GUIA PRÁTICO DE GESTÃO DE RISCOS PARA A INTEGRIDADE

Orientações para a administração pública federal direta, autárquica e fundacional

MINISTÉRIO DA TRANSPARÊNCIA E
CONTROLADORIA-GERAL DA UNIÃO

MINISTÉRIO DA TRANSPARÊNCIA
E CONTROLADORIA-GERAL DA UNIÃO
SAS, Quadra 01, Bloco A, Edifício Darcy Ribeiro
70070-905 - Brasília-DF - cgu@cgu.gov.br

Wagner de Campos Rosário
Ministro da Transparência e Controladoria-Geral da União

José Marcelo Castro de Carvalho
Secretário-Executivo

Antônio Carlos Bezerra Leonel
Secretário Federal de Controle Interno

Gilberto Waller Junior
Ouvidor-Geral da União

Antônio Carlos Vasconcellos Nóbrega
Corregedor-Geral da União

Claudia Taya
Secretária de Transparência e Prevenção da Corrupção

Brasília, setembro/2018.

SUMÁRIO

1. APRESENTAÇÃO 5

II. RISCOS PARA A INTEGRIDADE 8

1. O QUE SÃO RISCOS PARA A INTEGRIDADE? 8

Abuso de posição ou poder em favor de interesses privados 10

Nepotismo 10

Conflito de interesses 11

Pressão interna ou externa ilegal ou antiética para influenciar agente público 12

Solicitação ou recebimento de vantagem indevida 12

Utilização de recursos públicos em favor de interesses privados 13

2. O QUE É A GESTÃO DE RISCOS PARA A INTEGRIDADE E POR QUÊ REALIZÁ-LA? 13

III. PREPARANDO-SE PARA A GESTÃO DE RISCOS PARA A INTEGRIDADE 15

1. PRINCÍPIOS 15

a) Apoio e compromisso da alta administração 17

b) Engajamento das pessoas envolvidas no processo 18

c) Compartilhamento de conhecimento e experiências 19

2. INSTITUCIONALIZAÇÃO 19

a) Política de Gestão de Riscos 20

b) Atribuição de funções e responsabilidades 21

c) Estabelecimento de limites de exposição a riscos 22

d) Definição de instrumentos para registro do processo 23

IV. GESTÃO DE RISCOS PARA A INTEGRIDADE: TEORIA E PRÁTICA 23

1. PASSO 1 – SELEÇÃO E ESTUDO DO PROCESSO 24

2. PASSO 2 – IDENTIFICAÇÃO DE RISCOS 27

3. PASSO 3 – ANÁLISE DE RISCOS 31

4. PASSO 4 – AVALIAÇÃO DE RISCOS 35

5. PASSO 5 – TRATAMENTO DE RISCOS 39

6. PASSO 6 – COMUNICAÇÃO E MONITORAMENTO 45

ANEXO - EXEMPLOS DE ÁREAS E PROCESSOS DE RISCO 48

REFERÊNCIAS BIBLIOGRÁFICAS 52

1. APRESENTAÇÃO

Esse guia foi elaborado para auxiliar os órgãos e entidades da administração pública federal direta, autárquica e fundacional nas etapas iniciais de sua gestão de riscos para a integridade. Seu conteúdo deve ser estudado tendo em consideração que é destinado ao contexto da integridade pública.

INTEGRIDADE PÚBLICA REFERE-SE AO ALINHAMENTO CONSISTENTE E À ADESÃO DE VALORES, PRINCÍPIOS E NORMAS ÉTICAS COMUNS PARA SUSTENTAR E PRIORIZAR O INTERESSE PÚBLICO SOBRE OS INTERESSES PRIVADOS NO SETOR PÚBLICO.[1]

De acordo com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a adoção de abordagens tradicionais de combate à corrupção, baseadas na criação de mais regras, conformidade mais rigorosa e cumprimento mais rígido têm eficácia limitada. Nesse sentido, a integridade pública emerge como uma resposta estratégica e sustentável à corrupção que desloca o foco das políticas de integridade ad hoc para uma abordagem dependente do contexto, comportamental e baseada em risco, com ênfase em cultivar uma cultura de integridade em toda a sociedade.[2]

Entre as recomendações para a implementação desse arcabouço, está a garantia de uma abordagem estratégica para a gestão de riscos que inclua a avaliação dos riscos para a integridade pública. Tal abordagem contemplaria o endereçamento de deficiências de controle, bem como a criação de um mecanismo eficiente de monitoramento e garantia de qualidade para o sistema de gestão de riscos.[3]

A preocupação com a gestão de riscos na esfera pública já é uma realidade no arcabouço normativo brasileiro, ainda que sua efetiva adoção permaneça sendo um desafio. Com a Instrução Normativa

1 OCDE, 2018a.
2 Idem.
3 Idem.

(IN) Conjunta Ministério do Planejamento, Orçamento e Gestão (MP) e Controladoria-Geral da União (CGU) nº 1/2016[4] e, posteriormente, com o Decreto nº 9.203/2017[5], tornou-se obrigatória a adoção da gestão de riscos no âmbito do Poder Executivo federal. Nesse sentido, todo gestor público ciente de suas responsabilidades, ao tomar decisões para atingir os objetivos estabelecidos para a sua organização, precisa passar a adotar atividades estruturadas e formalizadas para esse fim.

A esses normativos, vem se somar a Portaria CGU nº 1.089/2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade. A Portaria trouxe previsão específica sobre a realização da gestão de riscos para a integridade, aspecto extremamente relevante para efetivo funcionamento do programa de integridade.[6]

---

4 No art. 13, foi definido que "[...] os órgãos e entidades do Poder Executivo Federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta Instrução Normativa" (BRASIL, 2016).

5 Art. 17. A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios: I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público; II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais; III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança (BRASIL, 2016).

6 BRASIL, 2018a.

PROGRAMA DE INTEGRIDADE É O CONJUNTO ESTRUTURADO DE MEDIDAS INSTITUCIONAIS VOLTADAS PARA A PREVENÇÃO, DETECÇÃO, PUNIÇÃO E REMEDIAÇÃO DE FRAUDES E ATOS DE CORRUPÇÃO, EM APOIO À BOA GOVERNANÇA.

É importante destacar que a gestão de riscos para a integridade não é um processo inteiramente novo e descolado da gestão de riscos prevista na IN Conjunta e no Decreto. O que precisaremos fazer é mudar o foco de análise, se antes para aspectos operacionais ou financeiros, por exemplo, agora tendo como lente a integridade. Explicaremos melhor no capítulo seguinte o que são os chamados riscos para a integridade para que seja facilitado o processo de sua identificação e posterior estabelecimento de medidas de tratamento.

Como usar esse guia?

Esse guia visa a convidar os órgãos e entidades a empreenderem, de forma orientada, a gestão dos riscos para a integridade que possam comprometer o alcance dos objetivos definidos pela sua organização, a partir de procedimentos simplificados e passíveis de evidenciação. As orientações têm caráter geral e podem receber adaptações para melhor adequação a situações específicas das organizações, sem perder de perspectiva o rigor e a qualidade das informações levantadas, produzidas e registradas.

CADA ÓRGÃO/ ENTIDADE PODE ADOTAR A METODOLOGIA QUE ENTENDER MAIS ADEQUADA PARA SUA GESTÃO DE RISCOS PARA A INTEGRIDADE. SE O ÓRGÃO/ ENTIDADE JÁ ADOTA UMA DETERMINADA METODOLOGIA DE AVALIAÇÃO DE RISCOS EM OUTRAS ÁREAS OU PROCESSOS, PODE SER UMA OPÇÃO APLICÁ-LA NO LEVANTAMENTO DOS RISCOS DE INTEGRIDADE E NA CONSTRUÇÃO DE UM PLANO DE INTEGRIDADE.[7]

Para que tenhamos um trabalho proveitoso, é necessário que tenhamos a disposição e o comprometimento para aprender-fazendo, aceitando cometer alguns erros, iniciando com estruturas flexíveis, que possam ser revisadas ou ampliadas ao se mostrarem insuficientes para responder às especificidades da organização, apenas solidificando à medida que a instituição ganha maturidade na apropriação desse processo.

Bom trabalho a todos!

II. RISCOS PARA A INTEGRIDADE

Antes de dar início à apresentação das etapas a serem executadas durante a gestão de riscos **para a integridade**, compartilharemos algumas noções relevantes para entender o que são esses riscos e como podem aparecer em nossas organizações, além de também elencarmos alguns de seus principais benefícios.

1. O QUE SÃO RISCOS PARA A INTEGRIDADE?

Existem diversas formas de nomear e conceituar riscos para a integridade: por vezes, são tratados como riscos de corrupção[8], também

7 BRASIL, 2017b, p. 36 (adaptado).
8 TRANSPARÊNCIA BRASIL; CGU, 2006; SELINŠEK, 2015.

aparecem como riscos de integridade[9] ou riscos à integridade[10]. Porém, tais discussões não são particularmente relevantes para o fim último de gerir de forma adequada esses riscos.

