TRIBUNAL DE CONTAS DA UNIÃO

BTCU Administrativo Especial

Boletim do Tribunal de Contas da União

Diário Eletrônico

Ano 37 | nº 1 | Quarta-feira, 24/01/2018

PORTARIA-SEGECEX Nº 2, DE 22 DE JANEIRO DE 2018.

Aprova o documento "Roteiro de Avaliação de Maturidade da Gestão de Riscos".

TRIBUNAL DE CONTAS DA UNIÃO
Boletim do Tribunal de Contas da União

http://www.tcu.gov.br btcu@tcu.gov.br

SAFS Lote 1 Anexo I sala 424 - CEP:70042-900 - Brasília - DF
Fones: 3316-7279/3316-7869/3316-2484/3316-5249

Boletim do Tribunal de Contas da União administrativo especial - Ano. 37, n. 11 (2017)- . Brasília: TCU, 2017- .

Irregular.
Continuação de: Boletim do Tribunal de Contas da União Especial.

1. Ato administrativo - periódico - Brasil. I. Brasil. Tribunal de Contas da União (TCU).

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

SECRETARIA-GERAL DE CONTROLE EXTERNO

PORTARIAS

PORTARIA-SEGECEX Nº 2, DE 22 DE JANEIRO DE 2018.

Aprova o documento "Roteiro de Avaliação de Maturidade da Gestão de Riscos".

O SECRETÁRIO-GERAL DE CONTROLE EXTERNO, no uso de suas atribuições e tendo em vista o disposto no art. 34, inciso III, da Resolução-TCU nº 284, de 30 de dezembro de 2016,

considerando o disposto no Plano Estratégico do Tribunal de Contas da União para o quinquênio 2015-2021, aprovado pela Portaria TCU 141, de 1º de abril de 2015, que definiu como objetivo estratégico "Induzir o aperfeiçoamento da gestão de riscos e controles internos da Administração Pública";

considerando que a correta implementação e aplicação sistemática, estruturada e oportuna da gestão de riscos contribui para o cumprimento da missão institucional de órgãos e entidades da administração pública de gerar, preservar e entregar valor público em benefício da sociedade, com eficiência, eficácia, efetividade, transparência e prestação de contas, em conformidade com as leis e os regulamentos aplicáveis;

considerando a necessidade de proporcionar um instrumento para apoiar autoavaliações da maturidade da gestão de riscos, por parte de unidades ou comitês que supervisionam ou coordenam atividades de gestão de riscos no setor público;

considerando a oportunidade de contribuir com orientações e ferramentas para avaliar o cumprimento das diretrizes estabelecidas na Instrução Normativa Conjunta MP/CGU Nº 1, de 11/5/2016, por parte dos órgãos e entidades do Poder Executivo Federal; e

considerando a necessidade de atualizar o documento "Roteiro de Auditoria de Gestão de Riscos" a fim de refletir as alterações ocorridas na estrutura do THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (Coso), uma das principais referências em gestão de riscos, bem como a conveniência e oportunidade de alterar o título da publicação de forma a deixar mais claro seu público-alvo, resolve:

Art. 1º Fica aprovado o documento "Roteiro de Avaliação de Maturidade da Gestão de Riscos", na forma do Anexo Único desta Portaria, com as finalidades de:

I - apoiar a avaliação da maturidade da gestão de riscos em organizações públicas e a identificação de aspectos que necessitam ser aperfeiçoados; e

II - disponibilizar ferramentas e orientações para a realização de auditorias de gestão de riscos em organizações públicas, bem como orientar sobre a forma e o conteúdo do relatório.

Art. 2º A Secretaria de Métodos e Suporte ao Controle Externo (Semec) manterá atualizado o documento de que trata o artigo anterior, cabendo-lhe, ainda, o esclarecimento de dúvidas e o recebimento de sugestões para o seu aperfeiçoamento.

Art. 3º Fica revogada a Portaria-Segecex nº 9, de 18 de maio de 2017, que aprovou o documento "Roteiro de Auditoria de Gestão de Riscos".

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

CLÁUDIO SOUZA CASTELLO BRANCO

ANEXO ÚNICO À PORTARIA-SEGECEX Nº 2, DE 22 DE JANEIRO DE 2018.

TRIBUNAL DE CONTAS DA UNIÃO
SECRETARIA-GERAL DE CONTROLE EXTERNO
SECRETARIA DE MÉTODOS E SUPORTE AO CONTROLE EXTERNO

ROTEIRO DE AVALIAÇÃO DE MATURIDADE DA GESTÃO DE RISCOS

SEGECEX / ADGECEX / SEMEC
JANEIRO - 2018

TRIBUNAL DE CONTAS DA UNIÃO

RESPONSABILIDADE PELO CONTEÚDO
Tribunal de Contas da União
Secretaria de Métodos e Suporte ao Controle Externo da Secretaria-Geral de Controle Externo

Brasil. Tribunal de Contas da União.
Roteiro de Avaliação de Maturidade da Gestão de Riscos: Tribunal de Contas da União. – Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018.
123 p.

1. Gestão de riscos, governança, accountability. 2. Auditoria, metodologia. I. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

SUMÁRIO

1. INTRODUÇÃO

1.1. FUNDAMENTO E PROPÓSITO DO ROTEIRO

1. Desde 2011, o TCU vem estabelecendo objetivos estratégicos voltados para a promoção e indução de práticas de gestão de riscos na administração pública. O plano estratégico em vigor (PET 2015-2021) contém o objetivo de:

> *Induzir o aperfeiçoamento da gestão de riscos e controles internos da Administração Pública.*

2. Conhecer o nível de maturidade e identificar os aspectos da gestão de riscos que necessitam ser aperfeiçoados nas organizações públicas constitui um subsídio relevante para que o TCU possa fazer recomendações e monitorar planos de ação com vistas a aprimorar esse importante componente da governança na administração pública.

3. Com esse objetivo, o TCU realizou levantamento, entre novembro de 2012 e fevereiro de 2013, envolvendo 65 entidades da administração federal indireta, para avaliar a maturidade da gestão de riscos nessas organizações e desenvolver um indicador que pudesse ser aplicado para medir o nível de maturidade de entidades públicas na gestão de riscos (BRASIL, 2013). Para isso foi concebido um modelo de avaliação que incorpora critérios das melhores práticas internacionais em uso no setor público, notadamente os modelos COSO GRC (COSO, 2004), britânico (UK, 2004 e 2009) e a norma ABNT NBR ISO 31000 Gestão de Riscos – princípios e diretrizes (ABNT, 2009). Adicionalmente, foram realizadas auditorias em sete entidades selecionadas do levantamento, com o objetivo de desenvolver o método e os papéis de trabalho para conduzir auditorias de gestão de riscos, com base nos critérios do modelo de avaliação desenvolvido. Este roteiro foi elaborado a partir da experiência adquirida nesses trabalhos, com o propósito de:

   a) apoiar a avaliação da maturidade da gestão de riscos de organizações públicas e a identificação de aspectos que necessitam ser aperfeiçoados; e

   b) fornecer orientação e disponibilizar ferramentas para a realização de auditorias de gestão de riscos em organizações públicas, de maneira eficiente e eficaz, bem como orientar sobre a forma e o conteúdo do relatório.

1.2. CONCEITOS FUNDAMENTAIS

4. São conceitos-chaves para a leitura deste roteiro[1]:

   a) **Evento** – um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a realização de objetivos de modo negativo, positivo ou ambos.

   b) **Risco** – possibilidade de ocorrência de um evento que afete adversamente a realização de objetivos.

   c) **Oportunidade** – possibilidade de ocorrência de um evento que afete positivamente a realização de objetivos.

   d) **Risco inerente** – nível de risco antes da consideração de qualquer ação de mitigação.

   e) **Risco residual** – nível de risco depois da consideração das ações adotadas pela gestão (por exemplo, controles internos) para reduzir o risco inerente.

   f) **Apetite a risco** – expressão ampla de quanto risco uma organização está disposta a enfrentar para implementar sua estratégia, atingir seus objetivos e agregar valor para as partes interessadas, no cumprimento de sua missão.

   g) **Tolerância a risco** – nível de variação aceitável no desempenho em relação à meta para o cumprimento de um objetivo específico, em nível tático ou operacional.

1.3. ABORDAGENS DO RISCO EM TRABALHOS DO TCU

5. O risco é inerente a todas as atividades humanas, em todos os campos. No âmbito da gestão de recursos públicos, o risco está presente tanto nas atividades que envolvem a aplicação desses recursos, como naquelas que envolvem a fiscalização e o controle da sua boa e regular aplicação, ambas relacionadas à atuação do Tribunal. Disso decorrem variadas abordagens do risco nos trabalhos do TCU, destacando-se principalmente as quatro a seguir:

1.3.1. Avaliação de riscos para o plano de controle externo

6. Avaliação de riscos que afetam objetos de nível macro, presentes no universo do controle externo, tais como políticas, programas, projetos e atividades governamentais. Os objetivos da avaliação de riscos para o plano de controle externo são revelar quais situações são mais importantes e requerem a atuação do TCU, selecionar os objetos de controle expostos a maiores riscos e estabelecer prioridades para as ações de controle externo.

[1] Para outros termos relacionados à terminologia de risco, consulte o Glossário adicionado ao final deste documento ou a norma ABNT ISO GUIA 73: *Gestão de Riscos: Vocabulário (ABNT, 2009a)*.

1.3.2. Avaliação de riscos em levantamentos

7. Avaliação de riscos relacionados a um objeto específico de controle externo, com o objetivo de revelar as áreas desses objetos que estão expostas a riscos significativos, analisar como a gestão responde a esses riscos, com vistas a priorizá-las para futuros trabalhos, bem como avaliar a viabilidade da realização de fiscalizações.

1.3.3. Avaliação de riscos em auditorias

8. Avaliação de riscos realizada na fase de planejamento das auditorias com objetivo de subsidiar a definição do escopo e as questões de auditoria (objetivos de auditoria específicos), selecionar os procedimentos de auditoria que sejam os mais eficientes e eficazes para abordá-los e determinar a sua natureza, época e extensão, a fim de reduzir ou administrar o risco de chegar a conclusões inapropriadas e fornecer um relatório de auditoria que seja inadequado às circunstâncias (ISSAI 100, 40 e 46). Geralmente esse processo envolve a:
   a) identificação dos objetivos do objeto de auditoria no contexto dos objetivos da organização e análise dos riscos inerentes associados, que sejam relevantes para o trabalho;
   b) estimativa do risco de controle mediante avaliação das respostas que a gestão adota para mitigar os riscos identificados e avaliados como significativos, incluindo o desenho e a implementação de controles internos;
   c) estimativa da significância dos riscos que ainda remanescem após considerado o efeito das respostas adotadas pela gestão, mediante combinação dos dois riscos anteriores; e
   d) definição do escopo, das questões de auditoria (objetivos específicos) e da estratégia de auditoria, focando os riscos de maior significância e os controles-chaves, de modo a satisfazer os objetivos do trabalho com o nível de confiança requerido.

1.3.4. Auditoria de gestão de riscos

9. Auditoria realizada com o objetivo de avaliar a maturidade da gestão de riscos em organizações públicas e identificar os aspectos que necessitam ser aperfeiçoados, mediante avaliação dos princípios, da estrutura e demais elementos do processo de gerenciamento de riscos colocados em prática pela organização para identificar, analisar, avaliar, tratar e comunicar riscos que possam impactar o alcance dos seus objetivos e, por conseguinte, os resultados que devem ser entregues à sociedade na forma de bens e serviços públicos. Este roteiro trata dessa abordagem.

1.4. COMO USAR ESTE ROTEIRO

10. O uso deste roteiro não dispensa, de forma alguma, a observância dos padrões e a conformidade

com os requisitos estabelecidos no Manual de Auditoria Operacional (BRASIL, 2010), nas NAT (BRASIL, 2011) e nas ISSAI correspondentes à auditoria operacional, ao contrário, o roteiro deve ser lido e seguido em conjunto com esses documentos, buscando-se orientações adicionais ou mais abrangentes, a menos que o assunto seja especificamente e exaustivamente tratado no roteiro. Além desta introdução, o roteiro está organizado nos seguintes capítulos:

- O capítulo 2 descreve a importância da gestão de riscos para apoiar a governança e a gestão das organizações do setor público no cumprimento das suas obrigações de *accountability*, destacando as características, as incertezas e os desafios envolvidos no seu cumprimento.
- O capítulo 3 fornece uma visão geral da gestão de riscos, tratando dos princípios, da estrutura e do processo, de modo a fornecer entendimento conceitual da gestão de riscos como objeto de auditoria.
- O capítulo 4 apresenta as características básicas dos principais modelos reconhecidos internacionalmente, que são utilizados pelas organizações para implementar e avaliar uma gestão de riscos de forma consistente e sistematizada.
- O capítulo 5 descreve o processo de gestão de riscos, detalha as suas etapas e as principais atividades em cada etapa, com o objetivo de fornecer uma base para que os auditores possam avaliar a qualidade dos processos de gestão de riscos das organizações.
- O capítulo 6 apresenta o modelo de avaliação da maturidade organizacional em gestão de riscos desenvolvido pelo TCU e o seu método de determinação do nível de maturidade.
- O capitulo 7 descreve as características específicas, os objetivos e os padrões gerais da auditoria de gestão de riscos, enquanto o capítulo 8 proporciona o método para a sua realização.
- No capítulo 9 é disponibilizado um glossário com definições de termos aplicáveis à gestão de riscos, visando facilitar a leitura e compreensão do roteiro.
- No capítulo 10 encontram-se as referências utilizadas na elaboração do roteiro.
- Finalmente, o capítulo 11, traz dois apêndices com ferramentas para facilitar a realização das auditorias de gestão de riscos de maneira eficiente e eficaz: os critérios para avaliação da gestão de riscos e as suas fontes, e a matriz de planejamento para realizar a avaliação.
- Acompanha ainda o roteiro uma planilha em Excel para ajudar o auditor a registrar o resultado final da avaliação das evidências de auditoria e calcular automaticamente os índices de maturidade de cada aspecto, bem como determinar o nível de maturidade global da gestão de riscos da organização.

2. IMPORTÂNCIA DA GESTÃO DE RISCOS

11. Este capítulo destaca a importância da gestão de riscos para apoiar os agentes da governança e da gestão das organizações públicas no cumprimento de suas responsabilidades de gerar, preservar e entregar valor público em benefício da sociedade (*accountability*).

12. A busca dos objetivos de uma organização pública envolve riscos decorrentes da natureza de suas atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração pública, bem como da necessidade de mais transparência e prestação de contas e de cumprir variados requisitos legais e regulatórios.

13. Assim, as organizações públicas necessitam gerenciar riscos, identificando-os, analisando-os e, em seguida, avaliando se eles devem ser modificados por algum tratamento, de maneira a propiciar segurança razoável para que os objetivos sejam alcançados.

14. A gestão de riscos corretamente implementada e aplicada de forma sistemática, estruturada e oportuna gera benefícios que impactam diretamente cidadãos e outras partes interessadas da organização ao viabilizar o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos, o aumento do grau de eficiência e eficácia no processo de criação, proteção e entrega de valor público, otimizando o desempenho e os resultados entregues à sociedade.

2.1. RELAÇÃO DA GESTÃO DE RISCOS COM A *ACCOUNTABILITY* PÚBLICA

15. O elemento basilar da *accountability* pública é o dever que têm as pessoas ou entidades às quais se tenha confiado a gestão de recursos públicos, de assumir responsabilidades pela realização de objetivos na implementação de políticas, no fornecimento de bens e serviços de interesse público, e de prestar contas à sociedade e a quem lhes delegou essas responsabilidades sobre o desempenho, os resultados obtidos e o uso apropriado dos recursos. É ainda obrigação de demonstrar que administrou ou controlou os recursos mediante estratégias que permitiriam segurança razoável do alcance desses objetivos. O não cumprimento dessas obrigações de *accountability* é cada vez mais percebido pela sociedade como quebra de responsabilidades confiadas.

16. Para cumprir tais obrigações, a gestão estratégica das organizações públicas (os órgãos de governança e a alta administração) define o direcionamento estratégico e estabelece a liderança para que os órgãos e as entidades do setor público possam cumprir suas missões. A gestão tática e operacional, por sua vez, implementa a estratégia para realizar os objetivos.

17. As ações da governança e da gestão, de forma integrada, buscam entregar o melhor valor para

os cidadãos na forma de políticas, bens e serviços públicos que atendam às suas necessidades e expectativas legítimas, e apresentem um retorno condizente com os recursos colocados à sua disposição, oriundos dos tributos arrecadados e de outras fontes de recursos que oneram o cidadão de forma direta ou indireta, como o endividamento público.

18. Para cumprir os objetivos inerentes às obrigações de *accountability*, tanto a tomada de decisão na definição da estratégia, por parte dos órgãos de governança e da alta administração, como a sua implementação, por parte da gestão executiva, enfrentam influências de fatores internos e externos, que tornam incerto se e quando tais objetivos serão atingidos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de "risco" (ABNT, 2009).

2.2. RELAÇÃO DA GESTÃO DE RISCOS COM A GOVERNANÇA

19. O desafio da governança nas organizações públicas é determinar quanto risco aceitar na busca do melhor valor para os cidadãos e outras partes interessadas, o que significa prestar o serviço de interesse público da melhor maneira possível, equilibrando riscos e benefícios (INTOSAI, 2007). O instrumento da governança para lidar com esse desafio é a gestão de riscos, um processo estratégico e fundamental para as organizações do setor público, e um componente relevante de seus sistemas de governança (BRASIL, 2014).

20. Uma gestão de riscos eficaz melhora as informações para o direcionamento estratégico e para as tomadas de decisões de responsabilidade da governança, contribui para a otimização do desempenho na realização dos objetivos de políticas e serviços públicos e, consequentemente, para o aumento da confiança dos cidadãos nas organizações públicas, além de prevenir perdas e auxiliar na gestão de incidentes e no atendimento a requisitos legais e regulamentares (BRASIL, 2014).

21. Integrar a gestão de riscos como elemento-chave da responsabilidade gerencial, implantar uma abordagem de controle interno baseada no risco e incluir a gestão de riscos nos programas de apoio ao desenvolvimento das competências dos gestores públicos são algumas das recomendações do relatório *"Avaliação da OCDE sobre o Sistema de Integridade da Administração Pública Federal Brasileira - Gerenciando riscos por uma administração pública mais íntegra"*, que também enfatiza a necessidade de promoção de uma liderança comprometida com a criação de uma cultura de gestão que promova a gestão de riscos como ferramenta estratégica do sistema de governança (OCDE, 2011).

3. VISÃO GERAL DA GESTÃO DE RISCOS

22. Este capítulo descreve os fundamentos e os aspectos estruturais da gestão de riscos, visando fornecer um entendimento conceitual básico da gestão de riscos como objeto de auditoria, sem a pretensão de cobrir todo o conhecimento necessário para uma equipe conduzir com êxito uma auditoria de gestão de riscos.

23. Os membros da equipe designada para realizar uma auditoria de gestão de riscos devem possuir, coletivamente, o conhecimento, as habilidades e a competência necessários para concluir com êxito a auditoria (ISSAI 100, 39; NAT, 52). Portanto, deve-se buscar satisfazer esses requisitos por meio de treinamento, compartilhamento de experiências e outros recursos oferecidos pelo Tribunal, como tutorias, e, principalmente, por meio do estudo do material indicado nas referências deste roteiro.

24. Em termos gerais, "gestão de riscos" refere-se à arquitetura (princípios, estrutura e processo) para gerenciar riscos eficazmente, enquanto "gerenciar riscos" refere-se à aplicação dessa arquitetura para o gerenciamento dos riscos nos diversos contextos específicos em que os objetivos de uma organização são perseguidos (ABNT, 2009).

25. A gestão de riscos compreende todas as atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. Não é uma atividade autônoma, separada das demais, mas sim parte de todos os processos organizacionais, incluindo o planejamento estratégico, os projetos e processos de gestão em todos os níveis da organização (ABNT, 2009). É parte integrante e indissociável das responsabilidades administrativas e inclui atividades como:
    a) estabelecer o ambiente apropriado, incluindo a estrutura para gerenciar riscos;
    b) definir, articular e comunicar os objetivos e o apetite a risco;
    c) identificar potenciais ameaças ou oportunidades ao cumprimento dos objetivos;
    d) avaliar os riscos (i.e., determinar o impacto e a probabilidade da ameaça se materializar);
    e) selecionar e implantar respostas aos riscos, por meio de controles e outras ações;
    f) comunicar as informações sobre os riscos de forma consistente em todos os níveis;
    g) monitorar e coordenar os processos e os resultados do gerenciamento de riscos; e
    h) fornecer avaliação (*assurance*) quanto à eficácia com que os riscos são gerenciados (ABNT, 2009; IIA, 2009a).

26. Essas atividades envolvem responsabilidades de pessoas, cargos e funções em todos os níveis da organização, conforme abordado no tópico 3.2.

3.1. PRINCÍPIOS, ESTRUTURA E COMPONENTES

27. Princípios da gestão de riscos representam as condições que precisam estar incorporadas aos componentes ou à estrutura e ao processo de gestão de riscos, para que ela seja eficaz e se torne parte da cultura da organização, traduzindo-se em um conjunto compartilhado de valores, comportamentos e práticas que caracterizam como a entidade aborda o risco.

28. Estrutura de gestão de riscos é a maneira como a entidade se organiza para gerenciar os riscos do negócio, representando o conjunto de componentes e arranjos organizacionais para a concepção, a implementação, o monitoramento, a análise crítica e a melhoria contínua da gestão de riscos por toda a organização, incluindo a política de gestão de riscos, os manuais, os recursos, a definição de responsabilidades e objetivos que permitirão incorporar a gestão de riscos em todos os níveis da organização (ABNT, 2009).

29. Gerenciamento de riscos representa as atividades realizadas pelas pessoas em todos os níveis da organização, desde a definição da estratégia até as atividades operacionais, aplicando os princípios, a estrutura e o processo de gestão de riscos para dar suporte à tomada de decisões e à implementação de ações para manter os riscos dentro do nível de apetite e das tolerâncias a riscos estabelecidos pela administração, proporcionando, assim, segurança razoável do cumprimento dos objetivos da organização (INTOSAI, 2007).

3.2. PAPÉIS E RESPONSABILIDADES

30. Cada pessoa na organização tem uma parcela de responsabilidade na gestão de riscos e todo o pessoal deve receber uma mensagem clara da governança e da alta administração de que as responsabilidades de gerenciamento de riscos devem ser levadas a sério (INTOSAI, 2007). Responsabilidades claras devem ser definidas para que cada grupo de profissionais (constante da ilustração da figura 3.1) entenda os limites de suas responsabilidades e como os seus cargos se encaixam na estrutura geral de gestão de riscos e controle da organização (IIA, 2013).

31. A alta administração e os órgãos de governança têm, coletivamente, a responsabilidade e o dever de prestar contas sobre o estabelecimento dos objetivos da organização, a definição de estratégias para alcançá-los e o estabelecimento de estruturas e processos de governança para melhor gerenciar os riscos durante a realização dos objetivos (IIA, 2013). É, portanto, uma responsabilidade primária dessas instâncias assegurar a existência, o monitoramento e a avaliação de um efetivo sistema de gestão de riscos e controle interno, bem como utilizar as informações resultantes desse sistema para apoiar seus processos decisórios (TCU, 2014).

