MINISTÉRIO DA INFRAESTRUTURA
DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

PORTARIA Nº 2319, DE 05 DE ABRIL DE 2019

A DIRETORIA COLEGIADA DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES - DNIT, no uso das atribuições que lhe conferem o artigo 12, do Regimento Interno aprovado pela Resolução nº 26, de 05 de maio de 2016, publicado no DOU, de 12 de maio de 2016, e tendo em vista o constante no processo nº 50600.009841/2018-29, resolve:

Art. 1º APROVAR o Manual de Procedimentos para Avaliação dos Mecanismos de Gestão de Riscos do DNIT, constituído do anexo desta portaria, no qual constam orientações sobre os procedimentos para executar a avaliação da governança da organização pela Auditoria Interna.

Art. 2º Os servidores da Auditoria Interna selecionados para executar o trabalho de avaliação da gestão de riscos desta autarquia deverão observar o disposto no Manual citado no art. 1º, o qual deverá ser atualizado periodicamente.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

ANDRÉ KUHN
Diretor-Geral Substituto

DNIT DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

MANUAL DE PROCEDIMENTOS PARA AVALIAÇÃO DOS MECANISMOS DA GESTÃO DE RISCOS DO DNIT PELA AUDITORIA INTERNA

Versão 1.0
1ª Edição - Julho/2018

V 1.0 - 1º EDIÇÃO – Brasília, abril/19.

DIRETOR GERAL Antônio Leite dos Santos Filho

DIRETOR EXECUTIVO André Kuhn

AUDITOR CHEFE Benedito Orlando Nava Castro

DIVISÃO DE AUDITORIA Danilo Fernandes de Medeiros

CHEFE DO APOIO GERAL DA AUDINT Lídia Lopes Martins

AUTOR:

Marina Braz de Castro Calil – Analista Administrativo/Contábil

COLABORADOR:

Danilo Fernandes de Medeiros – Analista em Infraestrutura de Transportes

EQUIPE TÉCNICA - INFRAESTRUTURA DE TRANSPORTES:

Alberto Yoshikasu Maeda – Analista em Infraestrutura de Transportes

Cleiton Lima de Moura – Técnico de Suporte em Infraestrutura de Transportes

Danilo Fernandes de Medeiros – Analista em Infraestrutura de Transportes

Kamila Meneses da Silva – Analista em Infraestrutura de Transportes

Pedro Murga Veloso Pinto - Analista em Infraestrutura de Transportes

Renan Xavier Ferreira – Analista em Infraestrutura de Transportes

Tiago Pereira Lopez – Analista em Infraestrutura de Transportes

Wilson Dias Almeida Júnior – Técnico de Suporte em Infraestrutura de Transportes

EQUIPE TÉCNICA –ADMINISTRATIVO-FINANCEIRA-CONTÁBIL

Alexandre Reche Correa – Analista Administrativo

Bruna Zanini Rodrigues – Técnico Administrativo

Izabel de Souza Leão – Técnico em Contabilidade

Marina Braz de Castro Calil – Analista Administrativo/Contábil

EQUIPE DE DEMANDAS EXTERNAS

Érica Mayumi Yamada Tajima – Analista Administrativo

Lídia Lopes Martins – Analista em Infraestrutura de Transportes

EQUIPE DE APOIO GERAL DA AUDINT

Lídia Lopes Martins – Analista em Infraestrutura de Transportes

SUMÁRIO

1. INTRODUÇÃO

1. O Manual de Procedimentos para Avaliação dos Mecanismos de Gestão de Riscos, de utilização pela Auditoria Interna do DNIT, tem o objetivo de atender uma parte da recomendação exarada no item 9.1.11 do Acórdão nº 2746/2015-TCU/Plenário. O item recomenda ao DNIT "[...] incluir nas atividades de auditoria interna a avaliação da governança, da gestão de riscos e dos controles internos da organização; [...]". Em reforço, o inciso III do artigo 2º da Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, versa que a auditoria interna deve 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, de controles internos, de integridade e de governança.

2. Desse modo, este Manual possui a finalidade de definir os procedimentos que serão utilizados pela Auditoria Interna/DNIT na avaliação dos mecanismos de gestão de riscos da autarquia. Objetiva-se, com isso, que a partir da ordem de auditoria, a equipe responsável avalie o nível da maturidade da gestão de riscos da organização com base em um padrão estabelecido. A avaliação da gestão de riscos deverá ocorrer periodicamente, em intervalos bianuais ou trianuais, de acordo com a disponibilidade de mão de obra na Auditoria Interna.