A definição adotada na Portaria CGU nº 1.089/2018 é:

> *Art. 2º, II – Riscos para a integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.*
>
> *Parágrafo único. Os riscos para a integridade podem ser causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem.*

Nesta definição, é importante pontuar que o favorecimento da ocorrência de fraudes e atos de corrupção no contexto da gestão de riscos para a integridade não deve ser entendido apenas em termos de infração de leis, normas, etc., mas como **quebras de integridade**, expressão que neste documento é utilizada de maneira ampla, englobando atos como recebimento/oferta de propina, desvio de verbas, fraudes, abuso de poder/influência, nepotismo, conflito de interesses, uso indevido e vazamento de informação sigilosa e práticas antiéticas.[11]

De um modo geral, atos relacionados a **quebras de integridade** compartilham as seguintes características:

- É um ato quase sempre doloso, à exceção de certas situações envolvendo conflito de interesses, nepotismo, etc.
- É um ato humano - praticado por uma pessoa ou por um grupo de pessoas
- Envolve uma afronta aos princípios da administração pública: legalidade, impessoalidade, moralidade, publicidade e eficiência, mas se destaca mais fortemente como uma quebra à impessoalidade e/ou moralidade.

9 SELINŠEK, 2015.
10 BRASIL, 2017b.
11 Ibidem, p. 6 (adaptado).

- Envolve alguma forma de deturpação, desvio ou negação da finalidade pública ou do serviço público a ser entregue ao cidadão.

Fonte: elaboração própria. Dados: BRASIL, 2017b, p. 12 – 13.

A partir dessas características, podemos identificar alguns dos riscos para a integridade mais relevantes e comuns nas organizações públicas conforme exposto a seguir.[12]

ABUSO DE POSIÇÃO OU PODER EM FAVOR DE INTERESSES PRIVADOS

Algumas das formas de abuso de posição ou poder em favor de interesses privados são:[13]

a) concessão de cargos ou vantagens em troca de apoio ou auxílio;

b) concussão;

c) outras formas de favorecimento – a outros ou a si mesmo;

d) esquivar-se do cumprimento de obrigações; e

e) falsificação de informação para interesses privados.

NEPOTISMO

O nepotismo pode ser entendido como uma das formas de abuso de posição ou poder em favor de interesses privados[14], em que se favorecem familiares.

O Decreto nº 7.203/2010 dispõe sobre a vedação do nepotismo no âmbito da administração pública federal. Para efeitos do decreto, familiar se trata de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau.

O nepotismo pode ser presumido ou requerer apuração específica.[15]

---

12 BRASIL, 2017b, p. 24 – 25.
13 SELINŠEK, 2015, p. 84-85.
14 Idem.
15 BRASIL, 2010.

Nepotismo presumido

- contratação de familiares para cargos em comissão e função de confiança;
- contratação de familiares para vagas de estágio e de atendimento a necessidade temporária de excepcional interesse público;
- contratação de pessoa jurídica de familiar por agente público responsável por licitação.

Apuração específica

- nepotismo cruzado;
- contratação de familiares para prestação de serviços terceirizados;
- nomeações, contratações não previstas expressamente no decreto.

CONFLITO DE INTERESSES

A Lei nº 12.813/2013 dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego.

De acordo com a Lei, conflito de interesses trata da situação gerada pelo confronto entre interesses públicos e privados, que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública.

Estas são as situações que configuram conflito de interesses conforme a Lei:[16]

a) uso de informação privilegiada;

b) relação de negócio com pessoa física ou jurídica que tenha interesse em decisão;

16 BRASIL, 2013.

c) atividade privada incompatível com o cargo;

d) atuar como intermediário junto à administração;

e) praticar ato em benefício de pessoa jurídica (em que participe o servidor ou parente);

f) receber presente de quem tenha interesse em decisão;

g) prestar serviços a pessoa jurídica sob regulação do órgão.

PRESSÃO INTERNA OU EXTERNA ILEGAL OU ANTIÉTICA PARA INFLUENCIAR AGENTE PÚBLICO

Algumas das formas de pressão interna ilegal ou antiética para influenciar agente público são:[17]

a) influência sobre funcionários subordinados para violar sua conduta devida;

b) ações de retaliação contra possíveis denunciantes.

Algumas das formas de pressão externa ilegal ou antiética para influenciar agente público são:[18]

a) lobby realizado fora dos limites legais ou de forma antiética;

b) pressões relacionadas a tráfico de influência.

SOLICITAÇÃO OU RECEBIMENTO DE VANTAGEM INDEVIDA

O artigo 317 do Código Penal dispõe sobre o crime de corrupção passiva, caracterizado como o recebimento ou solicitação, para si ou para outrem, direta ou indiretamente, ainda que fora da função ou antes de assumi-la, mas em razão dela, vantagem indevida, ou aceitar promessa de tal vantagem.[19]

17 SELINŠEK, 2015, p. 88.
18 Ibidem, p. 87.
19 BRASIL, 1940.

UTILIZAÇÃO DE RECURSOS PÚBLICOS EM FAVOR DE INTERESSES PRIVADOS

Algumas das formas de utilização de verbas e fundos públicos em favor de interesses privados são:[20]

a) apropriação indevida;

b) peculato;

c) outras formas de utilização de recursos públicos para uso privado (ex: carros, tempo de trabalho, equipamentos do escritório, etc.);

d) irregularidades em contratações públicas.

Os tipos mencionados não exaurem todas as possibilidades de manifestação de riscos para a integridade, tendo como intenção apenas facilitar a identificação dos riscos pelo órgão/entidade. O levantamento dos principais riscos e as medidas para seu tratamento aparecem como componentes do plano de integridade, documento que formaliza o programa de integridade no âmbito dos órgãos e entidades.

2. O QUE É A GESTÃO DE RISCOS PARA A INTEGRIDADE E POR QUÊ REALIZÁ-LA?

A **gestão de riscos** pode ser definida como o processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.[21]

A **gestão de riscos para a integridade** consiste em ferramenta que permite aos agentes públicos mapear os processos organizacionais das instituições que integram, de forma a identificar fragilidades que possibilitem a ocorrência de fraudes e atos de corrupção.

A partir disso, implementam-se mecanismos preventivos que minimi-

20 SELINŠEK, 2015, p. 86.
21 BRASIL, 2017b, art. 2º, IV.

zem as vulnerabilidades e evitem quebras de integridade.[22]

Tal processo consiste, ainda, em uma ferramenta de gestão para melhorar a governança das organizações, setores, projetos ou processos no setor público.[23] Nesse contexto, alguns dos benefícios decorrentes da realização de processos de gestão de riscos para a integridade são:

- Mantém as questões de prevenção da corrupção, integridade e boa governança na agenda e dá um passo em relação a uma abordagem puramente legalista.
- Permite a identificação de riscos comuns em uma determinada área ou setor que exija ação ou reforma institucional mais ampla.
- Permite partilhar conhecimentos e boas práticas na identificação de riscos e, em particular, em medidas de mitigação em determinado setor ou entre setores, instituições, projetos ou processos.
- Permite o intercâmbio efetivo de boas práticas que sirva como fonte de inspiração, ideias e apoio entre pares para a boa governança no setor público.

Fonte: elaboração própria. Dados: SELINŠEK, 2015, p. 24 (adaptado).

É importante observar que um processo de gestão de riscos realmente efetivo precisa ir além da previsão legal, sendo fundamental também poder contar com o comprometimento e engajamento de pessoas, conforme discutiremos no capítulo seguinte.

Se não for implementado adequadamente, pode se tornar um programa meramente formal por meio do qual apenas seja criada uma camada adicional de burocracia anticorrupção, sem que haja uma efetiva mudança de cultura.[24]

22 TRANSPARÊNCIA BRASIL; CGU, 2006, p. 5 (adaptado).
23 SELINŠEK, 2015, p. 11.
24 SELINŠEK, 2015, p. 69 (adaptado).

III. PREPARANDO-SE PARA A GESTÃO DE RISCOS PARA A INTEGRIDADE

Passar a gerir os riscos que possam comprometer o atingimento dos objetivos da organização significa uma nova forma de pensar a condução do "negócio" da instituição, elevando de forma expressiva a atenção dispensada à possibilidade da ocorrência de eventos que possam impedir o sucesso na realização do propósito institucional. Portanto, trata-se de uma mudança de cultura.

Medidas devem ser adotadas no ambiente com o intuito de contribuir para que essa mudança ocorra de forma gradual, contínua, harmoniosa e ao mesmo tempo consistente, visando a fundamentar uma gestão de riscos efetiva e integrada ao programa de integridade.

Além disso, é preciso levarmos em consideração as especificidades da gestão de riscos para a integridade. Poderá ser preciso lidar com sensibilidades adicionais na identificação, análise, avaliação e estabelecimento das medidas de tratamento para esses riscos, dado o forte componente humano envolvido.

A seguir, encontram-se boas práticas, que têm se revelado essenciais para contribuir com esse movimento de mudança.