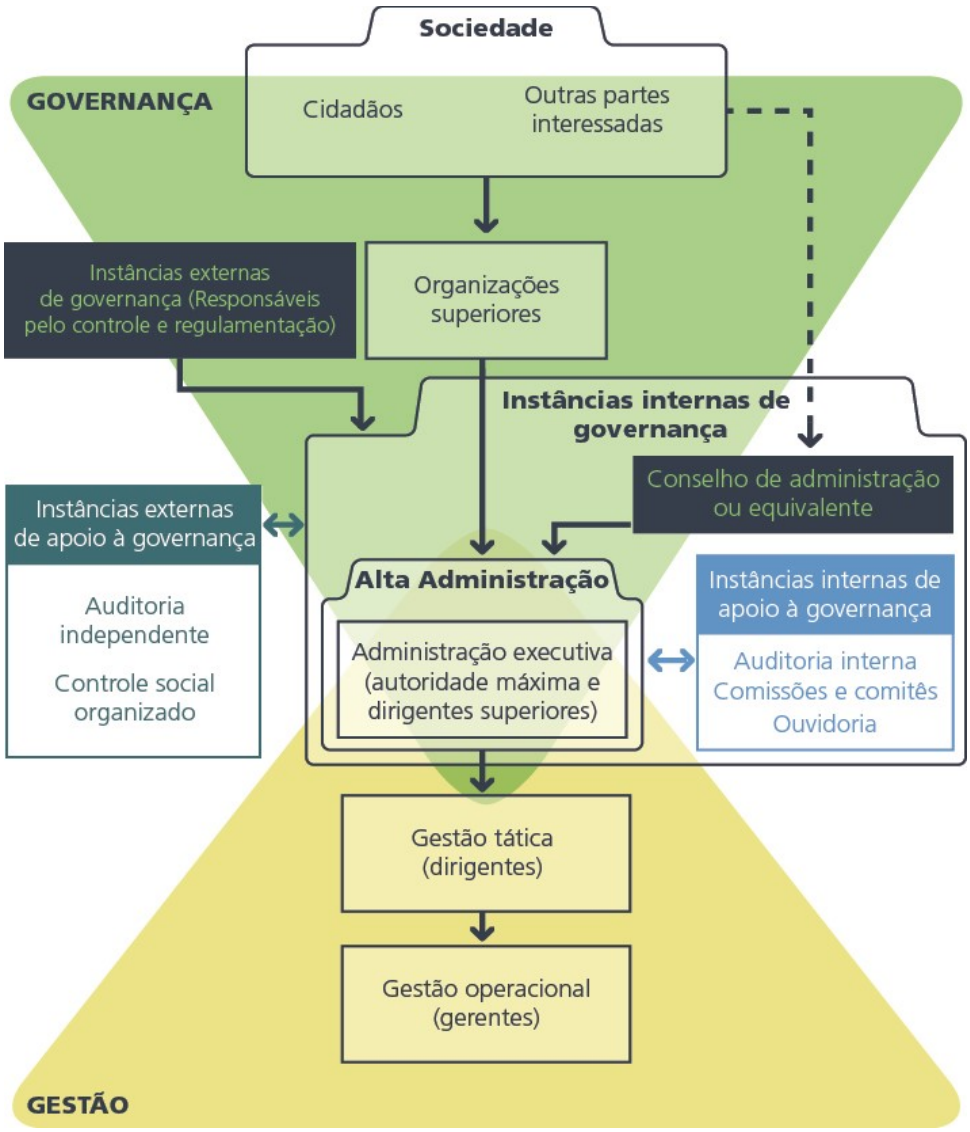


Figura 3.1: Sistema de governança de órgãos e entidades da administração pública (TCU, 2014).

32. Na prática, os órgãos de governança decidem e delegam a implantação e operação da gestão de riscos aos executivos da gestão, assumindo um papel de supervisão desses processos. Além disso, usam os serviços de asseguração da auditoria interna para monitorar e avaliar a eficácia dos processos de gerenciamento de riscos e controles por toda a organização.

33. A supervisão da gestão de riscos pelos órgãos de governança envolve:

a) saber até que ponto a administração estabeleceu um gerenciamento de risco eficaz;

b) estar ciente e de acordo com o apetite a risco;

c) revisar o portfólio de riscos assumidos em contraste com o apetite a risco; e

d) ser notificado em relação aos riscos mais significativos e saber se a administração está respondendo a esses riscos adequadamente (COSO, 2004).

34. A administração é diretamente responsável pela concepção, estruturação e implementação da gestão de riscos. Em qualquer organização, o presidente ou dirigente máximo é o depositário final dessa responsabilidade, cabendo-lhe assumir a iniciativa.

35. Os demais executivos apoiam a cultura e gerenciam os riscos dentro de suas esferas de responsabilidade, conforme as tolerâncias a risco estabelecidas, alinhadas ao apetite a risco da organização. São eles e os seus gerentes nos níveis operacionais que têm a propriedade dos riscos e a responsabilidade primária pela identificação e pelo gerenciamento dos riscos em suas áreas, conduzindo procedimentos de risco diariamente e mantendo controles internos eficazes sobre as operações (COSO, 2004).

36. Os funcionários da linha de frente, que lidam diariamente com questões operacionais críticas, estão em melhores condições para reconhecer e comunicar riscos que podem surgir e essa responsabilidade é geralmente atribuída a todos os funcionários, cujo cumprimento exige canais de comunicação para cima e clara disposição para ouvir (INTOSAI, 2007).

37. Em organizações grandes, e dependendo de fatores como o ambiente e o setor de atuação, a complexidade das operações, a natureza das atividades e o grau de regulamentação, pode haver uma função separada para coordenar as atividades de gestão de riscos por toda a organização e para fornecer habilidades e conhecimentos especializados.

38. A função de coordenar as atividades de gestão de riscos é mais bem-sucedida quando claramente estabelecida para dar suporte e facilitar os gestores a estabelecer processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade. São responsabilidades dessa função, por exemplo:

    e) fornecer metodologias e ferramentas para unidades de negócios com a finalidade de identificar, avaliar e gerenciar riscos;

    f) definir funções e responsabilidades pela gestão de riscos nas unidades de negócio;

    g) promover competência em gerenciamento de riscos;

    h) orientar a integração do gerenciamento de riscos com outras atividades de gestão;

    i) estabelecer uma linguagem uniforme de gestão de riscos, que inclua medidas comuns de probabilidade, impacto e categorias de riscos;

    j) comunicar ao presidente e à diretoria executiva o andamento do gerenciamento de riscos (COSO, 2004; IIA, 2009a).

39. Além disso, pode haver uma função de *compliance* que monitora riscos específicos de não conformidade com leis e regulamentos, reportando diretamente aos órgãos de governança, reguladores ou à alta administração, ou múltiplas funções com responsabilidades por tipos específicos de monitoramento da conformidade, como saúde e segurança, meio ambiente, licitações e contratos, controle de qualidade; bem como uma função de controladoria que monitore os riscos financeiros e questões de reporte financeiro (IIA, 2013).

40. Em organizações pequenas, com operações e regulamentação de baixa complexidade, pode ser que não exista uma estrutura ou sistema formal de gestão de riscos e a responsabilidade pela coordenação das atividades de gerenciamento de riscos pode ser atribuída a uma área que cuida de planejamento ou controladoria, ou ainda a uma assessoria do dirigente máximo.

41. A função de auditoria interna tem o papel de auxiliar a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança (IIA, 2009). A Figura 3.2 indica quais são os papéis fundamentais que auditoria interna deve assumir; os que pode assumir, com salvaguardas à sua independência e a objetividade dos auditores; e os que não deve assumir, porque comprometeriam esses valores fundamentais para que a auditoria forneça asseguração, livre que quaisquer influências, sobre a eficácia dos processos de gerenciamento de riscos e controles da organização.

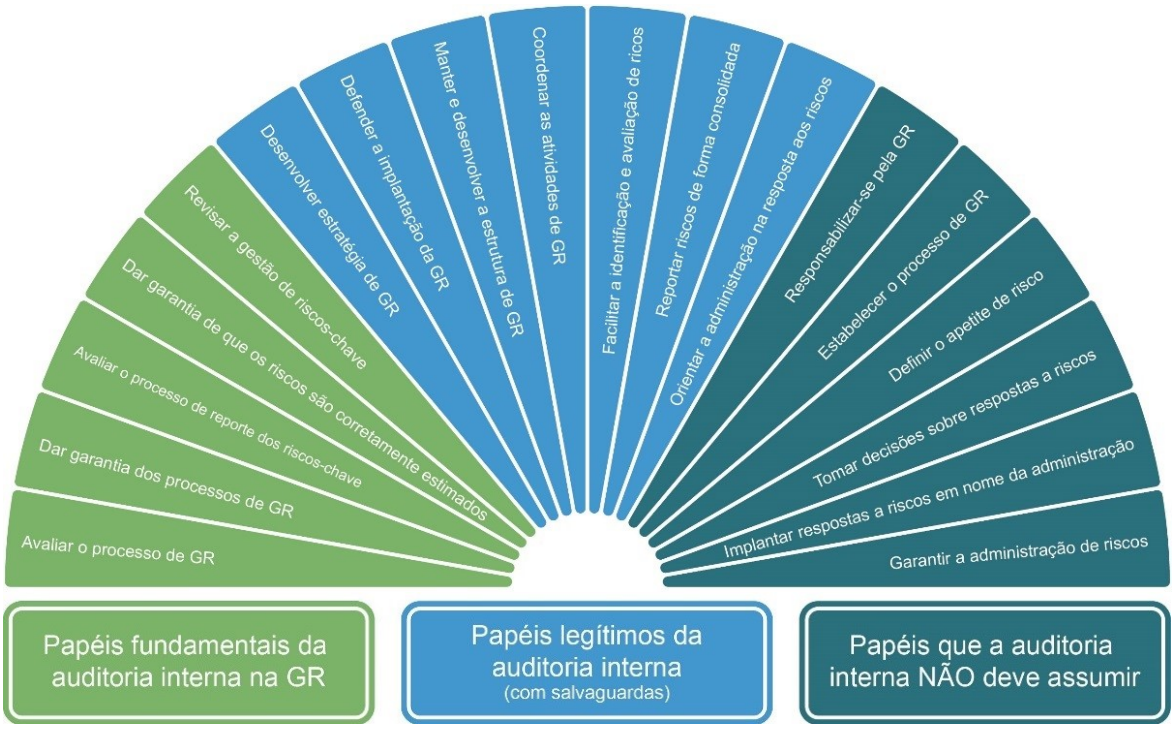


Figura 3.2: O papel da auditoria interna no gerenciamento de riscos (IIA, 2009a).

42. O papel fundamental da auditoria interna na gestão de riscos é fornecer asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gerenciamento de riscos operam de maneira eficaz e que os riscos significativos do negócio são gerenciados adequadamente em todos os níveis da organização. A auditoria interna deve ter uma compreensão clara da estratégia da organização e de como ela é executada, quais os riscos associados e como esses riscos estão sendo gerenciados. As atividades indicadas à esquerda da figura representam esse papel.

43. A estratégia da organização deve ser um elemento fundamental no desenvolvimento dos planos anuais de auditoria, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e a garantir que os seus recursos são alocados em áreas de maior risco (IIA 2120-3). Além disso, a fim de habilitar a auditoria interna a auxiliar a administração a identificar os riscos mais significativos para o alcance dos objetivos da organização, seus trabalhos devem utilizar uma abordagem baseada em risco, viabilizando que sejam efetivamente formulados, implementados e monitorados planos de ação para o tratamento dos riscos identificados.

44. Quando uma organização não dispõe de um processo formal de gestão de riscos, a auditoria interna deve levar o fato à atenção dos órgãos de governança e da alta administração, recomendando o estabelecimento de tal processo, podendo assumir um envolvimento direto nos primeiros estágios de sua implementação, mediante trabalhos de consultoria, como indicado no centro da Figura 3.2.

> *Em situações em que a organização não tenha processos formais de gestão de risco, o responsável pela auditoria precisa discutir formalmente com a administração e o conselho as suas obrigações de entender, gerenciar e monitorar os riscos da organização* (IIA 2009a, Norma 2120-1, 3).

45. Entretanto, se a auditoria interna ainda não tiver adotado uma abordagem baseada em risco, representada pelas atividades de asseguração descritas à esquerda da figura, é improvável que esteja apta a desempenhar as atividades de consultoria descritas no centro da figura (IIA, 2009a).

46. À medida que a maturidade da gestão de riscos da organização evolui e o gerenciamento de riscos torne-se mais inserido nas operações do negócio, o papel da auditoria interna em promover o gerenciamento de riscos vai se reduzindo, voltando a se concentrar em seu papel de asseguração (IIA, 2009a).

3.3. AS TRÊS LINHAS DE DEFESA

47. Em entidades onde não há uma estrutura ou sistema formal de gestão de riscos, como pode ser o caso de organizações pequenas (parágrafo 40), ainda assim é possível ajudar a aumentar a compreensão e a eficácia da abordagem de risco da organização, melhorando a delegação e a coordenação das tarefas essenciais de gerenciamento de riscos mediante a utilização de uma abordagem como a das *Três Linhas de Defesa* (IIA, 2013).

48. A abordagem das *Três Linhas de Defesa*, embora não seja um modelo de gestão de riscos, é uma forma simples e eficaz para melhorar a comunicação e a conscientização sobre os papéis e as responsabilidades essenciais de gerenciamento de riscos e controles, aplicável a qualquer organização – não importando o seu tamanho ou a sua complexidade – ainda que não exista uma estrutura ou sistema formal de gestão de riscos.

49. Por essa abordagem, há três linhas de defesa, ou grupos de responsáveis envolvidos com o gerenciamento de riscos, como explanado a seguir:

1º) **Funções que gerenciam e têm propriedade de riscos** (parágrafos 35-36): a gestão operacional e os procedimentos diários de controles constituem a primeira linha de defesa no gerenciamento de riscos. A gestão operacional serve naturalmente como a primeira linha de defesa, porque os controles são desenvolvidos como sistemas e processos sob sua orientação e responsabilidade. É nesse nível que se identificam, avaliam e controlam riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos e garantindo que as atividades estejam de acordo com as metas e objetivos.

2º) **Funções que supervisionam riscos** (parágrafos 37-39 e 40): a segunda linha defesa é constituída por funções estabelecidas para garantir que a primeira linha funcione como pretendido no tocante ao gerenciamento de riscos e controles. As funções específicas variam muito entre organizações e setores, mas são, por natureza, funções de gestão. Seu papel é coordenar as atividades de gestão de riscos, monitorar riscos específicos (funções de *compliance* ou de conformidade), ajudar a desenvolver controles e ou monitorar riscos e controles da primeira linha de defesa;

3º) **Funções que fornecem avaliações independentes** (parágrafos 41-46): a auditoria interna constitui a terceira linha de defesa no gerenciamento de riscos, fornecendo avaliações (asseguração) independentes e objetivas sobre os processos de gerenciamento de riscos, controle e governança aos órgãos de governança e à alta administração, abrangendo uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda

de ativos; confiabilidade e a integridade dos processos de reporte; conformidade com leis e regulamentos) e elementos da estrutura de gerenciamento de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

50. Embora os órgãos de governança e a alta administração (parágrafos 32-34) não estejam considerados entre as três linhas de defesa, nenhuma consideração sobre gerenciamento de riscos estaria completa sem levar em conta, em primeiro lugar, os papéis essenciais dessas duas instâncias, que são as principais partes interessadas e as que estão em melhor posição para instituir e assegurar o bom funcionamento das três linhas de defesa no processo de gerenciamento de riscos e controles da organização (IIA, 2013).

51. Órgãos de controle externo, reguladores, auditores externos e outros órgãos externos estão fora da estrutura da organização, mas podem desempenhar um papel importante em sua estrutura geral de governança e controle, podendo ser considerados linhas adicionais de defesa, que fornecem avaliações tanto às partes interessadas externas da organização, como ao próprio órgão de governança e à alta administração da entidade (IIA, 2013).

52. A Figura 3.3 ilustra como responsabilidades específicas são delegadas e coordenadas dentro da organização para que cada grupo de profissionais entenda seus papéis, os limites de suas responsabilidades e como seus cargos se encaixam na estrutura de gestão de riscos e controle, fornecendo uma contribuição significativa para a abordagem de risco da organização.

Figura 3.3: Modelo de Três Linhas de Defesa (IIA, 2013).

4. MODELOS DE GESTÃO DE RISCOS

53. Para lidar com riscos e aumentar a chance de alcançar objetivos, as organizações adotam desde abordagens informais até abordagens altamente estruturadas e sistematizadas de gestão de riscos, dependendo do seu porte e da complexidade de suas operações. Este capítulo apresenta os principais modelos reconhecidos internacionalmente, que são utilizados pelas organizações para implementar e avaliar uma gestão de riscos de forma consistente e sistematizada.

54. Todavia, somente as características gerais desses modelos são apresentadas, devendo os membros da equipe designada para realizar uma auditoria de gestão de riscos aprofundar o seu entendimento a respeito de componentes, princípios e práticas recomendados por esses modelos, mediante estudo do material indicado nas referências deste roteiro e de outros recursos oferecidos pelo TCU, conforme mencionado no parágrafo 23.

55. A implantação da gestão de riscos em uma organização é um processo de aprendizagem organizacional, que começa com o desenvolvimento de uma consciência sobre a importância de gerenciar riscos e avança com a implementação de práticas e estruturas necessárias à gestão eficaz dos riscos. O ápice desse processo se dá quando a organização conta com uma abordagem consistente para gerenciar riscos em atividades relevantes, e com uma cultura organizacional profundamente aderente aos princípios e práticas da gestão de riscos.

56. Um princípio da gestão de riscos é que ela deve ser feita sob medida, alinhada com o contexto interno e externo da organização e com o seu perfil de riscos. O desenho e a implementação de estruturas e processos de gestão de riscos devem levar em consideração as necessidades específicas da organização em face dos objetivos que dão suporte à sua missão e dos riscos associados, envolvendo aspectos como natureza, complexidade, estratégia, contexto, estrutura, operações, processos, funções, projetos, produtos, serviços ou ativos e práticas empregadas (ABNT, 2009). Em qualquer situação, é importante que a organização se apoie em modelos reconhecidos como os apresentados neste capítulo.

57. Adotar padrões e boas práticas estabelecidos em modelos reconhecidos é uma maneira eficaz de estabelecer uma abordagem sistemática, oportuna e estruturada para a gestão de riscos, que contribua para a eficiência e a obtenção de resultados consistentes (ABNT, 2009), evitando que a organização seja aparelhada com uma coleção de instrumentos e procedimentos burocráticos, descoordenados, que mais dão a falsa impressão da existência de um sistema de gestão de riscos e controle do que garantam efetivamente os benefícios desejados.

4.1. COSO GRC 2004 – GERENCIAMENTO DE RISCOS – ESTRUTURA INTEGRADA

58. O COSO é o modelo de gestão de riscos predominante no cenário corporativo internacional, especialmente na América do Norte. Foi desenvolvido pela PricewaterhouseCoopers LLP, sob encomenda do COSO – Comitê das Organizações Patrocinadoras *(Committe Of Sponsoring Organizations of the Treadway Commission)*, com o propósito de fornecer uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o gerenciamento de riscos.

59. O modelo é apresentado na forma de uma matriz tridimensional, demonstrando uma visão integrada dos componentes que uma administração precisa adotar para gerenciar riscos de modo eficaz, no contexto dos objetivos e da estrutura em uma organização.

Figura 4.1: Modelo de Gestão de Riscos COSO 2004 (COSO, 2007).

a) a face superior do cubo indica as categorias de objetivos que são comuns a todas as organizações, e que a gestão de riscos deve fornecer segurança razoável para seu alcance.

b) a face frontal indica os componentes que devem estar presentes e em funcionamento para que a gestão de riscos seja eficaz. Esses componentes foram derivados da maneira ideal como uma administração deveria conduzir o negócio de uma organização.

c) a face lateral representa a estrutura da organização, incluindo unidades, áreas, funções, processos, projetos e todas as demais atividades que concorrem para a realização de seus objetivos, em todos os níveis. Os componentes de gerenciamento de riscos devem também estar presentes e em funcionamento em cada uma dessas áreas, funções e atividades, na proporção requerida pelos seus riscos, com base em julgamento da administração.

4.2. COSO GRC 2017 – INTEGRADO COM ESTRATÉGIA E DESEMPENHO

60. Em junho de 2016, o COSO colocou em consulta pública uma revisão do modelo de 2004, adotando o título provisório *"Alinhando Risco com Estratégia e Desempenho"*, para destacar a importância do gerenciamento de riscos tanto na definição quanto na execução da estratégia e no gerenciamento do desempenho organizacional. Com a incorporação dessa perspectiva, o modelo proporciona maior alinhamento às expectativas em torno das responsabilidades da governança e da alta administração no cumprimento das suas obrigações de *accountability*.

61. A revisão atualiza os componentes, adota princípios, simplifica definições, enfatiza o papel da cultura e melhora o foco no valor: como as organizações criam, preservam e entregam valor, inserindo o gerenciamento de riscos em três dimensões fundamentais para a gestão eficaz de uma organização: (I) a missão, a visão e os valores fundamentais; (II) os objetivos estratégicos e de negócios; e (III) o desempenho organizacional.

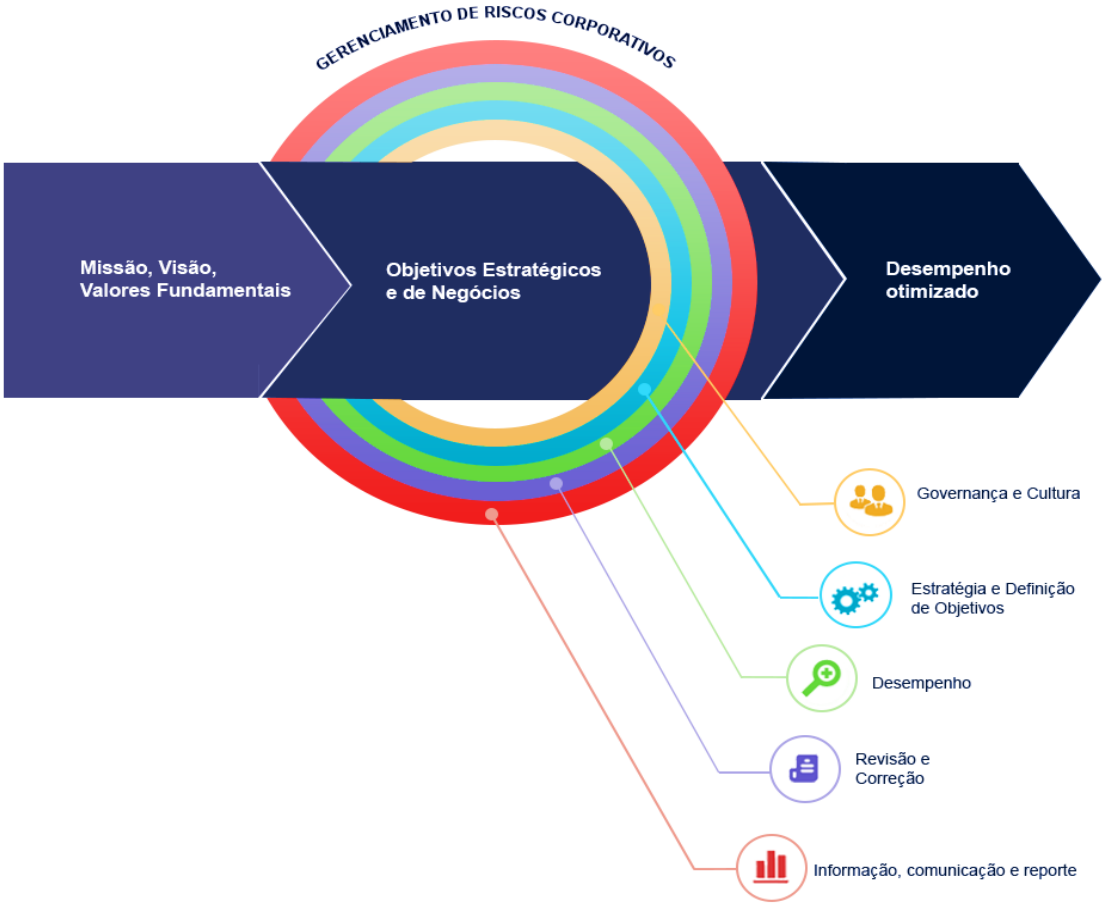


Figura 4.2: COSO Enterprise Risk Management – Aligning Risk with Strategy and Performance - Public Exposure (COSO, 2016, tradução própria).

62. Com a revisão, o modelo passa a integrar o gerenciamento de riscos com outros processos organizacionais, sobretudo os processos de governança, de definição da estratégia, de definição dos objetivos e de gestão do desempenho, indo além da tradicional aplicação do gerenciamento de riscos aos vários níveis da organização (por exemplo, no nível da entidade, de unidades de negócios, divisões etc.). A versão final, publicada em junho de 2017, recebeu o nome oficial de *Gerenciamento de Riscos Corporativos – Integrado com Estratégia e Desempenho*.

63. O novo modelo explora o papel do risco na seleção da estratégia, enfatizando dois aspectos principais que podem ter um grande efeito no valor da organização: a possibilidade da estratégia não se alinhar e as implicações das escolhas estratégicas. Isso torna ainda mais claras as responsabilidades da governança e da alta administração no seu papel de supervisionar e no seu dever de se envolver no processo de gerenciamento do risco corporativo de modo efetivo. Os aspectos enfatizados são:
    a) a possibilidade da estratégia – e, assim, os objetivos estratégicos e de negócios – não se alinhar com a missão, a visão e os valores fundamentais da organização; e
    b) as implicações da estratégia escolhida.

64. O novo modelo também melhora a integração da gestão de riscos com a gestão do desempenho, explorando como as práticas de gerenciamento de riscos apoiam a identificação e avaliação de riscos que impactam a implementação da estratégia e o alcance dos objetivos de negócios.

65. O modelo revisado reduz os componentes do gerenciamento de riscos de oito para cinco:
    a) Governança e cultura
    b) Estratégia e definição de objetivos
    c) Desempenho
    d) Revisão e correção
    e) Informação, comunicação e reporte

66. Associados aos componentes, foram adotados vinte princípios de gerenciamento de riscos, os quais representam diretrizes para práticas que podem ser aplicadas de diferentes maneiras por diferentes organizações, independentemente de tamanho ou setor, e cuja implementação permitirá que a governança e a administração tenham uma expectativa razoável de que a organização entende e é capaz de gerenciar os riscos associados com a sua estratégia e os seus objetivos de negócio, em um nível aceitável.

67. O COSO GRC 2004 continua sendo utilizado, porém a evolução das práticas, para convergir ao novo modelo, é um esforço fortemente recomendável.