3. A Auditoria Interna possui função de apoio à gestão, fornecendo insumos ao nível estratégico para que exerça a liderança necessária para conduzir à boa governança e gestão de riscos. A atividade de avaliação fornece informações estratégicas à tomada de decisão, no sentido em que monitora a implementação, gera indicadores do desempenho de programas e de agentes e direciona ao alcance dos objetivos organizacionais. A avaliação funcionará como uma Ordem de Auditoria, e as constatações, recomendações e informações do relatório oriundo de tal avaliação deverá gerar informações gerenciais no sentido de acrescentar valor à gestão de riscos na organização.

4. O resultado da avaliação da gestão de riscos deverá ser exposto na intranet da autarquia, conforme o princípio da transparência. Essa regra deverá estar explícita na Portaria que aprovar este Manual, cuja revisão deverá ser periodicamente efetuada.

5. Este Manual possui um Anexo: Anexo I - Questionário para avaliação.

2. GESTÃO DE RISCOS

6. Segundo o Referencial Básico de Gestão de Riscos do TCU (2018), a Gestão de Riscos consiste em um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos.

7. A adoção de padrões e boas práticas estabelecidos em modelos reconhecidos evita que a organização seja aparelhada com uma coleção de instrumentos burocráticos e ineficazes.

8. A gestão de riscos corretamente implementada fornece:

a. adequado suporte a decisões de alocação e uso apropriado dos recursos públicos;

b. aumento do grau de eficiência e eficácia;

c. entrega de valor público, otimizando o desempenho e os resultados.

PROCESSO DE GESTÃO DE RISCOS

9. O modelo de gestão de riscos presente no COSO II (Gerenciamento de Riscos Corporativos – Estrutura Integrada) apresenta a bem divulgada matriz tridimensional (cubo), conforme Figura 1, com os seguintes componentes de gestão de riscos:

a. Ambiente Interno;

b. Fixação de Objetivos;

c. Identificação de Eventos;

d. Avaliação de Riscos;

e. Resposta ao Risco;

f. Atividades de Controle;

g. Informação e Comunicação;

h. Monitoramento.

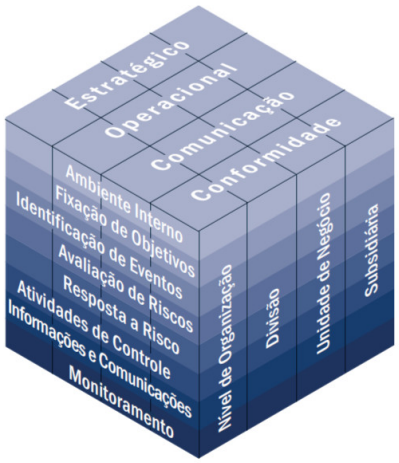

Figura 1 - Cubo COSO II

Ambiente Interno/Estabelecimento do Contexto

10. Ao traçar um paralelo com outros modelos, compara-se os componentes Ambiente Interno e Fixação de Objetivos com a nomenclatura Estabelecimento do Contexto, que envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno, no qual os objetivos são perseguidos, ou seja, é o ambiente no qual a organização busca atingir os seus objetivos.

11. O Estabelecimento do Contexto envolve:

a. entendimento da organização, dos objetivos e do ambiente;

b. fornecimento dos parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas;

c. o entendimento que os objetivos serão parte importante do contexto;

d. o estabelecimento de que a gestão de riscos ocorre no contexto dos objetivos da organização.

12. A documentação que se espera que a organização possua em relação a essa etapa é:

a. relato conciso dos objetivos organizacionais, dos fatores críticos e análise dos fatores internos e externos do ambiente;

b. análise de partes interessadas e seus interesses;

c. definição dos critérios mais importantes:

i. escalas de probabilidade;

ii. escalas de consequências ou impactos;

d. como será determinado se o nível de risco é tolerável ou aceitável;

e. se novas ações de tratamento são necessárias.

Processo de Avaliação de Riscos (Identificação, Análise e Avaliação)

13. Os componentes Identificação de Eventos e Avaliação de Riscos do modelo COSO II fazem parte do Processo de Avaliação de Riscos, que inclui a identificação, análise e avaliação dos riscos.

