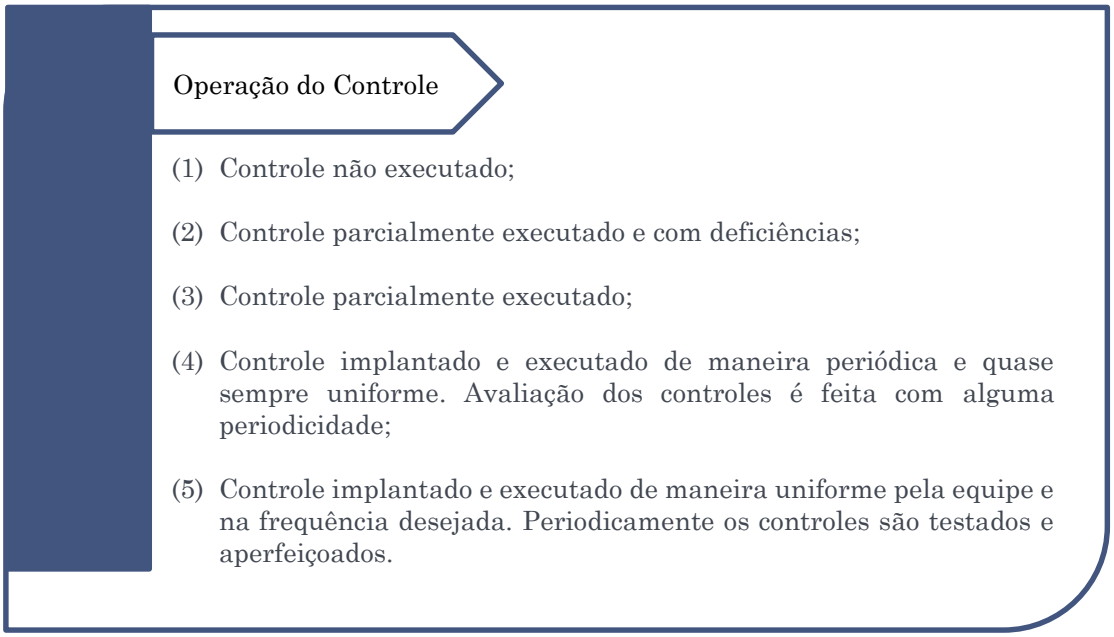

Figura 17 – Operação do Controle

3. Na **aba Cálculo do Risco Residual**, indique os pesos relativos ao impacto e à probabilidade, de forma similar à análise feita na aba Cálculo do Risco Inerente, considerando os controles identificados e o resultado da sua avaliação quanto ao desenho e à operação dos controles.

Ao finalizar o preenchimento das etapas, tem-se o nível de risco para cada evento identificado, como ilustrado na Figura 16. Valide com o gestor do processo para efetuar a próxima etapa, resposta a riscos.

Nível de Risco	
Impacto x Probabilidade	Descrição
25	Risco Crítico
8	Risco Alto
2	Risco Pequeno
6	Risco Moderado
1	Risco Pequeno
8	Risco Alto
16	Risco Crítico
12	Risco Alto
1	Risco Pequeno
4	Risco Moderado
2	Risco Pequeno

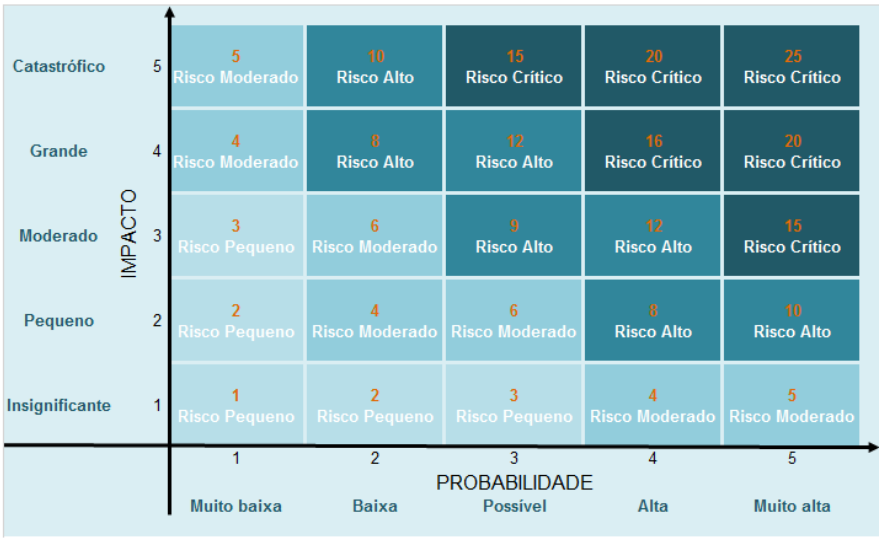

Figura 18 - Cálculo do risco residual

6.1.4 Etapa 4 - Resposta a Risco

Atividades de Controles são as políticas e os procedimentos estabelecidos e executados para reduzir os riscos que a unidade tenha optado por responder, também denominadas de procedimentos de controle. As atividades de controles devem estar distribuídas por toda a unidade, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão, que podem ser preventivos, corretivos ou de compensação, bem como a preparação prévia de planos de contingência/continuidade em resposta a possíveis materialização de eventos de riscos.