4.3. ISO 31000 – GESTÃO DE RISCOS – PRINCÍPIOS E DIRETRIZES

68. A ISO 31000 fornece princípios e diretrizes para gerenciar qualquer tipo de risco em toda ou em parte de qualquer organização. Trata-se de uma norma geral, independentemente de indústria, setor ou área, e não concorre com outras normas sobre gestão de riscos em áreas específicas (ABNT, 2009).

69. Seus objetivos são servir como guia mestre em matéria de gestão de riscos e harmonizar os processos de gestão de riscos, fornecendo uma abordagem comum, que pode ser aplicada a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos (ABNT, 2009). Assim, sua lógica é bastante simples e estrutura-se em três partes fundamentais inter-relacionadas: os princípios, a estrutura e o processo de gestão de riscos, conforme ilustrado na Figura 4.3, a seguir.

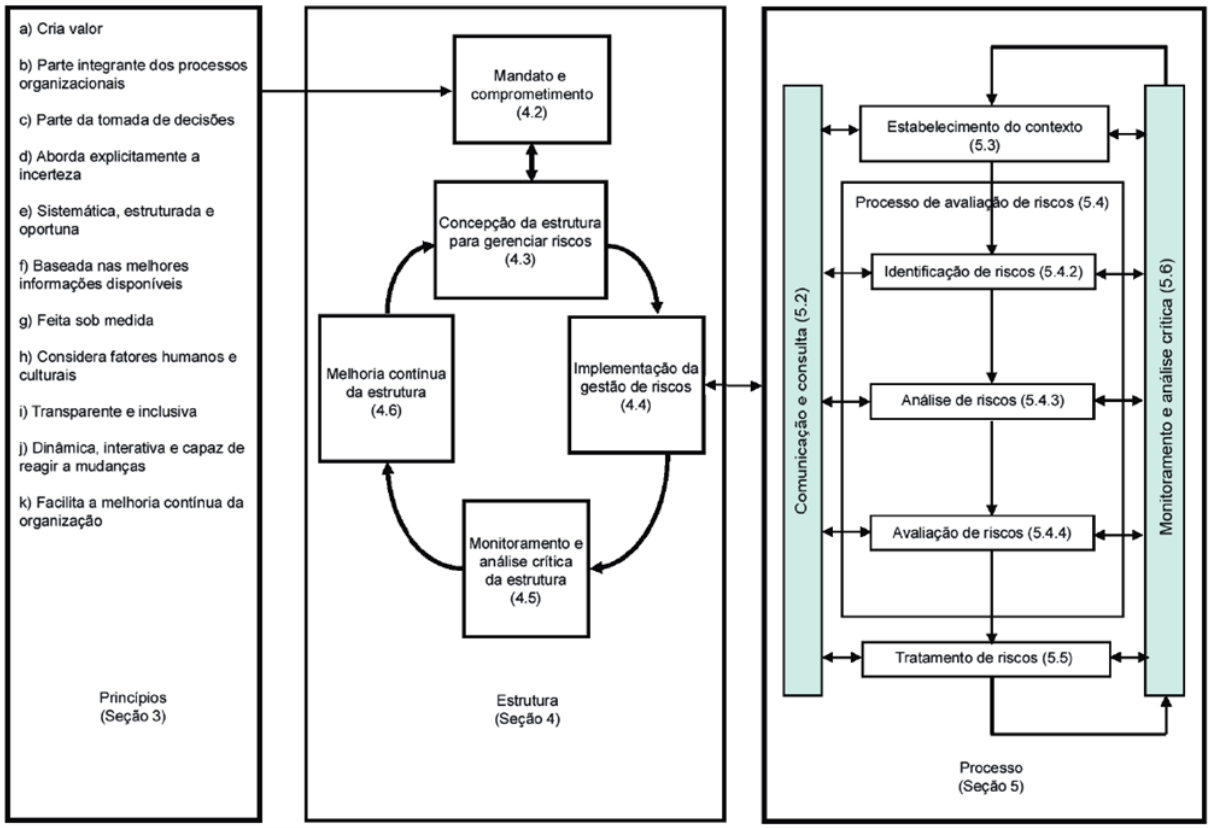


Figura 4.3: ISO 31000:2009 - Relacionamento entre Princípios, Estrutura e Processo (ABNT, 2009).

70. Uma contribuição fundamental da ISO 31000 é o detalhamento do processo de gestão de riscos, abordado no Capítulo 5 deste roteiro, cujo propósito é fornecer uma abordagem comum para a aplicação sistemática de políticas, procedimentos e práticas às atividades de gestão de riscos em organizações de qualquer área de atuação.

4.4. THE ORANGE BOOK – PRINCÍPIOS E CONCEITOS

71. O *The Orange Book Management of Risk - Principles and Concepts*, produzido e publicado pelo HM Treasury Britânico, foi a principal referência do programa de gerenciamento de riscos do governo do Reino Unido, iniciado em 2001. O modelo tem como vantagens, além de ser compatível com padrões internacionais de gerenciamento de riscos, como COSO e ISO 31000, apresentar uma introdução ao tema gerenciamento de riscos, tratando de forma abrangente e simples um tema complexo.

72. Com base no Orange Book, o então Ministério do Planejamento, Orçamento e Gestão produziu o Guia de Orientação para o Gerenciamento de Riscos, para apoiar o Modelo de Excelência do Sistema de Gestão Pública (GESPÚBLICA) e prover uma introdução ao tema gerenciamento de riscos (BRASIL, 2013).

73. Em 2009, oito anos após a edição do Orange Book, o governo britânico divulgou o *Risk Management Assessment Framework: a Tool for Departments* (UK, 2009), uma ferramenta para aferir a gestão de riscos nas organizações governamentais daquele país e identificar oportunidades de melhoria, derivada de um modelo de excelência de gestão utilizado por mais de trinta mil organizações, principalmente na Europa – *The EFQM Excellence Model* (EFQM, 2012). A ferramenta é estruturada em sete componentes (Figura 4.4) e, assim como este roteiro do TCU, pode ser aplicada por examinadores externos ou auto aplicada pelos gestores.

Figura 4.4: Modelo de avaliação da gestão de riscos do Reino Unido (UK, 2009).

74. Por ter sido desenvolvido especificamente para o setor público e por tratar-se de ferramenta com a mesma finalidade pretendida pelo TCU (avaliar a gestão de riscos e identificar oportunidades de melhoria), o modelo foi considerado no desenvolvimento da base conceitual do modelo de avaliação da maturidade em gestão de riscos do TCU.

5. PROCESSO DE GESTÃO DE RISCOS

75. Este capítulo descreve o processo de gestão de riscos, detalha as suas etapas e as principais atividades em cada etapa, de acordo com a norma ISO 31000, uma vez que essa norma tem o propósito de harmonizar os processos de gestão de riscos entre os diversos modelos e fornecer uma abordagem comum para aplicação em ampla gama de atividades (ABNT, 2009).

5.1. VISÃO GERAL DO PROCESSO DE GESTÃO DE RISCOS

76. O processo de gestão de riscos consiste na identificação, análise e avaliação de riscos, na seleção e implementação de respostas aos riscos avaliados, no monitoramento de riscos e controles, e na comunicação sobre riscos com partes interessadas, internas e externas, durante toda a aplicação do processo. Ele é aplicável a ampla gama das atividades da organização em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura (ambiente) de gestão de riscos da entidade.

77. As etapas do processo de gestão de riscos são as apresentadas na ilustração a seguir, descritas posteriormente nos subitens indicados entre parênteses na Figura 5.1.

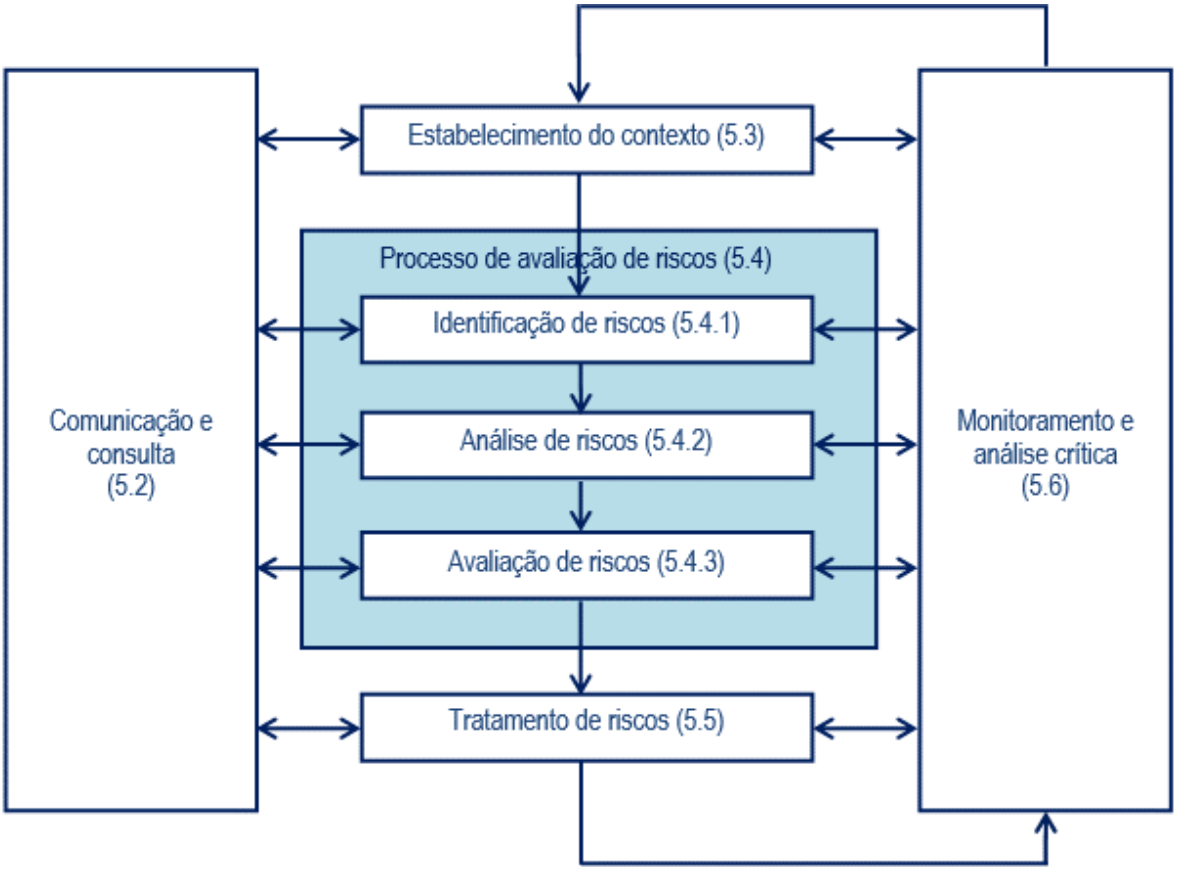


Figura 5.1: Processo de gestão de riscos da ISO 31000 (ABNT, 2009).

5.2. COMUNICAÇÃO E CONSULTA

78. Durante todas as etapas ou atividades do processo de gestão de riscos deve haver uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para:

a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;

b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização;

c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos.

79. Convém que seja desenvolvido um plano de comunicação e consulta interna e externa para apoiar essa atividade, seja por meio de um documento formal ou de uma lista de verificação.

5.3. ESTABELECIMENTO DO CONTEXTO

80. O estabelecimento do contexto envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas.

81. Contexto é o ambiente no qual uma organização[2] busca atingir os seus objetivos e estes são uma parte importante da definição daquele, pois a gestão de riscos ocorre no contexto dos objetivos da organização. Assim, os objetivos do processo, do projeto ou da atividade que está sendo objeto do processo de gestão de riscos devem ser considerados no contexto dos objetivos da organização como um todo, de modo a assegurar a identificação dos riscos do objeto que sejam significativos para os objetivos da organização.

82. Um dos primeiros passos da atividade de estabelecimento do contexto é identificar os fatores do ambiente, interno e externo, no qual a organização persegue seus objetivos. Não menos importante é a identificação das partes interessadas, bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, pois essas partes interessadas devem ser incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio do

[2] O conceito de organização aqui pode se referir a toda entidade ou parte dela, a um processo, como o planejamento estratégico, ou a projetos, processos de trabalho, operações, funções, decisões, produtos, serviços e ativos (ABNT, 2009).

processo de comunicação e consulta, abordado no tópico anterior.

83. A documentação dessa etapa normalmente é feita por meio de:

a) um relato conciso dos objetivos organizacionais, dos fatores críticos para o sucesso e uma análise dos fatores internos e externos do ambiente (SWOT, por exemplo);

b) análise de partes interessadas e seus interesses (análise de *stakeholder*, RECI, matriz de responsabilidades, por exemplo);

c) critérios mais importantes com base nos quais os níveis de risco serão analisados e avaliados: escalas de probabilidade; escalas de consequências ou impactos; como será determinado se o nível de risco é tolerável ou aceitável e se novas ações de tratamento são necessárias, isto é, diretrizes para priorização e tratamento de (ou resposta a) riscos.

5.4. PROCESSO DE AVALIAÇÃO DE RISCOS

84. O processo de avaliação de riscos é a parte do processo de gestão de riscos que compreende as atividades de identificação, análise e avaliação de riscos, descritas nos subitens a seguir.

5.4.1. Identificação de riscos

85. Identificação de riscos é o processo de busca, reconhecimento e descrição de riscos, tendo como base o contexto estabelecido e apoiado na comunicação e consulta com as partes interessadas, internas e externas (ABNT, 2009). O objetivo é produzir uma lista abrangente de riscos, incluindo causas, fontes e eventos, que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.

86. Para produzir uma lista de riscos, deve-se trabalhar com um processo sistemático e de modo estruturado (mapa de processos, fluxogramas, estrutura analítica de projeto) porém, em situações não claramente estruturadas, como a identificação de riscos estratégicos, utilizam-se processos de identificação mais genéricos ou análise de cenários.

87. Em muitos casos, a identificação de riscos em múltiplos níveis é útil e eficiente. Em uma etapa preliminar, pode-se adotar uma abordagem do tipo "*top-down*" para a identificação de riscos, indo do mais geral para o mais específico. Primeiro, identificam-se riscos em um nível geral ou superior, como ponto de partida para estabelecer prioridades para, em um segundo momento, identificarem-se e analisarem-se riscos em nível específico e ou mais detalhado.

88. A identificação de riscos pode se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, necessidades das partes interessadas. Convém que pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização

utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados (ABNT, 2009). Envolver a equipe diretamente responsável pela execução do processo, do projeto ou da atividade que está tendo os riscos identificados também ajuda a criar a responsabilidade em relação ao processo de gestão de riscos e o comprometimento em relação ao tratamento dos riscos.

89. A documentação dessa etapa geralmente inclui pelo menos:

a) o escopo do processo, projeto ou atividade coberto pela identificação;

b) os participantes do processo de identificação;

c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas;

d) o registro dos riscos identificados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências.

5.4.2. Análise de riscos

90. A análise de riscos é o processo de compreender a natureza do risco e determinar o nível de risco, fornecendo a base para a avaliação e para as decisões sobre o tratamento de riscos (ABNT, 2009).

91. O risco é uma função tanto da probabilidade como das consequências, portanto, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e de suas consequências, em termos da magnitude do impacto nos objetivos.

Risco = *f*unção (Probabilidade e Impacto)

92. O resultado final do processo de análise de riscos será o de atribuir, para cada risco identificado, uma classificação tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas e as fontes de risco, suas consequências positivas ou negativas, expressas em termos de impactos tangíveis ou intangíveis.

93. Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas, e ser mais ou menos detalhada (ABNT, 2009). O método e o nível de detalhamento da análise podem ser influenciados pelos objetivos, pela natureza do risco, pela disponibilidade de informações, dados e recursos.

94. Em análises qualitativas e semiquantitativas, considerando que a lógica subjacente ao nível de risco seja proporcional tanto em relação à probabilidade quanto ao impacto, a função '*Risco*' será essencialmente um produto dessas variáveis.

Risco = P x I

95. Contudo essa relação simples pode não refletir relações não lineares, sendo necessário, assim, incluir um fator de ponderação para uma das duas variáveis (probabilidade ou impacto, de modo a atingir a escala relativa necessária entre eles) e ou um operador exponencial para uma ou para ambas as variáveis (DE CICCO, 2009, adaptado).

Risco = $(P)^x$ x $(I \times \text{fator de ponderação})^y$

96. Em sua forma qualitativa mais simples, a relação entre o nível de risco e as variáveis que o compõe pode ser ilustrada por meio de uma matriz como a que segue.

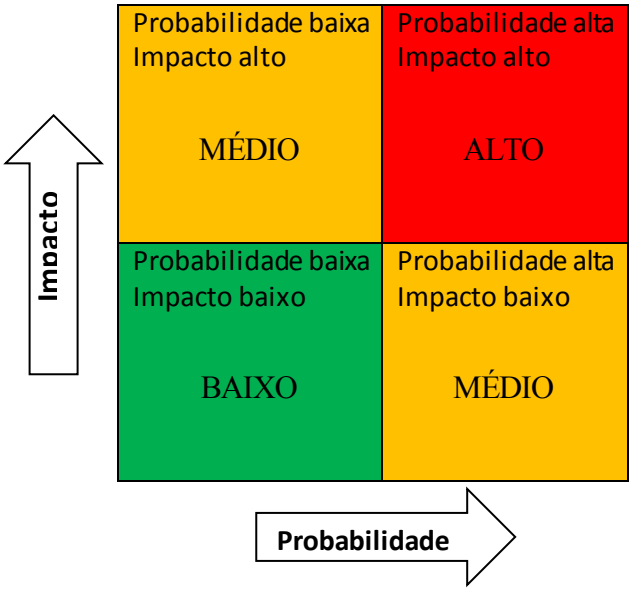


Figura 5.2: Matriz de Riscos simples (BRASIL, 2010a).

97. Essa abordagem, mais simples, é geralmente utilizada na avaliação inicial de riscos num nível geral ou superior, de modo a estabelecer prioridades de identificação e análise em nível mais específico ou detalhado; ou quando dados numéricos, tempo e recursos não estão disponíveis para a realização de análise numérica ou ainda quando não é exigida precisão quantitativa.

98. Análises semiquantitativas geralmente utilizam escalas, como as exemplificadas a seguir, para fornecer um entendimento comum das classificações de probabilidades e impacto. Em situações reais, essas escalas são elaboradas de modo compatível com o contexto e os objetivos específicos da atividade objeto da gestão de riscos.

Escala de Probabilidades

Probabilidade	Descrição da probabilidade, desconsiderando os controles	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Tabela 5.1: Exemplo de Escala de Probabilidades (BRASIL, 2012, adaptado).

Escala de Consequências

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Tabela 5.2: Exemplo de Escala de Consequências (BRASIL, 2012, adaptado).

99. O nível de risco inerente (NRI) de um evento é o nível de risco antes da consideração das respostas que a gestão adota, incluindo controles internos, para reduzir a probabilidade do evento e ou os seus impactos nos objetivos. Resulta da combinação da probabilidade com o impacto, conforme as tabelas anteriores (no nosso exemplo, multiplicação).

100. A política de gestão de riscos da organização geralmente estabelece categorias para classificar os níveis de risco resultantes do processo de análise, sejam inerentes ou residuais, de modo consistente com o seu apetite a risco, como as exemplificadas na Tabela 5.3.

Escala para classificação de Níveis de Risco

RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
0 – 9,99	10 – 39,99	40 – 79,99	80 – 100

Tabela 5.3: Níveis de classificação de risco (elaboração própria).

101. Os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz, como a seguir.

Matriz de Riscos

IMPACTO						
	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa 1	Baixa 2	Média 5	Alta 8	Muito Alta 10
		PROBABILIDADE				

Tabela 5.4: Matriz de riscos (BRASIL, 2012, adaptado).

102. Segue-se exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos inerentes (NRI), de acordo com o método apresentado.

Riscos Identificados	Probabilidade		Impacto		Nível de Risco Inerente (NRI)
Risco 1 – Descrição do risco 1	Alta	8	Muito Alto	10	80 RE (Extremo)
Risco 2 – Descrição do risco 2	Média	5	Alto	8	40 RA (Alto)
Risco 3 – Descrição do risco 3	Baixa	2	Médio	5	10 RM (Médio)
Risco *n* – Descrição do risco *n*	Muito Baixa	1	Médio	5	5 RB (Baixo)

Tabela 5.5: Registro de riscos parcial com níveis de risco inerente calculados (BRASIL, 2012, adaptado).

103. A análise de riscos só se completa quando as ações que a gestão adota para respondê-los são

também avaliadas, chegando-se ao nível de risco residual, o risco que remanesce depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e ou o impacto dos riscos, incluindo controles internos e outras ações. Formas de resposta a riscos podem variar entre reduzir, evitar, compartilhar ou aceitar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas pela administração sejam efetivamente aplicadas.

104. A avaliação das respostas a riscos e atividades de controle correspondentes – ou simplesmente controles – é parte integrante da análise de riscos. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco (ABNT, 2009).

105. As atividades de controle são as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos (COSO, 2013). As atividades de controle também são geralmente referidas como controles internos.

106. Uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação dos controles, utilizando uma escala como a exemplificada a seguir.

Nível de Confiança (NC)	Avaliação do desenho e implementação dos controles (Atributos do controle)	Risco de Controle (RC)
Inexistente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1,0
Fraco NC = 20% (0,2)	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.	Alto 0,8
Mediano NC = 40% (0,4)	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.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

Tabela 5.6: Exemplo de escala para avaliação de controles (adaptado de Dantas et al, 2010; e Avalos, 2009).

107. Observe-se, no exemplo apresentado, que o controle mais bem avaliado recebeu um NC = 80% (0,8). Isso se deve ao fato de que controles têm limitações que lhe são inerentes, como a possibilidade de se tornarem ineficazes pela ação de conluio, de contorno efetuado pela própria administração ou simplesmente de falhar por erro humano na sua aplicação. Logo, não importa quão efetivo seja o desenho e a implementação de um controle, ele só poderá fornecer uma segurança razoável, nunca absoluta, quanto ao cumprimento dos objetivos para os quais foi concebido. Portanto, não se deve atribuir 100% de confiança a um controle.

108. Uma vez determinado o nível de confiança (NC), pode-se determinar o risco de controle (RC), isto é, a possibilidade de que os controles adotados pela gestão não sejam eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. O RC é definido como complementar ao NC:

RC = 1 – NC

109. Pela fórmula é possível deduzir que quanto mais eficaz for o desenho e a implementação dos controles, ou seja, quanto maior for o NC, menor será o RC e vice-versa, porém este nunca será "zero", uma vez que o nível de confiança jamais será 100%.

110. Uma vez estabelecido o RC, é possível estimar o nível de risco residual (NRR), ou seja, o risco que permanece após o efeito das respostas adotadas pela gestão, incluindo controles internos e outras ações, para reduzir a probabilidade e ou o impacto do evento. Para isso, deduz-se do nível de risco inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo RC, utilizando a seguinte fórmula.

NRR = NRI x RC

111. Segue-se um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos residuais (NRR) de alguns riscos identificados, de acordo com o método apresentado.

Riscos Identificados	P	I	Nível de Risco Inerente (NRI)	Eficácia do Controle	Risco de Controle (RC)	Nível de Risco Residual (NRR)
Risco 1	Alta 8	M. Alto 10	RE 80	Inexistente	1,0	RE 80
Risco 2	Média 5	Alto 8	RM 40	Mediano	0,6	RM 24
Risco 3	Baixa 2	Alto 5	RM 10	Fraco	0,8	RB 8

Tabela 5.7: Registro de riscos parcial com níveis de risco residual calculados (BRASIL, 2012, adaptado).

112. A Tabela 5.8 apresenta os riscos residuais classificados por categorias, conforme os critérios da entidade para a classificação dos níveis de risco (Tabela 5.3) para alguns níveis de risco inerente selecionados da Tabela 5.4. O propósito é demonstrar o efeito dos controles (RC) sobre os riscos inerentes (NRI) (os valores foram arredondados).

Matriz de Riscos Residuais

Nível de Risco Inerente (NRI)						
	100 Extremo	20 RM	40 RA	60 RA	80 RE	100 RE
	80 Extremo	16 RM	32 RM	48 RA	64 RA	80 RE
	50 Alto	10 RM	20 RM	30 RM	40 RA	50 RA
	25 Médio	5 RB	10 RM	15 RM	20 RM	25 RM
	8 Baixo	2 RB	3 RB	5 RB	6 RB	8 RB
		0,2 Muito baixo	0,4 Baixo	0,6 Médio	0,8 Alto	1 Muito alto
		Risco de Controle (RC)				

Tabela 5.8: Matriz de riscos residuais (adaptado de Dantas et al, 2010; e Avalos, 2009).