14. A identificação de riscos abrange:

a. processo de busca, reconhecimento e descrição dos riscos.

b. lista abrangente de riscos, causas, fontes e eventos.

c. trabalho com processo sistemático e de modo estruturado.

d. documentação esperada:

i. escopo do processo, projeto ou atividade;

ii. participantes do processo;

iii. abordagem ou método utilizado para identificação e fontes de informação consultadas;

iv. registro dos riscos identificados em sistema, planilha ou matriz de avaliação de riscos, com detalhamento em componentes, causas, evento e consequências.

15. A etapa de análise de riscos abrange o processo de compreender a natureza do risco e determinar o nível de risco. O nível de risco é medido pela função: probabilidade x impacto:

a. probabilidade de ocorrência do evento;

b. impacto de suas consequências.

16. Essa relação simples pode não refletir relações não lineares, sendo necessário incluir um fator de ponderação para uma das variáveis:

a. Risco = (P) x (I x fator de ponderação).

17. Ainda sobre a etapa Análise de Riscos, destaca-se que a análise pode ser qualitativa, semiquantitativa, quantitativa ou uma combinação. Análises semiquantitativas geralmente utilizam escaladas, conforme exemplificado nos Quadros 1 e 2.

Quadro 1 -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

Fonte: TCU, 2018.

Quadro 2 - 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

Fonte: TCU, 2018.

18. Para melhor entender a etapa Análise de Riscos, é necessário se familiarizar com alguns conceitos e entendimentos:

a. Nível de Risco Inerente (NRI) 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 seus impactos nos objetivos;

b. a política de gestão de riscos estabelece categorias para classificar os níveis de risco, de modo consistente com o seu apetite a risco, conforme Figura 2;

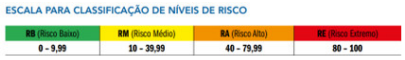

Figura 2

c. Nível de Risco Residual (NRR) é o risco que permanece depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e/ou o impacto dos riscos;

d. a avaliação de controles é parte integrante da análise de riscos;

e. 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;

f. uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar um Nível de Confiança de Controles (NC), que possuem limitações que lhe são inerentes, como a possibilidade de se tornarem ineficazes pela ação de conluio;

g. depois de determinado o Nível de Confiança de Controles (NC), pode-se determinar o risco de controle (RC);

i. RC = 1 – NC

h. depois de determinar o RC, é possível estimar o Nível de Risco Residual (NRR).

i. NRR = NRI x RC

i. **documentação** esperada (documentação dos riscos de níveis mais baixos pode ser menos detalhada):

i. abordagem ou método de análise utilizado, fontes de informação consultadas e participantes do processo;

ii. especificações utilizadas para classificações de probabilidade e impacto dos riscos;

iii. probabilidade de ocorrência de cada evento, severidade ou magnitude do impacto nos objetivos e sua descrição e o resultado de sua combinação, o risco inerente;

iv. descrição dos controles existentes e considerações quanto à sua eficácia, e o risco de controle;

v. nível de risco residual.

19. A terceira e última etapa do Processo de Avaliação de Riscos é a chamada avaliação de riscos, concluindo tal processo. Sua finalidade é auxiliar na tomada de decisões sobre quais riscos necessitam de tratamento e a prioridade para implementação do tratamento. A documentação desta etapa geralmente consiste em uma lista dos riscos que requerem tratamento, com suas respectivas classificações e prioridades.

20. Essa etapa considera os critérios estabelecidos quando o contexto foi considerado. Inclui decisões sobre:

a. se um determinado risco precisa de tratamento e qual 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.

21. Além disso, nessa etapa, deve-se estabelecer critérios para priorização e tratamento associados ao nível de risco. O Quadro 3 exemplifica diretrizes para essa priorização e tratamento.

Quadro 3 - Diretrizes para priorização e tratamento de riscos

Nível de Risco	Critérios para Priorização e Tratamento de Riscos
Risco Elevado	Nível de risco muito além do apetite ao 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.
Risco Alto	Nível de risco além do apetite ao risco. Qualquer risco nesse nível deve ser comunicado a alta administração e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente de área.
Risco Médio	Nível de risco dentro do apetite ao 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.
Risco Baixo	Nível de risco dentro do apetite ao risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefícios, como diminuir o nível de controles.

Fonte: TCU, 2018.

Respostas aos Riscos Avaliados/Tratamento dos Riscos

22. Após o Processo de Avaliação de Riscos, tem-se a seleção e a implementação de respostas aos riscos avaliados, ou o chamado tratamento dos riscos, conforme o modelo de gestão de riscos selecionado pela organização. São formas de tratar os riscos:

a. evitar;

b. reduzir;

c. transferir;

d. aceitar.