Em alguns casos a atividade de controle aborda diversos riscos e as vezes são necessárias diversas atividades para resposta a apenas um risco.

Conhecido o nível de risco residual, verifique qual estratégia a ser adotada para responder ao evento de risco. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecidos em confronto com a avaliação que se fez do risco (matriz de riscos).

A estratégia de respostas foi aprovada junto com a Matriz de Risco. Em função do nível de **risco residual**, tem-se sugestão de medida correspondente a ser adotada.

Nível de Risco	Descrição do Nível de Risco	Parâmetro de Análise para Adoção de Resposta	Tipo de Resposta	Ação de Controle
Risco Crítico	Indica que nenhuma opção de resposta foi identificada para reduzir a probabilidade e o impacto a nível aceitável	Custo desproporcional, capacidade limitada diante do risco identificado	**Evitar**	Promover ações que evitem, eliminem ou atenuem urgentemente as causas e/ou efeitos
Risco Alto	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Nem todos os riscos podem ser transferidos. Exemplo: Risco de Imagem, Risco de Reputação	**Reduzir**	Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos
Risco Moderado	Indica que o risco residual será reduzido a um nível compatível com a tolerância a riscos	Reduzir probabilidade ou impacto, ou ambos	**Compartilhar ou Transferir**	Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (seguro, transações de hedge ou terceirização da atividade).
Risco Pequeno	Indica que o risco inerente já está dentro da tolerância a risco	Verificar a possibilidade de retirar controles considerados desnecessários	**Aceitar**	Conviver com o evento de risco mantendo práticas e procedimentos existentes

Figura 19 - Resposta a risco

As ações para responder os eventos de riscos devem ser compatíveis com a tolerância a riscos, considerar a relação custo benefício, refletir se o efeito da resposta afeta a probabilidade ou o impacto, ou ambos, e designar um responsável pelas respostas (proprietário do risco).

Além disso, é permitido ao gestor do processo alterar a resposta a risco, tanto para adotar uma ação onde poderia aceitar o risco e não adotar controle, como deixar de adotar uma ação onde deveria adotar uma ação de controle, tudo isso com apresentação de justificativa e validação pela unidade de gestão de risco superior.

Ponto de Atenção

É preciso diferenciar **Apetite a Riscos** de **Tolerância a Riscos**. Enquanto este representa o nível aceitável de variação em relação à meta para o cumprimento de um objetivo específico, aquele se refere ao máximo nível de risco que uma organização está disposta a correr para atingir seus objetivos estratégicos. Apetite a riscos é estratégico e amplo. Tolerância a riscos é tático e operacional. Por exemplo:

- Apetite a Riscos: Um hospital tem um baixo apetite a riscos relacionado à segurança do paciente, ou seja, estabelece que apenas riscos pequenos sejam aceitos. Entretanto, sabe também que precisa balancear o atendimento tempestivo para todas as necessidades do paciente com os custos de fornecer esses serviços.
- Tolerância a Riscos: Esforçar-se para tratar pacientes críticos em até 15 minutos e os demais pacientes em quartos dentro de 2 horas. Entretanto a Direção aceita, em raras circunstâncias (5% do tempo) que pacientes que não tenham ameaças de morte, possam não receber atenção durante até 4 horas.

Plano de Implementação de Controles

O Plano de Implementação de Controles é um conjunto de ações necessárias para adequar os níveis de riscos, por meio da adoção de novos controles ou a otimização dos controles atuais do processo.

Para responder aos eventos de riscos é necessária a elaboração de um plano de implementação de controles estabelecendo atividades de controles para assegurar que a resposta seja conduzida.

Utilize um formulário próprio para registrar as ações propostas, orientando-se pelas seguintes informações:

Status do Andamento dos Controles Propostos	
Qtde ações realizadas	0
Qtde ações prevista	9

LEGENDA	
Em andamento	
Concluído	
Atrasado	

O que?			Onde?	Quem?	Como?		Quando?			
Controle Proposto	Tipo de Controle Proposto	Objetivo do Controle Proposto	Área Responsável pela Implementação do Controle Proposto	Responsável Implementação do Controle Proposto	Como será Implementado	Intervenientes	Data do Início	Data da Conclusão	Status	Situação
Segregação de Funções	Corretivo	Adotar Controle Novo					01/01/2017	30/01/2017	Em andamento	
x	Preventivo						01/01/2017	05/01/2017	Concluído	
y	Preventivo						01/01/2017	22/01/2017	Atrasado	
h	Preventivo								Atrasado	
j	Preventivo								Atrasado	
k	Preventivo								Atrasado	
ç	Preventivo								Atrasado	
t	Preventivo								Atrasado	
v	Preventivo								Atrasado	

Figura 20 – Plano de Implementação de Controles

Orientações:

1. Evento de Risco/Nível de Risco e Resposta a Risco: preenchidos automaticamente em função da mensuração do risco residual e respectiva resposta. Cabe ressaltar que a resposta poderá ser modificada mediante justificativa e aprovação do escalão competente.
2. Controles Propostos/Ações Propostas: registrar controles ou ações para responder ao evento de risco.
3. Tipo de controle proposto/ Ação Proposta: preventivo (atua na causa), corretivo (atenua o efeito) ou compensatório (mitiga eventos de risco temporariamente até a implementação de controle definitivo).
4. Objetivo do Controle Proposto/ Ação Proposta: melhorar o controle existente ou adotar controle novo.

