

# POLÍTICA DE GESTÃO DE RISCOS DO IBGE

2ª edição

Presidente da República  
**Jair Messias Bolsonaro**

Ministro da Economia  
**Paulo Roberto Nunes Guedes**

Secretário Especial de Fazenda  
**Waldery Rodrigues Junior**

**INSTITUTO BRASILEIRO  
DE GEOGRAFIA E  
ESTATÍSTICA - IBGE**

Presidente  
**Susana Cordeiro Guerra**

Diretor-Executivo  
**Fernando José de Araújo Abrantes**

ÓRGÃOS ESPECÍFICOS SINGULARES

Diretoria de Pesquisas  
**Eduardo Luiz G. Rios Neto**

Diretoria de Geociências  
**João Bosco de Azevedo**

Diretoria de Informática  
**David Wu Tai**

Centro de Documentação e Disseminação de Informações  
**Marise Maria Ferreira**

Escola Nacional de Ciências Estatísticas  
**Maysa Sacramento de Magalhães**


Ministério da Economia  
**Instituto Brasileiro de Geografia e Estatística - IBGE**  
Comitê de Governança, Conformidade e Riscos

# **Política de Gestão de Riscos do IBGE**

2ª edição

Rio de Janeiro  
2019



 Instituto Brasileiro de Geografia e Estatística	Fundação Instituto Brasileiro de Geografia e Estatística <b>RESOLUÇÃO</b> do Conselho Diretor	R. CD nº 34/2019
		Data: 6/9/2019
Aprovação da Metodologia de Gestão de Riscos do IBGE e Aprovação da Política de Gestão de Riscos do IBGE – 1ª Revisão		Folha: 1/1

**Competência:** Art. 12 do Estatuto aprovado pelo Decreto 4.740, de 13 de junho de 2003.

**Fundamentação Legal:** Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016.

**O CONSELHO DIRETOR da FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE), no uso de suas competências e,**

**RESOLVE:**

**Art. 1º** Aprovar a Metodologia de Gestão de Riscos do IBGE e detalhar as etapas necessárias à condução dos processos de identificação, análise, avaliação, tratamento e monitoramento de riscos na Instituição, sendo complementar à Política de Gestão de Riscos do IBGE, publicada em agosto de 2018 e revisada em agosto de 2019, pelo Comitê de Governança, Conformidade e Riscos (CGCR).

**Art. 2º** Esta Resolução entra em vigor a partir da data de sua publicação.



Susana Cordeiro Guerra  
 Presidente



# Sumário

<b>Apresentação .....</b>	<b>5</b>
<b>Introdução.....</b>	<b>6</b>
<b>Objetivos .....</b>	<b>7</b>
<b>Escopo.....</b>	<b>8</b>
<b>Termos e definições .....</b>	<b>8</b>
<b>Princípios.....</b>	<b>9</b>
<b>Diretrizes .....</b>	<b>9</b>
<b>Responsabilidades .....</b>	<b>10</b>
<b>Processo de gestão de riscos .....</b>	<b>13</b>
<b>Documentação .....</b>	<b>18</b>
<b>Referências .....</b>	<b>20</b>
<b>Apêndice 1 – Diagrama de Responsabilidades .....</b>	<b>21</b>
<b>Glossário .....</b>	<b>22</b>

## **Apresentação**

Todas as organizações estão expostas ao risco, sejam elas públicas ou privadas. Nas organizações, os riscos fazem parte inevitável das operações e estão presentes na condução de projetos, processos, atividades e na tomada de decisões, associados à possibilidade de ocorrência de eventos que impactem o alcance dos objetivos institucionais.

O IBGE, como produtor oficial de estatísticas e de informações geocientíficas, exerce um papel central em nossa sociedade, ao desenvolver, produzir e disseminar informações públicas imparciais e objetivas segundo os Princípios Fundamentais das Estatísticas Oficiais das Nações Unidas e cumprindo rigorosos requisitos de qualidade. Assegurar a produção e a divulgação regulares dessas informações é, portanto, questão essencial para a Instituição.

Neste sentido, apresentamos a Política de Gestão de Riscos do IBGE, documento institucional que orientará a condução do processo de gestão de riscos para assegurar o alcance dos objetivos e preservar a capacidade de cumprimento da missão institucional.

Esta segunda versão da Política ajusta e esclarece conceitos, considerando o estágio atual da discussão do tema no IBGE.

***Susana Cordeiro Guerra***

Presidente do IBGE



## Introdução

O IBGE tem como missão institucional *“Retratar o Brasil com informações necessárias ao conhecimento de sua realidade e ao exercício da cidadania”*. As informações estatísticas e geocientíficas produzidas e disseminadas pela Instituição são um bem público entregue à sociedade, de interesse de grupos de usuários diversos (governos, empresas e cidadãos), essenciais para orientar ações de planejamento e decisões sobre políticas públicas.

Todas as organizações enfrentam riscos que podem afetar o cumprimento de suas metas e objetivos. Nas organizações públicas, riscos podem ser decorrentes de vários fatores, entre eles, a natureza das atividades, a dinâmica da gestão pública, mudanças nas circunstâncias e nas demandas sociais, entre outros. Para proteção do ambiente institucional e suporte ao cumprimento da missão, organizações estão sendo estimuladas a, de forma sistemática, gerenciar os riscos identificados em processos, projetos e/ou escolhas estratégicas. A gestão de riscos objetiva prover confiança de que os objetivos serão alcançados e recursos públicos serão corretamente aplicados para o cumprimento das responsabilidades institucionais de gerar, preservar e entregar valor público, em benefício da sociedade. O processo de gestão de riscos promove a avaliação do efeito das incertezas nos objetivos, ou seja, o que pode acontecer, por que, com que probabilidade e que magnitude de consequências, o que determina o nível de risco. Diante das incertezas e do nível de risco, as organizações precisam rever e reforçar seus controles internos, implementar ações de prevenção aos eventos que possam impactar o alcance de seus objetivos e, também, instituir mecanismos de monitoramento e análise crítica para promover o aprendizado organizacional.