1. PRINCÍPIOS

De acordo com o Decreto nº 9.203/2017 são princípios da gestão de riscos:

> I. implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;
>
> II. integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III. estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício;

IV. utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.[25]

Adicionalmente, alguns outros aspectos relevantes a serem considerados durante a condução do processo de gestão de riscos para a integridade são:

- pleno apoio e compromisso da alta direção;
- engajamento de pessoas que garantam um panorama suficientemente completo do órgão/entidade e seus riscos;
- identificação e descrição dos riscos com o detalhamento necessário para sua análise;
- avaliação dos riscos com base em uma apreciação realista de sua probabilidade e impacto;
- documentação precisa;
- revisão periódica;
- comunicação efetiva que garanta o desenho de controles apropriados;
- estabelecimento de mecanismos de supervisão/controle adequados;
- adequação do processo à realidade do órgão/entidade;
- compartilhamento de conhecimento e experiências com outros órgãos/entidades;
- orientação para mudanças de mentalidade e estímulo ao comportamento íntegro na organização.[26]

25 BRASIL, 2017b, art. 17.
26 SELINŠEK, 2015, p. 73 (adaptado).

Trataremos brevemente a seguir de alguns desses aspectos, ao passo que os demais serão abordados ao longo deste e do próximo capítulo.

A) APOIO E COMPROMISSO DA ALTA ADMINISTRAÇÃO

Por se tratar de uma mudança de cultura na organização, na forma de pensar e agir dos seus atores, a gestão de riscos só terá credibilidade e contará com convergência efetiva dos diversos atores se ficar evidente que seus dirigentes acreditam no processo e desejam promover sua adoção, por compreender os benefícios advindos da sua implementação (comentamos alguns deles no capítulo anterior).

A responsabilidade por estabelecer, manter, monitorar e aperfeiçoar os controles internos da gestão é da alta administração da organização, e esses controles devem responder a riscos que possam comprometer objetivos organizacionais.

É ela quem deve responder quando os objetivos não forem alcançados em virtude da sua omissão em tratar riscos que poderiam acontecer e foram negligenciados ou subvalorizados.

Portanto, a gestão de riscos também é de responsabilidade da alta administração.

Se não ocorrer uma adesão verdadeira quanto à necessidade da gestão de riscos, o envolvimento da alta direção não surte os efeitos esperados: gerar a convergência dos diversos atores da instituição, alocar os recursos necessários, envolver pessoas com conhecimento e experiência no assunto, etc.

Assim sendo, quando o dirigente da organização, apesar de desejar cumprir o disposto nos normativos, ainda não se perceba convencido dos proveitos da gestão de riscos, sugerimos a adoção de medidas que se destinem a expandir seu conhecimento a respeito para, em seguida, perceber como se aplica em situações reais.

B) ENGAJAMENTO DAS PESSOAS ENVOLVIDAS NO PROCESSO

Ainda que o processo de gestão de riscos para a integridade seja liderado por uma área de gestão de riscos, quando houver, com apoio da **Unidade de Gestão da Integridade (UGI)**, para sua efetiva realização, é necessária ampla participação de outras áreas do órgão/entidade, em que estão os gestores dos riscos que serão levantados, avaliados e tratados.

Não existe uma forma de prever de forma genérica como garantir a adesão das pessoas envolvidas no processo de gestão de riscos para a integridade. Há indivíduos intrinsecamente motivados na esfera pessoal e profissional que participarão ativamente do processo sem a necessidade de incentivos adicionais. Em outros casos, será necessário adotar medidas para engajamento dos indivíduos no processo e reforço da importância da integridade profissional para elas, para seu órgão/entidade e para o setor público como um todo.[27]

Essas medidas podem ter caráter de incentivo (treinamento, elogio por um trabalho bem feito, etc.) ou sanção (medidas disciplinares, etc.), sendo a escolha feita a cada caso[28].

A OCDE publicou, em 2018, o estudo "*Insights* Comportamentais para a Integridade Pública: aproveitando o fator humano para conter a corrupção" que pode servir de apoio aos interessados em iniciar o estudo do tema.[29]

Entre as possibilidades de aplicar *insights* comportamentais nas políticas de integridade consta o desenvolvimento de competências (*capacity building*) na área de integridade[30]. Tratando especificamente da gestão de riscos para a integridade, a capacitação consiste em uma etapa essencial para que toda a organização possa se envolver, gradualmente, no tema. A alta direção deve garantir sua própria capacitação e a dos colaboradores, na medida do interesse

27 Ibidem, p. 69 – 70 (adaptado).
28 Ibidem, p. 70 (adaptado).
29 OCDE, 2018b.
30 Ibidem, p. 40.

e da necessidade de cada colaborador para o processo.

> **Dica:** *Para a alta administração, recomenda-se a realização de cursos abertos, voltados a executivos, nos quais seja possível a troca de informações e experiências entre dirigentes de várias organizações.*
> *Para os demais atores, recomendam-se cursos fechados, com a adoção de exercícios que considerem os próprios processos organizacionais.*

C) COMPARTILHAMENTO DE CONHECIMENTO E EXPERIÊNCIAS

Além da promoção de cursos, em uma fase seguinte, a capacitação pode evoluir por meio de intercâmbios, em visitas a órgãos/entidade, se possível com perfil similar[31], que já realizem a gestão de seus riscos, no intuito de aprofundar o conhecimento a partir de experiências na implementação e apropriação de todo o arcabouço para a gestão de riscos.

> **Dica:** *Preparar um roteiro para orientar as entrevistas nos órgãos/entidades a serem visitados, de forma a detalhar informações relativas aos acertos e possíveis erros identificados, na condução das etapas para a implementação e adoção do arcabouço para a gestão de riscos.*

2. INSTITUCIONALIZAÇÃO

A internalização da gestão de riscos pelo órgão ou entidade exige a adoção de arcabouço composto por mecanismos e instrumentos, definindo e criando as condições para seu adequado funcionamento. A seguir, encontram-se relacionadas condições essenciais para que a gestão de riscos promova os benefícios esperados.

---

31 Considerar no perfil: o tamanho da instituição, a forma como atua administrativamente e /ou no atendimento à sociedade.

A) POLÍTICA DE GESTÃO DE RISCOS

Segundo a Instrução Normativa conjunta MP/CGU nº 1/2016, art. 2º, XII, Política de Gestão de Riscos é a declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos. Portanto, os órgãos e entidades devem formular e disseminar a Política de Gestão de Riscos, aprovada pela Alta Direção.

A IN apresenta o conteúdo mínimo para a elaboração da Política de Gestão de Riscos. Vejamos:

> *Art. 17. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo federal em até doze meses a contar da publicação desta Instrução Normativa, deve especificar ao menos:*
>
> *I – princípios e objetivos organizacionais;*
>
> *II – diretrizes sobre:*
>
> *a) como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;*
>
> *b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;*
>
> *c) como será medido o desempenho da gestão de riscos;*
>
> *d) como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;*
>
> *e) a utilização de metodologia e ferramentas para o apoio à gestão de riscos; e*
>
> *f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos; e*
>
> *III – competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.*

Atenção: *Caso seu órgão/entidade ainda não possua política de gestão de riscos formalizada, essa é uma medida importante a constar no plano de integridade.*

B) ATRIBUIÇÃO DE FUNÇÕES E RESPONSABILIDADES

Para que qualquer processo de gestão de riscos seja efetivamente implementado é necessário o engajamento de diversas partes da organização. O mesmo vale para a gestão de riscos para a integridade, com o destaque do apoio adicional prestado pela Unidade de Gestão da Integridade - UGI.

A coordenação do processo de gestão de riscos para a integridade será realizada pela área responsável pela **gestão de riscos** na organização. Essa área tem atuação predominantemente de assessoramento, subsidiando a alta direção e demais áreas e atuando como facilitadora para a disseminação de procedimentos e rotinas que deem sustentação à internalização do arcabouço para a gestão de riscos na organização. Quando possível, deve contar com o apoio de profissionais com experiência mínima na implementação de gestão de riscos, além do necessário conhecimento no assunto.

A **UGI** é a área responsável pela coordenação da estruturação, execução e monitoramento do programa de integridade, no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional.[32] Ela apoiará a área responsável pela gestão de riscos na organização, fornecendo as orientações necessárias para a compreensão do que são riscos para a integridade e quais são as medidas de tratamento possíveis para mitigá-los.

Em complementação, *instâncias colegiadas*, como as previstas pela IN Conjunta MP/CGU nº 01/2016 e pelo Decreto nº 9.203/2017, podem e devem atuar garantindo a aderência da gestão de riscos com o direcionamento estratégico e o "negócio" da organização.

É importante entender que cada gestor é responsável por gerir os riscos no âmbito de sua unidade, processos e atividades.[33] Nesse contexto, a área responsável pela gestão de riscos e a UGI serão apenas facilitadoras do processo.

Por fim, mas não menos importante, está o papel da **alta adminis-**

32 BRASIL, 2018a, art. 4º, I.
33 BRASIL, 2016, art. 20.

tração. De acordo com a IN Conjunta MP/CGU nº1/2016, o dirigente máximo da organização é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão[34].

Por sua vez, o Decreto nº 9.203/2017 estabelece que a alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional[35].

C) ESTABELECIMENTO DE LIMITES DE EXPOSIÇÃO A RISCOS

De acordo com a IN Conjunta MP/CGU nº1/2016, é competência do Comitê de Governança, Riscos e Controles estabelecer limites de exposição a riscos globais do órgão, bem como os limites de alçada ao nível de unidade, política pública, ou atividade[36].