23. O tratamento de riscos envolve:

a. a seleção de uma ou mais opções para modificar o nível de risco;

b. a elaboração de planos de tratamento;

c. introdução de novos controles ou a modificação dos existentes.

24. Nesta etapa do processo de gestão de riscos, é necessário levar em consideração que:

a. a opção mais adequada envolve equilibrar os custos e esforços de implementação e os benefícios decorrentes;

b. a existência da possibilidade de que novos riscos sejam introduzidos pelo tratamento e existência de riscos cujo tratamento não seja economicamente viável;

c. quando se tem risco residual acima dos limites de tolerância a risco estabelecidos deve-se reconsiderar a opção de resposta ou os limites da tolerância;

d. documentação esperada do Tratamento de Riscos:

i. plano de tratamento de riscos que identifica a ordem de prioridade para implementação;

ii. razões para a seleção das opções de tratamento;

iii. responsáveis pela aprovação e implementação;

iv. ações propostas, recursos requeridos, contingências e cronograma;

v. medidas de desempenho e requisitos para reporte de informações;

vi. formas de monitoramento da implementação do tratamento de riscos.

Atividades de Controle

25. As atividades de Controle asseguram que:

a. os objetivos sejam alcançados;

b. as diretrizes administrativas sejam cumpridas;

c. as ações necessárias para gerenciar os riscos com vistas à consecução dos objetivos da entidade estejam sendo implementadas.

Informação e Comunicação

26. O componente de Informação e Comunicação deve estar presente em todas as etapas, garantindo uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas.

27. Quando efetivo, este componente deve:

a. auxiliar a estabelecer o contexto;

b. auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente;

c. garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades.

28. A organização deve elaborar um plano de comunicação e consulta interna e externa para apoiar essa atividade.

Monitoramento

29. O componente Monitoramento é uma das etapas mais importantes do processo de gestão de riscos, a qual é necessária a realização de uma análise crítica do trabalho efetuado na gestão de riscos.

30. As responsabilidades do monitoramento devem ser claramente definidas na política de gestão de riscos, na etapa do estabelecimento do Ambiente Interno (Contexto), contemplando as atividades:

a. monitoramento contínuo pelas funções de gestão que têm propriedade sobre os riscos;

b. análise crítica dos riscos e seus tratamentos pelas funções que gerenciam e têm propriedade de riscos ou pelas funções que supervisionam riscos;

c. auditorias realizadas pelas funções que fornecem avaliações independentes:

i. auditoria interna ou externa;

ii. avaliações com foco na estrutura e o processo de gestão de riscos.

31. As finalidades do componente Monitoramento são:

a. detectar mudanças no contexto externo e interno e identificação de riscos emergentes;

b. obter informações adicionais para melhorar a política, estrutura e processo;

c. analisar eventos, mudanças, tendências, sucessos e fracassos;

d. garantir que os controles sejam eficazes e eficientes no desenho e na operação.

e. assegurar que o registro de riscos seja mantido atualizado.

3. METODOLOGIA DE AVALIAÇÃO

32. O objetivo proposto é classificar a maturidade da governança no DNIT nos estágios Inicial, Básico, Intermediário, Aprimorado e Avançado, determinando, assim, o Índice de Maturidade de Gestão de Riscos (IMGR/DNIT). Adotou-se o método de avaliação do Tribunal de Contas da União , que atribui os valores de 0 a 20% para a maturidade em estágio Inicial; de 20,1% a 40% para o estágio Básico; 40,1 a 60% para o nível Intermediário; 60,1% a 80% para o estágio Aprimorado e 80,1 a 100% para Avançado, conforme Figura 3.

0 ← → 20%	20,1% ← → 40%	40,1% ← → 60%	60,1% ← → 80%	80,1% ← → 100%
Inicial	Básico	Intermediário	Aprimorado	Avançado

Figura 3: Escala de valores de maturidade de gestão de riscos - Índice de Maturidade de Gestão de Riscos (IMGR)

33. A avaliação será efetuada por meio de um questionário, presente no Anexo I. A metodologia de avaliação considera que os questionamentos estão divididos em Mecanismos de Gestão de Riscos (Ambiente, Processos e Resultados), que são subdivididos pelos respectivos Componentes (Liderança, Políticas e Estratégias, Pessoas, Identificação e análise de riscos, Avaliação e respostas a riscos, Monitoramento e Comunicação, Melhoria dos processos de governança e gestão, Resultados-chaves da gestão de riscos), conforme Figura 4. Os mecanismos de avaliação presentes no Anexo I englobam todos os componentes do COSO II, conforme demonstrado no Quadro 4. A partir dos Componentes, desmembra-se as Práticas de Gestão de Riscos, seguidas dos Questionamentos, que podem ser considerados como questões de auditoria da Ordem de Auditoria a fim da avaliação em comento.