A Instrução Normativa Conjunta MP/CGU n. 01, de 10.05.2016 (BRASIL, 2016), dispõe sobre controles internos, gestão de riscos e governança, no âmbito do poder executivo federal e orienta os órgãos e entidades dessa esfera governamental para que tenham um processo estruturado de gestão de riscos. Já a Portaria CGU n. 1089, 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 (BRASIL, 2018). Atento às orientações legais e aos movimentos da gestão contemporânea, o IBGE incluiu em seu Plano Estratégico 2017-2027 (IBGE, 2017a), como um dos desafios prioritários, a implementação da Política de Gestão de Riscos. Neste sentido, foi formado o Comitê de Governança, Conformidade e Riscos<sup>1</sup>, subordinado

<sup>1</sup> Para informações mais detalhadas sobre o tema, consultar: IBGE. Resolução do Conselho Diretor n. 28, de 25 de agosto de 2017. Cria o Comitê de Governança, Conformidade e Riscos. *Boletim de Serviço*, Rio de Janeiro, n. 2885, p. 1, 25 ago. 2017c. Ver também: IBGE. Portaria da Presidência n. 151, de 5 de março de 2018. Designa membros do Comitê de Governança, Conformidade e Riscos. *Boletim de Serviço*, Rio de Janeiro, n. 2913, p. 8-9, 9 mar. 2018.

ao Conselho Diretor, e seus integrantes se reúnem com regularidade para tratar esta temática. Foi criada, também, a Unidade de Gestão da Integridade (UGI)<sup>2</sup>. Três linhas (ou camadas) de defesa contra os riscos estão previstas: os controles internos da gestão constituem a primeira linha de defesa e são definidos e executados por todos os níveis de gestão dentro da Instituição, ou seja, são operados pelos gestores responsáveis pela condução de atividades e tarefas, no âmbito dos processos finalísticos e de apoio, levando-se em conta os riscos que se pretende tratar, tendo em vista os objetivos a alcançar. O Comitê de Governança, Conformidade e Riscos atua, junto ao Conselho Diretor, como segunda linha de defesa da Instituição, estando entre suas responsabilidades assegurar que as atividades de gerenciamento de riscos realizadas pela primeira linha sejam desenvolvidas e executadas de forma apropriada, supervisionar e monitorar os controles internos da gestão, fortalecendo-os contra ações irregulares, antiéticas, antieconômicas, ineficientes e ineficazes. Finalmente, as auditorias internas constituem a terceira linha de defesa, sendo responsáveis pela avaliação da operacionalização dos controles internos (1ª linha de defesa) e da supervisão dos controles internos (2ª linha de defesa).

A Política de Gestão de Riscos do IBGE é fruto do trabalho do Comitê e o primeiro documento institucional produzido para formalizar o processo sistemático de gestão de riscos na Instituição. Nesta segunda versão, alguns conceitos foram revistos e conteúdos acrescentados.

## **Objetivos**

A Política de Gestão de Riscos do IBGE define os elementos norteadores do processo de gestão de riscos na Instituição e visa aumentar a probabilidade de alcance dos objetivos institucionais, reduzindo os riscos a níveis aceitáveis.

A gestão de riscos visa assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso a informações suficientes quanto aos riscos aos quais está exposta a Instituição e possam instituir controles internos efetivos e implementar o plano de tratamento para reduzir a probabilidade de ocorrência e os impactos negativos decorrentes da materialização de riscos. A gestão de riscos no IBGE deve agregar valor e contribuir para a melhoria da qualidade de produtos e processos e para o aprimoramento da tomada de decisão.

<sup>2</sup> Para mais informações, consultar: IBGE. Resolução do Conselho Diretor n. 17, de 10 de maio de 2019. Cria a Unidade de Gestão da Integridade do IBGE (UGI). Boletim de Serviço, Rio de Janeiro, n. 2975, p. 1, 17 maio. 2019.

## Escopo

A Política de Gestão de Riscos do IBGE aplica-se a todos os níveis hierárquicos, funções, atividades e unidades organizacionais que tenham objetivos institucionais a cumprir com riscos identificados. Envolve, portanto, os programas, projetos e processos, nos níveis estratégico, tático e operacional. O processo de gestão de riscos se integra à gestão e à tomada de decisão e faz parte da estrutura, das operações e dos processos organizacionais.

Os controles internos da gestão e a gestão de riscos fazem parte das atividades, planos, ações, políticas, sistemas, recursos e esforços institucionais, sendo projetados para aumentar a segurança quanto ao alcance dos objetivos. Os controles internos baseiam-se na gestão de riscos e ambos compõem o processo de gestão institucional, dimensionados e desenvolvidos na proporção requerida pelos níveis de riscos identificados.

A Política de Gestão de Riscos do IBGE é sustentada e materializada pela Metodologia de Gestão de Riscos, documento elaborado pelo Comitê de Governança, Conformidade e Riscos que descreve e detalha as etapas para a implementação do processo de gestão de riscos no IBGE.

A metodologia de gestão de riscos institucional tem como referência principal a norma ABNT NBR ISO 31000 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018), documento que apresenta as diretrizes e a abordagem genérica para o gerenciamento dos riscos nas organizações.

A gestão de riscos de segurança da informação segue as orientações da POSIC (Política de Segurança da Informação e Comunicações do IBGE) (IBGE, 2017b) e os documentos e normas aplicáveis, como a ABNT NBR ISO/IEC 27005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

Tais Políticas estão alinhadas entre si e se complementam.

A Política de Gestão de Riscos está disponível no portal do IBGE, como parte dos documentos institucionais, assim como na intranet, acompanhada dos demais documentos complementares.

## Termos e definições

Para os efeitos da Política de Gestão de Riscos do IBGE, aplicam-se os termos e definições fundamentais apresentados no Glossário.