113. A documentação da etapa de análise de riscos é normalmente feita no registro de riscos e geralmente inclui:

a) a abordagem ou o método de análise utilizado, as fontes de informação consultadas e os participantes do processo de análise;

b) as especificações utilizadas para as classificações de probabilidade e impacto dos riscos;

c) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e sua descrição, bem como considerações quanto à análise desses elementos e o resultado de sua combinação, o risco inerente;

d) a descrição dos controles existentes e as considerações quanto à sua eficácia, e o risco de controle;

e) o nível de risco residual, resultante da combinação dos dois riscos anteriores (inerente e de controle).

114. A extensão da documentação dos riscos de níveis mais baixos pode ser menos detalhada, porém deve ser mantido registro do fundamento lógico para justificar a determinação inicial dos níveis de risco nesse patamar.

5.4.3. Avaliação de riscos

115. A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e ou sua magnitude é aceitável ou tolerável ou se algum tratamento é exigido (ABNT, 2009).

116. Nessa etapa, portanto, se faz uso da compreensão e do nível do risco obtidos na etapa de análise de riscos para tomar decisões acerca de ações sobre os riscos analisados, em especial:

a) se um determinado risco precisa de tratamento e a prioridade para isso;

b) se uma determinada atividade deve ser realizada, reduzida ou descontinuada;

c) se controles devem ser implementados, modificados ou apenas mantidos.

117. Uma boa prática para apoiar o processo de avaliação de riscos é estabelecer critérios para priorização e tratamento (apetite a risco, nível recomendado de atenção, tempo de resposta requerido, comunicação etc.) associados aos níveis de risco. Segue-se um exemplo simples.

Nível de Risco	Critérios para priorização e tratamento de riscos
RE	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas só com autorização do dirigente máximo.
RA	Nível de risco além do apetite a risco. Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
RM	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
RB	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custos x benefícios, como diminuir o nível de controles.

Tabela 5.9: Diretrizes para priorização e tratamento de riscos (adaptado de BRASIL, 2013a).

118. Em geral, a documentação dessa etapa é realizada no próprio registro de riscos e fornece uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

5.4.4. Tratamento de riscos

119. O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível do risco (a probabilidade ou o impacto) e a elaboração de planos de tratamento que, uma vez implementados, implicarão a introdução de novos controles ou a modificação dos existentes. Um dos benefícios da gestão de riscos é exatamente o rigor que proporciona ao processo de identificação e seleção de alternativas de respostas aos riscos (ABNT, 2009; COSO, 2004).

120. Formas de tratar riscos, não mutuamente exclusivas ou adequadas em todas as circunstâncias, incluem evitar, reduzir, transferir e aceitar o risco. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes. Deve-se considerar a possibilidade de que novos riscos sejam introduzidos pelo tratamento e a existência de riscos cujo tratamento não seja economicamente justificável, como riscos severos (com grande consequência negativa), porém raros (com probabilidade muito baixa) (ABNT, 2009; INTOSAI, 2007).

121. Ao avaliar os efeitos das diferentes respostas, a gestão deve decidir a melhor forma de tratar o risco. A resposta, ou a combinação de respostas selecionadas, não precisa necessariamente gerar a quantidade mínima de risco residual, mas se gerar um risco residual acima dos limites de tolerância a risco estabelecidos, a gestão terá que reconsiderar a opção de resposta ou os limites de tolerância (INTOSAI, 2007).

122. O processo de tratamento é cíclico e inclui: a avaliação do tratamento já realizado; a avaliação dos níveis de risco residual frente ao apetite e às tolerâncias a risco definidos; a definição e a implementação de tratamento adicional nos casos em que o risco residual extrapolar o apetite e as tolerâncias; e a avaliação da eficácia desse tratamento (ABNT, 2009).

123. A documentação dessa etapa geralmente integra o registro de riscos da organização e inclui um plano de tratamento de riscos que identifica claramente a ordem de prioridade para a implementação de cada tratamento, e também:

a) as razões para a seleção das opções de tratamento, incluindo os benefícios esperados;

b) os responsáveis pela aprovação e pela implementação do plano;

c) as ações propostas, os recursos requeridos, incluindo contingências, e o cronograma;

d) as medidas de desempenho e os requisitos para o reporte de informações;

e) as formas de monitoramento da implementação do tratamento e dos riscos (ABNT, 2009).

5.5. MONITORAMENTO E ANÁLISE CRÍTICA

124. O monitoramento e a análise crítica são partes integrantes e essenciais da gestão de riscos e uma das etapas mais importantes do processo de gestão de riscos, cuja finalidade é:

a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos atualmente adotados e suas prioridades, e levar à identificação de riscos emergentes;

b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;

c) analisar eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; e

d) garantir que os controles sejam eficazes e eficientes no desenho e na operação (ABNT, 2009).

125. As responsabilidades relativas ao monitoramento e à análise crítica devem estar claramente definidas na política de gestão de riscos e detalhadas nos planos, manuais ou normativos, contemplando atividades como:

a) monitoramento contínuo (ou, pelo menos, frequente) pelas funções de gestão que têm propriedade sobre os riscos e pelas funções que supervisionam riscos e medem o desempenho da gestão de riscos, por meio de indicadores-chaves de risco e verificações rotineiras de índices de desempenho, ritmo de atividades, operações ou fluxos atuais em comparação com os que seriam necessários para o alcance de objetivos ou a manutenção dentro das tolerâncias a riscos ou variações aceitáveis no desempenho;

b) análise crítica dos riscos e seus tratamentos realizada pelas funções que gerenciam e têm propriedade de riscos e ou pelas funções que supervisionam riscos, por meio de auto avaliação de riscos e controles (*Control and Risk Self Assessment - CRSA*); e

c) auditorias realizadas pelas funções que fornecem avaliações independentes (a auditoria interna ou externa), focando a estrutura e o processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez das situações específicas encontradas.

126. As atividades de monitoramento e análise crítica devem assegurar que o registro de riscos seja mantido atualizado, bem como que nele seja incluído pelo menos os resultados das ações mencionadas acima, com referências para a documentação original completa.

6. MODELO DE AVALIAÇÃO DE MATURIDADE DO TCU

127. Este capítulo fornece a visão geral do modelo de avaliação da maturidade organizacional em gestão de riscos desenvolvido pelo TCU, a partir das melhores práticas internacionais em uso no setor público, oriundas dos modelos de gerenciamento de riscos COSO GRC (COSO, 2004 e 2016), ABNT NBR ISO 31000 Gestão de Riscos – Princípios e Diretrizes (ABNT, 2009) e Orange Book (UK, 2004 e 2009), bem como da IN-MP/CGU Nº 1/2016.

128. O modelo é composto das quatro dimensões ilustradas na Figura 6.1 e sua aplicação apoia-se nos critérios descritos no Apêndice I – Critérios para avaliação da maturidade em gestão de riscos, que também indica as fontes dos critérios.

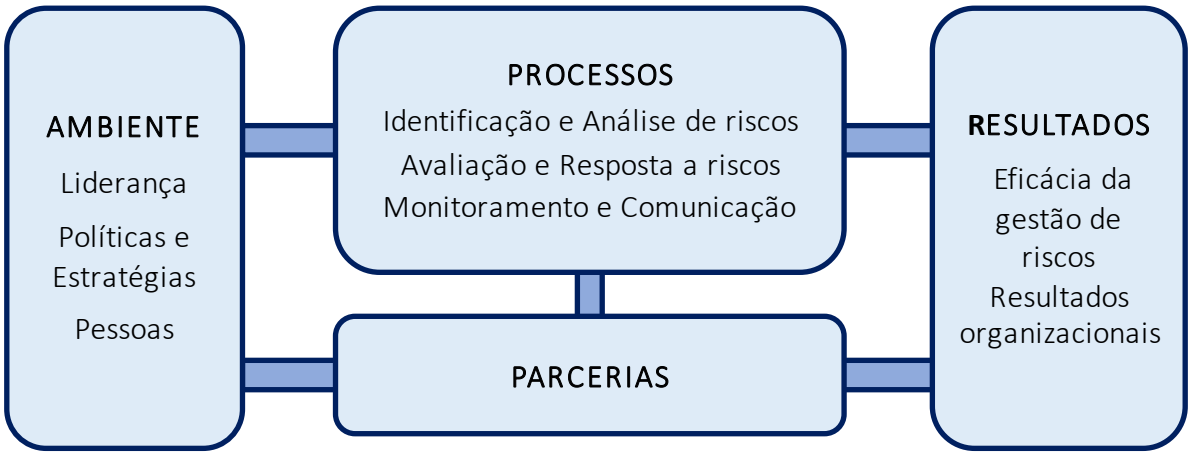


Figura 6.1: Modelo de avaliação da maturidade em gestão de riscos elaborado pelo TCU (BRASIL, 2013).

129. O modelo tem como premissas que a maturidade da gestão de riscos de uma organização é determinada pelas capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho da organização no cumprimento de sua missão institucional de gerar valor para as partes interessadas com eficiência e eficácia, transparência e accountability, e conformidade com leis e regulamentos.

6.1. DIMENSÕES DO MODELO

6.1.1. Ambiente

130. A dimensão "Ambiente", tomada do modelo COSO GRC, engloba boas práticas, também presentes no modelo britânico, relacionados com a *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia e dos objetivos* em todos os níveis, procurando avaliar as capacidades existentes para que a gestão de riscos tenha as condições necessárias para prosperar na organização.

6.1.1.1. Liderança

131. A importância do papel da alta administração na implementação e operação da gestão de riscos é destacado em todos os modelos. O GESPÚBLICA tem a Liderança como primeiro componente do modelo de gestão adotado pelo Poder Executivo federal, (BRASIL, 2009). O COSO GRC também destaca a importância da liderança para a gestão de riscos:

> Para que uma organização possa desfrutar de um gerenciamento de riscos eficaz, a atitude e o interesse da alta administração devem ser claros e definitivos, bem como permear toda a organização. Não é suficiente apenas dizer as palavras corretas, uma atitude de "faça o que digo e não o que faço" somente gerará um ambiente inadequado.

132. Em essência, busca-se avaliar em que medida os responsáveis pela governança e a alta exercem as suas *responsabilidades de governança de riscos* e *cultura*, assumindo um *compromisso* forte e sustentado e exercendo *supervisão* para obter *comprometimento* com a gestão de riscos em todos os níveis da organização, promovendo-a e dando *suporte*, de modo que possam ter uma expectativa razoável de que no cumprimento da sua missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de gerar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como vetores principais.

6.1.1.2. Políticas e Estratégias

133. A gestão de riscos deve fazer parte das considerações sobre estratégias e planos em todos os níveis críticos da entidade, concretizando-se pelo processo de gerenciamento de riscos nas operações, funções e atividades relevantes nas diversas partes da organização.

134. Nesta seção, busca-se avaliar em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.

135. Organizações com políticas e estratégias de gestão de riscos adequadas contam com:

a) um processo e métodos para definir claramente objetivos e tolerâncias a risco ou variações aceitáveis no desempenho para permitir que os seus riscos e resultados possam ser gerenciados, incorporando explicitamente indicadores-chaves de desempenho e de risco em seus processos de governança e gestão;

b) competências e capacidade para identificar eventos potenciais que podem impactar a

organização, o governo ou a comunidade e fazem uso de medidas práticas e razoáveis para gerenciar esses eventos;

c) asseguração de que a sua administração e o seu corpo executivo:

i. estão adequadamente informados sobre as exposições a risco da organização;

ii. estão completa e diretamente envolvidos em estabelecer e rever o processo de gestão de riscos em suas áreas; e

iii. alocam recursos adequados e suficientes para a gestão de riscos, levando em conta o perfil de risco, o tamanho, a complexidade, a estrutura e o contexto da organização.

6.1.1.3. Pessoas

136. O gerenciamento de riscos é um processo efetuado pelo conselho de administração, pela diretoria executiva e pelos demais empregados, isto é, pelas pessoas, mediante o que fazem e o que dizem. São as pessoas que estabelecem a missão, a estratégia e os objetivos e implementam os mecanismos de gerenciamento de riscos da organização (COSO, 2004).

137. O gerenciamento de riscos afeta as ações das pessoas, e estas o gerenciamento de riscos, uma vez que nem sempre entendem, se comunicam ou desempenham suas funções de forma consistente. A gestão de riscos deve proporcionar os mecanismos necessários para ajudar as pessoas a entender o risco no contexto dos objetivos da organização, bem como suas responsabilidades e seus limites de autoridade, criando uma associação clara e estreita entre os deveres das pessoas e como elas os cumprem no tocante à estratégia e aos objetivos da organização (COSO, 2004).

138. Assim, o grau de conhecimento das pessoas sobre os objetivos da organização, a existência de canais de comunicação para que questões relacionadas a risco sejam levantadas e decididas, a definição clara de responsabilidades e limites de autoridade em relação aos processos de gestão de riscos, a existência de arcabouço conceitual de risco uniformemente conhecido e utilizado na organização, bem como a oferta de cursos de capacitação sobre o tema são atributos importantes que devem estar presentes na conformação de um ambiente de gestão de riscos apropriado.

139. Nesta seção, busca-se avaliar em que medida as pessoas da organização estão informadas, habilitadas e autorizadas para exercer seus papéis e suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.

6.1.2. Processos

140. Os processos de gestão de riscos constituem o coração dos modelos de gestão de riscos. Para lidar com os riscos que podem impactar os objetivos de uma organização, processos devem ser estabelecidos para identificar riscos; avaliar a probabilidade de ocorrência e o impacto sobre os resultados pretendidos; escolher o tipo apropriado de resposta para cada risco; desenhar e implementar respostas para os riscos priorizados; comunicar os assuntos relacionados a risco às partes interessadas; e monitorar a integridade da estrutura e do processo de gestão de riscos. Tais processos devem estar incorporados e integrados aos processos de governança e de gestão, finalísticos e de apoio.

141. Esta dimensão, portanto, aborda os aspectos relacionados ao processo de gestão de riscos, procurando avaliar em que medida a organização estabeleceu um processo formal, com padrões e critérios definidos para a *identificação e análise de riscos*, *avaliação e resposta a riscos*, incluindo a seleção e a implementação de respostas aos riscos avaliados, e *monitoramento e comunicação* relacionada a riscos e controles com partes interessadas, internas e externas.

6.1.2.1. Identificação e análise de riscos

142. Nesta seção, busca-se avaliar em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente às operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização), de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.

6.1.2.2. Avaliação e resposta a riscos

143. Nesta seção, busca-se avaliar em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.

6.1.2.3. Monitoramento e comunicação

144. Nesta seção, busca-se avaliar em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação.

6.1.3. Parcerias

145. Parcerias são quaisquer arranjos estabelecidos para possibilitar relacionamento colaborativo entre partes, visando o alcance de objetivos de interesse comum. As parcerias são usualmente estabelecidas para atingir um objetivo estratégico ou a entrega de um produto ou serviço, sendo formalizadas por um determinado período, implicando a negociação e o claro entendimento das funções de cada parte, bem como dos benefícios decorrentes (BRASIL, 2009, p. 21). Envolvem, portanto riscos e benefícios compartilhados.

146. Esta dimensão trata de aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas, quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas, procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e sobre o seu gerenciamento.

6.1.4. Resultados

147. Esta dimensão trata de aspectos relacionados aos efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.

148. A razão de ser da gestão de riscos é apoiar as organizações na consecução dos resultados planejados. Portanto, todos os objetivos relevantes da organização devem fazer parte do escopo da gestão de riscos, que deverá contribuir para que haja efeitos positivos no alcance de todos eles. Os efeitos produzidos pela gestão de riscos em uma organização se dão em duas esferas: uma de efeitos imediatos e outra de efeitos mediatos.

149. Na esfera dos efeitos imediatos, denominada e*ficácia da gestão de riscos*, estão os efeitos das práticas de gestão de riscos na qualidade do processo decisório, na coordenação entre unidades organizacionais, no gerenciamento de riscos com parceiros, no aperfeiçoamento de planos e políticas organizacionais, na comunicação sobre riscos com partes interessadas e no envolvimento do pessoal com a avaliação e o controle dos riscos. Os efeitos ditos mediatos são aqueles que surgem a partir da presença dos efeitos imediatos. Em outras palavras, por meio de uma gestão de riscos eficaz consegue-se melhorar resultados, por meio da otimização do desempenho da organização na sua capacidade de gerar, preservar e entregar valor.

6.2. DETERMINAÇÃO DO NÍVEL DE MATURIDADE

150. Considerando que as capacidades existentes na organização em termos de liderança, políticas e estratégias, de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho, podem ser avaliadas separadamente, pode-se falar em maturidade de cada aspecto e de cada uma das dimensões do modelo, como também em nível de maturidade global, ao considerar todas as dimensões do modelo.

151. Para isso, é necessário avaliar se os princípios, a estrutura (ou os componentes) e os processos colocados em prática para o gerenciamento de riscos por toda a organização estão presentes e funcionando integrados aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chaves da organização.

6.2.1. Avaliando os índices de maturidade de cada aspecto

152. O cálculo dos índices de maturidade para cada aspecto da gestão de riscos é realizado atribuindo-se quatro pontos para a presença integral e consolidada da prática ou característica de gestão enfocada, um, dois ou três, quando a presença é parcial, de acordo com sua intensidade, e zero ponto à ausência total, conforme a escala para avaliação de evidências de auditoria, apresentada na Tabela 7.1, tópico 7.7, do próximo capítulo. No caso de questões que admitem respostas sim/não, atribuiu-se quatro pontos ao 'sim' e zero ponto ao 'não'.

153. Para as questões que se desdobram em itens, cada item obterá um número decimal como pontuação, resultante da divisão dos valores de pontuação possíveis (de zero a quatro, conforme explicado no parágrafo anterior) pelo número de itens que compõem a questão. Por exemplo, para uma questão com cinco itens, cada item poderá receber de zero a no máximo 0,8 (4/5).

6.2.2. Avaliando os índices de maturidade de cada dimensão

154. O índice de maturidade de cada dimensão (Ambiente; Processos; Parcerias; e Resultados) é apurado tomando-se o somatório de pontos do conjunto de questões que a compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível, expressando esse quociente com um número entre 0% e 100%. Se, por exemplo, uma dimensão obtém 40 pontos de 76 possíveis (19 questões x 4 pontos = 76 pontos), então o índice de maturidade dessa dimensão seria de 52,6% (40/76 x 100).

6.2.3. Determinando o nível de maturidade global da gestão de riscos

155. O índice de maturidade global da gestão de riscos é obtido pela média ponderada dos índices de maturidade das dimensões (IMD) pelos seguintes pesos:

Dimensão	Peso	Exemplo		
		IMD	Peso	Ponderado
Ambiente	40	52,6	0,4	21,0
Processos	30	45,9	0,3	13,8
Parcerias	10	80,1	0,1	8,0
Resultados	20	49,5	0,2	9,9
ÍNDICE DE MATURIDADE GLOBAL				52,7

Tabela 6.1: Pesos e exemplo de cálculo do índice de maturidade (adaptado de BRASIL, 2013).

156. Os pesos de cada dimensão foram determinados usando-se a técnica AHP (*Analytic Hierarchy Process*, COYLE, 2004) aplicada às respostas dadas por oito especialistas do TCU a comparações duas-a-duas da importância relativa das quatro dimensões do modelo. A técnica AHP presta-se a facilitar a tomada de decisão por meio da hierarquização de opções com base na opinião de um grupo de pessoas acerca dos atributos de cada opção.

157. O índice global derivado desse cálculo permite classificar o nível de maturidade de uma organização em uma das cinco faixas mostradas na Tabela 6.2.

Índice de maturidade apurado	Nível de Maturidade
De 0% a 20%	Inicial
De 20,1% a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 80%	Aprimorado
De 80,1% a 100%	Avançado

Tabela 6.2: Níveis de maturidade da gestão de riscos (BRASIL, 2013).

7. PADRÕES GERAIS DA AUDITORIA DE GESTÃO DE RISCOS

158. Para obter a segurança necessária para emitir a conclusão geral sobre o nível de maturidade da gestão de riscos da organização e as conclusões específicas e respectivas recomendações sobre os aspectos que necessitam ser aperfeiçoados, o titular da unidade de auditoria deve assegurar que:

a) a equipe de auditoria possua, coletivamente, o conhecimento, as habilidades e a competência necessários para concluir com êxito a auditoria, incluindo um entendimento abrangente sobre a organização e o seu contexto;

b) o trabalho seja adequadamente planejado e os procedimentos de auditoria planejados considerem, necessariamente, elementos de conhecimento prévio sobre a entidade, seus objetivos e riscos, complexidade de suas operações, sistemas e estruturas (NAT, 94-95);

c) o trabalho seja adequadamente supervisionado, nos termos prescritos em NAT, 73-75, e revisado à medida que a auditoria for se desenvolvendo, conforme NAT, 76-77; e

d) o relatório considere a perspectiva dos dirigentes da entidade, obtendo comentários dos gestores ao relatório preliminar, sobretudo em relação às ações corretivas que pretendem tomar (NAT, 144-148).

7.1. OBJETO DA AUDITORIA

159. O objeto de uma auditoria de gestão de riscos é a arquitetura – os princípios, a estrutura ou os componentes e os processos - colocada em prática para o gerenciamento de riscos por toda a organização, nos diversos níveis e nos vários contextos específicos em que seus objetivos são perseguidos, incluindo o processo de planejamento estratégico e sua implementação pelas diversas áreas ou funções da organização, os processos de governança, finalísticos e de apoio ou os programas, projetos e atividades relevantes para os objetivos-chaves da organização.

7.2. OBJETIVOS DA AUDITORIA

160. Os objetivos gerais do auditor[3] ao conduzir uma auditoria de gestão de riscos são:

a) determinar o nível de maturidade da gestão de riscos da organização;

b) identificar os aspectos que necessitam ser aperfeiçoados; e

c) emitir um relatório detalhado sobre os aspectos e uma conclusão geral sobre a maturidade.

[3] O termo "auditor" é aqui usado em referência às pessoas a quem é delegada a tarefa de realizar a auditoria e emitir o seu relatório.

7.3. TIPO DO TRABALHO E NÍVEL DE ASSEGURAÇÃO

161. A auditoria de gestão de riscos é do tipo operacional, com abordagem orientada a sistema e de relatório direto, devendo proporcionar um nível de asseguração sobre a avaliação do objeto (a gestão de riscos tal como descrita no tópico 7.1) de acordo com os critérios de auditoria aplicáveis (indicados no tópico 7.5), que seja significativo para suportar os processos decisórios dos usuários previstos, principalmente em relação às ações de aperfeiçoamento necessárias (ISSAI 100, 29-33; ISSAI 400, 21-23 e 26; ISSAI 3000, 32 e 40).

7.4. TIPO DE RELATÓRIO

162. O relatório de auditoria deve fornecer aos usuários o nível de asseguração necessário, descrevendo, de uma maneira equilibrada e fundamentada, como os achados, os critérios e as conclusões foram desenvolvidos, e porque a combinação de achados e critérios resultaram na conclusão geral sobre o nível de maturidade da gestão de riscos da organização e nas conclusões específicas sobre os aspectos que necessitam ser aperfeiçoados, e que estão sendo objeto de recomendações do relatório, com a devida consideração aos comentários ofertados pelos gestores (ISSAI 300, 21-23 e 39; ISSAI 3000, 32-34, 116-130; NAT, 144-146).

163. O relatório deve declarar os objetivos da auditoria e descrever como foram abordados no trabalho, incluindo o escopo da auditoria, a metodologia e as fontes de dados, os critérios e sua explicitação, e descrever quaisquer limitações significativas ao escopo da auditoria. Todas as informações e conclusões lançadas no relatório devem estar baseadas em evidência de auditoria suficiente e apropriada (ISSAI 300, 38-39; ISSAI 3000, 106-122).

164. Embora os critérios de auditoria utilizados para avaliar e relatar acerca de gestão de riscos sejam relativamente bem conhecidos, não se pode presumir que estarão disponíveis a todos os usuários do relatório, assim, além da indicação da fonte e localização do critério dentro da fonte (exemplo, ISO 31000:2009, 4.3.3), a descrição do critério deve explicitar o que ele preconiza e porque é aplicável à situação, porém evitando-se ao máximo transcrições.

7.5. CRITÉRIOS DE AUDITORIA

165. Os critérios da auditoria de gestão de riscos refletem as melhores práticas internacionais, consoante os modelos de gestão de riscos e o processo de gestão riscos apresentados nos capítulos 4 e 5, e a Instrução Normativa Conjunta MP/CGU Nº 01/2016.

166. Uma parte relevante desses critérios está incorporada ao modelo de avaliação da maturidade da gestão de riscos desenvolvido pelo TCU, que visa determinar a maturidade da gestão de riscos de uma organização, por meio da avaliação das capacidades existentes em termos de

liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades e pelos resultados decorrentes.

167. O Apêndice I detalha os critérios utilizados para avaliação da maturidade organizacional em gestão de riscos e para a identificação dos aspectos que necessitam ser aperfeiçoados, bem como as fontes desses critérios, para apoiar a aplicação do modelo de avaliação.