5. Área responsável pela implementação do controle proposto/ ação proposta: informar a coordenação/diretoria.
6. Responsável pela implementação do controle proposto/ ação proposta: gestor do processo ou servidor designado quando a implementação da ação for de competência de outra área.
7. Como será implementado: informar se por meio de projeto, melhoria no sistema, criação de norma, plano de contingência, etc.
8. Intervenientes: outras áreas e servidores intervenientes na ação.
9. Data do Início: informar data prevista para início
10. Data da Conclusão: informar data prevista para a conclusão.

Pontos de atenção

Na proposição de ações é importante instituir:

1. Controles automatizados em substituição aos manuais, quando possível;
2. Indicadores de desempenho: estabelecimento de indicadores (índice de rotação de pessoal, cumprimento de prazos legais, entre outros);
3. Segregação de funções: atribuição de obrigações entre pessoas com a finalidade de reduzir risco, erro ou fraude;
4. Limites para transações;
5. Combinação de controles manuais e informatizados (automatizados);
6. Políticas e procedimentos.

No setor público existem situações em que a ação ideal não pode ser implementada ou não pode ser implementada no curto prazo em função da sua complexidade, alto custo, alto nível de interveniência, etc. Nesses casos devem ser propostas, complementarmente, medidas alternativas de baixo custo e que atuem sobre o evento de riscos (controle compensatório).

Um controle compensatório tende a existir para contrabalancear uma falha na estrutura de controles, impedindo que eventos de risco ocorram, ou diminuindo sua severidade.
Exemplo: se a ação ideal é a informatização de um processo e o tempo previsto para sua implementação é longo, pode-se adotar, temporariamente, controles manuais.

Os controles devem ser propostos, ainda, sob a ótica de custo x benefício com o objetivo de otimizá-los. O custo de um controle não deve ser mais caro do que o benefício gerado por ele.

6.1.5 Etapa 5 - Informação, Comunicação e Monitoramento

O acesso a informações confiáveis, íntegras e tempestivas é vital para que a gestão de integridade, riscos e controles internos da gestão seja adequada e eficaz no alcance de seus objetivos. Para isso, o fluxo das comunicações deve permitir que informações fluam em todas as direções, e que os direcionamentos estratégicos, vindos do Comitê de Gestão Estratégica, alcance todo o MP. Além disso, as informações externas relevantes aos processos de trabalho também devem ser consideradas e compartilhadas tempestivamente. A comunicação em direção à sociedade também é objeto de controle, reduzindo riscos de respostas inadequadas às necessidades da população.

O monitoramento de toda a estrutura de governança e de gestão de integridade, riscos e controles internos da gestão permite que o MP se certifique da adequação dessa estrutura aos seus objetivos estratégicos. Com base nesse monitoramento, devem ser elaborados os Relatórios dos Planos de Implementação dos Controles, que serão avaliados pelas instâncias de supervisão. Caso sejam percebidas deficiências ou vulnerabilidades, recomendações serão feitas pela instância responsável para um aperfeiçoamento dos instrumentos de gestão de integridade, riscos e controles.

Meio de Comunicação

A comunicação entre as instâncias de supervisão de gestão de integridade, riscos e controles internos da gestão ocorre por meio dos níveis de relacionamento delineados no Modelo de Relacionamento a seguir.