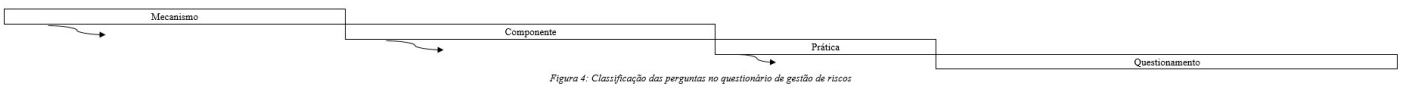

Figura 4: Classificação das perguntas no questionário de gestão de riscos

Quadro 4 - Objetos avaliados (Paralelo com COSO II)

Mecanismos de Avaliação – Anexo I	Componentes do COSO II
AMBIENTE	Ambiente Interno
	Fixação de Objetivos
PROCESSOS	Identificação de Eventos
	Avaliação de Riscos
	Resposta ao Risco
	Atividades de Controle
	Informação e Comunicação
	Monitoramento
RESULTADOS	-

34. O cálculo dos índices de maturidade de cada Prática, constante do Anexo I, coluna (c), é realizado atribuindo-se 4,0 pontos para a presença integral e consolidada da Prática, 1,0 - 2,0 ou 3,0 pontos quando a presença é parcial, de acordo com sua intensidade, e zero ponto à ausência total, conforme escala presente no Quadro 5.

Quadro 5 - Escala para avaliação de evidências quanto aos aspectos de gestão de riscos

PONTUAÇÃO	0,0	1,0	2,0	3,0	4,0
	Inexistente	Inicial	Básico	Aprimorado	Avançado
AMBIENTE	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 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.
PROCESSOS					
RESULTADOS	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.

Fonte: TCU, 2018.

35. O avaliador deverá responder o questionário de acordo com as evidências coletadas no processo de auditoria adequado, observando as documentações necessárias apresentadas neste Manual para cada etapa do gerenciamento de riscos. Após, deve-se atribuir a pontuação apresentada no Quadro 5 para os questionamentos cujas respostas possam ser escalonadas. Os questionamentos que podem ser respondidos por "SIM" ou "NÃO", atribui-se 4,0 pontos para o "SIM" e 0,0 ponto para o "NÃO".

36. Para as Práticas que se desdobram em questionamentos, cada questionamento obterá um número decimal como pontuação, resultante da divisão dos valores de pontuação possíveis (de 0 a 4) pelo número de questionamentos que compõem a questão. Por exemplo, para uma Prática com cinco questionamentos, cada questionamento poderá receber de zero a no máximo 0,8 (4/5 – sendo que 4 é a pontuação máxima). Se, nesse caso, um dos questionamentos receber nota Básica, este questionamento receberia a pontuação 0,4 (2/5 – sendo 2 a pontuação do questionamento e 5 o número de questionamentos da Prática analisada).

37. O índice de maturidade de cada mecanismo (Ambiente, Processos e Resultado) é calculado pela razão entre a pontuação alcançada e a pontuação máxima possível (obtidas na avaliação das Práticas), expressando esse quociente com um número de 0% a 100%. Por exemplo, se um componente obtém 40 pontos de 76 pontos possíveis (19 Práticas x 4 pontos = 76 pontos, ressaltando que 4 é a pontuação máxima), então o índice de maturidade desse componente seria de 52,6% (40/76 x 100).

38. O grau de maturidade, ou Índice de Maturidade de Gestão de Riscos (IMGR) varia de 0 a 100% e são calculados a partir da média ponderada dos índices de maturidade de cada mecanismo, conforme Quadro 6. A definição dos pesos para a ponderação segue a metodologia definida pelo modelo de maturidade do Tribunal de Contas da União (TCU, 2018), entretanto, como a avaliação presente neste Manual não contempla o mecanismo "Parcerias", atribui-se 40% para o mecanismo "Ambiente", 40% para "Processos" e 20% para "Resultados".