7.6. PROCEDIMENTOS DE AUDITORIA

168. O Apêndice II fornece a Matriz de Planejamento com as questões/subquestões de auditoria e as conclusões que o auditor deve alcançar em relação a cada aspecto da gestão de riscos. Cabe à equipe de auditoria desenvolver os procedimentos de auditoria e os instrumentos de coleta de dados necessários para cada auditoria, levando em consideração as características específicas da entidade e o princípio de que a gestão de riscos é feita sob medida, de acordo com a complexidade e o perfil de risco da organização, bem como a sua natureza e estrutura, e o seu tamanho e contexto.

169. Quanto mais complexa a organização e o seu perfil de riscos, espera-se que mais formais e extensas sejam as práticas implementadas por meio de políticas, procedimentos e controles para assegurar que os princípios, a estrutura ou os componentes e o processo de gestão de riscos estejam presentes e funcionem adequadamente, e vice-versa.

170. Assim, os procedimentos de auditoria e os respectivos instrumentos de coleta de dados para avaliar o objeto (tópico 7.1) em relação aos critérios aplicáveis (tópico 7.5 e Apêndice I), de modo a chegar às conclusões exigidas pelos objetivos gerais de auditoria (tópico 7.2, alíneas "a" e "b"), devem ser planejados para lidar com as circunstâncias específicas de cada entidade auditada, refletindo a sua maior ou menor complexidade e o seu perfil de riscos. Em qualquer caso, os procedimentos devem permitir a obtenção de evidência de auditoria suficiente e apropriada para realizar a avaliação indicada no tópico a seguir.

7.7. AVALIAÇÃO DA EVIDÊNCIA DE AUDITORIA

171. A evidência de auditoria obtida mediante aplicação dos procedimentos de auditoria e respectivos instrumentos de coleta de dados desenvolvidos para abordar as questões e subquestões de auditoria (Apêndice II) em face dos critérios (Apêndice I) deve permitir ao auditor concluir sobre a pontuação de cada aspecto da gestão de riscos da organização, utilizando a escala de avaliação a seguir.

Escala para avaliação das evidências de auditoria obtidas

Pontuação	0 INEXISTENTE	1 INICIAL	2 BÁSICO	3 APRIMORADO	4 AVANÇADO
Dimensão 1	Prática inexistente, não implementada ou não funcional.	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
Dimensão 2					
Dimensão 3					
Dimensão 4	Não há evidências de que o resultado descrito tenha sido obtido.	Existe a percepção entre os gestores e o pessoal de que o resultado descrito tenha sido obtido em alguma medida.	Existem indicadores definidos que mostram que o resultado descrito vem sendo obtido em grau baixo.	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau moderado.	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau elevado.

Tabela 7.1: Escala para avaliação de evidências quanto aos aspectos da gestão de riscos (adaptado de BRASIL, 2013).

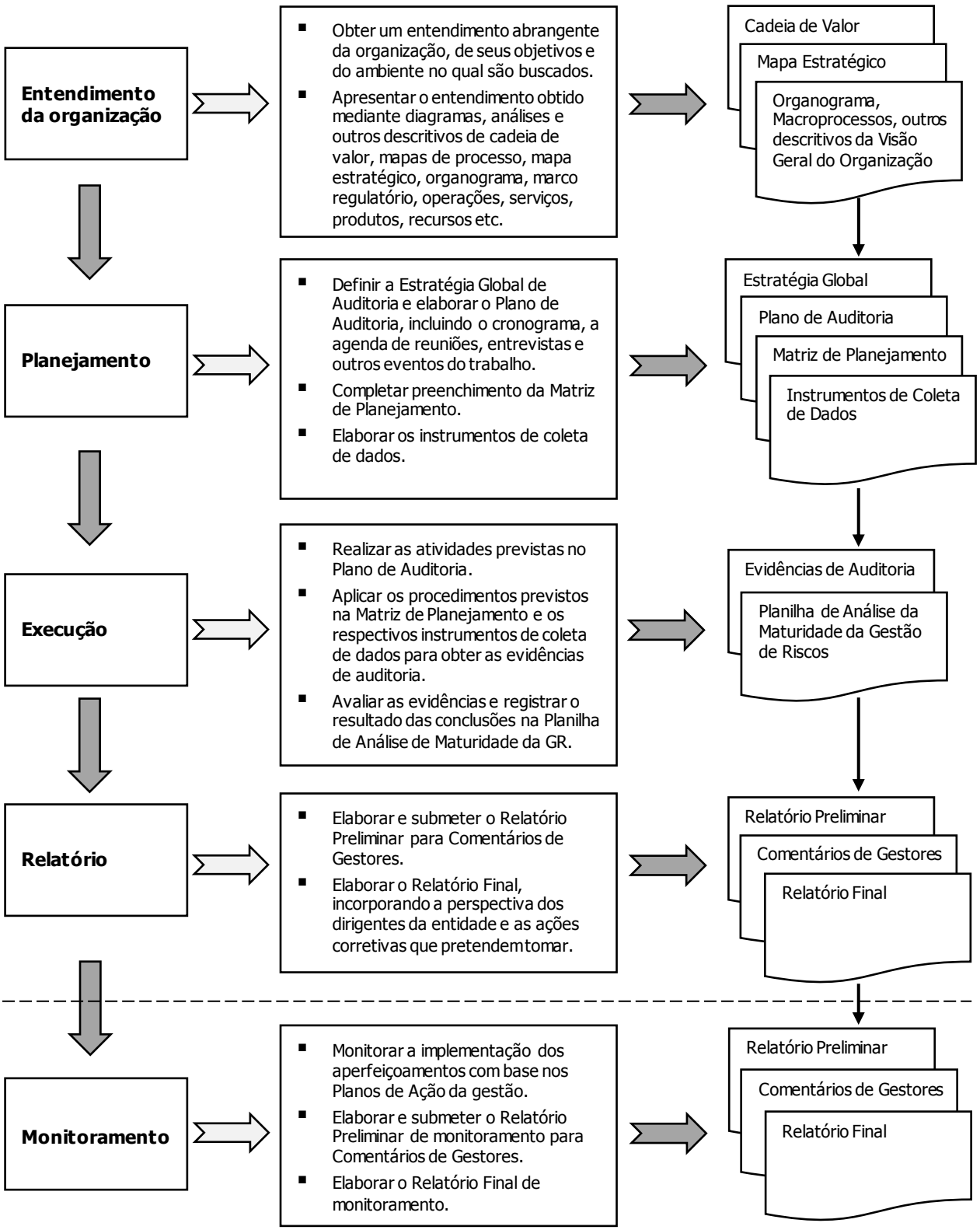
172. Para cada critério do Apêndice I, o auditor deve concluir se obteve a evidência necessária para fundamentar suas conclusões específicas e respectivas recomendações sobre os aspectos da gestão de riscos da organização que necessitam ser aperfeiçoados, bem como, se no conjunto, a evidência de auditoria é suficiente e apropriada para fundamentar a sua conclusão geral sobre o nível de maturidade da gestão de riscos da organização.

7.8. DOCUMENTAÇÃO DA AUDITORIA

173. A documentação de uma auditoria de gestão de riscos deve ser suficientemente detalhada, desde os levantamentos preliminares para entendimento da entidade e do seu ambiente até a compilação de resultados de avaliação das evidencias para formação de conclusões, de modo a permitir que um auditor experiente, sem nenhum conhecimento prévio da auditoria, entenda o raciocínio por trás de todas as questões relevantes que exigiram o exercício de julgamento profissional do auditor na determinação do escopo, da extensão e natureza dos procedimentos planejados e executados, na avaliação das evidências de auditoria obtidas, das conclusões geral e específicas resultantes, e das respectivas recomendações da auditoria (ISSAI 100, 42).

8. O PROCESSO DE AUDITORIA DE GESTÃO DE RISCOS

Figura 8.1: **Fluxo do processo da auditoria de gestão de riscos** (elaboração própria).



175. Para realizar com êxito uma auditoria de gestão de riscos, que atenda aos padrões gerais descritos no capítulo anterior, a equipe de auditoria deve conduzir o trabalho seguindo as etapas e atividades apresentadas no fluxo da Figura 8.1, detalhadas nos tópicos subsequentes, de modo a obter os produtos intermediários e finais indicados no lado direito do fluxo.

8.1. ENTENDIMENTO DA ORGANIZAÇÃO

176. A equipe de auditoria deve obter um entendimento abrangente da organização e do seu ambiente, a fim de conhecer como ela se organiza e funciona para otimizar o seu desempenho na entrega de valor público em benefício da sociedade, assim como os fatores relevantes do ambiente no qual ela busca atingir os seus objetivos e cumprir a sua missão institucional.

8.1.1. Objetivos da obtenção de entendimento da organização

177. O objetivo principal dessa etapa é identificar o direcionamento estratégico da organização (missão, visão, valores fundamentais); os objetivos-chaves, estratégicos e de negócios, e os macroprocessos e processos relevantes para a sua realização; as áreas, funções e atividades que concorrem de maneira relevante para a realização dos objetivos, bem como os respectivos responsáveis em todos os níveis; as medidas de desempenho (metas, indicadores-chaves de desempenho, de risco e variações aceitáveis no desempenho). O objetivo secundário é reunir informações para fornecer a *visão geral* da organização, de modo a oferecer ao leitor do relatório de auditoria o conhecimento e a compreensão necessários para bem entendê-lo.

178. O objetivo específico da obtenção dessas informações é formar uma base para estabelecer as áreas de foco e definir o escopo da auditoria de gestão de riscos, fornecendo direção clara para as demais atividades da fase de planejamento. Um bom entendimento pode ser obtido guiando-se pelas seguintes questões (adaptado de *Golden Circle Theory*. SINEK, 2011):

a) por que (*why*) a organização existe – o propósito: qual a demanda social, o problema ou a necessidade que motivou a criação e justifica a sua existência. É nesse âmbito que se identificam a missão e os objetivos-chaves da organização, a sua finalidade;

b) como (*how*) a organização faz – o processo: a maneira como a organização se estrutura e atua para atender seu propósito, incluindo os objetivos estratégicos e de negócios e os macroprocessos, processos, áreas, funções e atividades relevantes para a sua realização. É também nesse âmbito que se identificam a visão e os valores fundamentais que fixam o tom do topo da organização. Todos esses elementos de entendimento são estabelecidos pela governança e a alta administração.

c) o que (w*hat*) a organização faz – o resultado: os produtos, bens e serviços oferecidos

pela organização para cumprir o seu propósito, alterando, por meio de seu processo de geração, preservação e entrega de valor, a realidade social ou melhorando a capacidade do próprio Estado para atender as demandas sociais. É também nesse âmbito que se identificam as medidas de desempenho (metas, indicadores-chaves de desempenho, de risco e variações aceitáveis no desempenho) e o histórico de resultados alcançados.

179. Ao final da etapa de obtenção de entendimento, o auditor deve ter uma visão clara do negócio da organização e das áreas, funções e atividades que concorrem de maneira relevante para os resultados que são entregues à sociedade, bem como dos respectivos responsáveis em todos os níveis. É isso que vai permitir ao auditor:

a) identificar quem deve ser entrevistado e o que deve ser questionado;

b) priorizar as áreas que devem ter seus processos de gerenciamento de riscos examinados;

c) definir a informação requerida ou a evidência que será buscada e a fonte de informação.

d) determinar o instrumento de coleta de dados ou procedimento de auditoria mais adequado às circunstâncias (exemplo: entrevista, se poucos gestores, ou questionário, se muitos);

e) programar a agenda com as partes envolvidas da maneira mais conveniente e elaborar o cronograma do trabalho; e,

f) completar o preenchimento da Matriz de Planejamento, fornecida no Apêndice II, tendo por base o entendimento obtido por meio das informações acima.

8.1.2. Procedimentos para obtenção de entendimento

180. O entendimento da organização pode originar-se daqueles conhecimentos que os auditores já possuem em função de trabalhos anteriores e ou dos que adquirirem a partir de procedimentos calcados em técnicas de entrevista, de observação e inspeção, e de procedimentos analíticos. A escolha de qual procedimento utilizar e a extensão da sua aplicação depende de julgamento profissional do auditor sobre o alcance e a profundidade do entendimento necessário em cada auditoria. Em qualquer caso, porém, deve ser suficiente para permitir à equipe ter a visão do negócio e realizar as atividades a que se referem o parágrafo anterior.

181. Muito provavelmente, a equipe começará obtendo um entendimento preliminar mediante inspeção de relatórios de gestão da organização, de levantamentos anteriormente realizados, de informações sobre a estrutura, as competências e operações disponibilizadas em páginas da Internet, de informações orçamentárias e financeiras publicadas ou obtidas no Siafi. A partir desse entendimento preliminar, a equipe pode planejar os procedimentos adicionais para aprofundar o entendimento da organização, incluindo a elaboração de uma agenda de

entrevistas e um cronograma para a aplicação dos demais procedimentos necessários para a conclusão dessa fase de obtenção de entendimento, que deverá permitir à equipe atingir os objetivos descritos nos parágrafos 178 e 179, acima.

182. A seguir, exemplos de informações[4] consideradas essenciais, mas não limitado a elas, para a obtenção de um entendimento relevante para uma auditoria de gestão de riscos:

a) natureza jurídica, competências legais e marco regulatório, dos quais são derivados os objetivos-chaves da organização;

b) missão e visão declaradas, em contraste com as competências legais;

c) definição do valor público entregue à sociedade, consistente nos objetivos-chaves da organização, frequentemente também denominados macroprodutos, macro-objetivos ou resultados finalísticos (ver, por exemplo, cadeia de valor do Banco Central do Brasil, da Receita Federal do Brasil, realizando uma busca na Internet);

d) estruturas organizacional, de governança e operacional, bem como, se for o caso, societária e de financiamento e investimento;

e) fontes de receitas e execução orçamentária e financeira (aplicações de recursos definidos em programas, ações e projetos orçamentários constantes do Plano Plurianual (PPA) e da Lei Orçamentária Anual (LOA), e seus respectivos objetivos;

f) mapa estratégico em vigor, com a descrição das perspectivas e a enumeração das ações estratégicas dentro de cada área foco de atuação e ou perspectiva[5];

g) macroprocessos relevantes com breve descrição das finalidades do conjunto de processos que os compõem, associados com as ações mencionadas no item "f"; e, quando disponível, um diagrama da sua cadeia de valor.

h) detalhamento de cada macroprocesso incluindo: o objetivo, as atividades ou processos, os aspectos organizacionais, o histórico de alocação de recursos orçamentários e financeiros, o marco regulatório, o fluxograma, mapa de processo ou diagrama de blocos;

i) histórico de insumos e produtos em termos monetários, quantitativos e ou qualitativos.

8.1.3. Documentação do entendimento

183. O entendimento obtido deve ser apresentado por meio de uma visão geral da organização descritiva, complementada por diagramas, análises e gráficos resultantes da aplicação de

[4] Recomenda-se à equipe de auditoria seguir, no que for aplicável, as orientações quanto à análise preliminar do objeto, incluindo informações requeridas e fontes de informação para esse fim, que constam do Manual de Auditoria Operacional (TCU, 2010) e do Manual de Levantamento (TCU, 2017).

[5] Para os itens "d", "f", "g" e "h", ver um bom exemplo em TC 014.483/2016-5 (Acórdão 2959/2016-TCU-Plenário).

procedimentos analíticos; organograma, diagramas de cadeia de valor, mapas de processo, mapa estratégico; marco regulatório e, se aplicável, um resumo dos seus aspectos relevantes.

184. Os elementos de entendimento mencionados nos parágrafos 177 a 179 e 182, devem ser organizados de tal maneira que forneça uma compreensão clara do negócio da organização e das áreas, funções e atividades que concorrem de maneira relevante para os resultados entregues à sociedade. A descrição da visão geral deve atender os requisitos de legibilidade, especialmente os de relevância, concisão, clareza e completude (ver NAT, 129). Elementos complementares de entendimento, como diagramas, tabelas, relações, listas etc. deverão ser colocados em apêndices ou anexos.

185. A documentação do entendimento deve integrar a parte inicial do plano de auditoria, logo após a caracterização do trabalho e a declaração de seus objetivos.

8.2. PLANEJAMENTO DA AUDITORIA

8.2.1. Definição da estratégia global de auditoria

186. Depois de concluída a fase de entendimento preliminar (parágrafo 181), é iniciada a etapa de definição da estratégia global de auditoria, que deve conter as decisões-chaves e a indicação dos temas e fatores mais importantes que, no julgamento profissional do dirigente e ou do supervisor da auditoria, são significativos para direcionar os esforços da equipe de trabalho.

187. A estratégia global é parte obrigatória da documentação de auditoria e seu objetivo é registrar e comunicar à equipe o direcionamento do trabalho em termos do alcance, da época e da condução da auditoria, para orientar o desenvolvimento do plano de auditoria. Isso inclui, por exemplo, as datas-chaves (como a de envio do relatório preliminar para comentários de gestores, a de entrega do relatório final); a determinação da materialidade, com a indicação preliminar das áreas, funções e atividades que, em função de sua relevância ou risco, deverão ser inclusas no escopo de aplicação dos instrumentos de coleta de dados e dos procedimentos de auditoria, cuja evidência de auditoria obtida deverá ser avaliada com base na escala estabelecida na Tabela 7.1.

188. Além disso, estratégia global de auditoria deve trazer elementos que permitam identificar os recursos (humanos, tecnológicos e outros) a serem utilizados no trabalho, quando eles devem ser alocados, como serão supervisionados e terão seus trabalhos revisados, incluindo:

a) a determinação da natureza, época e extensão dos recursos necessários para realizar o trabalho, envolvendo:

i. recursos a serem alocados em áreas específicas da auditoria, tais como membros da equipe com experiência adequada para áreas de alto risco ou o envolvimento de especialistas em temas complexos;

ii. recursos a alocar a áreas específicas da auditoria, tais como o número de membros da equipe alocados para observar atividades em locais relevantes, a extensão da revisão do trabalho de outros auditores, se for o caso, o tempo de auditoria a ser alocado nas áreas de alto risco;

iii. utilização do trabalho dos auditores internos e ou a colaboração/cooperação destes;

iv. quando os recursos devem ser alocados, por exemplo, se em etapa intermediária ou em determinada data; e

v. como os recursos serão gerenciados, direcionados e supervisionados, por exemplo, para quando estão previstas as reuniões preparatórias e de atualização, como devem ocorrer as revisões do supervisor e do coordenador do trabalho (por exemplo, em campo ou fora dele) e se devem ser realizadas revisões de controle de qualidade do trabalho durante o seu curso (por exemplo, painéis de referência).

189. A estratégia global e o plano de auditoria são intimamente relacionados e não são processos isolados ou sequenciais, necessariamente. Mudanças em um podem resultar em mudanças no outro. Embora a estratégia global deva ser concluída antes da elaboração do plano de auditoria, ela poderá sofrer alterações ao longo das atividades desenvolvidas para elaboração do plano, em função de imprevistos, de mudanças nas condições ou identificação de informação que difere significativamente da informação disponível quando o dirigente e ou o supervisor da auditoria definiu inicialmente a estratégia. Assim, a estratégia global e o plano de auditoria devem ser alterados e atualizados, sempre que necessário, no curso da auditoria.

190. A documentação da estratégia global de auditoria pode ser feita na forma de um memorando contendo as decisões-chaves e a indicação dos temas e fatores mais importantes. Alterações significativas ocorridas na estratégia global de auditoria, e as razões dessas alterações, também devem ser documentadas.

8.2.2. Determinação da materialidade

191. A determinação da materialidade é um tema da estratégia global de auditoria e tem por base o julgamento profissional do auditor. O conceito de materialidade é relacionado à expressão "em todos os aspectos relevantes" a que se referem as normas de auditoria, e que deve estar presente na conclusão geral do relatório, no que diz respeito à conformidade do objeto aos

critérios aplicados para sua avaliação (ISSAI 100, 33).

192. Assim, com base no entendimento obtido, especialmente no que diz respeito às áreas, funções e atividades que concorrem de maneira relevante para os resultados da organização, considerando aspectos quantitativos (por exemplo, materialidade dos recursos financeiros alocados por áreas) e qualitativos (por exemplo, riscos de qualidade ou de colapso dos serviços prestados aos usuários, riscos à imagem/reputação da organização), o auditor deve estabelecer quais áreas, funções ou atividades relevantes da organização para a realização dos seus objetivos-chaves deverão compor o escopo de aplicação dos instrumentos de coleta de dados e dos procedimentos de auditoria.

193. Embora a materialidade seja uma questão de julgamento profissional do auditor, no caso da auditoria operacional de gestão de riscos, devido às suas características voltadas para ajudar aqueles com responsabilidades de governança e gestão a melhorar o desempenho (ISSAI 300, 12), o auditor pode considerar ouvir os responsáveis pela governança e administradores da entidade sobre se alguma área, função ou atividade relevante, além das que ele considerou materialmente relevantes, deveria ser parte do escopo da auditoria.

8.2.3. Elaboração do Plano de Auditoria

194. Seguindo as diretrizes estabelecidas na estratégia global de auditoria, a equipe deve elaborar o plano de auditoria, levando em conta a necessidade de atingir os objetivos da auditoria por meio do uso eficiente dos recursos.

195. Como mencionado anteriormente, as atividades desenvolvidas para elaboração do plano de auditoria podem levar a alterações na estratégia global, devido a imprevistos, mudanças nas condições ou da identificação de informação que difere significativamente da informação disponível quando o dirigente e ou o supervisor da auditoria definiu inicialmente a estratégia. Isso é normal ocorrer, principalmente em razão do entendimento mais profundo da entidade, que a equipe vai adquirindo ao trabalhar melhor as informações para elaborar o planejamento. Neste caso, a direção/supervisão da auditoria deve ser notificada para atualizar a estratégia.

196. Para elaborar o plano de auditoria a equipe deve, considerando as datas-chaves estabelecidas na estratégia global de auditoria, determinar a duração das atividades de planejamento, de aplicação dos procedimentos de coleta e análise de dados, de avaliação das evidências, de elaboração da matriz de achados e dos relatórios preliminar e final, incluindo o tempo de comentários de gestores, programar a agenda com as partes envolvidas, e elaborar o cronograma definitivo do trabalho.

197. Os resultados de todas essas atividades devem estar documentados no plano de auditoria, o qual, na parte inicial, logo após a caracterização do trabalho e a declaração de seus objetivos, deve conter a descrição da visão geral da organização, conforme abordada no tópico 8.2.3. Assim, o plano deve incluir um cronograma, a agenda de reuniões, entrevistas e outros eventos do trabalho, de modo a:

a) auxiliar a equipe de trabalho na execução da auditoria;

b) permitir que a equipe possa se responsabilizar e ser responsabilizada por seu trabalho;

c) permitir que os responsáveis pela direção e supervisão do trabalho cumpram suas responsabilidades de revisão.

8.2.4. Elaboração da Matriz de Planejamento

198. Com base nas diretrizes da estratégia global de auditoria e no entendimento obtido da organização, a equipe deve:

a) definir por áreas, funções ou atividades relevantes, as questões/subquestões de auditoria aplicáveis, com base na matriz de planejamento constante do Apêndice II;

b) determinar, em relação a cada área, função ou atividade do item anterior, a natureza (o que e como fazer), a época (quando fazer) e a extensão (o quanto fazer) em termos de procedimentos de coleta e análise de dados para atingir as conclusões previstas na coluna "o que a análise vai permitir dizer", da matriz de planejamento (Apêndice II).

c) identificar quem deve ser entrevistado e o que deve ser questionado, para fins de definir a agenda de reuniões e determinar o instrumento de coleta de dados ou procedimento de auditoria mais adequado às circunstâncias (por exemplo, questionário, se muitos, ou entrevista, se poucos);

d) preencher as colunas "informações requeridas", "fontes de informação", "procedimentos de coleta de dados", "procedimentos de análise de dados" da matriz de planejamento (Apêndice II) e desenvolver os instrumentos de coleta de dados necessários.

8.3. EXECUÇÃO DA AUDITORIA

8.3.1. Aplicação dos procedimentos e instrumentos de coleta de dados

199. Uma vez que o plano de auditoria, incluindo a matriz de planejamento, tenha sido concluído e homologado, cada membro da equipe realizará suas atividades conforme designado no plano de auditoria, aplicando os procedimentos de auditoria planejados e os instrumentos de coleta de dados para obter as evidências de auditoria necessárias às conclusões.

200. À proporção que os trabalhos de campo forem se desenvolvendo, deve-se preencher a matriz de achados, conforme o modelo estabelecido no Manual de Auditoria Operacional (BRASIL, 2010). Dadas as características desse tipo de auditoria, e dependendo da complexidade da organização, pode ser necessário o preenchimento de matrizes de achados por área, função ou atividade, especialmente no que diz respeito à dimensão 2 – Processos. Neste caso, será necessário um trabalho de consolidação posterior, utilizando procedimento semelhante ao que é adotado na matriz de achados consolidadora de fiscalizações de orientação centralizada (FOC, Portaria-Adplan 2/2010).

201. A coluna "situação encontrada" deve ser preenchida estabelecendo-se uma relação direta com cada item da coluna "o que a análise vai permitir dizer" da matriz de planejamento (Apêndice II), confirmando ou negando cada uma das hipóteses ou conclusões formuladas, descrevendo o contexto específico da situação encontrada na organização.