## Princípios

A Política de Gestão de Riscos do IBGE observa os princípios a seguir listados, que servem de base para sua aplicação e interpretação. São eles:

- a) **Criação e proteção de valor:** agregação de valor e proteção do ambiente institucional;
- b) **Integração:** parte integrante dos processos e atividades organizacionais e de seu modelo de gestão;
- c) **Estruturação e abrangência:** abordagem estruturada e abrangente contribui para resultados consistentes e comparáveis;
- d) **Personalização:** a estrutura e o processo consideram os objetivos institucionais, o ambiente interno e o contexto externo em que se insere a Instituição e com os quais ela interage;
- e) **Inclusão:** o envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados e resultem em melhor conscientização e em uma gestão de riscos mais inclusiva e fundamentada;
- f) **Dinamismo:** a gestão de riscos é dinâmica e deve acompanhar as modificações que possam propiciar o surgimento, a mudança ou o desaparecimento de riscos. O processo de gestão de riscos deve antecipar, detectar, reconhecer e responder a alterações e eventos, oportuna e apropriadamente;
- g) **Uso de melhores fontes disponíveis:** as entradas ao processo de gestão de riscos são baseadas nas melhores fontes disponíveis, em informações históricas e atuais, bem como em expectativas futuras, levando em consideração, explicitamente, quaisquer limitações e incertezas associadas;
- h) **Influência de fatores humanos e culturais:** fatores humanos e culturais influenciam significativamente todos os aspectos da gestão de riscos, em cada nível e estágio; e
- i) **Melhoria contínua:** a gestão de riscos é melhorada continuamente a cada ciclo de gestão, incorporando as lições aprendidas, as experiências e o aprendizado institucional.

## Diretrizes

O conjunto de diretrizes a seguir orienta a condução do processo de gestão de riscos no IBGE. As iniciativas de gestão de riscos no IBGE devem ser:

- a) Empreendidas com o apoio do Conselho Diretor e o suporte dos integrantes do Comitê de Governança, Conformidade e Riscos, que juntos atuam como segunda linha de defesa, supervisionando os controles internos para propiciar o alcance dos objetivos;
- b) Realizadas para apoiar a tomada de decisão e a elaboração da estratégia e do plano estratégico e para a melhoria contínua de processos organizacionais;

- c) Implementadas de forma gradual, priorizando, inicialmente, os riscos identificados nos processos e projetos que impactem diretamente as metas institucionais e os objetivos estratégicos, tendo o plano estratégico como principal referência para a priorização;
- d) Exercidas por todos os integrantes dos processos de trabalho, projetos e ações estratégicas, táticas e/ou operacionais no IBGE, segundo seu nível e hierarquia;
- e) Sistemáticas, estruturadas e oportunas, implementadas de modo permanente e contínuo, de acordo com a metodologia formalizada;
- f) Associadas a um agente responsável pelo gerenciamento do risco, ou seja, ao gestor de risco, com alçada suficiente para orientar e acompanhar as ações de avaliação e tratamento do risco e que tenha participado de nivelamento conceitual e metodológico em gestão de riscos;
- g) Geridas de forma integrada, objetivando o estabelecimento de um ambiente de controle e gestão de riscos que respeite valores, interesses e expectativas da Instituição e, também, das partes interessadas, tendo o cidadão e a sociedade como principais vetores;
- h) Proporcionais ao nível de riscos, observada a relação custo/benefício e destinadas a agregar valor à Instituição;
- i) Revistas em ciclos periódicos de gerenciamento de riscos de até dois anos para cada processo de trabalho com riscos identificados e tratamentos definidos;
- j) Medidas quanto ao seu desempenho, mediante atividades contínuas e/ou avaliações independentes; e
- k) Melhoradas continuamente como parte da evolução da maturidade da gestão de riscos.

## Responsabilidades

Gerenciar riscos é parte da governança e da liderança e é fundamental para a maneira como a Instituição é gerenciada em todos os níveis, o que contribui para a melhoria do sistema de gestão.

Ao Conselho Diretor do IBGE compete:

1. **Aprovar e publicar** a Política de Gestão de Riscos do IBGE, seus documentos complementares e suas atualizações;
2. **Assegurar** a existência, o monitoramento e a avaliação de um efetivo sistema de gestão de riscos e controles internos, **atuando** junto ao Comitê de Governança, Conformidade e Riscos como segunda linha de defesa para propiciar o alcance dos objetivos;
3. **Incluir** na pauta da reunião do Conselho Diretor questões específicas relacionadas à governança, riscos e controles internos, sempre que necessário;
4. **Convocar** reunião do Conselho Diretor ampliado para avaliação de riscos estratégicos, aprovação do respectivo Plano de Tratamento de Riscos, incluindo definição de prazos e responsáveis (gestor do risco); e

5. **Deliberar** sobre questões, recomendações e relatórios apresentados pelo Comitê de Governança, Conformidade e Riscos do IBGE.

Ao **Presidente do Comitê de Governança, Conformidade e Riscos do IBGE** compete:

6. **Coordenar** as atividades do Comitê de Governança, Conformidade e Riscos;
7. **Encaminhar** ao Conselho Diretor do IBGE para apreciação a Política de Gestão de Riscos do IBGE, seus documentos complementares e atualizações;
8. **Encaminhar** ao Conselho Diretor do IBGE para apreciação e discussão o resultado da avaliação preliminar de riscos estratégicos e respectiva proposta de Plano de Tratamento de Riscos;
9. **Encaminhar** relatórios e recomendações ao Conselho Diretor do IBGE sobre o andamento da gestão de riscos e controles internos na Instituição;
10. **Buscar e manter** contatos externos sobre governança, riscos e controles internos, representando o IBGE, para identificação de oportunidades e possibilidades de compartilhamento e aprendizado.

Ao **Comitê de Governança, Conformidade e Riscos do IBGE** compete:

11. **Propor** a Política de Gestão de Riscos do IBGE e os documentos complementares, bem como sua revisão e aprimoramento;
12. **Institucionalizar** estruturas adequadas de governança, gestão de riscos e controles internos;
13. **Assegurar** a implementação, a manutenção, o monitoramento e a revisão do processo de gestão de riscos;
14. **Estabelecer** o nível de risco tolerável, alinhado às diretrizes do Conselho Diretor;
15. **Identificar, analisar e avaliar**, preliminarmente, riscos estratégicos e **propor** o Plano de Tratamento de Riscos, conforme o nível de risco;
16. **Aprovar** a relação de processos priorizados para a avaliação de riscos operacionais e para a integridade;
17. **Aprovar** Plano de Tratamento de Riscos propostos pelos Coordenadores ou Chefes de Unidades Estaduais e aprovar a indicação dos gestores dos riscos operacionais;
18. **Atuar junto ao Conselho Diretor e à UGI** como segunda linha de defesa da Instituição;
19. **Disseminar** a versão mais recente e aprovada da Política de Gestão de Riscos do IBGE e seus documentos complementares, assegurando ampla comunicação;
20. **Dar** suporte metodológico à implementação e operacionalização da gestão de riscos;
21. **Estimular** ações de capacitação e conscientização sobre o tema e **promover** seu desenvolvimento contínuo;
22. **Elaborar relatórios e emitir** recomendações em temas relacionados ao processo de gestão de riscos do IBGE para deliberação pelo Conselho Diretor; e
23. **Avaliar** sugestões ou contribuições eventualmente encaminhadas pelos servidores.