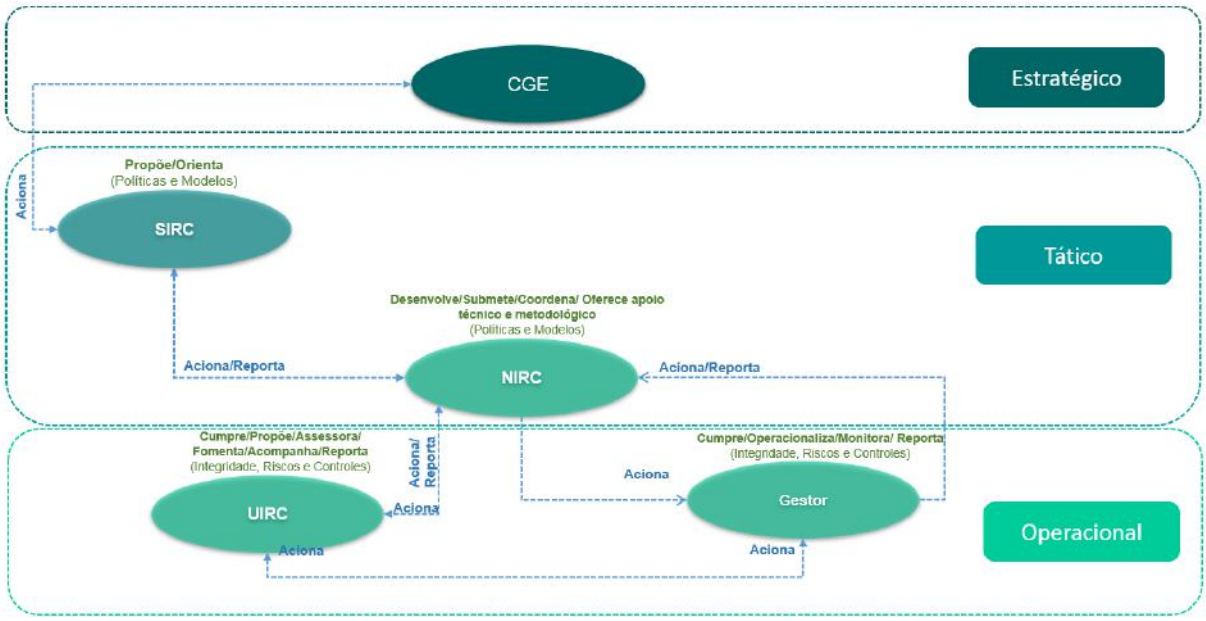

Figura 21 – Níveis de Relacionamento

O nível operacional, representado pelo UIRC e pelo gestor do processo, poderá acionar o nível tático, representado pelo NIRC, para orientações técnicas relativas ao modelo de gestão de integridade, riscos e controles internos da Gestão. Ainda, o nível operacional será responsável pelo reporte ao nível tático sobre o monitoramento das ações definidas no plano de implementação de controles e das ações de gestão de integridade, riscos e controles de forma ampla.

O nível tático, representado pelo NIRC, poderá acionar o nível operacional durante o monitoramento das ações de integridade, riscos e controles. Ainda, será responsável pelo reporte realizado ao SIRC sobre o andamento das ações definidas para o modelo de gestão de integridade, riscos e controles de gestão.

O nível tático, representado pelo SIRC, poderá acionar e ser acionado pelo nível estratégico, representado pelo CGE, para o monitoramento das ações definidas na política de gestão de integridade, riscos e controles de gestão.

Meios de Monitoramento

O Mapa de Risco será a principal ferramenta de monitoramento do processo de gestão de integridade, riscos e controle da unidade. Além dele, o Relatório de Implementação do Plano de Controles, construído na periodicidade definida pelas instâncias de supervisão, será de suma importância para o acompanhamento dos trabalhos realizados pela unidade.

É importante que as informações apresentadas nos meios de monitoramento possuam qualidade contextual e de representação como base nos critérios a seguir:

- Relevância: a informação deve ser útil para o objetivo do trabalho;
- Integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;
- Adequação: volume de informação adequado e suficiente;
- Concisão: informação deve ser apresentada de forma compacta;
- Consistência: as informações apresentadas devem ser compatíveis;
- Clareza: informação deve ser facilmente compreensível;
- Padronização: informação deve ser apresentada no padrão aceitável.

Indicadores de Monitoramento da Implementação dos Controles

As unidades devem estabelecer indicadores de acompanhamento da implementação da metodologia de gestão de integridade, riscos e controles internos da gestão, assim como desenvolver indicadores próprios para o monitoramento da implementação dos controles planejados.

Sugerimos uma lista exemplificativa e não exaustiva de indicadores que podem ser acompanhados e reportados, tais como:

Tabela 1 – Indicadores de Monitoramento

Indicador	Fórmula
% processos mapeados por unidade	processos mapeados/total de processos
% processos essenciais mapeados por unidade	processos essenciais mapeados/processos essenciais
% processos relevantes mapeados por unidade	processos relevantes mapeados/processos essenciais
% processos moderados mapeados por unidade	processos moderados mapeados/processos essenciais
% processos essenciais com riscos mapeados por unidade	processos essenciais com riscos mapeados/processos essenciais
% processos relevantes com riscos mapeados por unidade	processos relevantes com riscos mapeados/processos relevantes
% processos moderados com riscos mapeados por unidade	processos moderados com riscos mapeados/processos moderados
% controles implementados por processo	controles concluídos/total de controles do processo
% controles em andamento por processo	controles em andamento/total de controles do processo
% controles atrasados por processo	controles atrasados/total de controles do processo
% controles não iniciados por processo	controles não iniciados/total de controles do processo

Avaliação da Qualidade do Desempenho dos Controles Internos

Após implementados, os controles devem ser continuamente avaliados ao longo do tempo no que diz respeito ao seu desenho e operação.

Como fonte de entrada para as avaliações, poderão ser utilizados reclamações e denúncias registradas na ouvidoria, relatórios, recomendações ou demandas do Ministério da Transparência, Fiscalização e Controle – Controladoria Geral da União e do Tribunal de Contas da União, mudanças nos objetivos estratégicos, mudanças de normas e regulamentações, entre outras fontes.

Relatório

Cada unidade deve desenvolver um relatório sobre a gestão de integridade, riscos e controles internos a cada seis meses para as partes interessadas.

O relatório deve conter minimamente as seguintes seções: introdução; estrutura organizacional da unidade; processos da unidade; metodologia aplicada; documentos de referência; gestão de integridade, riscos e controles com inventário de riscos, avaliação dos riscos e ações de controle propostas; considerações finais e anexos. Mais detalhes sobre o relatório poderão ser encontrados no Modelo de Relatório anexado.

Considerações Finais

Este manual apresentou a Metodologia de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério do Planejamento, Desenvolvimento e Gestão (MP), que tem como principal objetivo auxiliar, sistematizar e padronizar a gestão de integridade, riscos e controles internos nas unidades do MP. Almeja-se contribuir para a implantação de boas práticas de Gestão de Integridade, Riscos e Controles Internos e para a tomada de decisões de governança.