202. A coluna "critério" deve indicar não apenas as fontes dos critérios, fornecidas no Apêndice II, mas explicitar o que o critério preconiza, devendo o auditor, a partir da indicação da fonte, localizar e descrever o que ele preconiza e porque é aplicável à situação, porém evitando-se ao máximo transcrições.

8.3.2. Avaliação das evidências e conclusões

203. A evidência de auditoria obtida mediante aplicação dos procedimentos de auditoria e respectivos instrumentos de coleta dados, devidamente registrada na matriz de achados (após a consolidação, se aplicável), deverá ser avaliada utilizando a escala de avaliação constante da Tabela 7.1, registrando-se a conclusão quanto ao resultado da pontuação de cada aspecto na Planilha de Análise da Maturidade da Gestão de Riscos, fornecida juntamente com este roteiro, que calculará, automaticamente, o nível de maturidade de cada aspecto e de cada uma das dimensões do modelo, como também em nível de maturidade global.

8.4. RELATÓRIO DA AUDITORIA

204. Por tratar-se de uma auditoria operacional, o relatório da auditoria de gestão de riscos deve seguir os padrões estabelecidos no Manual de Auditoria Operacional (BRASIL, 2010), com as seguintes observações específicas:

a) cada capítulo principal tratará de uma dimensão do modelo de avaliação;

b) cada subtítulo tratará de uma seção do modelo, quando aplicável;

c) os textos explicativos que constam do Apêndice I, bem como da descrição do modelo de avaliação (capítulo 6), podem ser aproveitados para descrever o objetivo do capítulo, fazer a sua contextualização e descrever o seu conteúdo, como exemplificado a seguir.

AMBIENTE

O **objetivo do capítulo** é descrever o resultado da avaliação das capacidades existentes na organização, em termos de **liderança**, **políticas & estratégias** e preparo das **pessoas**, incluindo aspectos relacionados com a ***cultura***, a ***governança de riscos*** e a ***consideração do risco na definição da estratégia e dos objetivos*** em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas.

Contextualização específica do capítulo

Para que uma organização possa desfrutar de um gerenciamento de riscos eficaz, a atitude e o interesse da alta administração devem ser claros e definitivos, bem como permear toda a organização. Não é suficiente apenas dizer as palavras corretas, uma atitude de "faça o que digo e não o que faço" somente gerará um ambiente inadequado, assim, a liderança é um aspecto fundamental, avaliado neste capítulo, para que uma gestão de riscos eficaz possa prosperar na organização.

A gestão de riscos deve fazer parte das considerações sobre estratégias e planos em todos os níveis críticos da organização, concretizando-se pelo processo de gerenciamento de riscos nas operações, funções e atividades relevantes nas diversas partes da organização.
Organizações com políticas e estratégias de gestão de riscos adequadas contam com:

a) um processo e métodos para definir claramente objetivos e tolerâncias a risco ou variações aceitáveis no desempenho para permitir que os seus riscos e resultados possam ser gerenciados, incorporando explicitamente indicadores-chaves de risco e desempenho em suas estruturas de governança e gestão;

b) competências e capacidade para identificar eventos potenciais que podem impactar a organização, o governo ou a comunidade e fazem uso de medidas práticas e razoáveis para gerenciar esses eventos;

c) asseguração de que sua administração e seu corpo executivo:
   i. estão adequadamente informados sobre as exposições a risco da organização;
   ii. estão completa e diretamente envolvidos em estabelecer e rever o processo de gestão de riscos em suas áreas; e
   iii. alocam recursos adequados e suficientes para a gestão de riscos, levando em conta a natureza e o nível dos riscos identificados e o tamanho da organização.

O gerenciamento de riscos é um processo efetuado pelo conselho de administração, pela diretoria executiva e pelos demais empregados, isto é, pelas pessoas, mediante o que fazem e o que dizem. São as pessoas que estabelecem a missão, a estratégia e os objetivos e implementam os mecanismos de gerenciamento de riscos da organização (COSO, 2004). Assim, o gerenciamento de riscos afeta as ações das pessoas, e estas o gerenciamento de riscos, uma vez que nem sempre entendem, se comunicam ou desempenham suas funções de forma consistente. A gestão de riscos deve proporcionar os mecanismos necessários para ajudar as pessoas a entender o risco no contexto dos objetivos da organização, bem como suas responsabilidades e seus limites de autoridade, criando uma associação clara e estreita entre os deveres das pessoas e como elas os cumprem no tocante à estratégia e aos objetivos da organização (COSO, 2004).

Portanto, o grau de conhecimento das pessoas sobre os objetivos da organização, a existência de canais de comunicação para que questões relacionadas a risco sejam levantadas e decididas, a definição clara de responsabilidades e limites de autoridade em relação aos processos de gestão de riscos, a existência de arcabouço conceitual de risco uniformemente conhecido e utilizado na organização, bem como a oferta de cursos de capacitação sobre o tema são atributos importantes que devem estar presentes na conformação de um ambiente de gestão de riscos apropriado.

Descrição do conteúdo do capítulo

Este capítulo está dividido em três seções, na primeira, que trata da **liderança**, avalia-se em que medida os responsáveis pela governança e a alta administração assumem um compromisso forte e sustentado e exercem supervisão para obter comprometimento com a gestão de riscos em todos os níveis da organização, promovendo-a e dando suporte, de modo que possam ter uma expectativa razoável de que no cumprimento da missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir seus objetivos de gerar valor para as partes interessadas, tendo o cidadão e a sociedade como vetores principais.

Na segunda seção, avalia-se em que medida a organização dispõe de **políticas e estratégias** de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.

Por fim, a terceira seção do capítulo, avalia se as **pessoas** na organização estão informadas, habilitadas e autorizadas para exercer os seus papéis e as suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.

205. Além disso, a combinação de outros textos que constam do apêndice de critérios e da matriz de planejamento, pode ajudar o auditor a descrever os achados de auditoria e as boas práticas da organização, devendo o auditor, neste caso, realizar as adaptações necessárias ao contexto específico do trabalho, tomando o devido cuidado de não apenas realizar uma cópia, mas utilizar os textos como inspiração.

8.4.1. Comentários de gestores

206. Por ser uma auditoria operacional, a regra é submeter o relatório preliminar aos comentários dos gestores, inclusive os achados, as conclusões e as propostas de encaminhamento formuladas pela equipe. A inclusão desses comentários no relatório final resulta em um documento que não só apresenta os achados, as conclusões e as propostas da equipe, mas também a perspectiva dos dirigentes da entidade e as ações corretivas que pretendem tomar. Os comentários recebidos dos gestores devem, sempre que possível, ser incorporados, de forma resumida, no relato dos achados e serão analisados pela equipe juntamente com os demais fatos (NAT, 144-145 e 147).

207. O relatório preliminar a ser submetido aos gestores deve ser antes revisado pelo supervisor e deve ser remetido por intermédio de ofício da unidade técnica, estipulando-se prazo reduzido, porém factível, para que os gestores encaminhem seus comentários. O ofício deve informar que a obtenção desses comentários não representa abertura do contraditório e, portanto, não significa exercício de direito de defesa, o qual, se necessário, poderá ser exercido nas etapas processuais posteriores. Deve, ainda, esclarecer que a não apresentação dos comentários, no prazo estipulado, não impedirá o andamento normal do processo nem será considerada motivo de sanção (NAT, 146)

8.4.2. Propostas de encaminhamento

208. As propostas de determinação e de recomendação devem ser formuladas focando "o quê" deve ser aperfeiçoado ou corrigido e não "o como", dado à discricionariedade que cabe ao gestor e ao fato de que a equipe de auditoria não detém a única ou a melhor solução para o problema identificado. Recomendações geralmente sugerem o aperfeiçoamento necessário, mas não a forma de alcançá-lo (NAT, 165).

209. Quando o gestor apresentar planos de ação consistentes para os aperfeiçoamentos necessários apontados no relatório preliminar, estes planos devem ser noticiados no relatório final, sem formulação de propostas de encaminhamento, a não ser para a realização de monitoramento posterior da implementação do plano de ação, se relevante.

210. Para que as propostas da equipe sejam relevantes, convém levar em conta que uma prática, componente ou dimensão de nível aprimorado ou avançado, só deveriam ter propostas formuladas considerando uma vantagem clara em termos de custo-benefício que a sua implementação poderá proporcionar para o alcance dos resultados da gestão de riscos.

9. GLOSSÁRIO

***Accountability* pública** – obrigação que têm as pessoas, físicas ou jurídicas, públicas ou privadas, às quais se tenha confiado recursos públicos, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a sociedade e a quem lhes delegou essas responsabilidades sobre o cumprimento de objetivos e metas e o desempenho alcançado na gestão dos recursos públicos. É, ainda, obrigação imposta a uma pessoa ou entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram confiados em conformidade com os termos segundo os quais eles lhe foram entregues (TCU, 2011). Ver também Responsabilização.

Aceitar risco – ver Resposta a risco.

Alta administração – gestores que integram o nível executivo mais elevado da organização com poderes para estabelecer as políticas, os objetivos e conduzir a implementação da estratégia para realizar os objetivos da organização.

Análise de riscos – processo de compreender a natureza e determinar o nível (magnitude, severidade) de um risco ou combinação de riscos, mediante a combinação das consequências e de suas probabilidades (ABNT, 2009).

Apetite a risco – quantidade de risco em nível amplo que uma organização está disposta a aceitar na busca de seus objetivos (INTOSAI, 2007). Quantidade e tipo de risco*s* que uma organização está preparada para buscar, reter ou assumir (ABNT, 2009a).

Arranjos de contingência – acordos que estabelecem como as partes devem proceder caso um ou mais riscos se concretizem.

Atividade – termo genérico utilizado para expressar operações, ações ou transações que uma organização, pessoa ou entidade realiza com vistas ao alcance de objetivos determinados, refletindo os fluxos de trabalho cotidianos que formam os processos de trabalho (TCU, 2012).

Atividades de controle – ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos (COSO, 2013).

Avaliação de riscos – processo de comparar os resultados da análise de riscos com os critérios de risco da organização, para determinar se um risco e/ou sua magnitude é aceitável ou tolerável (ABNT, 2009).

Consequência – resultado de um evento que afeta positiva ou negativamente os objetivos da organização.

Controles internos – ver **Atividades de controle**.

Critérios de auditoria – referências usadas para mensurar ou avaliar o objeto de auditoria (ISSAI 100; ISA/NBCTA Estrutura Conceitual para trabalhos de asseguração). O referencial que indica o estado requerido ou desejado ou a expectativa em relação ao objeto de auditoria. Reflete como deveria ser a gestão, provendo o contexto para compreensão dos achados de auditoria e para a avaliação das evidências de auditoria (BRASIL, 2011).

Estrutura de gestão de riscos – conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização (ABNT, 2009).

Nota 1 Os fundamentos incluem a política, objetivos, mandatos e comprometimento para gerenciar riscos.

Nota 2 Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades. (ABNT, 2009).

Evento – um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a implementação da estratégia e a realização de objetivos de modo negativo, positivo ou ambos (INTOSAI, 2007). Eventos com impacto negativo representam riscos. Eventos com impacto positivo representam oportunidades; ocorrência ou mudança em um conjunto específico de circunstâncias, podendo consistir em alguma coisa não acontecer. A expressão "eventos potenciais" é muitas vezes utilizada para caracterizar riscos (ABNT, 2009).

Evitar risco – ver Resposta a risco.

Fonte de risco – elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (ABNT, 2009).

Gerenciamento de riscos – aplicação de uma arquitetura (princípios, estrutura e processo) para identificar riscos, analisar e avaliar se devem ser modificados por algum tratamento a fim de atender critérios de risco. Ao longo desse processo, comunica-se e consulta-se as partes interessadas, monitora-se e analisa-se criticamente os riscos e os controles que os modificam, a fim de assegurar que nenhum tratamento de risco adicional é requerido (ABNT, 2009).

Gerenciamento de riscos corporativos – processo efetuado pelo conselho de administração, gestores e outras pessoas, aplicado na definição da estratégia e através de toda a entidade, estruturado para identificar potenciais eventos que possam afetar a entidade e gerenciá-los para mantê-los dentro de seu apetite a risco, de modo a fornecer uma garantia razoável quanto à realização dos objetivos da entidade (COSO GRC, 2004; INTOSAI, 2007).

Gestão – estruturas responsáveis pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a consecução de seus objetivos, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas (TCU, 2014).

Gestão de riscos – atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco (ABNT, 2009).

Gestor – pessoa que ocupa função de gestão em qualquer nível hierárquico da organização.

Governança – conjunto de políticas e processos que moldam a maneira como uma organização é dirigida, administrada, controlada e presta contas do cumprimento das suas obrigações de *accountability*. No setor público, a governança compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (BRASIL, 2014).

Identificação de riscos – processo de busca, reconhecimento e descrição de riscos; envolve a identificação das fontes de risco, os eventos, suas causas e suas consequências potenciais (ABNT, 2009), pode envolver análise de dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas.

Indicadores-chaves de desempenho – número, percentagem ou razão que mede um aspecto do desempenho na realização de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização, com o objetivo de comparar esta medida com metas preestabelecidas (TCU, 2010d, adaptado).

Indicadores-chaves de risco – número, percentagem ou razão estabelecido para monitorar as variações no desempenho em relação à meta para o cumprimento de objetivos estratégicos e operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização (TCU, 2010d, adaptado).

Macroprocessos – processos mais abrangentes da organização. Representam conjuntos de atividades agregadas em nível de abstração amplo, que formam a cadeia de valor de uma organização, explicitando como ela opera para cumprir sua missão e atender as necessidades de suas partes interessadas (BRASIL, 2011). Ver também **Processo**.

Mapa de processo – representação gráfica da sequência de atividades que compõem um processo, fornecendo uma visão dos fluxos operacionais do trabalho, incluindo, a depender do nível de análise que se deseja realizar, a evidenciação dos agentes envolvidos, os prazos, o fluxo de documentos, o processo decisório (BRASIL, 2003).

Matriz de achados – papel de trabalho que estrutura o desenvolvimento dos achados, explicitando para cada um a situação encontrada (ou condição) o critério de auditoria, as causas, os efeitos, as evidências de auditoria, as propostas de encaminhamento (BRASIL, 2011).

Matriz de avaliação de riscos – papel de trabalho que estrutura e sistematiza a identificação de riscos, a análise de riscos e a avaliação de riscos, incluindo a avaliação de controles internos e outras respostas a riscos, podendo incluir as decisões sobre o tratamento de riscos.

Matriz de planejamento – papel de trabalho que organiza e sistematiza o planejamento do trabalho de auditoria e documenta o programa de auditoria, discriminando o objetivo de auditoria e as questões de auditoria formuladas para alcançar tal objetivo; as informações requeridas, as fontes de informações e os procedimentos de auditoria para responder às questões. (NAT, 94, 96-97, BRASIL, 2011).

Matriz de risco – matriz gráfica que exprime o conjunto de combinações de probabilidade e impacto de riscos para classificar os níveis de risco.

Medidas de contingência – ações previamente planejadas que devem ser executadas caso um ou mais riscos se concretizem.

Mitigar risco – ver **Resposta a risco**.

Monitoramento – verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. Monitoramento pode ser aplicado a riscos, a controles, à estrutura de gestão de riscos e ao processo de gestão de riscos.

Nível de risco – magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências [impacto] e de suas probabilidades (ABNT, 2009).

Objetivos-chaves – os macro-objetivos, macroprodutos ou resultados finalísticos que geram, preservam e entregam valor público em benefício do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos (SERRA, 2008).

Obrigações de accountability – ver ***Accountability* pública**.

Órgão de governança – conselho de administração, diretoria colegiada ou semelhantes ou ainda órgãos com responsabilidade de supervisão geral da direção estratégica de entidades e das responsabilidades relacionadas às obrigações de *accountability*.

Parceria – arranjo estabelecido a fim de possibilitar um relacionamento colaborativo entre as partes (denominadas parceiras) visando o alcance de objetivos específicos previamente acordados entre elas.

Parte interessada *(stakeholder)* – pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade da organização (ABNT, 2009).

Plano de gestão de riscos – esquema dentro da estrutura de gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos, incluindo, tipicamente, procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades (ABNT, 2009). Um manual ou complemento à política de gestão de riscos que pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização (ABNT, 2009, adaptado).

Política de gestão de riscos – documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis em todos os níveis, dentre outros aspectos (ABNT, 2009).

Processo – conjunto de atividades inter-relacionadas ou interativas que transformam insumos (entradas) em produtos/serviços (saídas) com valor agregado. Processos são geralmente planejados e realizados de maneira contínua para agregar valor na geração de produtos e serviços. Processos podem ser agrupados em macroprocessos e subdivididos em subprocessos (BRASIL, 2011).

Processo de avaliação de riscos – processo global representado pelo conjunto de métodos e técnicas que possibilitam a identificação de riscos, a análise de riscos e a avaliação de riscos que possam impactar os objetivos de organizações, programas, projetos e atividades. Envolve a identificação das fontes de risco, dos eventos e de sua probabilidade de ocorrência, de suas causas e suas consequências potenciais, das áreas de impacto, das circunstâncias envolvidas, inclusive aquelas relativas a cenários alternativos (ABNT, 2009, adaptado).

Processo de gestão de riscos – aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica de riscos (ABNT, 2009). Sinônimo de **gerenciamento de riscos**.

Processos de governança – os processos que integram os mecanismos de liderança, estratégia e controle e que permitem aos responsáveis pela governança avaliar, direcionar e monitorar a atuação da gestão (BRASIL, 2014).

Responsabilização (*accountability*) – responsabilidade de uma organização ou indivíduo perante suas decisões e atividades e prestação de contas a seus órgãos de governança, autoridades legais e, de modo mais amplo, as suas outras partes interessadas no que se refere a essas decisões e atividades (ABNT, 2010). Ver também ***Accountability* pública**.

Responsáveis pela governança – pessoas ou organizações com responsabilidade de supervisão geral da direção estratégica da entidade e das responsabilidades relacionadas às obrigações de *accountability* da organização (ISSAI 1003).

Respostas a risco – opões e ações gerenciais para tratamento de riscos. Inclui evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco porque o risco está além do apetite a risco da organização e outra resposta não é aplicável; transferir o risco a outra parte ou compartilhar o risco com outra parte; aceitar o risco por uma escolha consciente; ou mitigar o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências (INTOSAI, 2007).

Risco – possibilidade de um evento ocorrer e afetar adversamente a realização de objetivos (COSO GRC, 2004); possibilidade de algo acontecer e ter impacto nos objetivos, sendo medido

em termos de consequências e probabilidades (BRASIL, 2010c); efeito da incerteza nos objetivos (ABNT, 2009).

Risco de controle – possibilidade de que os controles adotados pela administração não sejam eficazes para tratar o risco a que se propõe.

Risco de oportunidade – risco associado a aproveitar oportunidades que podem gerar benefícios à organização.

Risco estratégico – risco de longo prazo ou risco de oportunidade relacionado aos objetivos estratégicos e às estratégias adotadas para alcançá-los.

Risco inerente – o risco intrínseco à natureza do negócio, do processo ou da atividade, independentemente dos controles adotados.

Risco operacional – risco de perdas resultantes direta ou indiretamente de falha ou inadequação de processos internos, pessoas e sistemas ou de eventos externos.

Risco residual – o risco retido de forma consciente ou não pela administração, que remanesce mesmo após o tratamento de riscos.

Risco significativo – aquele com grande probabilidade de ocorrer e, se ocorrer, ter um impacto relevante nos objetivos (LONGO, 2011).

Riscos-chaves – riscos estratégicos e riscos operacionais relevantes para o negócio, relacionados aos objetivos-chaves da organização.

Transferir risco – Ver **Repostas a riscos**.

Tratamento de riscos – processo de implementar respostas a risco selecionadas. Ver Repostas a riscos.

Valor público – produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização pública que representem respostas efetivas e úteis às necessidades ou demandas de interesse público e modifiquem certos aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos (SERRA, 2008).

10.REFERÊNCIAS

ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO 31000: *Gestão de Riscos: Princípios e diretrizes*. Rio de Janeiro, 2009.

_____. ABNT ISO GUIA 73: *Gestão de Riscos: Vocabulário*, 2009a.

_____. ABNT NBR ISO 26000:2010 – Diretrizes sobre responsabilidade social. Rio de Janeiro, 2010.

AVALOS, José Miguel Aguilera. *Auditoria e gestão de riscos;* Instituto Chiaventato (org.) – São Paulo : Saraiva, 2009.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. *Guia de Orientação para o Gerenciamento de Riscos*. Secretaria de Gestão Pública. Departamento de Inovação e Melhoria da Gestão. Gerência do Programa GESPÚBLICA. Brasília, 2013. Disponível em <http://www.planejamento.gov.br/secretarias/upload/Arquivos/segep/projeto/2013_03_01_Produto_VII_Risco_Oportunidade_PT.pdf>. Acesso em: março, 2017.

_____. _____ e Controladoria-Geral da União. *Instrução Normativa Conjunta Nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.* Brasília, 2016. Disponível em < http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=14&data=11/05/2016>. Acesso em: maio 2016.

_____. Tribunal de Contas da União. *Técnica de Auditoria Mapa de Processo*. – Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2003.

_____. _____. *Manual de auditoria operacional*. Brasília: TCU, 2010. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. Análise *SWOT e Diagrama de Verificação de Risco aplicados em Auditoria.* Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010a. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Técnica de pesquisa para auditorias*. Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010b. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Instrução Normativa 63/2010*. Estabelece normas de organização e de apresentação dos relatórios de gestão e das peças complementares que constituirão os processos de contas da administração pública federal, para julgamento do Tribunal de Contas da União, nos termos do Art. 7º da Lei nº 8.443, de 1992. – Brasília: TCU, 2010c. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Técnica de Indicadores de Desempenho para Auditorias*. – Brasília: TCU, Segecex, Secretaria de Fiscalização e Avaliação de Programas de Governo (Seprog), 2010d. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Padrões de Levantamento.* Portaria-Segecex 15/2011. – Brasília: TCU, Segecex, Secretaria Adjunta de Planejamento e Procedimentos (Adplan) e Secretaria Adjunta de Supervisão e Suporte (Adsup), 2011. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Curso Avaliação de Controles Internos*. Conteudistas: Antonio Alves de Carvalho Neto, Bruno Medeiros Papariello. Aula 2. Modelos de referência para controle interno. 2. ed. – Brasília: TCU, Instituto Serzedello Corrêa, 2012.

_____. _____. Acórdão nº 2467/2013-TCU-Plenário. Ata 35, Sessão de 11/09/2013. *Levantamento de auditoria para elaboração de indicador para medir o grau de maturidade de entidades públicas na gestão de riscos*. Brasília, 2013. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Curso Gestão de Riscos – Princípios e Diretrizes*. Antonio Alves de Carvalho Neto. 1. ed. presencial (slides) – Brasília: TCU, Instituto Serzedello Corrêa, 2013a.

_____. _____. *Técnica de grupo focal para auditorias*. Brasília: TCU, Secretaria de Métodos Aplicados e Suporte à Auditoria (Seaud), 2013b. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Resolução-TCU nº 246, de 30 de novembro de 2011. Altera o Regimento Interno do Tribunal de Contas da União*, aprovado pela Resolução TCU nº 155, de 4 de dezembro de 2002. Brasília, 2015. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Normas de Auditoria do Tribunal de Contas da União*. Revisão Junho 2011. Brasília: TCU, 2011. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Regimento Interno do Tribunal de Contas da União*. Brasília: TCU, 2012. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

_____. _____. *Referencial básico de governança aplicável a órgãos e entidades da administração pública*. Versão 2. - Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2014. Disponível em: <http://www.tcu.gov.br>. Acesso em: março, 2017.

CANADÁ. Secretaria do Conselho do Tesouro do Canadá. *Framework for the management of risk*. Ottawa, 2010a. Disponível em: <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text>. Acesso em: maio de 2012.

_____. Secretaria do Conselho do Tesouro do Canadá. *Guide to integrated risk management. Ottawa*, 2010b. Disponível em: <http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirtb-eng.asp>. Acesso em: maio de 2012.

COYLE, G. *The Analytic Hierarchy Process*. Pearson Educational: New York, 2004.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). *Controle Interno: Estrutura Integrada: Sumário Executivo e Estrutura*. Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2013. Disponível em: <http://www.iiabrasil.org.br/new/2013/downs/coso/COSO_ICIF_2013_Sumario_Executivo.pdf>. Acesso em: março, 2017.

_____. *Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura* (COSO GRC, 2004). Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2007. Disponível em: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em: março, 2017.

_____. *Enterprise Risk Management: Align Risk with Strategy and Performance.* COSO, 2016. Disponível em: <http:// http://erm.coso.org/Pages/viewexposuredraft.aspx>. Acesso em: março, 2017.

_____. *Enterprise Risk Management: Integrating with Strategy and Performance*. Executive Summary, COSO, 2017. Disponível em: <https://www.coso.org/Pages/default.aspx>. Acesso em: dezembro, 2017.