Quadro 6 - Ponderação do cálculo do Índice de Maturidade por Mecanismo

MECANISMO	PESO	EXEMPLO		
		IMC	PESO	PONDERADO
Ambiente	40	65,0	0,4	26,0
Processos	40	50,0	0,4	20,0
Resultados	20	61,0	0,2	12,2
Índice de Maturidade de Gestão de Riscos =				58,2

39. Com os valores de cada questão, pode-se calcular o grau de maturidade de cada Prática de Gestão de Riscos, Componente e Mecanismos, assim como o grau de maturidade da Gestão de Riscos, per se, da organização. Como exemplo, considera-se os valores da Tabela 1 para as questões do mecanismo Resultados:

Tabela 1 – Exemplo Mecanismo Resultado

MECANISMOS	COMPONENTES	PRÁTICAS	Questões	Valores
RESULTADOS	3.1. – Melhoria dos processos de governança e gestão - Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos? **12 pontos (3,0 + 2,0 + 4,0 + 3,0).**	3.1.1. Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização?	98	**3,0**
		3.1.2. 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?	99	**2,0**
		3.1.3. Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?	100	**4,0**
		3.1.4. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?	101	**3,0**
	3.2. – Resultados-Chaves da gestão de riscos - Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização? **5,25 pontos (1,0 + 3,25 + 1,0)**	3.2.1. Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?	102	**1,0**
			-	-
		3.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização? **3,25 pontos (1,0 + 0,5 + 1,0 + 0,75)**	103	1,0 (4,0/4 x 1,0)
			104	0,5 (2,0/4 x 1,0)
			105	1,0 (4,0/4 x 1,0)
			106	0,75 (3,0/4 x 1,0)
		3.2.3. Os riscos da organização estão dentro dos seus critérios de risco?	107	**1,0**

40. Conforme explicitado anteriormente, quando a Prática possui mais de um questionamento, divide-se o número da pontuação máxima possível (4,0) pelo número de questionamentos (4). Assim, na Prática 3.2.2, a pontuação máxima de cada questionamento é 1,0 (4,0/4: pontuação máxima/número de questões). O cálculo da pontuação de cada prática é a divisão da pontuação original do questionamento (de 0 a 4) pela pontuação original máxima (4) e posteriormente multiplicado pela pontuação máxima de cada questionamento, que neste caso é 1,0. Assim, a questão 106, por exemplo, recebe a pontuação de 0,75 (3,0/4 x 1,0), sendo 3,0 a pontuação original, 4 a pontuação original máxima e 1,0 a pontuação máxima de cada questionamento desta questão, cuja Prática foi subdivida em vários questionamentos. Assim nota-se que a Prática 3.2.2 ficou com a nota 3,25, sem ultrapassar a pontuação máxima original de 4,0.

41. Com a pontuação dos Componentes (3.1 = 12 pontos; 3.2 = 5,25 pontos), calcular-se-á o índice de maturidade do Mecanismo Resultados. O Componente 3.1 possui 4 Práticas, desse forma, a pontuação máxima a ser obtida seria 16 (4,0 x 4); o Componente 3.2 possui 3 Práticas, logo, com pontuação máxima de 12 (4,0 x 3). O índice de maturidade do mecanismo do exemplo apresentado é 61,61%:

$$\text{Mecanismo Resultado} = \frac{\text{Pontuação Obtida}}{\text{Pontuação Máxima Possível}} \times 100 = \frac{12 + 5{,}25}{16 + 12} \times 100 = \frac{17{,}25}{28} \times 100 = \mathbf{61{,}61\ \%}$$

42. Para o cálculo do Índice de Maturidade de Gestão de Riscos/DNIT, sugere-se a utilização dos pesos do Quadro 6.

4. PROCEDIMENTOS DE AUDITORIA

43. O avaliador deverá preencher o questionário apresentado no Quadro do Anexo I, de acordo com seu julgamento profissional sobre o escalonamento das respostas a partir dos testes de auditoria efetuados. A aplicação desses testes de auditoria deve ser pautada na finalidade de se chegar às conclusões necessárias e fundamentadas.

44. O produto final da Ordem de Auditoria aberta para avaliar a gestão de riscos desta autarquia será um Relatório, no qual se deve evitar a exposição inadequada de pessoas físicas e jurídicas, tendo em vista que o mesmo será publicado na intranet da organização.