A Metodologia de Gestão de Integridade, Riscos e Controles Internos é composta pelas etapas: Análise de Ambiente e de Fixação de Objetivos; Identificação de Eventos de Riscos; Avaliação de Eventos de Riscos e Controles; Resposta a Riscos; e Informação, Comunicação e Monitoramento. Cada etapa visa atingir os objetivos específicos do processo de gestão de integridade, riscos e controles internos da gestão.

A metodologia incorpora boas práticas reconhecidas, apresentando características da estrutura do COSO ERM. Além disso, é aderente ao Programa de Integridade, estabelecido pela Portaria nº 150 de 14 de maio de 2016, à Instrução Normativa Conjunta CGU/MP nº 01, de 10 de maio de 2016, e à Política de Gestão de Integridade, Riscos e Controles Internos da Gestão, estabelecida pela Portaria nº 426 de 30 de dezembro de 2016, sendo também uma implementação desta.

Na aplicação dessa metodologia, é importante registrar, organizar, documentar e referenciar os dados e informações considerados, visando evidenciar o embasamento do resultado e subsidiar a sua aprovação pela instância competente.

Cabe ressaltar que em qualquer iniciativa de desenvolvimento de metodologias, é fundamental a realização de ajustes para se adequar ao contexto da unidade de gestão de integridade, riscos e controles. Com o intuito de manter-se adequado as necessidades do MP, este manual estará em constante processo de melhoria. Para tanto, estão previstas ações de desenvolvimento de projetos pilotos nas unidades e de desenvolvimento de um *software* aderente à metodologia.

Por fim, ressalta-se que o levantamento e gerenciamento de riscos devem fazer parte dos processos das unidades, assim, é necessário elaborar cronograma para a realização dos trabalhos, observados os prazos institucionais, e submeter às instâncias para aprovação e acompanhamento.

7. Referências Bibliográficas

AHP - **Analytic Hierarchy Process**, Excel MS Excel 2010 (extensão xlsx). O modelo AHP foi desenvolvido por Goepel, Klaus D., modelo BPMSG AHP Excel, disponível em http://bpmsg.com, cuja versão é de livre uso.

BB – Diretoria de Controles Internos. **Priorização de Processos, Escopo de Atuação**. Visita Técnica em 26.jul.2015.

BCB – **Fundamentos de Gestão de Riscos Não-Financeiros**. Disponibilizada pela UniBacen, curso realizado de 30/06 a 036/07/2015.

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **Gestão de Riscos: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000**: Primeira Edição, 2009.

BRASIL. Ministério do Planejamento. Secretaria de Gestão Pública. Programa Gespública - **O Modelo de Excelência em Gestão Pública**. Brasília, 2014a.

BRASIL. Ministério do Planejamento. Secretaria de Gestão Pública. Programa Gespública - **Instrumento para Avaliação da Gestão Pública**. Brasília, 2014b.

BRASIL. Tribunal de Contas da União. Processo TC 020.905/2014-9 - **Relatório de Levantamento de Auditoria**, Acórdão nº 927/2015 - TCU Plenário, Brasília, 2014c

BRITO, Claudenir; FONTENELLE, Rodrigo. **Auditoria privada e governamental: Teoria de forma objetiva e mais de 500 questões comentadas.** Niterói: Impetus. 3. ed. 2016.

COSO ERM. Gerenciamento de Riscos Corporativos - Estrutura Integrada, 2004.

COSO. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

IIA. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles**. Disponível em https://na.theiia.org/standards-guidance/Public%20Documents. Acesso em 17.nov.2015.

IBGC, **Guia de Orientação para Gerenciamento de Riscos Corporativos**.

INTOSAI GOV 9100. **Guidelines for Internal Controls Standards for the Public Sector**. 2004. Disponível em: < http://www.intosai.org/en/issai-executive-summaries/intosai-guidance-for-good-governance-intosai-gov.html >. Acesso em 28 out. 2015.

ISO (ISO - International Organization for Standardization). ISO 31000 – **Risk Management System – Principles and Guidelines**. Tradução: Associação Brasileira de Normas Técnicas (ABNT) Projeto 63:000.01- 001. Agosto, 2009.

ISO (ISO - International Organization for Standardization). ISO Guide 73, **Vocabulary for Risk Management, 2009**.

KPMG - **The Audit Committee's Role in Control and Management of Risk.**

TCU. **Avaliação de controles internos na administração pública federal**. 2012. Disponível em http://portal2.tcu.gov.br/portal/pls/portal/docs/2436815.PDF. Acesso em 14.set.2013.

8. ANEXOS

Anexo I – Termos e Definições

Accountability: conjunto de procedimentos adotados pelo Ministério e pelos indivíduos que o integram para evidenciar as responsabilidades inerentes por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho;

Apetite a risco: nível de risco que o Ministério está disposto a aceitar;

Atividades de controles internos: são as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos do Ministério;

Avaliação de risco: processo de identificação e análise dos riscos relevantes para o alcance dos objetivos do Ministério e a determinação de resposta apropriada;

Consequência: resultado de um evento que afeta positiva ou negativamente os objetivos do Ministério;

Controle: qualquer medida aplicada no âmbito do Ministério, para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados;

Controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão do Ministério;

Ética: refere-se aos princípios morais, sendo pré-requisito e suporte para a confiança pública;

Fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

Gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza no alcance dos objetivos do Ministério do Planejamento, Desenvolvimento e Gestão;

Gestão da Integridade: conjunto de medidas de prevenção de possíveis desvios na entrega dos resultados esperados pela sociedade;

