Gestão de Riscos
SCGE-PE

Secretaria da Controladoria Geral do Estado

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

GUIA PRÁTICO DE MATURIDADE
em Gestão de Riscos - 2025

Expediente

GOVERNO DO ESTADO DE PERNAMBUCO

RAQUEL TEIXEIRA LYRA LUCENA
Governadora do Estado

PRISCILA KRAUSE BRANCO
Vice-Governadora do Estado

RENATO BARBOSA CIRNE
Secretário da Controladoria-Geral do Estado Ouvidor-Geral do Estado

TIAGO BARBOSA DA FONSECA
Gerente Geral de Governança e Riscos

Elaboração:

MARIANA DE ANDRADE BARROS DOS SANTOS
Chefe da Unidade de Desenvolvimento de Projetos

Revisão:

CRISTIANA BORGES DE B. E S. NOVELLINO
Coordenadora de Gestão de Riscos

Colaboração:

ALEXANDRE OTÁVIO CARVALHO
Gestor Governamental de Controle Interno

EMANUELLA FRANCKLIN CORDEIRO DE SOUSA
Gestora Governamental de Controle Interno

LUCAS MILET DO AMARAL MERCÊS
Chefe da Unidade de Gestão de Riscos

MARCELO ALVES CAVALCANTI
Gestor Governamental de Controle Interno

www.scge.pe.gov.br | www.transparencia.pe.gov.br
www.ouvidoria.pe.gov.br | www.lai.pe.gov.br
instagram: @scge_pe
SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO
Rua Santo Elias, 535 - Espinheiro - Recife - PE - CEP.: 52020-095
Telefone: (81) 3183-0800

Sumário

1. INTRODUÇÃO

A gestão de riscos é um componente estruturante dos sistemas de governança, contribuindo para a tomada de decisões, o fortalecimento dos controles internos e o aprimoramento da integridade e da transparência da gestão pública. Nesse contexto, torna-se fundamental dispor de instrumentos que permitam não apenas a implementação, mas também a avaliação do grau de maturidade dos processos de gestão de riscos.

Este Guia Prático de Maturidade em Gestão de Riscos tem por finalidade apresentar, de forma sistematizada, os requisitos de maturidade, suas respectivas referências normativas e conceituais, as prescrições técnicas para sua implementação e os instrumentos de comprovação (evidências).

A estrutura do guia foi elaborada com base em modelos consolidados de gestão de riscos, como a ISO 31000:2018 e o COSO ERM:2017, além de boas práticas extraídas de metodologias aplicadas no setor público. Os requisitos são organizados de forma a permitir a identificação de lacunas, a definição de planos de ação e o monitoramento da evolução da maturidade em gestão de riscos ao longo do tempo.

Ao integrar teoria, prática e mecanismos de verificação, este guia visa apoiar a institucionalização da gestão de riscos como processo contínuo e transversal, promovendo maior alinhamento entre riscos, objetivos estratégicos e mecanismos de controle.

2. METODOLOGIA

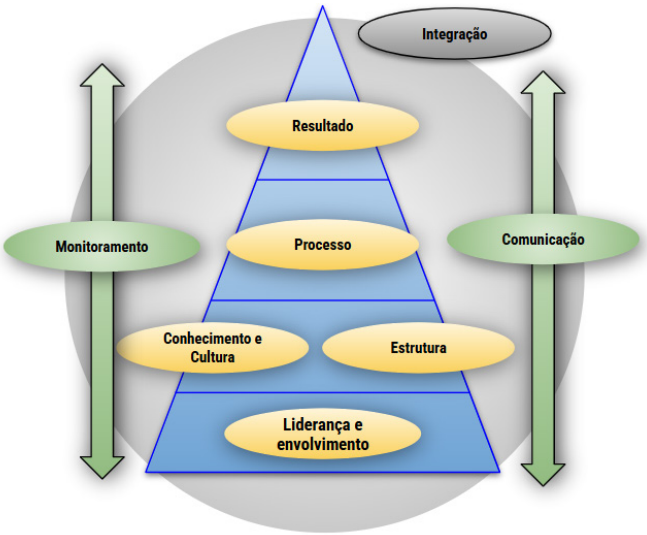
2.1 Modelo de Maturidade da SCGE

O modelo de maturidade em gestão de riscos adotado pela SCGE é representado por uma pirâmide, cuja estrutura tem o **“Resultado”** no topo, refletindo o propósito central e a razão de existir da gestão de riscos. Esse “Resultado” é sustentado por camadas hierárquicas de elementos interdependentes, que representam os fundamentos, práticas e mecanismos necessários para alcançar uma gestão eficaz e integrada de riscos:

- **Liderança e Envolvimento:** Base da pirâmide, responsável por inspirar o comprometimento e a responsabilidade pela gestão de riscos. A liderança é crucial para criar engajamento e orientar a prática de gestão de riscos.
- **Conhecimento e Cultura:** Segunda camada, essencial para garantir que todos compreendam os riscos e adotem uma mentalidade preventiva. Fomenta um ambiente de aprendizado e conscientização.
- **Estrutura:** Também faz parte da segunda camada, que provê uma fundação sólida para a gestão de riscos. Inclui políticas, normas e uma infraestrutura apropriada.
- **Processo:** Representa a aplicação prática dos conhecimentos, da cultura e da estrutura para gerenciar riscos de maneira contínua e eficaz.