45. As técnicas de auditoria prioritárias a serem utilizadas na avaliação são:

a. indagação oral/escrita: uso de entrevistas junto ao pessoal da unidade auditada para obtenção de dados e informações. A entrevista é um método de coleta de informações que consiste em conversas individuais ou em grupo com pessoas selecionadas cuidadosamente e cujo grau de pertinência, validade e confiabilidade auxilie na coleta de informações. As entrevistas poderão ser reduzidas a termo, se o auditor considerar necessário. A indagação oral poderá ter auxílio de instrumentos como:

i. fluxogramas;

ii. narrativas.

b. observação das atividades e condições: tem a finalidade de avaliar se o levantamento do processo foi efetivo, materializado na narrativa e no fluxograma elaborado. Pode ser chamado de teste de percurso, que é efetuado por meio do exame de todas as fases do processo sobre uma amostra limitada de transações. Ele deverá comprovar que o sistema de controle interno funciona de forma coerente, eficaz e continuada. Os elementos da observação são:

i. identificação da atividade específica a ser observada;

ii. observação de sua execução;

iii. comparação do comportamento observado com os padrões estabelecidos;

iv. avaliação e conclusão.

c. inspeção física: exame usado para testar a efetividade dos controles, particularmente daqueles relativos à segurança de quantidades físicas ou qualidade de bens tangíveis;

d. rastreamento: investigação minuciosa, com exame de documentos, setores, unidades e procedimentos interligados, visando dar segurança à opinião do responsável pela execução do trabalho sobre o fato observado.

REFERÊNCIAS

BRASIL. Controladoria-Geral Da União. Ministério do Planejamento, Orçamento e Gestão. **Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2015**: Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos**. Brasília: TCU, 2018.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade**. Brasília: TCU, 2018.

BRASIL. Tribunal de Contas da União. **Acórdão 2746-43/2015 – Plenário**: Auditoria realizada no Dnit no âmbito de Fiscalização de Orientação Centralizada com objetivo de avaliar as práticas de governança e de gestão de aquisições públicas adotadas pela Administração Pública Federal.

ANEXO I

	Quadro x - QUESTIONÁRIO PARA AVALIAÇÃO DA GESTÃO DE RISCOS			
MECANISMOS (a)	**COMPONENTES (b)**	**PRÁTICAS (c)**	**Nº**	**QUESTIONAMENTOS (d)**
AMBIENTE	1.1 Liderança - Em que medida os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos e cultura?	1.1.1 Cultura - 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?	1	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?
			2	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?
			3	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?
			4	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?
		1.1.2 Governança de Riscos - 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?	5	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?
			6	As instâncias internas de apoio à governança de riscos exercem suas atribuições mediante uma abordagem planejada, sistemática e disciplinada?
			7	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 relevantes para o alcance dos objetivos-chaves da organização?
		1.1.3 Supervisão da Governança e da alta administração - Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos?	8	Os processos de governança e gestão incorporam explicitamente indicadores-chaves de risco e indicadores-chaves de desempenho, monitorados regularmente?
			9	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?

		10	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?
		11	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?
		12	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?
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?	1.2.1 Direcionamento Estratégico - A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico?	13	A 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?
		14	O direcionamento estratégico é alinhado com as finalidades e competências legais da entidade?
		15	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?
	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?	16	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?
		17	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?
	1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos?	18	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 (práticas 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?
		19	São consideradas as várias alternativas de cenários e os riscos associados na definição dos objetivos estratégicos e na seleção das estratégias para atingi-los?
		20	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?
	1.2.4. A administração define e comunica os objetivos e as respectivas medidas de desempenho em termos específicos e mensuráveis?	21	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?
		22	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?
		23	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?
		24	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?
	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?	25	A alta administração aprovou a política de gestão de riscos e assumiu a liderança no compromisso com a sua implementação?
		26	A política de gestão de riscos é apropriadamente comunicada e está disponível para acesso a todos, dentro e fora da organização?
		27	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?
		28	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?
		29	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?
		30	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?