DAHMS, T. *Risk management and corporate governance: are they the same?* 2008. Disponível em: <http://www.plumcon.com.au/PDF/Risk_Gov_1.pdf>. Acesso em: junho de 2013.

DANTAS, José Alves; RODRIGUES, Fernanda Fernandes; MARCELINO, Gileno Fernandes; LUSTOSA, Paulo Roberto Barbosa. *Custo-benefício do controle: proposta de um método para avaliação com base no COSO*. Revista de Contabilidade, Gestão e Governança. 2010.

DE CICCO, Francesco (Rev.). *Gestão de Riscos: Diretrizes para implementação da ISO 31000:2009 (Série Risk Management)*. Risk Tecnologia Editora, 2009.

ESTADOS UNIDOS. General Accounting Office (GAO). GAO-01-1008G: *Ferramenta de gestão e avaliação de controle interno.* Washington, D.C., 2001.

INSTITUTO DOS AUDITORES INTERNOS (IIA). *Normas Internacionais para a Prática Profissional de Auditoria Interna.* Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009.

_____. *Declaração de Posicionamento do IIA: O Papel da Auditoria Interna no Gerenciamento de Riscos.* Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009a.

_____. *Declaração de Posicionamento do IIA: As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles.* Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2013.

INTOSAI (International Organization of Supreme Audit Institutions). *Reporting Standards in Government Auditing* (ISSAI 400). Vienna, 2001. Disponível em: <www.issai.org>. Acesso em: junho 2015.

_____. *Performance Audit Methodology – to ISSAI 3000 (ISSAI 3000/Appendix 1, 2004)*. Viena: Intosai, 2004. Disponível em: <www.issai.org>. Acesso em: junho 2015.

_____. Subcomitê de Normas de Controle Interno. *Diretrizes para Normas de Controle Interno do Setor Público – Informações Adicionais sobre Gestão de Risco nas Entidades*. INTOSAI GOV 9130. Áustria, 2007. Tradução: Antonio Alves de Carvalho Neto. Brasília, 2013.

KNIGHT, K. *Risk Management: an integral component of corporate governance and good management*. ISO Bulletin, p.21-24, Out. 2003.

LONGO, Cláudio Gonçalo. *Manual de Auditoria e Revisão de Demonstrações Financeiras.* São Paulo: Atlas, 2011.

MARTINS, N. C.; SANTOS, L. R.; DIAS FILHO, J. M. *Governança empresarial, riscos e controles internos: a emergência de um novo modelo de controladoria.* Revista Contabilidade & Finanças, São Paulo,n. 34, p. 7-22, jan./abr. 2004.

OCDE (OECD - Organisation for Economic Co-operation and Development). *Avaliações da OCDE Sobre Governança Pública: Avaliação da OCDE sobre o Sistema de Integridade da*

Administração Pública Federal Brasileira - Gerenciando riscos por uma administração pública mais íntegra. OECD Publishing, 2011. Disponível em: <http://www.cgu.gov.br/assuntos/articulacao-internacional/convencao-da-ocde/arquivos/avaliacaointegridadebrasileiraocde.pdf/view>. Acesso em: março, 2017.

REINO UNIDO (UK). National Audit Office. Focus Groups. *How to apply the technique to vfm work*. London: NAO, 1997.

_____. _____. Comptroller and Auditor General. *Supporting innovation: Managing risk in government departments*. Londres, 2000. Disponível em: <http://www.nao.org.uk/wp-content/uploads/2000/08/9900864.pdf>. Acesso em: outubro de 2014.

_____. HM Treasury. *Management of Risk - Principles and Concepts - The Orange Book*. HM Treasury do HM Government, 2004._____._____. Risk management assessment framework: a tool for departaments. London, 2009. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf>. Acesso em: maio de 2012.

_____. _____. *Risk management assessment framework: a tool for departments*. Londres, 2009. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf>. Acesso em: maio de 2012.

SERRA, Alberto. Modelo aberto de gestão para resultados no setor público. tradução de Ernesto Montes-Bradely y Estayes. – Secretaria de Estado da Administração e dos Recursos Humanos (SEARH/RN): Natal, RN, 2008.

SINEK, Simon. *Start with Why: How Great Leaders Inspire Everyone to Take Action*. Penguin Group: New York, 2011.

APÊNDICES

11.APÊNDICES

APÊNDICE I – CRITÉRIOS PARA AVALIAÇÃO DA MATURIDADE EM GESTÃO DE RISCOS

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
1. AMBIENTE **Nesta dimensão, busca-se avaliar as capacidades existentes na organização em termos de liderança, políticas, estratégias e de preparo das pessoas, incluindo aspectos relacionados com *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia e dos objetivos* em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas.**	
1.1. Liderança **Nesta seção, busca-se avaliar em que medida os responsáveis pela governança e a alta administração exercem suas *responsabilidades de governança de riscos* e *cultura*, assumindo um *compromisso* forte e sustentado e exercendo *supervisão* para obter *comprometimento* com a gestão de riscos em todos os níveis da organização, promovendo-a e dando *suporte*, de modo que possam ter uma expectativa razoável de que no cumprimento da sua missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir os seus objetivos de agregar, preservar e entregar valor às partes interessadas, tendo o cidadão e a sociedade como vetores principais.**	
Cultura **1.1.1. A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos, e da consciência de riscos como aspectos-chaves para o reforço da *accountability*:**	IN-MP/CGU Nº 1/2016, Art. 8º, I e II; Art. 11, I; Art. 16, I e Art. 21; COSO GRC 2004, 2; COSO GRC *Public Exposure* (PE) 2016, Princípios 3, 4 e 5; ISO 31000:2009, 3, "h" e 4.2;
a) fornecendo normas, orientações e supervisionando a inclusão desses aspectos-chaves nos programas de apoio ao desenvolvimento de gestores;	
b) reforçando o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização; e	

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
c) instituindo políticas, programas e medidas definindo padrões de comportamento desejáveis, tais como códigos de ética e de conduta, canais de comunicação para cima e de denúncia, ouvidoria, e avaliação da aderência à integridade e aos valores éticos.	OCDE, 2011.
Governança de riscos **1.1.2. Os responsáveis pela governança e a alta administração utilizam instâncias internas (p.ex.: comitês de governança, riscos e controles, auditoria, coordenação de gestão de riscos etc.) e outras medidas para apoiar suas responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chaves da organização.**	IN-MP/CGU Nº 1/2016, Art. 23, II, Art. 17, II, "a" e "d"; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, e 2; ISO 31000:2009, 3, "b", "c", "e" e 4.1.
Supervisão da governança e da alta administração **1.1.3. Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos, inclusive mediante:**	
a) incorporação explícita e monitoramento regular de indicadores-chaves de risco e indicadores-chaves de desempenho nos seus processos de governança e gestão;	IN-MP/CGU Nº 1/2016, Art. 16, parágrafo único; Art. 19, 20 e 23, IX; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, 2 e 5; ISO 31000:2009, 4.2.
b) notificação regular e oportuna sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos;	
c) revisão sistemática da visão de portfólio de riscos em contraste com o apetite a riscos e fornecimento de direção clara para gerenciamento dos riscos;	
d) utilização dos serviços da auditoria interna e de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controle; e	

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
e) definição do nível de maturidade almejado para a gestão de riscos e monitoramento do progresso das ações para atingir ou manter-se no nível definido.	
1.2. Políticas e estratégias **Nesta seção, busca-se avaliar em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.**	
Direcionamento estratégico **1.2.1. A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico (objetivos-chaves, missão, visão e valores fundamentais da organização), alinhado com as finalidades e as competências legais da entidade, traduzindo uma expressão inicial do risco aceitável (apetite a risco) para a definição da estratégia e a fixação de objetivos estratégicos e de negócios, e para o gerenciamento dos riscos relacionados.**	IN-MP/CGU Nº 1/2016, Art. 2º, II; Art. 14, II; Art. 16, II; e Art. 19; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 1, 3 e 7. ISO 31000:2009, 5.3.3.
1.2.2. A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o *apetite a risco* na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas, a fim de orientar a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco.	IN-MP/CGU Nº 1/2016, Art. 2º, II, e Art. 14, II; Art. 16, II, e V; COSO GRC 2004, 1, 2 e 3; COSO GRC PE 2016, Princípios 1, 7 e 8; ISO 31000:2009, 3, "g" e 5.3.3.
Integração da gestão de riscos ao processo de planejamento **1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos de modo que, a partir do direcionamento estratégico e do apetite a risco definidos conforme abordado nas questões 1.2.1 e 1.2.2, são definidos:**	IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 14, IV; Art. 16, II.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
a) os *objetivos estratégicos* de alto nível alinhados e dando suporte à missão, à visão e aos propósitos da organização e selecionadas as estratégias para atingi-los, considerando as várias alternativas de cenários e os riscos associados, de modo a estabelecer uma base consistente para a definição dos objetivos de negócios específicos em todos os níveis da organização; e	COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 9, 10 e 11; INTOSAI GOV 9130/2007, 1.3 e 2.2.
b) os *objetivos de negócios* específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas *tolerâncias a risco* (ou variações aceitáveis no desempenho), alinhados aos objetivos estratégicos e ao apetite a risco estabelecidos.	
1.2.4. A administração define os objetivos mencionados na alínea "b", acima, e as respectivas medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), explicitando-os com clareza suficiente, em termos específicos e mensuráveis, comunicando-os a todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização e aos responsáveis em todos os níveis, a fim de permitir a identificação e avaliação dos riscos que possam ter impacto no desempenho e nos objetivos.	IN-MP/CGU Nº 1/2016, Art. 16, II; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 10 e 11; COSO 2013, Princípio 6, atributos "a" e "b"; INTOSAI GOV 9130, 2.2.
Política de gestão de riscos **1.2.5. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, comunicada apropriadamente e disponível para acesso a todos, que aborde os seguintes aspectos:**	IN-MP/CGU Nº 1/2016, Art. 17; ISO 31000:2009, 4.3.2.
a) os princípios e objetivos relevantes da gestão de riscos na organização e as ligações entre os objetivos e políticas da organização com a política de gestão de riscos;	IN-MP/CGU Nº 1/2016, Art. 17, I. ISO 31000:2009, 4.3.2.
b) as diretrizes para a integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações;	IN-MP/CGU Nº 1/2016, Art. 17, II, "a"; ISO 31000:2009, 3, "b" e 4.3.4;

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
c) a definição clara de responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas (unidades, departamentos, divisões, processos e atividades), incluindo a responsabilidade pela implementação e manutenção do processo de gestão de riscos e de asseguração da suficiência, eficácia e eficiência de quaisquer controles;	IN-MP/CGU Nº 1/2016, Art. 17, II, "d" e III; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípio 5;
d) diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados, através de um plano de implementação do processo de gestão de riscos, em todos os níveis, funções e processos relevantes da organização;	IN-MP/CGU Nº 1/2016, Art. 17, II, "b" e 18; ISO 31000:2009, 4.3.4 e 4.4.2. COSO GRC 2004, 4 a 9; COSO GRC PE 2016, Princípios 12 a 16 e 21.
e) diretrizes sobre como o desempenho da gestão de riscos, a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política de gestão de riscos serão medidos e reportados; e	IN-MP/CGU Nº 1/2016, Art. 17, II, "c"; ISO 31000:2009, 4.3.2, 4.3.3 e 4.5; COSO GRC 2004, 8 e 9; COSO GRC PE 2016, Princípios 20 e 21.
f) atribuição clara de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como diretrizes sobre a forma e a periodicidade como as alterações devem ser efetivadas.	IN-MP/CGU Nº 1/2016, Art. 17, II, "c" e III; ISO 31000:2009, 4.3.3, 4.5 e 4.6. COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 22 e 23.
Comprometimento da gestão **1.2.6. A alta administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade.**	IN-MP/CGU Nº 1/2016, Art. 12 e 16, § único; Art. 17, II, "e" e "f"; Art. 19 e 20; ISO 31000:2009, 4.2 e 4.3.3.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
Alocação de recursos **1.2.7. A administração aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas de TI, programas de treinamento, métodos e ferramentas para gerenciar riscos) para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chaves, bem como com a natureza e o nível dos riscos.**	IN-MP/CGU Nº 1/2016, Art. 17, II, "f"; Art. 23, II, III e IX. ISO 31000:2009, 4.3.5. COSO GRC PE 2016, Princípio 2.
1.3. Pessoas **Nesta seção, busca-se avaliar em que medida as pessoas na organização estão informadas, habilitadas e autorizadas para exercer seus papéis e suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.**	
Reforço da *Accountability* **1.3.1. Todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de se levar a sério suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes. Ademais, o pessoal designado para atividades de identificação, avaliação e tratamento de riscos recebe capacitação suficiente para executá-las, inclusive no que diz respeito à identificação de oportunidades e à inovação.**	IN-MP/CGU Nº 1/2016, Art. 11, IV e II; e Art. 16, III a VI; INTOSAI GOV 9130/2007, 2.7.3. ISO 31000:2009, 5.2. COSO GRC 2004, 2, 8 e 10; COSO GRC PE 2016, Princípios 3, 5, 20.
Estrutura de gerenciamento de riscos e controles **1.3.2. Os grupos de pessoas que integram as *três linhas de defesa* na estrutura de gerenciamento de riscos e controles por toda a organização têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização, especialmente quanto aos seguintes aspectos:**	IN-MP/CGU Nº 1/2016, Art. 2º, III; e 3º e 6º; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.
a) Na *primeira linha de defesa*, os gestores:	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 3º;

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
I. têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e **II. são regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.**	IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.
b) Na *segunda linha de defesa*, o pessoal que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização: **I. apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade;** **II. fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos;** **III. define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização;** **IV. estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos;** **V. orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la;** **VI. comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização.**	IN-MP/CGU Nº 1/2016, Art. 2º, III; e Art. 6º; IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.
c) Na *terceira linha de defesa*, o pessoal que integra a auditoria interna, especialmente o dirigente dessa função: **I. tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, previstos na Declaração de**	IN-MP/CGU Nº 1/2016, Art. 2º, III; IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo;

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
Posicionamento do IIA: *"O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo",* e de fato exerce seus papéis em conformidade com essas orientações; **II. tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com as prioridades da organização;** **III. detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.**	IIA 2013, As Três Linhas de Defesa no gerenciamento eficaz de riscos e controles; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B. IIA IPPF Norma 2010, 2100, 2110 e 2210. RES CNJ 171/2013, Art. 10 e 12.
2. PROCESSOS **Nesta dimensão, examinam-se os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida a organização dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas.**	
2.1. Identificação e análise de riscos **Nesta seção, busca-se avaliar em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente às operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização), de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.**	
Estabelecimento do contexto **2.1.1. O processo de identificação de riscos é precedido de uma etapa de estabelecimento do contexto envolvendo o entendimento, por parte de todos os participantes do processo, da organização, dos seus objetivos-chaves e do ambiente no qual eles são perseguidos, com o fim de obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização de atingir seus objetivos, incluindo:**	ISO 31000:2009, 5.3. COSO GRC 2004, 4; COSO GRC PE 2016, Princípio 7.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
a) a identificação dos objetivos-chaves da atividade, do processo ou do projeto objeto da identificação e análise de riscos é realizada considerando o contexto dos objetivos-chaves da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados;	IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 16, II; ISO 31000:2009, 5.3.3, "a" e "b"; COSO GRC 2004, 3; COSO GRC PE 2016, Princípio 10.
b) a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta; e	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 5.3.2 e 5.3.3; COSO GRC 2004, 3; COSO GRC PE 2016, 1, item 1.
c) a comunicação e consulta com partes interessadas (internas e externas) para assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos;	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 5.2. COSO GRC PE 2016, Princípio 20.
Documentação do estabelecimento do contexto **2.1.2. A documentação da etapa de estabelecimento do contexto inclui pelo menos os seguintes elementos essenciais, para viabilizar um processo de avaliação de riscos consistente:**	ISO 31000:2009, 5.3.4, 5.3.5 e 5.7.
a) a descrição concisa dos objetivos-chaves e dos fatores críticos para que se tenha êxito (ou fatores críticos para o sucesso) e uma análise dos fatores do ambiente interno e externo (por exemplo, análise SWOT);	
b) a análise de partes interessadas e seus interesses (por exemplo, análise de *stakeholder*, análise RECI, matriz de responsabilidades); e	
c) os critérios com base nos quais os riscos serão analisados, avaliados e priorizados (como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados).	

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
Identificação e análise dos riscos **2.1.3. Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos, notadamente quanto aos seguintes aspectos:**	
a) são envolvidas pessoas com conhecimento adequado, bem como os gestores executivos das respectivas áreas;	ISO 31000:2009, 5.4.2 e A.3.2.
b) são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco;	ISO 31000:2009, 5.4.2.
c) o processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos;	ISO 31000:2009, 5.4.2; COSO 2013, Princípio 8.
d) o processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto;	IN-MP/CGU Nº 1/2016, Art. 16, III; ISO 31000:2009, 5.4.2.
e) a seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos; e	IN-MP/CGU Nº 1/2016, Art. 14, IV; ISO 31000:2009, 3, “b”.
f) os riscos identificados são analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos.	IN-MP/CGU Nº 1/2016, Art. 16, IV; ISO 31000:2009, 5.4.3.
Documentação da identificação e análise de riscos	ISO 31000:2009, 5.4.2, 5.4.3 e 5.7.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
2.1.4. No registro de riscos, a documentação da identificação e análise de riscos contém elementos suficientes para apoiar o adequado gerenciamento dos riscos, incluindo pelo menos:	
a) o registro dos riscos identificados e analisados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto;	
b) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos;	
c) os participantes das atividades de identificação e análise;	
d) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas;	
e) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos;	
f) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco;	
g) a descrição dos controles existentes e as considerações quanto à sua eficácia e confiabilidade; e	ISO 31000:2009, 5.5.1
h) o risco residual.	

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
2.2. Avaliação e Resposta a riscos **Nesta seção, busca-se avaliar em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.**	
Critérios para priorização de riscos **2.2.1. Os critérios estabelecidos para priorização de riscos levam em conta, por exemplo, a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, critérios de comunicação a instâncias competentes, o tempo de resposta requerido, revelando-se adequados para orientar decisões seguras quanto a:** **a) se um determinado risco precisa de tratamento e a prioridade para isso;** **b) se uma atividade deve ser realizada, reduzida ou descontinuada; e** **c) se controles devem ser implementados, modificados ou apenas mantidos.**	IN-MP/CGU Nº 1/2016, Art. 16, V; ISO 31000:2009, 5.4.4; COSO GRC 2004, 6; COSO GRC PE 2016, Princípio 14.
Avaliação e seleção das respostas a riscos **2.2.2. A avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificados considera a relação custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas, além de controles internos, para mitigar os riscos.**	IN-MP/CGU Nº 1/2016, Art. 14, III; ISO 31000:2009, 5.5.2; COSO GRC PE 2016, Princípio 15.
2.2.3. Todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento, bem como são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas.	IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, 5.5.2 e A.3.2;

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
Planos e medidas de contingência **2.2.4. Todas as áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) para a realização dos objetivos-chaves da organização têm identificados os elementos críticos de sua atuação e têm definidos planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres.**	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.5.3.
Documentação da avaliação e seleção de respostas a riscos **2.2.5. A documentação da avaliação e seleção de respostas aos riscos inclui:**	ISO 31000:2009, 5.5.3 e 5.7.
a) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos da organização, identificando claramente os riscos que requerem tratamento e suas respectivas classificações (de probabilidade, impacto, níveis de risco etc.);	
b) a ordem de prioridade para cada tratamento;	
c) as respostas a riscos selecionadas e as razões para a seleção das opções de tratamento, incluindo a justificativa de custo-benefício;	
d) as ações de tratamento, os recursos requeridos, o cronograma e os benefícios esperados;	
e) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; e	
f) os responsáveis pela aprovação e pela implementação do plano de tratamento de riscos, com autoridade suficiente para gerenciá-lo.	

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
2.3. Monitoramento e comunicação **Nesta seção, busca-se avaliar em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação.**	
Informação e comunicação **2.3.1. As atividades de informação e comunicação estão estabelecidas em diretrizes e protocolos efetivamente aplicados durante o processo de gerenciamento de riscos:** **a) diretrizes e protocolos estão estabelecidos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito da organização, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos; e**	IN-MP/CGU Nº 1/2016, Art. 16, VII; ISO 31000:2009, 5.2 e A.3.4; COSO GRC 2004, 8; COSO GRC PE 2016, Princípio 20.
b) há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos.	ISO 31000:2009, 5.2 e A.3.4.
Sistema de informação **2.3.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação que:** **a) apoia a gestão de riscos da organização e facilita a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação; e**	ISO 31000:2009, 5.7.
b) é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas a seguir), pelo menos quanto aos seus resultados e com referências para a documentação original completa.	ISO 31000:2009, 5.7 e 5.6 (final).

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
Monitoramento contínuo e autoavaliações	IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013, Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.
2.3.3. Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (*primeira linha de defesa*) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade:	
a) de modo contínuo, ou pelo menos frequente, por meio de indicadores-chaves de risco, indicadores-chaves de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho;	
b) por meio de autoavaliações periódicas de riscos e controles *(Control and Risk Self Assessment – CRSA)*, que constam de um ciclo de revisão periódica estabelecido; e	
c) a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança.	
2.3.4. As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa):	
a) exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa; e	
b) fornecem orientação e facilitação na condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém sua documentação e comunica os seus resultados às instâncias apropriados da administração e da governança.	
Monitoramento periódico e avaliações independentes	
2.3.5. A função de auditoria interna exerce o seu papel de auxiliar a organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança:	IIA IPPF – Definição da atividade de Auditoria Interna.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
a) estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança;	IIA IPPF Norma 2010, 2100 e 2110. RES CNJ 171/2013, Art. 10 e 12.
b) utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos, incluindo a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável; e	IIA IPPF Norma 2201 e 2210. RES CNJ 171/2013, Art. 24.
c) fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização.	IIA 2009, O papel da Auditoria Interna no gerenciamento de riscos corporativo.
2.3.6. Há planos e as medidas de contingência definidos para os elementos críticos da atuação da entidade, em todos as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização e estes são periodicamente testados e revisados.	ISO 31000:2009, 5.6.
Monitoramento de mudanças significativas **2.3.7. Estão estabelecidos e em funcionamento procedimentos e protocolos para monitorar e comunicar mudanças significativas nas condições que possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos da organização.**	COSO 2013, Princípio 9; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 22.
Correção de deficiências e melhoria contínua **2.3.8. Os resultados das atividades de monitoramento são utilizados para as tomadas de medidas necessárias à correção de deficiências e à melhoria contínua do desempenho da gestão de riscos, incluindo, por exemplo:** **a) comunicação às instâncias apropriados da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias;** **b) elaboração e devido acompanhamento de planos de ação para corrigir as deficiências identificadas e melhorar o desempenho da gestão de riscos.**	IN-MP/CGU Nº 1/2016, Art. 8º, XV; ISO 31000:2009, 4.5, 4.6 e A.3.1; COSO 2013, Princípio 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 23.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
3. PARCERIAS **Nesta dimensão, examinam-se os aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas (quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas), procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento.**	
3.1. Gestão de riscos em parcerias **Nesta seção, busca-se avaliar em que medida a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão adequadamente gerenciados e os objetivos alcançados.**	
Avaliação da capacidade de gestão de riscos das entidades parceiras **3.1.1. O compartilhamento dos riscos é precedido de avaliação fundamentada e documentada da capacidade das potenciais organizações parceiras para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado.**	ISO 31000:2009, 4.3.3 e A.3.3;
Definição de responsabilidades, informação e comunicação **3.1.2. São designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou resultado esperado das políticas de gestão compartilhadas por meio de parcerias, e são definidas em quais condições e para quem cada responsável deve fornecer informações.**	IN-MP/CGU Nº 1/2016, Art. 20 e 16, VII; ISO 31000:2009, 4.3.3 e A.3.2.
Processo de gestão de riscos em parcerias **3.1.3. O processo de gestão de riscos é aplicado para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas.**	ISO 31000:2009, 4.4.2;

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
3.1.4. Pessoas de todas as áreas, funções ou setores das organizações parceiras com envolvimento na parceria e outras partes interessadas no seu objeto participam do processo de identificação e avaliação dos riscos relacionados a cada objetivo, meta ou resultado esperado das parcerias.	ISO 31000:2009, 5.4.2 e A.3.2.
3.1.5. Um registro de riscos único é elaborado na identificação e avaliação dos riscos e é atualizado conjuntamente pelas organizações parceiras em função das atividades de tratamento e monitoramento de riscos.	ISO 31000:2009, 5.7 e 5.6 (final).
3.1.6. Há informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado.	IN-MP/CGU Nº 1/2016, Art. 16, VII;ISO 31000:2009, 5.2 e A.3.4; COSO GRC PE 2016, Princípio 20.
3.2. Planos e medidas de contingência **Nesta seção, busca-se avaliar em que medida a organização estabelece, em conjunto com as entidades parceiras, planos e medidas de contingência para garantir a recuperação e a continuidade da prestação de serviços em caso incidentes.**	
Planos e medidas de contingência **3.2.1. As organizações parceiras definem planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar.** **3.2.2. Os planos e medidas de contingência são periodicamente testados e revisados.**	IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.6.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
4. RESULTADOS **Nesta dimensão, examinam-se os efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.**	
4.1. Melhoria dos processos de governança **Nesta seção, busca-se avaliar em que medida a organização integra a gestão de riscos em seus processos de governança e gestão e isso tem sido eficaz para a sua melhoria.**	
Integração da gestão de riscos aos processos organizacionais **4.1.1. Os responsáveis pela governança e a alta administração sabem até que ponto a administração estabeleceu uma gestão de riscos eficaz, integrada e coordenada por todas as áreas, funções e atividades relevantes e críticas para a realização dos objetivos-chaves da organização, tendo consciência do nível de maturidade atual e do progresso das ações em curso para atingir ao nível almejado.**	IN-MP/CGU Nº 1/2016, Art. 8º, II; Arts. 19, 20, 21, parágrafo único, 22 e 23; ISO 31000:2009, 4.3.4 e A.3.5; COSO GRC 2004, 10. COSO GRC PE 2016, Princípio 1.
4.1.2. Os objetivos-chaves, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, na missão e visão e da organização e nos seus valores fundamentais, formando a base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.	IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 3 "a" e 5.3.1; COSO GRC 2004/2016, Premissa.
4.1.3. Os objetivos estratégicos e de negócios estão estabelecidos, alinhados com o direcionamento estratégico (item anterior), juntamente com as medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), permitindo medir o progresso e monitorar o desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chaves.	IN-MP/CGU Nº 1/2016, Art. 16, II; ISO 31000:2009, 4.2, itens 3 e 4; COSO GRC 2004, 3. COSO GRC PE 2016, Dimensão 2.
4.1.4. Estão identificados, avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, com o desempenho sendo comunicado aos níveis apropriados da administração e da governança.	IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, A.2 e A.3.2. COSO GRC 2004, 4; COSO GRC PE 2016, Princípios 12 a 16.