Governança: combinação de processos e estruturas implantadas pela alta administração do Ministério do Planejamento, Desenvolvimento e Gestão, para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos;

Governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

Identificação de riscos: processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

Incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;

Impacto: efeito resultante da ocorrência do evento;

Mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade de sua ocorrência;

Monitoramento: é um componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;

Nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência;

Operações econômicas: ocorre quando a aquisição dos insumos necessários se der na quantidade e qualidade adequadas, forem entregues no lugar certo e no momento preciso, ao custo mais baixo;

Operações eficientes: ocorre quando consumirem o mínimo de recursos para alcançar uma dada quantidade e qualidade de resultados, ou alcançarem o máximo de resultado com uma dada qualidade e quantidade de recursos empregados;

Política de gestão de integridade, riscos e controles internos da gestão: declaração das intenções e diretrizes gerais do Ministério relacionadas à integridade, riscos e controles;

Procedimento de controle: são as políticas e os procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos do Ministério;

Procedimentos de controle interno: procedimentos que o Ministério executa para o tratamento do risco, projetados para lidar com o nível de incerteza previamente identificado;

Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

Proprietário do risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;

Probabilidade: possibilidade de ocorrência de um evento;

Resposta a risco: qualquer ação adotada para lidar com risco. As respostas podem se enquadrar num destes tipos: aceitar o risco por uma escolha consciente; transferir/compartilhar o risco a outra parte; evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar/reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando as consequências do risco;

Risco: possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade dos riscos ou seu impacto;

Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

Riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do Ministério do Planejamento, Desenvolvimento e Gestão em cumprir sua missão institucional;

Riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do Ministério do Planejamento, Desenvolvimento e Gestão de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

Riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do Ministério do Planejamento, Desenvolvimento e Gestão; e

Riscos operacionais: eventos que podem comprometer as atividades do Ministério do Planejamento, Desenvolvimento e Gestão, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

Tolerância ao Risco: é o nível de variação aceitável quanto à realização dos objetivos;

Tratamento de riscos: processo de estipular uma resposta a risco;

Categoria de riscos: é a classificação dos tipos de riscos definidos pelo Ministério do Planejamento, Desenvolvimento e Gestão que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público;

Método de priorização de processos: classificação de processos baseadas em avaliação qualitativa e quantitativa, visando o estabelecimento de prazos para a realização de gerenciamento de riscos.

Anexo II – Matriz de Responsabilidades

Níveis	Nível Estratégico		Nível Tático		Nível Operacional		
Ocupantes das Funções	ME	ME e Secretários	Servidores das Secretarias indicados por seus dirigentes titulares:	Vinculado à AECI	Dirigente da Uniadade e Servidor especialista em GIRC (Analista de GIRC)	Responsável pela execução do processo	Servidor responsável pela execução do processo
Funções/Atividades	Ministro de Estado	Comitê de Gestão Estratégica - CGE	Subcomitê de Gestão de Integridade, Riscos e Controles Internos da Gestão - SIRC	Núcleo de Gestão de Integridade, Riscos e Controles Internos da Gestão	Unidade de Gestão de Integridade, Riscos e Controles Internos da Gestão - URIC	Gestor do Processo	Analista de Risco
Práticas e princípios de conduta e padrões de comportamento	I	A/P	R/P	P/C	P	R	R
Inovação e a adoção de boas práticas de governança, gestão de integridade, riscos e controles internos da gestão	I	C	P	C/P	P	R	R
Aderência às regulamentações, leis, códigos, normas e padrões na condução das políticas e na prestação de serviços de interesse público	I	P	C	C	R	R	R
Objetivo estratégico que norteia as boas práticas de governança, gestão de integridade, riscos e controles internos da gestão	I	A/R	R/C	C	R	R	
Adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência e efetividade das informações	I	P	P	P/C	P/R	R	
Integração e o desenvolvimento contínuo dos agentes responsáveis pela governança, gestão da integridade, riscos e controles internos da gestão	I	P	P	P/C	R	R	R
Estruturas adequadas de governança, gestão de integridade, riscos e controle internos da gestão	I	A/R	C	C	C		
Políticas, diretrizes, metodologias e mecanismos de monitoramento e comunicação para a gestão de integridade, riscos e controles internos da gestão	I	A	R	R	C		
Capacitação dos agentes públicos no exercício do cargo, função e emprego em gestão de integridade, riscos e controles internos da gestão	I	A	P	P/C	P/R		
Ações para disseminação da cultura de gestão de integridade, riscos e controles internos da gestão	I	P	P	P/C	R	R	
Método de priorização de processos para a gestão de integridade, riscos e controles internos da gestão	I	A	R	C			
Categorias de riscos a serem gerenciados	I	A	R	C			
Estabelecimento de limites de exposição a riscos e níveis de conformidade	I	A/R	R				
Estabelecimento de limites de alçada para exposição a riscos de órgãos de assistência direta e imediata ao Ministro de Estado do Planejamento, Desenvolvimento e Gestão e dos órgãos específicos singulares do Ministério	I	A/R	R				
Supervisão dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público	I	R	C				
Modelo de gestão de integridade, riscos e controles internos da gestão	I	A	R/C	C			
Tomada de decisões considerando as informações sobre gestão de integridade, riscos e controles internos da gestão e assegurar que estejam	I	R	C	C	C	C	
Emissão e monitoraramento das recomendações e orientações para o aprimoramento da governança, gestão de integridade, riscos e controles	I	R	C	C			
Gerenciamento de riscos dos processos de trabalho priorizados					I/C	A/R	R
Plano de Implementação de Controles	I	I	I	I	A	A/R	R
Monitoramento dos riscos ao longo do tempo	I	I	I	I	R	C	C
Implementação de metodologias e instrumentos na gestão de integridade, riscos, e controles internos da gestão	I	I	I	C	P	A/R	R
Disponibilidade de informações adequadas sobre gestão de integridade, riscos e controles internos da gestão em todos os níveis, no âmbito da unidade	I	I	I	I	R	C	C