Aos **Coordenadores e Chefes de Unidade Estadual do IBGE** compete:

24. **Propor** ao Comitê de Governança, Conformidade e Riscos os processos que devam ter os riscos operacionais avaliados e tratados com prioridade, a cada ciclo, conforme Metodologia de Gestão de Riscos;
25. **Identificar, analisar e avaliar** os riscos operacionais e para a integridade no âmbito de sua unidade e dos processos e atividades que lhes são afetos;
26. **Propor** o Plano de Tratamento de Riscos (operacionais e para a integridade), conforme nível de risco, **fixar prazo** de implementação e **propor** os gestores de risco responsáveis por cada risco; e
27. **Acompanhar e avaliar** resultados obtidos, **monitorar** riscos ao longo do tempo e **garantir** que as respostas adotadas resultem na manutenção do risco em níveis adequados.

Aos **Gestores de Risco do IBGE** compete:

28. **Implementar** as ações definidas no Plano de Tratamento de Riscos e **reportar** resultados;
29. **Atuar como primeira linha de defesa** da Instituição, implementando, mantendo, monitorando e revisando controles internos da gestão, no âmbito de macroprocessos finalísticos e de apoio, integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, conforme a Metodologia de Gestão de Riscos; e
30. **Documentar, relatar e garantir** que as informações sobre o risco e sua gestão estejam disponíveis, sejam monitoradas e apropriadamente comunicadas nos seus espaços de atuação.

A **todos os servidores de carreira, agentes com contrato temporário e demais pessoas que atuam nas diversas instâncias do IBGE** compete:

31. **Colaborar** com o processo de gestão de riscos, **fornecendo informações e dando retorno** às eventuais consultas;
32. **Operacionalizar** os controles internos da gestão; e
33. **Comunicar** à Chefia imediata eventuais deficiências, eventos ou fontes de risco identificados e encaminhar sugestões relativas à Política de Gestão de Riscos do IBGE e documentos complementares, quando for o caso.

À **Auditoria Interna do IBGE** compete:

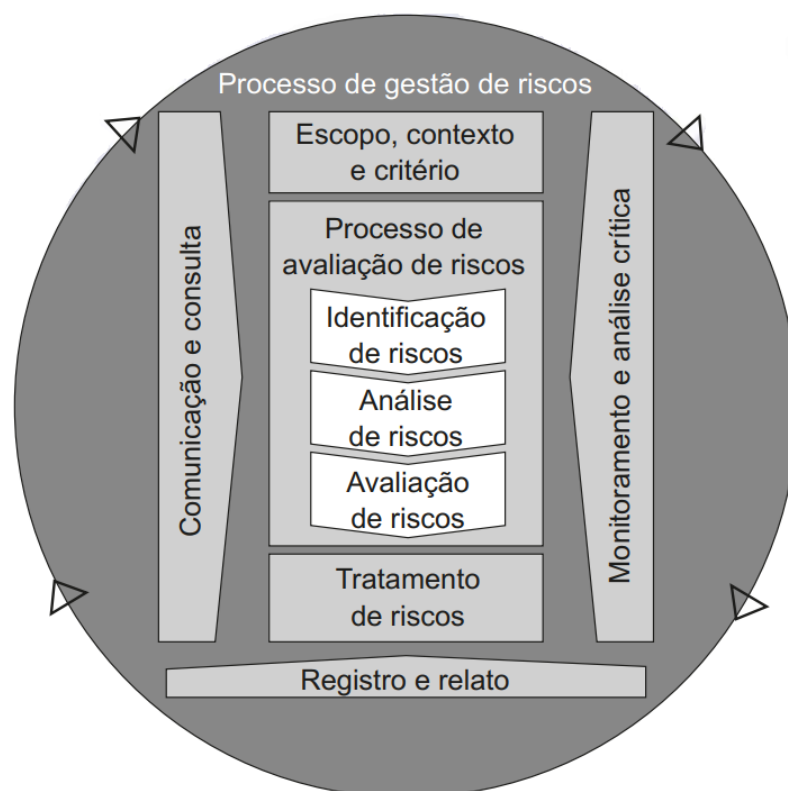
34. **Atuar** como terceira linha de defesa da Instituição, apoiando a estruturação e efetivo funcionamento da primeira e da segunda linha de defesa da gestão, por meio da prestação de serviços de consultoria (assessoria e aconselhamento) e da avaliação (análise objetiva de evidências) dos processos de governança, gerenciamento de riscos e controles internos;

35. **Avaliar** os processos de gestão de riscos e controles contemplando: a adequação e a suficiência dos mecanismos de gestão de riscos e de controles estabelecidos, a eficácia da gestão dos principais riscos e a conformidade das atividades executadas em relação à política de gestão de riscos; e
36. **Informar** prontamente ao Presidente do Comitê de Governança, Conformidade e Riscos sobre não conformidades e riscos identificados em ações de auditorias internas ou externas ou sobre outros elementos que possam impactar os riscos e os controles internos, de forma a permitir uma atuação institucional preventiva ou corretiva.

## Processo de gestão de riscos

O processo de gestão de riscos envolve a aplicação sistemática da Política, da metodologia, procedimentos e práticas relativas às atividades direcionadas à gestão dos riscos, quais sejam: comunicação e consulta; estabelecimento do escopo, contexto e critérios de risco; processo de avaliação de riscos (que compreende a identificação, a análise e a avaliação de riscos); tratamento de riscos; monitoramento e análise crítica; e registro e relato de riscos. A Figura 1 ilustra as atividades que compõem o processo de gestão de riscos no IBGE.

**Figura 1 – Processo de gestão de riscos**



Fonte: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 31000: gestão de riscos - princípios e diretrizes*. Rio de Janeiro, 2018.