			31	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?
			32	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?
		1.2.6. Toda a gestão da organização é comprometida com a gestão de riscos?	33	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?
		1.2.7. A administração aloca recursos suficientes e apropriados para a gestão riscos?	34	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?
	1.3 - Pessoas - Em que medida as pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas para exercê-los?	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?	35	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?
			36	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?
		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?	37	Os gestores, que integram a primeira linha de defesa, 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?
			38	Os gestores, que integram a primeira linha de defesa, 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?
			-	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:
			39	i. apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade?
			40	ii. fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos?
			41	iii. define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização?
			42	iv. estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos?
			43	v. orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la?
			44	vi. comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização?
			-	O pessoal da auditoria interna, que integra a terceira linha de defesa, especialmente o dirigente dessa função:
			45	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?
			46	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?
			47	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?
	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)?	2.1.1. A identificação de riscos é precedida de uma etapa de estabelecimento do contexto?	48	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?
			49	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 objetivoschaves da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados?

PROCESSOS			50	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?
			51	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?
		2.1.2. A documentação da etapa de estabelecimento do contexto inclui elementos essenciais para viabilizar um processo de avaliação de riscos consistente?	-	A documentação da etapa de estabelecimento do contexto inclui pelo menos:
			52	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)?
			53	ii. a análise de partes interessadas e seus interesses (por exemplo, análise de stakeholder, análise RECI, matriz de responsabilidades)?
			54	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)?
		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?	55	Nos processos de identificação de riscos são envolvidas pessoas com conhecimento adequado, bem como os gestores das áreas?
			56	São utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de riscos?
			57	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?
			58	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?
			59	A seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos?
			60	São analisados o impacto e a probabilidade 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?	61	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?
			-	No registro de riscos da organização, a documentação das atividades de identificação e análise de riscos inclui pelo menos:
			62	i. o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise?
			63	ii. os participantes das atividades de identificação e análise de riscos?
			64	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?
			65	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?
			66	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?
			67	vi. a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade?
			68	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?	2.2.1. Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por toda a organização?	69	Existem critérios estabelecidos para orientar as decisões sobre riscos em relação a todas as operações, funções e atividades relevantes da organização?
			70	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?
			-	Os critérios estabelecidos são adequados para orientar decisões quanto a se:
			71	i. um determinado risco precisa de tratamento e a prioridade para isso?

		72	ii. uma atividade deve ser realizada, reduzida ou descontinuada?
		73	iii. controles devem ser implementados, modificados ou apenas mantidos?
	2.2.2. A seleção de respostas para tratar riscos considera todas as opções de tratamento e o seu custo-benefício?	74	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?
	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?	75	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?
	2.2.4. Os elementos críticos da atuação da organização estão identificados e têm definidos planos e medidas de contingência?	76	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?
	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?	-	A documentação da avaliação e seleção de respostas aos riscos inclui pelo menos:
		77	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?
		78	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?
		79	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?
		80	iv. a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las?
2.3. – Monitoramento e comunicação - Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização?	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?	81	As diretrizes e os 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?
		82	Há uma efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos?
	2.3.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado?	83	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?
		84	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?
	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?	-	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:
		85	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?
		86	ii. por meio de auto avaliações periódicas de riscos e controles (Control and Risk Self Assessment – CRSA), que constam de um ciclo de revisão periódica estabelecido?
		87	iii. 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) exercem suas atribuições de modo efetivo?	88	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 auto avaliações da primeira linha de defesa?
		89	Essas funções fornecem orientação e facilitação para a condução das atividades de monitoramento contínuo e auto avaliações da primeira linha de defesa, mantém a sua documentação e comunica os seus resultados às instâncias apropriadas da administração e da governança?
	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?	90	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?
		91	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?
			92	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?	93	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?
			94	Os planos e as medidas de contingência são periodicamente testados e revisados?
		2.3.7. A organização monitora as mudanças que podem aumentar sua exposição a riscos ter impacto nos seus objetivos?	95	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?
		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?	96	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?
			97	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?
RESULTADOS	3.1. – Melhoria dos processos de governança e gestão - Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos	3.1.1. Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização?	98	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?
		3.1.2. 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?	99	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?
		3.1.3. Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?	100	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?
		3.1.4. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?	101	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?
	3.2. – Resultados-Chaves da gestão de riscos - Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização?	3.2.1. Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?	102	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?
		3.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização?	-	Os responsáveis pela governança e a administração, com base nas informações resultantes da gestão de riscos, têm garantia razoável de que:
			103	i. entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização?
			104	ii. entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados?
			105	iii. a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável?
			106	iv. as leis e os regulamentos aplicáveis estão sendo cumpridos?
		3.2.3. Os riscos da organização estão dentro dos seus critérios de risco?	107	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?

Setor de Autarquias Norte | Quadra 3 | Lote A
CEP 70040-902
Brasília/DF |