O estabelecimento desses limites, que pode ser tratado em termos de apetite a risco ou tolerância ao risco[37], é necessário para que seja realizada a etapa de avaliação de riscos e sejam definidas as medidas de tratamento de riscos, conforme veremos no próximo capítulo.

---

34 Idem.

35 BRASIL, 2017b, art. 17.

36 BRASIL, 2016, art. 23, § 2º, X.

37 Apetite a risco pode ser definido como o "nível de risco que uma organização está disposta a aceitar." (BRASIL, 2016, art. 2º, II). Já a tolerância ao risco pode ser definida como a "disposição da organização ou parte interessada em suportar o risco após o tratamento do risco, a fim de atingir seus objetivos." (ABNT, 2009b)

D) DEFINIÇÃO DE INSTRUMENTOS PARA REGISTRO DO PROCESSO

Todo o modelo para a gestão de riscos de um processo organizacional precisa ser registrado. A partir da implementação da gestão de riscos, a ocorrência de eventos não desejáveis deve ser devidamente justificada à luz dos registros realizados.

É possível iniciar o processo com o uso de planilhas e quadros para registrar, comunicar e monitorar o processo.

Veremos no próximo capítulo algumas orientações para facilitar a realização dessa primeira rodada do processo de gestão de riscos para a integridade nos órgãos e entidades.

IV. GESTÃO DE RISCOS PARA A INTEGRIDADE: TEORIA E PRÁTICA

Nesse capítulo, forneceremos uma metodologia simplificada de gestão de riscos para a integridade, da seleção do processo à comunicação e monitoramento das medidas de tratamento. É importante notar que, como todo o processo de instituição e gestão do programa de integridade, essa metodologia de gestão de riscos não será algo permanente em seu órgão/entidade. Nossa sugestão é que comece com uma abordagem simplificada, que será aprimorada continuamente, conforme cresça a maturidade em relação ao tema.

> **Atenção:** *Conforme comentamos na Apresentação deste Guia, caso seu órgão/entidade já possua metodologia de gestão de riscos, poderá aplicá-la também para as análises relacionadas à integridade. Nesse caso, é importante observar se os riscos para a integridade levantados correspondem às características apresentadas no capítulo 1.*

1. PASSO 1 – SELEÇÃO E ESTUDO DO PROCESSO

A gestão de riscos pode ser reaplicada muitas vezes permitindo que, de forma contínua, os processos possam ser revisitados e os controles possam ser revisados e aprimorados à luz de novos riscos identificados, assim como daqueles já conhecidos. Iniciaremos pela seleção de um processo organizacional no qual será aplicada a metodologia.

PROCESSO ORGANIZACIONAL PODE SER DEFINIDO COMO QUALQUER CONJUNTO DE ATIVIDADES INTER-RELACIONADAS QUE RECEBEM INSUMOS E OS TRANSFORMA EM SERVIÇOS OU PRODUTOS PARA OS CIDADÃOS, SEGUINDO UMA LÓGICA PREESTABELECIDA COM AGREGAÇÃO DE VALOR.[38]

Nesse momento, é esperado que alguns gestores, por se sentirem ainda inseguros em relação ao tema, pensem em selecionar um processo acessório para a organização. Isso não é o sugerido.

Mas como escolher o processo?

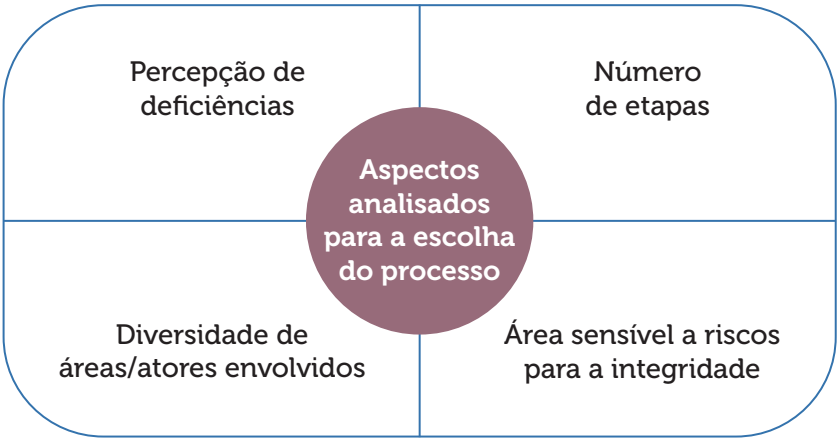
Os riscos à integridade podem ocorrer em diferentes áreas e processos de uma organização, assim como suas ocorrências de forma reiterada também podem variar a depender de cada caso específico.[39] Seguem algumas orientações para a escolha do processo:

- Há percepção de deficiências - em um processo com deficiências ficam ainda mais evidentes os benefícios obtidos da adoção da gestão de riscos.
- Envolve número moderado de etapas - em um processo com menos etapas fica mais fácil a percepção completa do processo para aqueles que irão participar da aplicação da metodologia.
- Não envolve grande diversidade de áreas/atores - em um pro-

38 TRANSPARÊNCIA BRASIL; CGU, 2006, p. 11 (adaptado).
39 BRASIL, 2017b, p. 25.

cesso envolvendo poucas áreas/atores, fica mais fácil evitar polêmicas que decorram de diferentes interesses na condução do processo.

- Pertence a uma área sensível a riscos para a integridade – existem algumas áreas e processos mais sensíveis a riscos para a integridade, que podem ser identificados a partir de normativos que trazem as competências institucionais do órgão/entidade, seu regimento interno, organograma e documentos como o planejamento estratégico[40]. O Anexo A deste documento traz uma relação de possíveis áreas e processos de risco para a integridade.



MÃOS À OBRA!

Selecione um processo da instituição com base nas orientações prestadas acima.

Para que um processo organizacional seja submetido ao escrutínio da metodologia de gestão de riscos, é necessário estar minimamente documentado, de forma a permitir que todos os participantes que irão contribuir na aplicação da metodologia, possam ter conhecimen-

40 BRASIL, 2017b, p. 25.

to alinhado, necessário e suficiente. Nesse sentido, o processo deve possuir, além dos normativos aplicáveis, pelo menos as seguintes informações adicionais:

- Descrição resumida – relato que contemple as principais etapas, atividades, produtos e atores envolvidos.
- Objetivos gerais e específicos – declaração de objetivos que permite a identificação dos riscos.
- Responsável – área da organização e dirigente na qual encontra-se a competência principal para a realização do processo em questão.
- Periodicidade - quantas vezes é realizado o processo e a sua média de duração em horas, dias, semanas etc.

Nas próximas vezes em que o ciclo de gestão de riscos for realizado, sugerimos ampliar essa etapa de estudo do processo para a realização do chamado estabelecimento do contexto[41].

De acordo com a norma ISO 31000, estabelecimento do contexto contempla a definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e estabelecimento do escopo e dos critérios para a política de gestão de riscos. Tais parâmetros são baseados em avaliação a) do contexto externo da organização – como as relações com partes interessadas externas e suas percepções e valores; mas também b) do contexto interno – como a governança, estrutura organizacional, funções e responsabilidades[42].

Reúna as informações sugeridas sobre o processo e outras que julgar pertinentes. Elas serão utilizadas nas etapas seguintes.

---

41 Caso haja tempo hábil para realizar essa etapa de forma completa já nesse primeiro ciclo, sugerimos o estudo dos itens "4.3.1. Entendimento da organização e seu contexto" e "5.3. Estabelecimento do contexto" da ABNT NBR ISO 31000 (ABNT, 2009a, p. 10; 15-17).

42 ABNT, 2009a, p. 3.

2. PASSO 2 – IDENTIFICAÇÃO DE RISCOS

Selecionado e estudado o processo, com o levantamento dos objetivos organizacionais envolvidos, é possível iniciar a identificação dos riscos.

RISCO É O EFEITO DA INCERTEZA SOBRE OS OBJETIVOS.[43]

De acordo com a ISO 31000, a *identificação de riscos* é o processo da busca, reconhecimento e descrição dos riscos; envolvendo a identificação das fontes de risco, eventos, causas e consequências potenciais[44]. A finalidade da etapa de identificação de risco é gerar uma lista abrangente de riscos baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos[45].

Os responsáveis pela identificação dos riscos podem e devem utilizar-se de ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos e capacidades e aos riscos enfrentados. Por esse motivo é importante que as pessoas envolvidas nesse processo tenham um conhecimento adequado sobre o negócio, bem como sejam incentivadas a não se restringirem aos acontecimentos do passado.[46]

Entre as técnicas utilizadas na identificação de riscos, sugerimos, nesse estágio inicial, a utilização de brainstorming (tempestade de ideias). Essa técnica tem como objetivo explorar o potencial criativo dos participantes. De forma resumida e simplificada, consiste em permitir que todos os participantes contribuam com ideias acerca de um determinado tema sem sofrer nenhum tipo de crítica. Os integrantes são incentivados a contribuir com o máximo possível de ideias que conseguirem. Tem-se, então, como o próprio nome sugere, uma tempestade de ideias. Na gestão de riscos, essa técnica permite, principalmente, a identificação de riscos que não se materializaram

43 Ibidem, p. 1.
44 Ibidem, p. 4.
45 Ibidem, p. 17.
46 BRASIL, 2017c, p. 22.

no passado, aqueles com baixa probabilidade de ocorrência, mas de significativos impactos, chamados de "Cisne Negro".[47]

Vale notar que, nesta etapa, faremos o exercício de identificação dos chamados **riscos inerentes**.