## Comunicação e consulta

A comunicação busca promover a conscientização e auxiliar na compreensão do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisões, no âmbito de cada etapa e ao longo de todo o processo de gestão de riscos.

**Comunicação e consulta** são processos contínuos, conduzidos para fornecer, compartilhar ou obter informações envolvendo as partes interessadas, com vistas ao gerenciamento de riscos.

## Escopo, contexto e critérios

O propósito do estabelecimento do escopo, do contexto e dos critérios é personalizar o processo de gestão de riscos, permitindo uma avaliação de riscos eficaz e um tratamento apropriado dos riscos identificados na Instituição.

Como o processo de gestão de riscos pode ser aplicado em diferentes níveis é importante identificar claramente o escopo e os objetivos a serem considerados, bem como o alinhamento aos objetivos organizacionais.

Os contextos externo e interno representam o ambiente no qual a Instituição define e alcança seus objetivos. O contexto do processo de gestão de riscos deve ser estabelecido a partir da compreensão dos ambientes externo e interno nos quais a Instituição opera, refletindo o ambiente específico da atividade ao qual o processo de gestão de riscos é aplicado. A estrutura da gestão de riscos, no que se refere à definição dos fatores externos e internos considera:

- a) No que diz respeito ao contexto externo: fatores sociais, culturais, políticos, legais, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e/ou ambientais, em âmbito internacional, nacional, regional ou local e fatores e tendências que afetem os objetivos institucionais. Também se incluem aqui os relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas, as relações e compromissos contratuais e a complexidade das redes de relacionamento e dependências;
- b) No que concerne ao contexto interno: visão, missão e valores; governança, estrutura organizacional, funções e responsabilidades; estratégia, objetivos e políticas; cultura institucional; normas, diretrizes e modelos adotados, além das capacidades entendidas em termos de recursos e conhecimentos (por exemplo, capital, tempo, pessoas, processos, sistemas, tecnologias), dados, sistemas de informação e fluxos de

informação, cultura, percepções e valores dos servidores de carreira e agentes de contrato temporário e relacionamentos com partes interessadas internas.

Finalmente, é preciso especificar o nível de risco que a Instituição pode ou não assumir em relação aos objetivos e estabelecer os critérios para avaliar a significância do risco e apoiar os processos de tomada de decisão relativos aos riscos, de acordo com o propósito específico e o escopo da atividade em consideração. Os critérios de risco devem refletir os valores, objetivos e recursos e serem consistentes com a Política de Gestão de Riscos. Os critérios de riscos serão estabelecidos na Metodologia de Gestão de Riscos e devem ser, periodicamente, submetidos à análise crítica e alterados, se necessário.

**Critérios de riscos** são os parâmetros de referência contra os quais a magnitude de um risco é avaliada.

## **Processo de Avaliação de Riscos**

### **a) Identificação de riscos**

A identificação de riscos é o processo de encontrar, reconhecer e descrever os riscos que possam afetar o alcance dos objetivos, independentemente de suas fontes estarem ou não sob seu controle, tendo como base o contexto estabelecido e o apoio na comunicação e consulta com as partes interessadas internas e externas.

Pessoas com experiências e conhecimentos adequados devem ser envolvidas na identificação dos riscos. A identificação dos riscos pode se basear em dados históricos, análises teóricas, opiniões de especialistas e de partes interessadas.

### **b) Análise de riscos**

Consiste na compreensão das causas e consequências do risco e da determinação do nível de risco.

O **nível de risco** é a magnitude de um risco, expressa em termos da combinação da probabilidade de ocorrência do evento (causas) e impacto de suas consequências.

A análise de riscos considera as causas (fontes de risco e respectivas vulnerabilidades) e suas probabilidades de ocorrência e os efeitos, analisados quanto ao impacto gerado, caso o risco se materialize. A análise de riscos é feita tendo a Matriz de Riscos como referência, documento que estará contido na Metodologia de Gestão de Riscos e apresenta os parâmetros para reduzir a subjetividade do julgamento.

Um evento pode ocorrer porque há uma vulnerabilidade associada a uma fonte de risco, formando a causa. Um evento pode ser, inclusive, algo não acontecer e pode ter uma ou várias causas. São possíveis fontes de risco as pessoas, os processos, os sistemas, a estrutura organizacional, a infraestrutura física, as tecnologias. Fontes de risco, quando associadas a vulnerabilidades, podem ser causas de riscos (**Quadro 1**).

**Quadro 1 – Exemplos de causas de riscos**

Fonte	Vulnerabilidade
Pessoas	- Em número insuficiente - Sem capacitação - Desmotivadas
Sistemas	- Obsoletos - Não integrados
Infraestrutura física	- Localização inadequada - Inexistência de controles de acesso físico

Fonte: AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. ANS. Manual de Gestão de Riscos da Agência Nacional de Saúde Suplementar. Rio de Janeiro, RJ, 2018. Disponível em: <[http://www.ans.gov.br/images/stories/A\\_ANS/Transparencia\\_Institucional/gestao\\_de\\_riscos/manual-de-gestao-de-riscos-da-ans.pdf](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/manual-de-gestao-de-riscos-da-ans.pdf)>. Acesso em: jul. 2019. Adaptado.

A análise de riscos fornece uma entrada para a avaliação de riscos, para decisões sobre se o risco necessita ser tratado e como deve ser tratado e sobre a estratégia e os métodos mais apropriados para o tratamento de riscos.

### c) Avaliação dos riscos

Consiste na comparação dos resultados da análise de riscos com o nível de risco tolerável para determinar onde é necessária ação adicional, o que pode levar a uma decisão de não fazer mais nada, considerar as opções de tratamento de riscos, realizar análises adicionais para melhor compreender o risco, manter os controles existentes ou reconsiderar os objetivos.

A finalidade da avaliação dos riscos é auxiliar na decisão sobre os riscos que necessitam de tratamento e a prioridade para a implementação das ações. A avaliação resulta em uma lista de riscos que requerem tratamento, com respectivas classificações e indicação de prioridades.

## Tratamento de riscos

O tratamento de riscos tem como objetivo a seleção e implementação das opções mais viáveis e adequadas para abordar riscos. O tratamento de riscos envolve um processo iterativo de formular e selecionar opções para tratamento de riscos; elaborar e implementar o Plano de Tratamento do Risco; avaliar a eficácia do tratamento; decidir se o risco remanescente é aceitável; se não for aceitável, realizar tratamento adicional.