Responsabilidades

P - Promotor (adicionado)	É quem promove ou fomenta a execução da atividade.
R - Responsável	É quem executa a atividade efetivamente.
A - Aprovador	É quem aprova ou valida formalmente a atividade ou o produto dela resultante.
C - Consultado	É quem gera uma informação que agrega valor para execução de uma atividade ou quem apoia a sua execução.
I - Informado	É quem precisa ser notificado do resultado da atividade.

Anexo III - Lista de Eventos de Risco Operacional

Segue uma lista sugestiva e não exaustiva de eventos de risco operacional.

Risco Operacional	
Fator	**Subfator e Exemplos de Riscos (Taxonomia)**
PROCESSOS	**COMUNICAÇÃO INTERNA**: ▪ Os insumos e as informações não são recebidos em tempo adequado para a execução do processo ▪ Ausência de padrões mínimos definidos para a execução do processo ▪ Erros e falhas de informações que afetam a execução do processo **MODELAGEM**: ▪ Fluxo desatualizado e não reflete a prática atual utilizada na execução do processo ▪ Ausência de avaliações periódica sobre a adequabilidade do desenho do processo ▪ Ausência ferramenta para análise e melhoria contínua do processo ▪ Falha ou falta de metodologia que auxilie no mapeamento do processo **SEGURANÇA FÍSICA**: ▪ Falha ou falta de segurança no ambiente de trabalho que afeta a execução do processo ▪ Acesso a áreas consideradas como críticas sem que as pessoas estejam devidamente credenciadas e identificadas **ADEQUAÇÃO À LEGISLAÇÃO**: ▪ Descumprimento de prazos legais na execução do processo ▪ Ausência de compilação e distribuição de legislação pertinente ao processo em execução ▪ Execução do processo em desacordo com o regimento interno/normas ▪ Descumprimento de prazo judicial na execução do processo ▪ Descumprimento de obrigação regulatória na execução do processo
PESSOAS	**CARGA DE TRABALHO**: ▪ Rotatividade (*turnover*) de pessoal acima do esperado que afeta a execução do processo ▪ Capacidade operacional insuficiente para a execução do processo ▪ Falha ou falta de dimensionamento da capacidade operacional com impacto na execução do processo **COMPETÊNCIAS**: ▪ Capacitação da equipe é insatisfatória para a execução do processo ▪ Concentração de conhecimentos em determinados servidores afetando a execução do processo ▪ Falha ou falta de disseminação de conhecimento afetando a execução do processo ▪ Falha ou falta de capacitação que afeta a execução do processo **AMBIENTE ORGANIZACIONAL**: ▪ Ausência de satisfação e/ou de bem-estar do servidor na execução de sua tarefa ▪ Desconhecimento dos objetivos do processo por parte dos Servidores ▪ Servidores desconhecem as suas responsabilidades individuais na execução do processo ▪ Ausência de recursos necessários para execução das tarefas ▪ Resistência de Servidores em promover alterações nas condições de trabalho **CONDUTA**: ▪ Ausência de postura ética nas atividades e nos relacionamentos interpessoais ▪ Falta de atenção e zelo na execução do processo ▪ Ausência de imparcialidade, cumprimento das leis e normas/regulamentares, confidencialidade e comprometimento na execução do processo ▪ Quebra de sigilo e confidencialidade