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.[48]

A seguir, durante a análise de riscos, serão levantados e avaliados os controles já estabelecidos em relação aos riscos para que sejam obtidos os **riscos residuais**.

RISCO RESIDUAL É O RISCO A QUE UMA ORGANIZAÇÃO ESTÁ EXPOSTA APÓS A IMPLEMENTAÇÃO DE AÇÕES GERENCIAIS PARA O TRATAMENTO DO RISCO.[49]

Após a identificação do risco, deverão ser apontadas todas as suas causas e consequências significativas, associadas a determinado evento:

- causa é o motivo que pode promover a ocorrência do risco[50];
- evento é a ocorrência ou mudança em um conjunto específico de circunstâncias – pode ter várias causas e consistir em uma ou mais ocorrências[51] e;
- consequência é o resultado de um evento que afeta os objetivos[52].

47 Idem.
48 BRASIL, 2016, art. 2º, XIV.
49 Ibidem, art. 2º, XV.
50 BRASIL, 2018b.
51 ABNT, 2009a, p. 4.
52 Ibidem, p. 5.

MÃOS À OBRA!

Como fazer:	Brainstorming (Uma ou mais reuniões) **Atenção:** *Criar um ambiente descontraído, de forma a estimular a memória da história do processo organizacional e a criatividade dos participantes.*
Participantes:	• Área responsável pela gestão de riscos • UGI • Colaboradores que trabalham diretamente no processo organizacional
Insumos:	• Documentos elaborados no estudo do processo

Passo a passo:	1.Informar aos participantes o propósito da oficina de identificar riscos para a integridade que possam comprometer o sucesso do processo organizacional em atingir os seus objetivos. **Atenção:** *Acordar com todos os participantes que nenhuma crítica será feita às contribuições apresentadas pelos demais.* 2. Distribuir cópia dos documentos apontados como insumos. 3. Fazer uma leitura esclarecedora da descrição resumida sobre o funcionamento e os objetivos do processo, incluindo observações quando aos controles identificados. 4. Para cada objetivo apresentado no estudo do processo, perguntar aos participantes quais os riscos para a integridade percebidos que podem comprometer (atrapalhar, impossibilitar) o alcance desse objetivo. **Atenção:** *Muitos riscos trazem a visão dos colaboradores sobre os problemas que ocorrem com alguma frequência na instituição. Ademais, em muitos casos, os colaboradores, principalmente aqueles que estão iniciando a aplicação da metodologia, enunciarão causas e não necessariamente riscos que podem comprometer os objetivos ou propósitos da instituição. Lembre-se que riscos representam incertezas, enquanto as causas são mais tangíveis para os participantes da oficina.* 5. Para cada risco identificado, transposto para a planilha, completar as colunas de causas e consequências. **Atenção:** *pode haver mais de uma causa e/ou consequência por risco, bem como a causa/ consequência pode ser relacionada a mais de um risco.* 6. Redigir uma descrição do risco, contemplando os itens identificados: "Devido a <CAUSAS>, poderá acontecer <RISCO/EVENTO>, o que poderá levar a <CONSEQUÊNCIAS> impactando no/na <DIMENSÃO DE OBJETIVO IMPACTADA>.*" * BRASIL, 2017c, slide 53 (adaptado).

<table>
<tr><td>Pro-
dutos
Gera-
dos:</td><td>• Lista de presença (Data, nome, área, cargo/função, assinatura)
• Planilha de levantamento de riscos
<table>
<tr><th>Processo</th><th>Objeti-
vos</th><th>Descri-
ção do
risco</th><th>Causa</th><th>Evento</th><th>Conse-
quência</th></tr>
<tr><td rowspan="2"></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
</table>

3. PASSO 3 – ANÁLISE DE RISCOS

De acordo com a ISO 31000, *análise de riscos* é o processo de compreender a natureza do risco e determinar o nível de risco. Ela fornece a base para a avaliação de riscos, bem como para as decisões quanto ao tratamento dos riscos.[53]

Inicialmente serão analisados os **riscos inerentes**. Dado que o risco é uma função tanto da probabilidade como do impacto, o nível do risco é expresso pela combinação da probabilidade da ocorrência do evento e de suas consequências caso se concretize, em termos da magnitude do impacto nos objetivos.[54]

NÍVEL DE RISCO = PROBABILIDADE x IMPACTO

Há diversas formas de estimar e apresentar a probabilidade e o impacto de um risco, que variam muito em relação à precisão e à complexidade. Caso o órgão/entidade esteja iniciando seu contato com processos de gestão de riscos, recomendamos a utilização de metodologia mais simples, sem ponderações para impacto e probabilidade.

Seguem propostas de métricas que podem ser utilizadas nesse processo inicial.

53 ABNT, 2009a, p. 5.
54 TCU, 2018, p. 40 (adaptado).

PROBABILIDADE	IMPACTO
Muito baixa (1) – baixíssima possibilidade de o evento ocorrer. **Baixa (2)** – o evento ocorre raramente. **Média (3)** – o evento já ocorreu algumas vezes e pode voltar a ocorrer. **Alta (4)** – o evento já ocorreu repetidas vezes e provavelmente voltará a ocorrer muitas vezes.	**Muito baixo (1)** – consequências insignificantes caso o evento ocorra. **Baixo (2)** – consequências menores em processos e atividades secundários. **Médio (3)** – consequências relevantes em processos e atividades secundários ou consequências menores em processos e atividades prioritárias. **Alto (4)** – consequências relevantes em processos e atividades prioritárias.

Dados: BRASIL, 2017b, p. 31 – 32.

Adicionalmente, o mapa de calor é uma ferramenta que pode ser utilizada para a análise de riscos, apresentando de forma simples e visual suas relevâncias através do cruzamento das probabili¬dades e dos níveis de impacto. Cada órgão/entidade pode utilizar mais ou menos escalas de classificação de impacto e probabilidade para construir seu mapa de calor, a depender da complexidade que queira dar a essa etapa de mapeamento. Para um primeiro levantamen¬to, sugere-se usar uma matriz 4x4 (quatro níveis de probabilidade e quatro níveis de im¬pacto) ou 5x5.[55]

Como sugestão, apresentamos neste guia uma matriz 4x4, construída com base nas métricas de impacto e probabilidade enunciadas acima. Graficamente, aparecem riscos baixos em cinza, moderados em verde, elevado em amarelo e extremo em vermelho. Este é apenas um exemplo, que pode ser adaptado para o formato considerado mais pertinente para seu órgão/entidade.

55 BRASIL, 2017b, p. 32.

Impacto → / Probabilidade ↓	Muito baixo	Baixo	Médio	Alto
Alta	Risco Moderado (4x1 = 4)	Risco Elevado (4x2 = 8)	Risco Elevado (4x3 = 12)	Risco Extremo (4x4 = 16)
Média	Risco Baixo (3x1 = 3)	Risco Moderado (3x2 = 6)	Risco Elevado (3x3 = 9)	Risco Elevado (4x3 = 12)
Baixa	Risco Baixo (2x1 = 2)	Risco Moderado (2x2 = 4)	Risco Moderado (2x3 = 6)	Risco Elevado (2x4 = 8)
Muito baixa	Risco Baixo (1x1 = 1)	Risco Baixo (1x2 = 2)	Risco Baixo (1x3 = 3)	Risco Moderado (1x4 = 4)

Fonte: BRASIL, 2017b, p. 33 (adaptado).

Para concluir a etapa de análise de riscos, é necessário avaliar os controles que já estão atuando em relação aos **riscos inerentes**, de modo a obter os riscos residuais.

CONTROLE É UMA MEDIDA QUE ESTÁ (OU PRETENDE ESTAR) MODIFICANDO O RISCO, PODENDO SER QUALQUER PROCESSO, POLÍTICA, DISPOSITIVO, PRÁTICA OU OUTRAS AÇÕES.[56]

A IN Conjunta MP/CGU nº 01/2016 define os controles internos da gestão como o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade.[57]

56 ABNT, 2009a, p. 6 (adaptado).
57 BRASIL, 2016, art. 2º, V.

Uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar o fator obtido a partir da análise do grau de efetividade da implementação dos controles[58], conforme proposta apresentada na tabela a seguir.

Nível	Descrição	Fator
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

Fonte: BRASIL, 2018b, p. 22. Adaptado de: TCU, 2018, p. 44.

Na abordagem proposta, o valor final da multiplicação entre o valor do nível de **risco inerente** e o **fator de avaliação dos controles** corresponde ao nível de **risco residual**.[59]

RISCO RESIDUAL = RISCO INERENTE x FATOR DE AVALIAÇÃO DOS CONTROLES

Por exemplo, caso o nível de risco obtido para o risco inerente tenha sido "9" (3 impacto x 3 probabilidade) e o controle existente tenha sido avaliado como satisfatório (fator 0, 4), teríamos: RISCO RESIDUAL = 9 X 0,4 = 3,6. Pelo novo valor, conforme nosso mapa de calor, o risco passaria de elevado para mais próximo do nível moderado.