Dimensões do modelo de avaliação e Práticas relacionadas	Fontes dos critérios
4.2. Resultados-chaves da gestão de riscos **Nesta seção, busca-se avaliar em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.**	
Entendimento dos objetivos, riscos, papéis e responsabilidades **4.2.1. Os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos.**	ISO 31000:2009, A.2.
Garantia proporcionada pela gestão de riscos **4.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, que:**	COSO GRC 2004, 1, Anexo 1.1.
a) entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização;	COSO GRC 2004, 1, Anexo 1.1.
b) entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados;	
c) a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável;	
d) as leis e os regulamentos aplicáveis estão sendo cumpridos.	
Eficácia da gestão de riscos **4.2.3. Os riscos da organização estão dentro dos seus critérios de risco, vale dizer, dentro do apetite a risco definido e das variações aceitáveis no desempenho ou tolerâncias a risco estabelecidas, conforme a documentação resultante da aplicação do processo de gestão de risco, atualizada pelas atividades de monitoramento.**	ISO 31000:2009, A.2.

APÊNDICE II – MATRIZ DE PLANEJAMENTO

Objetivo da auditoria: avaliar a maturidade da gestão de riscos e identificar os aspectos que necessitam ser aperfeiçoados.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
1. AMBIENTE Nesta dimensão, o objetivo da equipe de auditoria é avaliar as capacidades existentes na organização, em termos de **liderança**, **políticas & estratégias** e preparo das **pessoas**, incluindo aspectos relacionados com a *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia e dos objetivos* em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas.					
1.1. – Liderança[6] Em que medida os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos e cultura?					Se os responsáveis pela governança e a alta administração assumem um compromisso forte e sustentado e exercem supervisão para obter comprometimento com a gestão de riscos em todos os níveis da organização, promovendo-a e dando suporte, de modo que possam ter uma expectativa razoável de que no cumprimento da missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir seus objetivos de gerar valor para as partes interessadas, tendo o cidadão e a sociedade como vetores principais.

[6] Quando a questão de auditoria se desdobrar em subquestões, como neste caso, a sua conclusão (o que a análise vai permitir dizer) é obtida mediante avaliação conjunta das evidências obtidas na execução dos procedimentos de análise das subquestões que a compõe. O nível de maturidade (ou pontuação) correspondente à questão será calculado conforme orientações constantes do tópico **Determinação do nível de maturidade**.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Cultura 1.1.1. A alta administração e os responsáveis pela governança reconhecem a importância da cultura, da integridade, dos valores éticos e da consciência de riscos como aspectos-chaves para o reforço da *accountability*?	Estes campos devem ser preenchidos pela equipe de auditoria, conforme orientações constantes do tópico **Elaboração da Matriz de Planejamento**.				• Se a alta administração e os responsáveis pela governança fornecem normas, orientações e supervisionam as questões afetas a cultura, integridade, valores éticos e consciência de riscos. • Se as questões relacionadas a cultura, integridade, valores éticos e consciência de riscos integram o conteúdo de cursos e programas voltados para o desenvolvimento de gestores. • Se a alta administração e os responsáveis pela governança reforçam o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização. • Se estão instituídos programas, políticas ou outras medidas que definem os padrões de comportamento desejáveis, tais como códigos de ética e de conduta, canais de denúncia e de comunicação para cima, ouvidoria, avaliações de aderência aos padrões de integridade e valores éticos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Governança de riscos 1.1.2. Existem estruturas e processos definidos para apoiar as responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão?					• Se existem instâncias internas de apoio à governança de riscos, tais como comitês de governança, riscos e controles; auditoria interna; coordenação central da gestão corporativa de riscos. • Se as instâncias internas de apoio à governança de riscos exercem suas atribuições mediante uma abordagem planejada, sistemática e disciplinada. • Se a gestão de riscos é integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades[7] relevantes para o alcance dos objetivos-chaves da organização.

[7] Áreas (por exemplo: unidades, departamentos, divisões), funções (por exemplo: finanças, aquisições, contabilidade, gestão de pessoas, TI), atividades (por exemplo: processos, projetos, sistemas).

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Supervisão da Governança e da alta administração 1.1.3. Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos?					• Se os processos de governança e gestão incorporam explicitamente indicadores-chaves de risco e indicadores-chaves de desempenho, monitorados regularmente. • Se o órgão de governança e a alta administração são notificados de modo regular e oportuno sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos. • Se o órgão de governança faz uma revisão sistemática da visão de portfólio dos riscos em contraste com o apetite a riscos, fornecendo direção clara para gerenciamento dos riscos. • Se o órgão de governança e a alta administração utilizam os serviços da auditoria interna e de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controles. • Se o órgão de governança definiu um nível de maturidade almejado para a gestão de riscos e monitora o progresso das ações para atingir ou manter-se no nível definido.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
1.2. – Políticas e estratégias Em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?					Se organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização.
Direcionamento estratégico 1.2.1. A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico?					• Se alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico traduzido nos objetivos-chaves, na missão, na visão e valores fundamentais da organização. • Se o direcionamento estratégico é alinhado com as finalidades e competências legais da entidade. • Se o direcionamento estratégico fornece uma base suficiente para a definição da estratégia e a fixação dos objetivos estratégicos e de negócios, traduzindo uma expressão inicial do risco aceitável (apetite a risco) para o gerenciamento dos riscos relacionados.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
1.2.2. A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o *apetite a risco*?					• Se a alta administração, com a supervisão e a concordância do órgão de governança, define, comunica, monitora e revisa o apetite a risco na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas. • Se a expressão do apetite a risco fornece uma base consistente para orientar a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Integração da gestão de riscos ao processo de planejamento 1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos?					• Se os objetivos estratégicos de alto nível são alinhados e dão suporte à missão, à visão e aos propósitos da organização, e se são estabelecidos em consistência com o direcionamento estratégico e o apetite a risco definidos (subquestões 1.2.1 e 1.2.2), de modo a fornecer uma base consistente para a definição dos objetivos de negócios em todos os níveis da organização. • Se são consideradas as várias alternativas de cenários e os riscos associados na definição dos objetivos estratégicos e na seleção das estratégias para atingi-los. • Se os objetivos de negócios específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho) são definidos alinhados aos objetivos estratégicos e ao apetite a risco.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
1.2.4. A administração define e comunica os objetivos e as respectivas medidas de desempenho em termos específicos e mensuráveis?					• Se a administração define os objetivos de negócios de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, explicitando-os com clareza suficiente, em termos específicos e mensuráveis. • Se a administração define as medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho) para todos os objetivos definidos. • Se os objetivos e as medidas de desempenho são comunicados aos responsáveis, em todos os níveis, de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização. • Se o modo como os objetivos são definidos, explicitados e comunicados permite a identificação e avaliação dos riscos que possam ter impacto no desempenho e no alcance dos objetivos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Política de gestão de riscos 1.2.5. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, apropriadamente comunicada, abordando todos os aspectos relevantes?					• Se a alta administração aprovou a política de gestão de riscos e assumiu a liderança no compromisso com a sua implementação. • Se a política de gestão de riscos é apropriadamente comunicada e está disponível para acesso a todos, dentro e fora da organização. • Se a política de gestão de riscos estabelece os princípios e objetivos relevantes da gestão de riscos na organização e as ligações entre os objetivos e políticas da organização com a política de gestão de riscos. • Se a política de gestão de riscos estabelece as diretrizes para a integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Política de gestão de riscos (Continuação da questão 1.2.5).					• Se a política de gestão de riscos contém uma definição clara de responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas (unidades, departamentos, divisões, processos e atividades), incluindo a implementação e manutenção do processo de gestão de riscos e a asseguração da suficiência, eficácia e eficiência de quaisquer controles. • Se a política de gestão de riscos estabelece diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados, por meio de um plano de implementação do processo de gestão de riscos, em todos os níveis, funções e processos relevantes da organização. • Se a política de gestão de riscos estabelece diretrizes sobre como o desempenho da gestão de riscos, a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política de gestão de riscos, serão medidos e reportados.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Política de gestão de riscos (Continuação da questão 1.2.5).					• Se a política de gestão de riscos estabelece atribuição clara de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como diretrizes sobre a forma e a periodicidade como as alterações devem ser efetivadas.
Comprometimento da gestão 1.2.6. Toda a gestão da organização é comprometida com a gestão de riscos?					• Se a alta administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade.
Alocação de recursos 1.2.7. A administração aloca recursos suficientes e apropriados para a gestão riscos?					• Se a administração aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas de TI, métodos, treinamento e ferramentas) para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chaves, bem como com a natureza e o nível dos riscos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
1.3. – Pessoas Em que medida as pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los?					Se as pessoas na organização estão informadas, habilitadas e autorizadas para exercer os seus papéis e as suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização.
Reforço da *accountability* 1.3.1. A gestão transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gerenciamento riscos e o pessoal recebe orientação e capacitação suficiente para exercer essas responsabilidades?					• Se todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de cumprir suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes. • Se o pessoal designado para atividades de identificação, avaliação e tratamento de riscos recebe capacitação suficiente para executá-las, inclusive no que diz respeito à identificação de oportunidades e à inovação.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Estrutura de gerenciamento de riscos e controles 1.3.2. Os grupos de pessoas que integram as *três linhas de defesa* na estrutura de gerenciamento de riscos e controles por toda a organização têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização?					• Se os gestores, que integram a *primeira linha de defesa*: i) têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e ii) são regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema. • Se o pessoal da *segunda linha de defesa*, que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização: i) apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade;

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Estrutura de gerenciamento de riscos e controles (Continuação da questão 1.3.2).					ii) fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos; iii) define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização; iv) estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos; v) orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la; vi) comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização. • Se o pessoal da auditoria interna, que integra a *terceira linha de defesa*, especialmente o dirigente dessa função:

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Estrutura de gerenciamento de riscos e controles (Continuação da questão 1.3.2).					i) tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, conforme previsto na Declaração de Posicionamento do IIA: *"O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo"*, e de fato os exerce em conformidade. ii) tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com essas prioridades da organização; iii) detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
2. PROCESSOS Nesta dimensão, o objetivo da equipe de auditoria é examinar os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida a organização dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas.					
2.1. – Identificação e análise de riscos Em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente a todas operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização)?					Se a identificação e análise de riscos é realizada de forma consistente em relação a todas operações, funções e atividades relevantes para a realização dos objetivos-chaves da organização, de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos.
Estabelecimento do contexto 2.1.1. A identificação de riscos é precedida de uma etapa de estabelecimento do contexto?					• Se previamente ao processo de identificação de riscos, todos os participantes desse processo obtêm entendimento da organização e dos seus objetivos-chaves, bem como do ambiente no qual esses objetivos são buscados, a fim de obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização para atingir seus objetivos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Estabelecimento do contexto (Continuação da questão 2.1.1).					• Se a identificação dos objetivos-chaves da atividade, do processo ou do projeto objeto da identificação e análise de riscos é realizada considerando o contexto dos objetivos-chaves da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados. • Se é realizada a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta. • Se é realizada comunicação e consulta com partes interessadas (internas e externas) para assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Documentação do estabelecimento do contexto 2.1.2. A documentação da etapa de estabelecimento do contexto inclui elementos essenciais para viabilizar um processo de avaliação de riscos consistente?					• Se a documentação da etapa de estabelecimento do contexto inclui pelo menos: i) a descrição concisa dos objetivos-chaves e dos fatores críticos para que se tenha êxito (ou fatores críticos para o sucesso) e uma análise dos fatores do ambiente interno e externo (por exemplo, análise SWOT); ii) a análise de partes interessadas e seus interesses (por exemplo, análise de *stakeholder*, análise RECI, matriz de responsabilidades); iii) os critérios com base nos quais os riscos serão analisados, avaliados e priorizados (como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados).

Identificação e análise dos riscos 2.1.3. Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos?					• Se nos processos de identificação de riscos são envolvidas pessoas com conhecimento adequado, bem como os gestores das áreas. • Se são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de riscos. • Se o processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos. • Se o processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução daqueles objetivos identificados na etapa de estabelecimento do contexto. • Se a seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos. • Se são analisados o impacto e a probabilidade dos riscos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Documentação da identificação e análise dos riscos 2.1.4. No registro de riscos (sistema, planilhas ou matrizes de avaliação de riscos), a documentação da identificação e análise dos riscos contém elementos suficientes para apoiar um adequado gerenciamento dos riscos?					• Se há registro dos riscos identificados e analisados em sistema, planilhas ou matrizes de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto. • Se no registro de riscos da organização, a documentação das atividades de identificação e análise de riscos inclui pelo menos: i) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise; ii) os participantes das atividades de identificação e análise de riscos; iii) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas;

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Identificação e análise dos riscos (Continuação da questão 2.1.4).					iv) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos; v) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco; vi) a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e vii) o risco residual.
2.2. – Avaliação e resposta a riscos Em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?					Se a avaliação de riscos e a seleção de respostas aos riscos identificados e analisados como significativos é realizada de forma consistente, para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Critérios para priorização de riscos 2.2.1. Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por toda a organização?					• Se existem critérios estabelecidos para orientar as decisões sobre riscos em relação a todas as operações, funções e atividades relevantes da organização. • Se os critérios estabelecidos levam em conta fatores como a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, critérios de comunicação a instâncias competentes, o tempo de resposta requerido. • Se os critérios estabelecidos são adequados para orientar decisões quanto a se: i) um determinado risco precisa de tratamento e a prioridade para isso; ii) uma atividade deve ser realizada, reduzida ou descontinuada; iii) controles devem ser implementados, modificados ou apenas mantidos.

Avaliação e seleção das respostas a riscos 2.2.2. A seleção de respostas para tratar riscos considera todas as opções de tratamento e o seu custo-benefício? 2.2.3. Os responsáveis pelo tratamento de riscos são envolvidos no processo de avaliação e seleção das respostas e são formalmente comunicados das ações de tratamento decididas? **Planos e medidas de contingência** 2.2.4. Os elementos críticos da atuação da organização estão identificados e têm definidos planos e medidas de contingência?					• Se a avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificados considera a relação custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas, além de controles internos, para mitigar os riscos. • Se todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento, bem como são formalmente comunicados das ações de tratamento decididas para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas. • Se todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização têm identificados os elementos críticos de sua atuação e têm definidos planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres.

Documentação da avaliação e seleção das respostas a riscos 2.2.5. A documentação da avaliação e seleção de respostas a riscos inclui elementos suficientes para permitir o gerenciamento adequado da implementação das respostas?					• Se a documentação da avaliação e seleção de respostas aos riscos inclui pelo menos: i) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos, identificando claramente os riscos que requerem tratamento, suas respectivas classificações (probabilidade, impacto, níveis de risco etc.), a ordem de prioridade para cada tratamento; ii) as respostas a riscos selecionadas e as razões para a seleção, incluindo justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados; iii) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; iv) a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
2.3. – Monitoramento e comunicação Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização?					Se as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação.
Informação e comunicação 2.3.1. Diretrizes e protocolos de informação e comunicação estão estabelecidos e são efetivamente aplicados em todas as fases do processo de gestão de riscos?					• Se diretrizes e protocolos estão estabelecidos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito da organização, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos. • Se há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Sistema de informação 2.3.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado?					• Se há um registro de riscos ou sistema de informação apoia a gestão de riscos da organização e facilita a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação; • Se o registro de riscos ou sistema de informação é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas na sequência), pelo menos quanto aos seus resultados e com referências para a documentação original completa.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Monitoramento contínuo e autoavaliações 2.3.3. Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (primeira linha de defesa) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade?					• Se os gestores com propriedade sobre os riscos e como primeira linha de defesa monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade: i) de modo contínuo, ou pelo menos frequente, por meio de indicadores-chaves de risco, indicadores-chaves de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho; ii) por meio de autoavaliações periódicas de riscos e controles *(Control and Risk Self Assessment – CRSA)*, que constam de um ciclo de revisão periódica estabelecido; e iii) a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Monitoramento contínuo e autoavaliações (Continuação). 2.3.4. As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa) exercem suas atribuições de modo efetivo?					• Se as funções que supervisionam riscos ou coordenam atividades de gestão de riscos exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa. • Se essas funções fornecem orientação e facilitação para a condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém a sua documentação e comunica os seus resultados às instâncias apropriadas da administração e da governança.
Monitoramento periódico e avaliações independentes 2.3.5. A função de auditoria interna auxilia a organização a realizar seus objetivos aplicando abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança?					• Se a função de auditoria interna estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Monitoramento periódico e avaliações independentes (Continuação da questão 2.3.5).					• Se a função de auditoria interna utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos, o que implica a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável. • Se a função de auditoria interna fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização.
2.3.6. Há planos e medidas de contingência definidos para os elementos críticos da atuação da organização e estes são periodicamente testados e revisados?					• Se os planos e as medidas de contingência definidos para os elementos críticos da atuação da entidade, em todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização • Se os planos e as medidas de contingência são periodicamente testados e revisados.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Monitoramento de mudanças significativas 2.3.7. A organização monitora as mudanças que podem aumentar sua exposição a riscos ter impacto nos seus objetivos?					• Se existem procedimentos e protocolos estabelecidos e em funcionamento para monitorar e comunicar mudanças significativas nas condições que possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos da organização.
Correção de deficiências e melhoria contínua 2.3.8. São tomadas as medidas necessárias para a correção de deficiências e a melhoria contínua do desempenho da gestão de riscos em função dos resultados das atividades de monitoramento?					• Se os resultados das atividades de monitoramento são comunicados às instâncias apropriados da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias. • Se são elaborados e devidamente acompanhados planos de ação para corrigir as deficiências identificadas nas atividades de monitoramento e para melhorar o desempenho da gestão de riscos.
3. PARCERIAS Nesta dimensão, o objetivo da equipe de auditoria é examinar os aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas (quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas), procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento.					

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
3.1. – Gestão de riscos em parcerias Em que medida a organização estabelece arranjos com clareza para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito das parcerias?					Se a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão gerenciados adequadamente e os objetivos alcançados.
Avaliação da capacidade de gestão de riscos das entidades parceiras 3.1.1. A capacidade das potenciais organizações parceiras para gerenciar os riscos das políticas de gestão compartilhadas é avaliada antes da realização das parcerias?					• Se o compartilhamento dos riscos com potenciais organizações parceiras é precedido de avaliação fundamentada e documentada da capacidade da organização para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado das políticas de gestão compartilhadas.
Definição de responsabilidades, informação e comunicação 3.1.2. Existe clara e adequada designação de responsáveis pelo gerenciamento de riscos nas parcerias e de protocolos de informação e comunicação entre eles?					• Se são designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou resultado esperado das políticas de gestão compartilhadas por meio de parcerias. • Se são definidas em quais condições e para quem cada responsável deve fornecer informações relacionadas a risco e desempenho.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Processo de gestão de riscos em parcerias 3.1.3. O processo de gestão de riscos é aplicado no âmbito das parcerias?					• Se o processo de gestão de riscos é aplicado para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas.
3.1.4. A identificação e avaliação de riscos em parcerias envolve as pessoas apropriadas das organizações parceiras e outras partes interessadas?					• Se pessoas de todas as áreas, funções ou setores com envolvimento na parceria, de ambas organizações parceiras, e outras partes interessadas no seu objeto participam do processo de identificação e avaliação dos riscos relacionados a cada objetivo, meta ou resultado esperado das parcerias.
3.1.5. A gestão de riscos nas parcerias é apoiada por um registro de riscos único ou sistema de informação efetivo e atualizado?					• Se um registro de riscos único é elaborado na identificação e avaliação dos riscos e é atualizado conjuntamente pelas organizações parceiras em função das atividades de tratamento e monitoramento de riscos.
3.1.6. Os riscos e o desempenho das parecerias são monitorados mediante troca regular de informação confiável?					• Se há informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado das parcerias.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
3.2. – Planos de medidas de contingência Em que medida são estabelecidos planos ou medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas?					Se a organização estabelece, em conjunto com as entidades parceiras, planos e medidas de contingência para garantir a recuperação e a continuidade da prestação de serviços em caso de incidentes.
Planos e medidas de contingência 3.2.1. São definidos planos e medidas de contingência no âmbito das parcerias, periodicamente testados e revisados?					• Se as organizações parceiras definem planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços, em casos de desastres, ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público, quando uma ou outra parte falhar. • Se os planos e as medidas de contingência são periodicamente testados e revisados.
4. RESULTADOS Nesta dimensão, o objetivo da equipe de auditoria é examinar os efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.					
4.1. – Melhoria dos processos de governança e gestão Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão?					Se a organização integra a gestão de riscos em seus processos de governança e gestão e isso tem sido eficaz para a sua melhoria.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Integração da gestão de riscos aos processos organizacionais 4.1.1. Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização?					• Se os responsáveis pela governança e a alta administração sabem até que ponto a administração estabeleceu uma gestão de riscos eficaz, integrada e coordenada por todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, tendo consciência do nível de maturidade atual e do progresso das ações em curso para atingir o nível almejado.
4.1.2. Os objetivos-chaves da organização estão identificados e refletidos na sua cadeia de valor e nos seus demais instrumentos de direcionamento e comunicação da estratégia?					• Se os objetivos-chaves, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, na missão e visão e da organização e nos seus valores fundamentais, formando a base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
4.1.3. Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?					• Se os objetivos estratégicos e de negócios estão estabelecidos, alinhados com o direcionamento estratégico (questão anterior), com as respectivas medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), permitindo medir o progresso e monitorar o desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chaves.
4.1.4. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?					• Se estão identificados, avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, com o desempenho sendo comunicado aos níveis apropriados da administração e da governança.
4.2. – Resultados-Chaves da gestão de riscos Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização?					Se os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Entendimento dos objetivos, riscos, papéis e responsabilidades 4.2.1. Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?					• Se os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos.
Garantia proporcionada pela gestão de riscos 4.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização?					• Se os responsáveis pela governança e a administração, com base nas informações resultantes da gestão de riscos, têm garantia razoável de que: i) entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização;

QUESTÕES DE AUDITORIA	INFORMAÇÕES REQUERIDAS	FONTES DE INFORMAÇÃO	PROCEDIMENTOS DE COLETA DE DADOS	PROCEDIMENTOS DE ANÁLISE DE DADOS	O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)
Garantia proporcionada pela gestão de riscos (Continuação da questão 4.2.3).					ii) entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados; iii) a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável; iv) as leis e os regulamentos aplicáveis estão sendo cumpridos.
Eficácia da gestão de riscos 4.2.3. Os riscos da organização estão dentro dos seus critérios de risco?					• Se, de acordo com a documentação resultante do processo de gestão de riscos e os critérios de risco definidos pela alta administração com a supervisão e concordância dos responsáveis pela governança, (apetite a risco, tolerâncias a risco ou variações aceitáveis no desempenho), os riscos da organização estão dentro dos seus critérios de risco.

Elaborado por:	/ /
Revisado por:	/ /
Supervisionado por:	/ /