Risco Operacional	
Fator	**Subfator e Exemplos de Riscos (Taxonomia)**
AMBIENTE TECNOLÓGICO	**SEGURANÇA LÓGICA**: ▪ Ausência de estrutura de perfis de acesso aos sistemas para execução do processo ▪ Ausência de controle de acesso lógico ▪ Ausência de *logon* próprio na rede institucional ▪ Falha ou falta de meios seguros de acesso aos sistemas ▪ Inexistência de registro nos sistemas (*log*) das transações críticas ▪ Ausência de formalização que defina as responsabilidades do usuário externo do sistema ▪ Incapacidade do sistema de prover informações confiáveis e suficientes sobre o processo em execução **INFRAESTRUTURA TECNOLÓGICA**: ▪ Grau de informatização do processo inadequado para execução do processo ▪ Informações e dados armazenados em diretórios não protegidos e sem controle de acesso ▪ Ausência de backup de arquivos, planilhas e bancos de dados essenciais à execução do processo ▪ A estação de trabalho não possui acionado dispositivo de *time-out* ▪ Descarte de mídias sem antes terem apagados os com conteúdo reservado ▪ Sobrecarga de sistemas de processamento de dados no momento da execução do processo ▪ Inadequação de sistemas operacionais/aplicativos para execução do processo ▪ Falhas de hardware, faltas de backup e de legalização do software afetando a execução do processo ▪ Obsolescência dos sistemas e equipamentos afetando a execução do processo ▪ Ataques lógicos à rede de computadores afetando a execução do processo **SOLUÇÃO DE TI**: ▪ Inexistência de controle nas requisições e nas melhorias requeridas nos sistemas cuja falta de implementação afeta a execução do processo ▪ Falha ou falta de homologação de sistema impedindo a execução do processo de forma automatizada **COMUNICAÇÃO**: ▪ Instabilidade nos sistemas operacionais que afeta a execução do processo ▪ Incompatibilidade e/ou indisponibilidade de informações afetando a execução do processo
EVENTOS EXTERNOS	**DESASTRES NATURAIS E CATASTROFE**: ▪ *Ação Humana*: ações intencionais executadas por terceiros para lesar o órgão, como por exemplo: (i) roubos, falsificações, furtos, atos de vandalismos, fraudes externas; (ii) degradação do meio ambiente; e (iii) alterações no ambiente econômico, político e social ▪ *Força Maior*: (i) enchentes, terremotos, catástrofes (queda de prédio) e outros desastres naturais **AMBIENTE REGULATÓRIO**: ▪ Alterações inesperadas na legislação ou em marcos regulatórios pelos órgãos fiscalizadores e reguladores **AMBIENTE SOCIAL**: ▪ Cenário socioeconômico interfere na execução do processo ▪ Retrações ou não-aproveitamento de oportunidades de mercado provocadas por eventos relacionados a segurança patrimonial que impede a execução do processo **FORNECEDORES**: ▪ Indisponibilidade de recursos em virtude de concentração em um único fornecedor que impede a execução do processo ▪ Falhas ou indisponibilidade de serviços públicos que afeta a execução do processo

Anexo IV – Controles Básicos

Segue uma lista sugestiva e não exaustiva de controles básicos.

Categoria de Risco	Fatores	Subfatores	Controles Básicos
Risco de Integridade			Postura da alta administração
			Políticas e procedimentos anticorrupção
			Mapeamento dos Riscos de Corrupção
			Criação de indicadores dos riscos de corrupção dos passos decisórios
Risco de Conformidade			Acompanhamento e Análise de Normas e Regulamentos Externos
			Pareceres da Assessoria Jurídica
			Atividades de Treinamento
			Normas e Procedimentos
Risco Operacional	**Pessoas**	Carga de Trabalho	Planejamentos de longo, médio e curto prazos
			Acordo de Trabalho
			Pesquisa de Clima Organizacional
			Reuniões Participativas
		Competências	Identificação da Necessidade de Conhecimento / Habilidades
			Atividades de Treinamento
			Normas e Procedimentos
			Ferramentas de autoavalização de Conhecimentos / Habilidades
		Qualidade de Vida no Trabalho	Pesquisa de Clima Organizacional
			Condições Ambientais
			Comunicação com a Administração
			Processo de Gerenciamento de Equipes
		Conduta	Valores Éticos e Normas de Conduta do Órgão / Unidade
			Alçadas e Limites
			Mecanismos de Motivação / Recompensa / Punição – Práticas de Disciplina e Demissão
			Reconhecimento de Responsabilidade por Escrito
			Conferências e Autorizações
			Rodízio de Funcionários
			Segregação de Funções
			Testes de Conformidade
			Canais de Comunicação – Com a Sociedade
Risco Operacional	**Processos**	Comunicação Interna	Canais de Comunicação – Com os Servidores
			Normas e Procedimentos

		Modelagem	Ferramentas para Análise e Melhoria Contínua de Processos
			Metodologia de Autoavalização de Riscos e Controles
			Validações – *Backtesting*
		Segurança Física	Mecanismos de Segurança Física
			Controles de Acesso Físico
			Manutenção de Equipamentos
		Pontos de Controle	Normas e Procedimentos
			Metodologia de Autoavalização de Riscos e Controles
			Mecanismos de Monitoramento e Reporte
		Adequação à Legislação	Testes de Conformidade
			Normas e Procedimentos
Risco Operacional	**Sistemas**	Segurança Lógica	Políticas e Diretrizes
			Controles de Acesso Lógico
			Arquivo e Preservação de Registros
		Hardware e *Software*	Manutenção de Equipamentos
			Layout de formulários e Sistemas
			Planos de Contingência
		Análise e Programação	*Layout* de Formulários e Sistemas
			Validações - *Backtesting*
			Atividades de Treinamento
		Rede de Comunicação	Planos de Contingência
			Manutenção de Equipamentos
Risco Operacional	**Eventos Externos**	Desastres Naturais e Catástrofe	Planos de Contingência
			Atividades de Treinamento
		Ambiente Regulatório	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Ambiente Social	Análise da Conjuntura Política e Econômica Nacional e Internacional
		Fornecedores	Controles de Serviços Terceirizados
			Planos de Contingência
		Clientes	Controles de Acesso Lógico
		Meio Ambiente	Valores Éticos e Normas de Conduta da Empresa
Risco de Imagem			Valores Éticos e Normas de Conduta da Empresa
			Normas e Procedimentos
			Controles de Serviços Terceirizados
			Pesquisa de Satisfação
			Canais de Comunicação - Com a Sociedade
			Canais de Comunicação – Com os Servidores