58 TCU, 2018, p. 43 (adaptado).
59 BRASIL, 2018b, p. 22.

4. PASSO 4 – AVALIAÇÃO DE RISCOS

De acordo com a ISO 31000, **avaliação de riscos** é o processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.[60]

Nesse sentido, para que não haja desperdício de esforços, os riscos para a integridade a serem inicial-mente gerenciados por um plano de integridade precisam ser os mais relevantes para a organização, isto é, os de maior impacto e probabili¬dade dentro de um limite previamente definido pela alta direção. Após realizada a avaliação de riscos, o órgão ou entidade pode estabelecer uma ordem de prioridade para o tratamento de riscos, de acordo com seu **apetite a risco**.[61]

APETITE A RISCO É O NÍVEL DE RISCO QUE UMA ORGANIZAÇÃO ESTÁ DISPOSTA A ACEITAR.[62]

O apetite a riscos pode ser único para toda a organização ou variar em função de critérios definidos – por exemplo, dependendo da categoria de riscos, do programa governamental correspondente ou da área da instituição envolvida.

Sua definição usualmente é representada como uma linha que delimita a aceitação de forma gráfica. No mapa de calor a seguir os níveis de risco maiores que 8 (cores amarela e vermelha) são considerados acima do **apetite a risco** da organização.

60 ABNT, 2009a, p. 6.
61 BRASIL, 2017b, p. 31.
62 BRASIL, 2018b, p. 9.

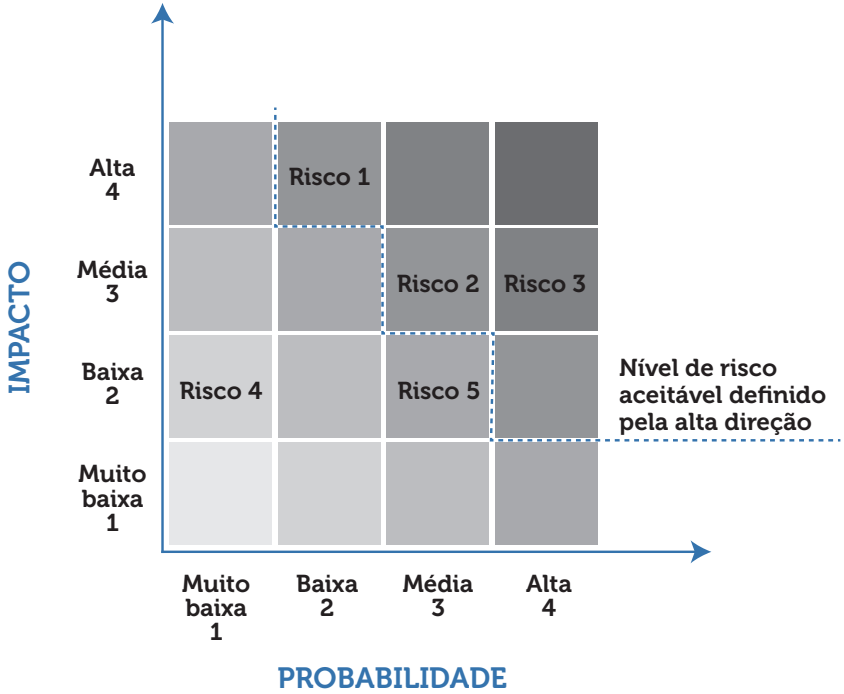
Impacto → / Probabilidade ↓	Muito baixo	Baixo	Médio	Alto
Alta	Risco Moderado (4x1 = 4)	Risco Elevado (4x2 = 8)	Risco Elevado (4x3 = 12)	Risco Extremo (4x4 = 16)
Média	Risco Baixo (3x1 = 3)	Risco Moderado (3x2 = 6)	Risco Elevado (3x3 = 9)	Risco Elevado (4x3 = 12)
Baixa	Risco Baixo (2x1 = 2)	Risco Moderado (2x2 = 4)	Risco Moderado (2x3 = 6)	Risco Elevado (2x4 = 8)
Muito baixa	Risco Baixo (1x1 = 1)	Risco Baixo (1x2 = 2)	Risco Baixo (1x3 = 3)	Risco Moderado (1x4 = 4)

APETITE DE RISCO

Apresentamos a seguir um exemplo de mapa de calor preenchido, elaborado por um órgão público fictício, responsável por ações de fiscalização em obras públicas[63]. Foram avaliados os seguintes riscos:

- risco 1: acesso indevido e vazamento de informações sensíveis nos bancos de dados acerca de futuros projetos;
- risco 2: pressões indevidas de superiores hierárquicos para alterar posicionamentos técnicos de subordinados;
- risco 3: servidores solicitarem/receberem valores indevidos em fiscalizações feitas pelo órgão ;
- risco 4: nepotismo em nomeação ou designação de pessoa para cargo em comissão ou função de confiança e;
- risco 5: utilização de bens públicos (carros, terceirizados e material de expediente) em atividades privadas.[64]

63 Ibidem, p. 34.
64 Ibidem, p. 35.



Fonte: BRASIL, 2017b, p. 34.

Conforme é possível notar na figura acima, o órgão concluiu que os riscos de 1 a 3 estavam acima de seu apetite a riscos, devendo, portanto, ser priorizados na etapa de tratamento de riscos.

MÃOS À OBRA!

Como fazer:	Brainstorming (Uma ou mais reuniões) *Debate visando a atingir o consenso.*
Participantes:	• Área responsável pela gestão de riscos • UGI • Participantes com muita experiência no processo organizacional e, preferencialmente, com poder de decisão.
Insumos:	• Documentos elaborados no estudo do processo • Planilha de levantamento de riscos

Passo a passo:	1. Informar aos participantes o propósito da reunião de analisar e avaliar os riscos previamente identificados, determinando sua probabilidade, impacto e nível de risco. **Atenção:** *Acordar com todos os participantes que nenhuma crítica será feita às contribuições apresentadas pelos demais.* 2. Distribuir cópia dos documentos apontados como insumos. 3. Relacionar os riscos indicados na planilha de levantamento de riscos. 4. Perguntar qual o impacto na ocorrência do risco inerente. Discutir visando a obter o consenso e anotar as informações na planilha de análise/avaliação de riscos. **Atenção:** *Caso não haja consenso, atribuir o maior valor de impacto que foi percebido.* 5. Perguntar a probabilidade percebida para a ocorrência do risco inerente. Discutir visando a obter o consenso e anotar as informações na planilha de análise/avaliação de riscos. **Atenção:** *Caso não haja consenso, atribuir o maior valor de probabilidade que foi percebido.* 6. Calcular o nível de risco (produto entre o valor do impacto e da probabilidade) e anotar as informações na planilha de análise/avaliação de riscos. 7. Perguntar quais os controles existentes no processo organizacional, que mitigariam o risco em avaliação. Discutir visando a obter o consenso e anotar as informações na planilha de análise/avaliação de riscos. 8. Perguntar qual a avaliação sobre o funcionamento dos controles para mitigar o risco. Discutir visando a obter o consenso e anotar as informações na planilha de análise/avaliação de riscos. 9. Fazer a multiplicação entre o valor do nível de risco inerente e o fator de avaliação dos controles existentes, obtendo o nível de risco residual. 10. Situar os riscos residuais no mapa de calor, indicando aqueles que se encontrem fora do apetite a riscos adotado na organização.

<table>
<tr><td>Produtos Gerados:</td><td>

- Lista de presença (Data, nome, área, cargo/função, assinatura)
- Planilha de análise/avaliação de riscos

<table>
<tr><th>Risco</th><th>Probabilidade</th><th>Impacto</th><th>Nível de risco inerente</th><th>Controles existentes</th><th>Avaliação dos controles existentes</th><th>Nível de risco residual</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

</td></tr>
</table>

Atenção: *A avaliação de riscos realizada em reunião precisa ser* **validada** *pelo responsável pelo processo organizacional na alta administração. Essa pessoa definirá se é necessário alterar a gradação em termos do impacto e/ou probabilidade indicados, bem como poderá alterar a ordem dos riscos que serão tratados prioritariamente. Seja qual for a decisão tomada, é importante que seja* **justificada e documentada**.

5. PASSO 5 – TRATAMENTO DE RISCOS

De acordo com a ISO 31000, tratamento de riscos é o processo para modificar o risco.[65] Nesta etapa, devem ser estabelecidas as medidas (controles) que a organização pode tomar para evitar, mitigar ou transferir os seus riscos de integri¬dade mais relevantes.[66]

Podemos agrupar respostas aos riscos em quatro tipos de tratamento:

1. Aceitar: a entidade decide não atuar em relação ao ris¬co. A sua probabilidade e impacto são tão baixos que não justificam a criação de controles para mitigação, ou os controles existentes já resguardam boa parte de suas consequências. É geralmente uma ação escolhida para riscos com baixo impacto e probabilidade.

2. Transferir: o risco possui probabilidade e impacto tão altos que a organização não pode suportar e decide transferi-los a outra enti-

65 ABNT, 2009a, p. 6.
66 BRASIL, 2017b, p. 36.

dade. Por exemplo, um órgão público decide contratar um seguro de acidentes para certos empregados que exercem ativida¬des muito perigosas – ele transfere o seu risco de sinistro para uma outra entidade.