A seleção das opções mais apropriadas de tratamento de riscos envolve equilibrar, de um lado, os custos e os esforços de implementação e, de outro, os benefícios decorrentes, ou seja, as decisões estão baseadas na avaliação da magnitude dos impactos e dos custos de se estabelecerem controles internos.

A seleção de opções de tratamento de riscos deve ser feita de acordo com os objetivos, nível de risco tolerável e recursos disponíveis.

As opções de tratamento de riscos não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias e podem envolver uma ou mais das seguintes alternativas:

- **Evitar o risco** ao decidir não iniciar ou descontinuar com a atividade que dá origem ao risco;
- **Remover a fonte de risco** (Eliminar o risco);
- **Alterar a probabilidade de ocorrência e/ou a consequência do impacto (modificar o risco)**, implantando medidas ou controles que reduzam a probabilidade de ocorrência das causas que podem levar ao risco ou o impacto das consequências;
- **Compartilhar o risco** com outra(s) parte(s) externa(s) que possa(m) gerenciá-lo de forma mais eficaz, **transferir** a responsabilidade pelo tratamento do risco e/ou suas consequências para outra parte interessada;
- **Reter (ou aceitar) o risco** por decisão fundamentada; não adotar ação específica para modificar o risco, assumindo o risco por uma decisão consciente e embasada, escolha justificada formalmente (aprovada pelo Comitê de Governança, Conformidade e Risco), podendo implementar sistemática de monitoramento; manter o risco no nível atual de impacto e probabilidade. A aceitação do risco também é chamada de **retenção do risco**.

Após o tratamento dos riscos, é preciso conhecer a natureza e extensão do risco residual, que deve ser documentado e submetido a monitoramento, análise crítica e, se apropriado, a tratamento adicional.

**Risco residual** é o risco remanescente após o tratamento do risco.

Um Plano de Tratamento de Riscos deve ser elaborado, especificando como as opções de tratamento escolhidas serão implementadas. O progresso em relação ao Plano deve ser monitorado.

O Plano de Tratamento de Riscos indica a justificativa para a seleção das opções de tratamento, as ações a serem implementadas, o responsável por implementá-las (gestor de risco) e o prazo de implementação, o que deve resultar em melhorias nos processos, introdução de novos controles internos ou na modificação dos controles existentes.

## Monitoramento e análise crítica

O monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados têm por finalidade assegurar e melhorar a qualidade e a eficácia da concepção, implementação e resultados do processo de gestão de riscos.

O monitoramento e a análise crítica devem ocorrer em todos os estágios do processo e incluem planejamento, coleta e análise de informações, registros de resultados e fornecimento de retorno. Resultados devem ser incorporados nas atividades de gestão de desempenho, medição e relatos da Instituição.

## Registro e relato

O processo de gestão de riscos e os seus resultados devem ser documentados e relatados pelo Comitê de Governança, Conformidade e Riscos, por meio de Relatórios apropriados, encaminhados ao Conselho Diretor. Gestores de risco devem documentar, relatar e garantir que as informações sobre os riscos e sua gestão estejam disponíveis e sejam monitoradas e apropriadamente comunicadas. O relato é parte integrante da governança e visa os seguintes aspectos: comunicar atividades e resultados de gestão de riscos; fornecer informações para a tomada de decisões; melhorar as atividades de gestão de riscos; e auxiliar a interação com as partes interessadas.

## Documentação

O processo de gestão de riscos é suportado, principalmente, pelos seguintes documentos:

- Política de Gestão de Riscos do IBGE;
- Metodologia de Gestão de Riscos, documento que descreve e detalha a metodologia de implementação e o processo de gestão de riscos e apresenta e descreve os diferentes documentos a serem utilizados, tais como:
  - ✓ Matriz de Riscos, documento a ser usado na análise de riscos para a definição do nível de risco, considerando escalas de probabilidade de ocorrência e de consequências e áreas de impacto;
  - ✓ Relatório de Riscos, documento elaborado pelos gestores de riscos, para cada processo avaliado, que registra em cada Unidade Organizacional o resultado das atividades de identificação, análise, avaliação e tratamento de riscos;
  - ✓ Plano de Tratamento de Riscos, documento que especifica as ações a serem implementadas para modificar o risco, prazos de conclusão e responsáveis (gestores de risco);

- ✓ Mapa de Riscos, documento de responsabilidade do Comitê de Governança, Conformidade e Riscos que consolida as informações acerca dos riscos institucionais, ou seja, os riscos a que a Instituição está exposta, suas causas, consequências e níveis de risco, bem como sintetiza as informações dos Planos de Tratamento de Riscos;
- ✓ Relatório de Registro e Relato, documento que comunica as atividades e resultados de gestão de riscos, também de responsabilidade do Comitê de Governança, Conformidade e Riscos.

Os documentos são revistos e atualizados em ciclos de até dois anos, tempo previsto para monitoramento e análise crítica do ciclo de avaliação do processo de gestão de riscos no IBGE.

## Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO 31000: gestão de riscos - princípios e diretrizes*. Rio de Janeiro, 2018.

\_\_\_\_\_. *ABNT ISO GUIA 73: gestão de riscos - vocabulário*. Rio de Janeiro, 2009.

\_\_\_\_\_. *ABNT NBR ISO/IEC 27005: tecnologia da informação - técnicas de segurança - gestão de riscos de segurança da informação*. Rio de Janeiro, 2011.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. ANS. *Manual de Gestão de Riscos da Agência Nacional de Saúde Suplementar*. Rio de Janeiro, RJ, 2018. Disponível em: <[http://www.ans.gov.br/images/stories/A\\_ANS/Transparencia\\_Institucional/gestao\\_de\\_riscos/manual-de-gestao-de-riscos-da-ans.pdf](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/manual-de-gestao-de-riscos-da-ans.pdf)>. Acesso em: jul. 2019.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União. *Instrução normativa conjunta MP/CGU n. 01, de 10 de maio de 2016*. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do poder executivo federal. Brasília, DF, 2016. Disponível em: <[http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in\\_cgu\\_mpog\\_01\\_2016.pdf](http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf)>. Acesso em: set. 2018.