3. Mitigar: o órgão/entidade decide atuar para reduzir a pro¬babilidade e/ou impacto do risco, tornando-o menor ou mesmo removendo-o da lista dos principais riscos.

4. Evitar: envolve alterar o processo visando a evitar a ocorrência do risco. Por exemplo, um órgão pode decidir evitar o oferecimento de determinado serviço por envolver riscos de alto impacto e proba¬bilidade.[67]

Quando se trata de riscos, a perspectiva não deve ser a de garantir sua eliminação, pois se está lidando com a incerteza. Portanto, na maioria das vezes, serão tomadas ações para minimizar ou mitigar o risco, por meio de medidas que visam reduzir o impacto e/ou probabilidade do risco, resultando em níveis aceitáveis do risco, compatível com o que a organização possa lidar sem maiores danos.

Uma diversidade de medidas pode ser concebida para o tratamen¬to de riscos para a integridade, a exemplo das listadas a seguir:

- treinamento de pessoal;
- procedimentos de controle envolvendo áreas e processos sensíveis (aquisições, regulação de mercado, con¬cessão de licenças e benefícios etc.);
- diluição do excesso de poder e discricionariedade em poucos indivíduos ou áreas; e
- promoção da transparência e do controle social.[68]

É interessante observar que as medidas de mitigação dos riscos podem possuir efeitos mais amplos do que o tratamento do risco em

67 Ibidem, p. 33-34 (adaptado).
68 Ibidem, p. 38.

si. Por exemplo, uma capacitação sobre normas e procedimentos licitatórios pode mitigar não ape¬nas o risco de ocorrer algum desvio nesse tipo de processo, mas também melhorar a qualidade técnica dos trabalhos da área de licitações como um todo. É também comum que certas medidas mitigadoras possuam maior abrangência e acabem por abarcar o tratamento de mais de um risco para a integridade, como a elaboração/atualização de um código de ética/conduta, por exemplo.[69]

Apresentamos a seguir rol exemplificativo com ideias de medidas para o tratamento de riscos para a integridade, mas ressaltamos que outras podem ser pensadas, a depender dos riscos específicos de cada órgão/entidade e dos recursos disponíveis:[70]

- Publicação de informações relevantes no endereço eletrônico, tais como planejamento estratégico, fluxos de processos e próximas licitações
- Estabelecimento de políticas, normas e procedimentos internos que definam os procedimentos mais sensíveis do órgão/entidade
- Verificação periódica de informações classificadas como sigilosas/reservadas
- Previsão de mecanismos formais e regulares de participação cidadã
- Disponibilização da lista dos servidores públicos em quarentena, com informação sobre período da medida e área de proibição para atuação
- Redução do nível de discricionariedade do tomador de decisão em processos sensíveis, como a instituição de segregação de funções
- Padronização de especificações que são mais comuns (limpeza, vigilância, telefonia, material de expediente etc.), como o uso

69 Ibidem, p. 40.
70 Ibidem, p. 39-40.

de editais-padrão

- Definição de alçadas de aprovação, dependendo do valor envolvido em licitações, contratos e concessão de benefícios
- Realização de diligência nas empresas contratadas com o intuito de verificar possíveis casos de fraude e conluio
- Implementação de mecanismos de decisão colegiada no órgão, compartilhando o poder de decisão
- Criação de sistemas informatizados que exerçam controle sobre atividades sensíveis à quebra de integridade
- Estabelecimento de critérios objetivos para indicação de ocupantes de cargos diretivos, como capacitação e experiência
- Exigência de motivação detalhada nos casos em que houver discordância entre os posicionamentos da área técnica e da direção superior
- Mapeamento de servidores, ex-servidores e terceirizados visando identificar relacionamentos com empresas e grupos econômicos
- Publicação de informações gerais sobre programas que resultem em renúncia de receitas

> **Atenção:** *Os mecanismos de controle devem ser concebidos e implementados para assegurar que as respostas aos riscos sejam executadas de forma apropriada e tempestiva. É fundamental dimensionar os controles às reais necessidades da organização, tendo em vista que a implantação de controles para riscos de baixo impacto e baixa probabilidade de ocorrência pode tornar a administração pública desnecessariamente burocrática e lenta. Os controles internos devem auxiliar, e não impedir, a realização dos objetivos da organização (BRASIL, 2017b, p. 38).*

Segue abaixo exemplo fictício de registro de análise de risco de nepo-

tismo em uma área de gestão de pessoas:[71]

- Processo: nomeação ou designação de pessoa para cargo em comissão ou função de confiança.
- Risco: nepotismo – nomeação ou designação de familiar de ministro de Estado, familiar da máxima autoridade administrativa correspondente ou familiar de ocupante de cargo em comissão ou função de confiança para cargo em comissão ou função de confiança.

#	Fatores de risco	Controles existentes	Análise
1	Desconhecimento do Decreto nº 7.203/2010 pelos servidores da área.	Servidores da Coordenação-Geral de Recursos Humanos receberam uma capacitação na época da aprovação do Decreto. Não houve capacitações posteriores apesar de vários servidores terem saído e chegado à área.	Apesar de existir previsão de capacitação, ela não foi continuada.
2	Ausência de procedimento de verificação de laços de parentesco das pessoas nomeadas, contratadas ou designadas com o Ministro de Estado, autoridade máxima correspondente ou ocupantes de cargos em comissão e funções de confiança.	Nenhuma.	Não há medidas.
3	Ausência de regras claras para ocupação de cargos em comissão e funções de confiança.	Normativo recente estipulou regras claras para ocupação de cargos DAS somente até nível 3 e em algumas unidades do órgão.	Medidas não abarcam todos os cargos e unidades.

Fonte: BRASIL, 2017b, p. 37 – 38.

71 Ibidem, p. 37.

Como fazer:	Leitura e debate sobre cada risco (Uma ou mais reuniões)
Partici-pantes:	• Área responsável pela gestão de riscos • UGI • Participantes com muita experiência no processo organizacional e, preferencialmente, com poder de decisão.
Insumos:	• Documentos elaborados no estudo do processo • Planilha de levantamento de riscos • Planilha de análise/avaliação de riscos • Mapa de calor com riscos preenchidos e apetite a riscos delimitado
Passo a passo:	1. Informar aos participantes o propósito da oficina de definir medidas de tratamento para os riscos priorizados na etapa anterior. 2. Distribuir cópia dos documentos apontados como insumos. 3. Para cada risco priorizado, preencher a planilha de tratamento de riscos com as seguintes informações: • risco; • tipo de tratamento; • medidas de tratamento propostas; • ações a serem implementadas; • responsável por cada ação (área/colaborador); • prazo para implementação (início e término); • situação (prevista, em andamento, concluída).
Produtos Gerados:	• Lista de presença (Data, nome, área, cargo/função, assinatura) • Planilha de tratamento de riscos

Risco	Proba-bilidade	Impac-to	Nível de risco inerente	Con-troles existen-tes	Avalia-ção dos contro-les exis-tentes	Nível de risco residual

Atenção: *A planilha de tratamento de riscos deverá integrar o plano de integridade, demonstrando que o programa de integridade está customizado às necessidades de seu órgão/entidade. Caso prefira, o órgão/entidade poderá omitir a informação sobre o risco ou adotar descrição mais genérica que a formulada no âmbito do levantamento de riscos.*

6. PASSO 6 – COMUNICAÇÃO E MONITORAMENTO

De acordo com a ISO 31000, tanto a comunicação como a consulta às partes interessadas internas e externas devem ocorrer durante todas as fases da gestão de riscos[72] por serem processos que uma organização conduz para fornecer, compartilhar ou obter informações e dialogar com suas contrapartes. Tais informações podem se referir à existência, natureza, forma, probabilidade, significância, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos[73].

A esse respeito, a IN MP/CGU nº 01/2016 ressalta que informações relevantes devem ser identificadas, coletadas e comunicadas a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas que possibilitem o gerenciamento de riscos e a tomada de decisão. Lembra, ainda, que a comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos.[74]

Dica: *Algumas questões a serem consideradas na comunicação sobre riscos são:*
O que precisa ser comunicado?
Quem precisa saber?
Qual o prazo?
Qual o melhor formato para apresentar as informações?

72 ABNT, 2009a, p. 14.
73 Ibidem, p. 3.
74 BRASIL, 2016, art. 16, VII.

Qual análise precisa ser previamente realizada para a entrega de dados robustos?
Qual ação de follow-up é necessária?

(AUSTRALIA, 2016, p. 20)

Por sua vez, o **monitoramento** é definido no contexto da ISO 31000 como a verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado[75]. São apontadas como finalidades do monitoramento e análise crítica:

- garantir que os controles sejam eficazes e eficientes no projeto e na operação;
- obter informações adicionais para melhorar o processo de avaliação dos riscos;
- analisar os eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles;
- detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades;
- identificar os riscos emergentes.[76]

A IN MP/CGU nº 01/2016 destaca o objetivo do monitoramento de avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.[77]

> **Atenção:** *É importante prever a revisão periódica da gestão dos riscos para a integridade, que pode ocorrer de forma concomitante com o processo geral de gestão de riscos do*

75 ABNT, 2009a, p. 7.
76 Ibidem, p. 20.
77 BRASIL, 2016, art. 16, VIII.

órgão/entidade. Essa é uma informação importante a ser incluída no plano para integridade.

Concluímos, assim, nossa discussão sobre a gestão de riscos para a integridade. Para avançar para a elaboração do plano de integridade, você pode buscar orientações no "Guia prático de implementação de programa de integridade pública: orientações para a administração pública federal direta, autárquica e fundacional".

ANEXO - EXEMPLOS DE ÁREAS E PROCESSOS DE RISCO[78]

Um levantamento prévio de informações realizado através das reco¬mendações relacionadas com integridade pela CGU gerou as cor¬relações de áreas de risco e processos de risco abaixo. Certamente existem outras áreas e processos que podem ser relacionados a riscos de integridade, conforme as competências e atividades de cada órgão ou entidade.

O intuito dessa lista e dessa correlação é servir como ilustração e também como demonstrativo de áreas e processos que já foram previamente relacionadas a eventuais riscos à integridade.

ÁREA DE RISCO	PROCESSOS DE RISCO
Acesso à informação	- Atendimento presencial de cidadãos no SIC - Fornecimento de informações no âmbito do direito previsto na Lei nº 12.527/2011
Acordos e convênios	- Seleção de beneficiários e convenentes - Celebração de convênio - Aprovação da prestação de contas do convênio - Contratação ou realização de convênio com recursos relativos a transferências voluntárias
Alta direção	- Fixação de metas e padrões de desempenho - Avaliação dos resultados envolvendo metas e padrões de desempenho - Reuniões de autoridades públicas com administrados
Atendimento ao público	- Atendimento presencial - Fornecimento de serviços públicos
Auditoria e fiscalização	- Identificação e apuração de fatos presumidamente ilegais ou irregulares
Compras públicas	- Aquisição de bens e contratação de serviços - Compras efetuadas com cartão de pagamento

78 BRASIL, 2017b, p. 53 – 56.

Concessão de crédito	- Destinação do crédito - Seleção e hierarquização de empreendimentos a serem apoiados - Contratação do empreendimento
Conselhos de políticas públicas	- Nomeação ou designação de pessoas para representação em conselho de política pública - Processo de tomada de decisão nos conselhos de políticas públicas
Conselhos e órgãos colegiados	- Processo de tomada de decisões colegiadas - Processo de seleção de contratos, convênios e congêneres em conselhos administrativos
Correição	- Apuração de responsabilidade administrativa
Diárias e passagens	- Compra de passagens e pagamento de diárias - Deslocamento de servidores públicos por motivo privado
Formulação e acompanhamento de políticas públicas	- Tomada de decisão em políticas públicas - Prospecção de novas estratégias e inovações - Estabelecimento de ação de participação social
Gestão de informações	- Gestão de informações estratégicas e confidenciais
Gestão de pessoas	- Concurso público - Contratação de consultores e terceirizados - Contratação de pessoa para atendimento a necessidade temporária de excepcional interesse público - Contratação de pessoa para vaga de estágio - Nomeação de servidores para cargo em comissão ou função de confiança - Exoneração de servidores - Exoneração/demissão de servidores ocupantes de cargos - de direção, chefia ou assessoramento - Deslocamento de servidores públicos por motivo privado - Pagamentos de verbas indenizatórias
Gestão patrimonial	- Programas de desinvestimentos (venda de ativos)

Licenças, outorgas e autorizações	- Processos de avaliação - Emissão de licenças e autorizações públicas - Processos de concessão de outorga
Licitações e contratos	- Contratações diretas, sem licitação - Contratações de produto ou serviço em processo licitatório - Definição dos objetos, serviços e empreendimentos a serem implementados - Definição da ordem de prioridade dos projetos a serem implementados ou da solução tecnológica a ser contratada - Definição das aquisições e contratações a serem realizadas no exercício - Quantificação da demanda do bem ou serviço a ser licitado - Elaboração de cláusulas restritivas à competitividade no edital do processo licitatório - Elaboração do preço de referência da licitação - Análise de preços em contratos de obras públicas - Critérios de avaliação e adjudicação das propostas - Gestão de contratos - Aditivo de contratos - Fiscalização de contratos - Aquisição de serviços de informática - Controle de estoque de softwares - Contratação de serviços de consultoria - Contratação de serviços de publicidade e propaganda - Cadastro de Fornecedores fora do SICAF – inclusões, atualizações e utilização

Ouvidoria	- Processo de recebimento, análise inicial (triagem) e resposta de manifestações provenientes do sistema E-ouv - Tratamento de manifestações - Apuração de fatos presumidamente ilegais/irregulares - Verificação da existência de denúncias contra pessoas indicadas para cargos em comissão nos sistemas E-ouv, Banco de Denúncias e SGI
Parceria e cooperação	- Estabelecimento de termo de parceria - Gestão de termo de parceria - Cessão de servidores
Patrocínio	- Seleção do beneficiário
Prestação de serviços	- Prestação de serviço em regime de monopólio
Processos sancionadores	- Processo de investigação de suposto ato ilícito - Definição e aplicação de sanções
Regulação e fiscalização	- Edição de normas e regras voltadas aos serviços regulados pelo Estado - Fiscalização dos entes regulados - Autuação - Decisões colegiadas
Relações internacionais	- Avaliação do cumprimento, pelo Brasil, das recomendações de organismos internacionais - Tramitação de pedidos de cooperação jurídica internacional
Renúncias e incentivos	- Seleção de proponentes e beneficiários
Subvenções e benefícios	- Seleção dos beneficiários

REFERÊNCIAS BIBLIOGRÁFICAS

AUSTRALIA. Department of Finance, Commercial and Government Services. *Implementing the Commonwealth Risk Management Policy* – Guidance 2016. Camberra, 2016. Disponível em: <https://www.finance.gov.au/sites/default/files/implementing-the-rm-policy.PDF>. Acesso em 29 ago. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. ABNT NBR ISSO 31000. *Gestão de riscos* — Princípios e diretrizes. Rio de Janeiro, nov. 2009a. ISBN 978-85-07-01838-4.

_____. ISO GUIA 73:2009. Gestão de Riscos – Vocabulário. Rio de Janeiro, 2009b.

BRASIL. Decreto nº 9.203, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. *Diário Oficial da União*, Brasília, DF, seção 1, p. 3, 23 nov. 2017a.

_____. Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. *Diário Oficial da União*, Brasília, DF, 11 mai. 2016.

_____. Lei nº 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei no 9.986, de 18 de julho de 2000, e das Medidas Provisórias nos 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. *Diário Oficial da União*, Brasília, DF, seção 1, p. 1., 17 mai. 2013.

_____. Decreto nº 7.203, de 4 de junho de 2010. Dispõe sobre a vedação do nepotismo no âmbito da administração pública federal. *Diário Oficial da União*, Brasília, DF, seção 1, p. 4, 07 jun. 2010.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. *Diário Oficial da União*, Brasília, DF, seção 1, p. 23911, 31 dez. 1940.

_____. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO - CGU. Portaria CGU nº 1.089, de 25 de abril de 2018. Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. *Diário Oficial da União*, Brasília, DF, ed. 80, seção 1, p. 81, 26 abr. 2018a.

_____. _____. *Metodologia de Gestão de Riscos*. Brasília, abr. 2018b. Disponível em: <http://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf>. Acesso em 29 ago. 2018.

_____. _____. *Manual para implementação de programas de integridade: orientações para o setor público*. Brasília, jul. 2017b. Disponível em: <http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual_profip.pdf>. Acesso em 29 ago. 2018.

_____. _____. *Curso "Gestão de Riscos e Controles Internos no Setor Público"* – Apostila. Brasília, abr. 2017c.

_____. TRIBUNAL DE CONTAS DA UNIÃO – TCU. Roteiro de Avaliação de Maturidade da Gestão de Riscos. Brasília: TCU, Secretaria e Métodos e Suporte ao Controle Externo, 2018. 164 p.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECNOÔMICO - OCDE. *Recomendação do Conselho da OCDE sobre Integridade Pública*. Tradução não oficial. Mar. 2018a, p.7. Disponível em: <http://www.oecd.org/gov/ethics/integrity-recommendation-brazilian-portuguese.pdf>. Acesso em 21 abr. 2018

_____. *Behavioural Insights for Public Integrity:* harnessing the human factor to counter corruption. OECD Public Governance Reviews. Paris: OECD Publishing, 2018b.

SELINŠEK, L. *Corruption Risk Assessment in Public Institutions in South East Europe:* Comparative Study and Methodology. Saravejo: Regional Cooperation Council, 2015. Disponível em: <http://rai-see.org/wp-content/uploads/2015/10/CRA_in_public_ins_in_SEE-WEB_final.pdf>. Acesso em 29 ago. 2018.

TRANSPARÊNCIA BRASIL. CGU. *Metodologia de Mapeamento de Riscos de Corrupção*. 2006. Disponível em: <http://www.pm.al.gov.br/intra/downloads/bc_corrupcao/cor_04.pdf>. Acesso em 29 ago. 2018.

www.cgu.gov.br

@cguonline

cguonline

cguoficial

MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO

GOVERNO FEDERAL