\_\_\_\_\_. Ministério da Transparência e Controladoria-Geral da União. *Portaria 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. Brasília, DF, 2018a. Disponível em: <<https://www.cgu.gov.br/noticias/2018/04/cgu-lanca-regulamentacao-para-programas-de-integridade-no-governo-federal/portaria-cgu-1089-2018.pdf>>. Acesso em: jun. 2019.

IBGE. *Plano estratégico do IBGE 2017-2027*. Rio de Janeiro, 2017a. Edição de junho.

\_\_\_\_\_. *Política de segurança da informação e comunicações do IBGE 2017-2018*. Rio de Janeiro, 2017b. 28 p. Disponível em: <<https://www.ibge.gov.br/institucional/documentos-ibge.html>>. Acesso em: set. 2018.

\_\_\_\_\_. Resolução do Conselho Diretor n. 28, de 25 de agosto de 2017c. Cria o Comitê de Governança, Conformidade e Riscos. *Boletim de Serviço*, Rio de Janeiro, n. 2885, p. 1, 25 ago. 2017.

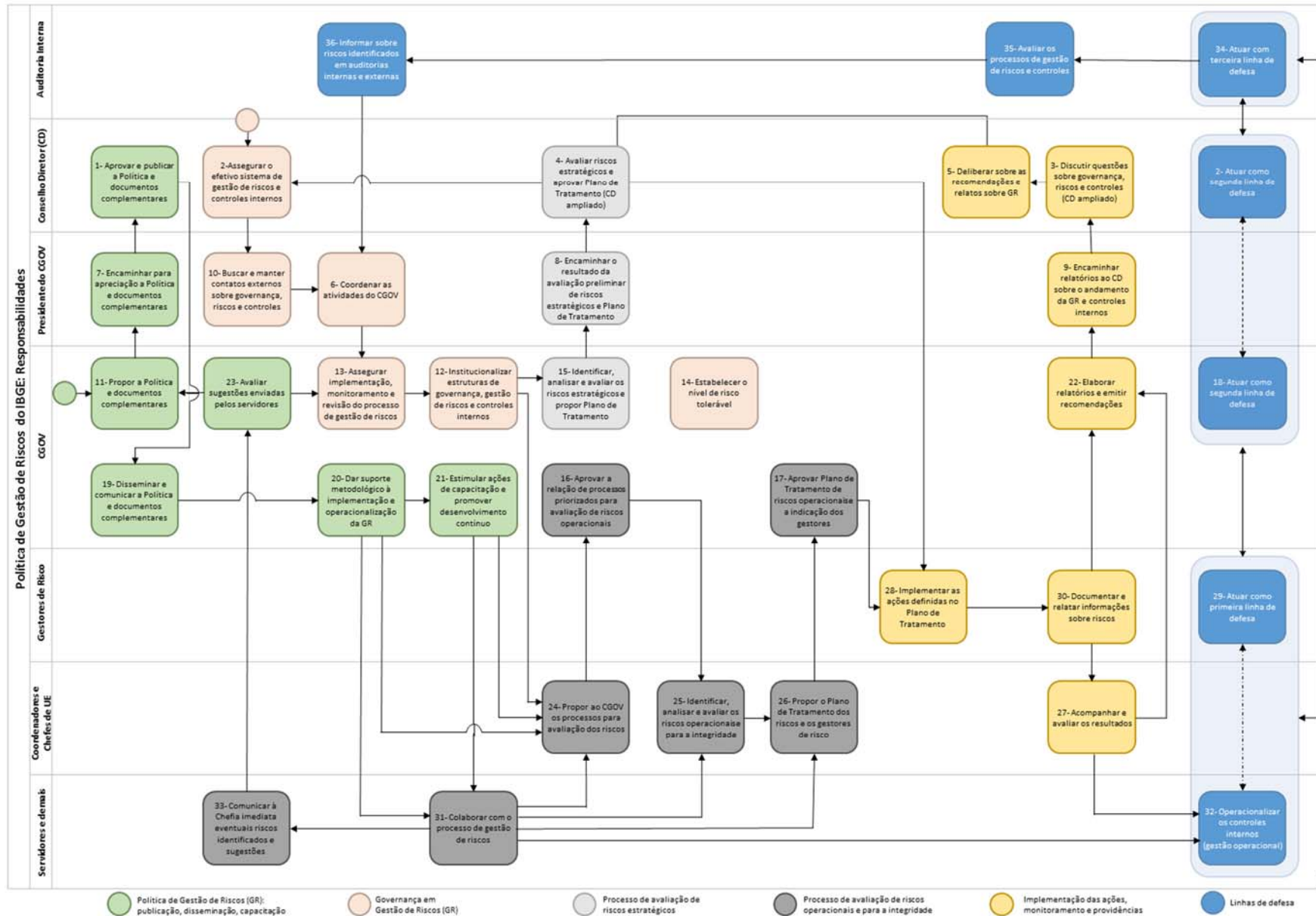
\_\_\_\_\_. Portaria da Presidência n. 151, de 5 de março de 2018. Designa membros do Comitê de Governança, Conformidade e Riscos. *Boletim de Serviço*, Rio de Janeiro, n. 2913, p. 8-9, 9 mar. 2018.

\_\_\_\_\_. Resolução do Conselho Diretor n. 17, de 10 de maio de 2019. Cria a Unidade de Gestão da Integridade do IBGE (UGI). *Boletim de Serviço*, Rio de Janeiro, n. 2975, p. 1, 17 maio. 2019.

## Apêndices

### 1 – Diagrama de Responsabilidades

# 1 – Diagrama de Responsabilidades





## Glossário<sup>3</sup>

**ameaça** Possibilidade de ocorrência de um evento que afete negativamente ou adversamente a realização do objetivo (risco ou risco negativo).

**causa** Fonte de risco associada a uma vulnerabilidade. Uma causa gera um evento que pode resultar em um ou mais efeitos ou consequências.

**comunicação e consulta** Processos contínuos conduzidos para fornecer, compartilhar ou obter informações e para envolver no diálogo as partes interessadas, com vistas ao gerenciamento de riscos no IBGE.

**consequência** Resultado de um evento que afeta os objetivos organizacionais. Uma consequência pode ser certa ou incerta, ter efeitos positivos ou negativos, diretos ou indiretos nos objetivos, e pode ser expressa qualitativa ou quantitativamente. Qualquer consequência pode ter efeitos em cascata e cumulativos. O termo impacto pode ser usado como alternativa ao termo consequência.

**controles internos da gestão** Atividades e medidas implementadas pela gestão para manter e/ou modificar e/ou diminuir os riscos e assegurar o alcance de objetivos organizacionais, podendo ser preventivas (reduzem a probabilidade de ocorrência de eventos de risco, por meio do foco nas causas), detectivas (possibilitam a identificação da ocorrência dos eventos de risco) ou corretivas (permitem reduzir o impacto caso o risco se materialize), implementadas de forma manual ou automatizada. Os controles internos da gestão se constituem na primeira linha de defesa para propiciar o alcance dos objetivos institucionais e são operados pelos gestores de risco e demais gestores responsáveis pela condução de atividades e tarefas, no âmbito dos processos de negócio e dos processos de apoio e sua operacionalização deve levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos a alcançar. Em função do nível de risco devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência e/ou seu impacto sobre os objetivos organizacionais.

**critérios de risco** Parâmetros de referência contra os quais a magnitude de um risco é avaliada.

**evento** Incidente, ocorrência ou mudança em um conjunto específico de circunstâncias que afete a consecução de um ou mais objetivos, de modo negativo, positivo ou ambos. Um evento pode

<sup>3</sup> Conceitos e definições adaptados de Associação Brasileira de Normas Técnicas (2009, 2018).

consistir em uma ou mais ocorrências, com várias causas e consequências; pode, também, ser algo que é esperado, mas não acontece, ou algo que não é esperado, mas acontece. Um evento pode ser uma fonte de risco.

**fonte de risco** Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.

**gestor de risco** Gestor formalmente designado no Mapa de Riscos como sendo o responsável pelo gerenciamento de determinado risco identificado, analisado e avaliado, tendo alçada suficiente para implementar, orientar, acompanhar e reportar as ações de tratamento do risco.

**incerteza** Estado, mesmo que parcial, de deficiência de informações relacionadas a um evento, envolvendo sua compreensão, seu conhecimento, suas consequências ou sua probabilidade. Incapacidade de saber com antecedência a probabilidade real ou impacto de eventos futuros.

**nível de risco** Magnitude de um risco, expressa em termos da combinação da probabilidade de ocorrência do evento (causas) e impacto de suas consequências.

**nível de risco inerente** Magnitude de um risco sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

**nível de risco residual** Magnitude de um risco remanescente após considerar os controles existentes (após a implementação de ações para o tratamento do risco).

**nível de risco tolerável** Magnitude aceitável de um risco, após o tratamento do risco, a fim de atingir o objetivo em questão. Relaciona-se ao apetite ao risco, nível de risco que a organização está disposta a aceitar.

**oportunidade** Possibilidade de ocorrência de um evento que afete positivamente a realização do objetivo (risco positivo).

**parte interessada** Pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade.

**probabilidade** Chance de algo acontecer. Na terminologia de gestão de riscos, o termo "probabilidade" é utilizado para se referir à chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se

descrita com termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo).

**risco** Efeito da incerteza nos objetivos. Possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos organizacionais. O risco é normalmente expresso em termos de fontes de risco, eventos potenciais, combinação de consequências de um evento e probabilidade de ocorrência associada. Um efeito é um desvio em relação ao esperado; pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades (eventos que afetem positivamente a realização de objetivos) e ameaças (ocorrência de eventos que afetem adversamente a realização dos objetivos).

**risco estratégico** Risco de ampla abrangência, transversal, que impacte mais de uma Unidade Organizacional e que pode comprometer a missão e as metas institucionais. Risco relacionado à estratégia, às políticas institucionais, aos resultados e ao desempenho institucional, sendo acompanhados pelo Conselho Diretor.

**risco operacional** Risco que afeta objetivos relacionados a projetos específicos, processos de trabalho e atividades finalísticas ou de suporte e gestão, sendo o acompanhamento de responsabilidade dos gestores de Unidade Organizacional.

**risco para a integridade** Risco relacionado a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta.

**vulnerabilidades** Inexistências, inadequações, lacunas ou deficiências em uma fonte de risco.

## **Equipe técnica**

(Nomeada pela portaria P.PR nº 371/2018, de 19 de junho de 2018)

### **Comitê de Governança, Conformidade e Riscos**

#### **Presidência**

Ana Cristina Martins Bruno

#### **Secretaria Executiva**

Gylcilene Ribeiro Storino

#### **Demais integrantes**

##### **Gabinete da Presidência do IBGE**

Roberto Neves Sant Anna

Luís César Seixas de Oliveira

##### **Diretoria Executiva**

Rose Mary Rodrigues

Bruno Taranto Malheiros

##### **Diretoria Pesquisas**

Andréa Bastos da Silva Guimarães

Paula Leite da Cunha e Melo

##### **Diretoria de Geociências**

Miriam Mattos da Silva Barbuda

Diego Araújo de Carvalho Nascimento

##### **Diretoria de Informática**

Arnaldo Lyrio Barreto

Sandra Martins Lino

##### **Centro de Documentação e Disseminação de Informações**

Marise Maria Ferreira

Carlos José Lessa de Vasconcellos

##### **Escola Nacional de Ciências Estatísticas**

José André de Moura Brito

Ana Paula Donizetti Lins de Albuquerque

##### **Coordenação Operacional dos Censos**

Wolney Cogoy de Menezes

Ricardo Baptista

##### **Unidades Estaduais**

Alceu José Vanzella (SC)

Andréa Machado Barbosa (SC)

Maria Antônia Esteves da Silva (MG)

Rúbia Francisca Silva Lenza (MG)

##### **Comitê Institucional da Qualidade**

Marcos Paulo Soares de Freitas

José de Souza Pinto Guedes

##### **Comitê de Segurança da Informação e Comunicações do IBGE**

Andréia Fernandes da Silva

José Luiz Thomaselli Nogueira

Se o assunto é **Brasil**,  
procure o **IBGE**.



/ibgecomunica



/ibgeoficial



/ibgeoficial



/ibgeoficial

**[www.ibge.gov.br](http://www.ibge.gov.br)** 0800 721 8181