Para apoiar essas camadas, o modelo também traz práticas de **Comunicação, Monitoramento e Integração** da gestão de riscos com o planejamento e os processos organizacionais. Esses elementos transversais garantem a eficácia, a transparência e a adaptabilidade contínua do processo, permitindo que a gestão de riscos seja constantemente ajustada conforme as necessidades e os objetivos da organização.

Figura 1: Framework



Fonte: Elaboração própria

2.2 Pesos dos grupos na pontuação do questionário

A definição dos pesos dos requisitos do questionário foi realizada com base no método estatístico AHP (Analytic Hierarchy Process), que permite atribuir ponderações de forma estruturada e consistente entre critérios hierárquicos.

Tabela 1: Peso por agrupamento

No	Agrupamento	Peso
1	Liderança e Envolvimento	6,00%
2	Estrutura	3,70%
3	Conhecimento e Cultura	26,80%
4	Processo	12,70%
5	Resultado	31,50%
6	Monitoramento	8,50%
7	Comunicação	5,10%
8	Integração	5,70%
	Total	100,00%

Fonte: Elaboração própria

2.3 Estruturação dos requisitos de maturidade

Foram definidos vinte e quatro (24) requisitos de maturidade, agrupados de acordo com a Tabela 1, cujas respostas são obtidas por autoavaliação da Unidade de Controle Interno (UCI). Esses requisitos representam aspectos essenciais da prática de gestão de riscos que permitem avaliar o estágio de desenvolvimento do órgão ou entidade.

As respostas foram estruturadas utilizando a escala Likert de cinco pontos, na qual o respondente deve indicar em qual estágio de maturidade determinado requisito se enquadra no órgão/entidade, entre as seguintes opções: **0 - Inexistente, 1 - Inicial, 2 - Parcial, 3 - Estabelecida e 4 - Integrada.**

Recomenda-se que as unidades utilizem evidências e registros internos como apoio à análise, de forma a tornar o diagnóstico mais consistente e fundamentado.

Para cada ponto da escala é atribuída uma correspondência percentual de **0% a 100%, sendo: 0% para 0 - Inexistente, 25% para 1 - Inicial, 50% para 2 - Parcial, 75% para 3 - Estabelecida e 100% para 4 - Integrada.**

O cálculo da pontuação por questão é realizado por meio de uma **nota ponderada**, que considera a resposta atribuída pelo participante e o peso definido para cada questão. A soma das pontuações de todas as questões resulta na nota final, que será comparada aos níveis de maturidade apresentados a seguir.

Figura 2: Níveis de maturidade

Fonte: Elaboração própria

2.4 Metodologia de Aplicação do Guia

Este guia foi estruturado para apoiar os órgãos e entidades do Poder Executivo Estadual na avaliação e no aprimoramento da maturidade em gestão de riscos. Sua aplicação deve seguir as etapas abaixo, de forma a garantir uniformidade, confiabilidade e comparabilidade dos resultados obtidos.

A. Preparação

- Identifique os responsáveis pela condução da autoavaliação e assegure que possuam conhecimento básico sobre gestão de riscos. A Unidade de Controle Interno deve fazer parte do rol de responsáveis, atuando em conformidade com suas competências institucionais e sem prejuízo das responsabilidades das áreas gestoras;
- Reúna previamente as normas, políticas, relatórios e demais documentos que possam servir como evidência.

B. Leitura e Compreensão dos Requisitos

- Analise cada requisito de maturidade apresentado no guia, observando:
  - Referências: indicam o embasamento legal, regulatório ou técnico.
  - Prescrição descreve o que deve ser implementado para o atendimento ao requisito.
  - Evidências: documentos que demonstram a efetividade da prática, apresentados em lista exemplificativa, devendo a comprovação considerar os aspectos descritos na prescrição.

C. Autoavaliação

- Para cada requisito, atribua o nível de atendimento conforme os critérios estabelecidos (ex.: Inexistente, Inicial, Parcial, Estabelecida e Integrada)
- Registre as justificativas e evidências associadas a cada pontuação.

D. Consolidação e Análise dos Resultados

- Compile as respostas para identificar pontos fortes, lacunas e oportunidades de melhoria;
- Utilize os resultados para elaborar um plano de ação voltado à evolução do nível de maturidade.

E. Monitoramento e Revisão

- Repita a avaliação periodicamente, comparando os resultados para acompanhar a evolução;
- Atualize os registros e evidências sempre que houver mudanças nos processos ou nos controles.

Importante:

A aplicação do guia deve ser conduzida de forma objetiva e baseada em evidências, evitando julgamentos subjetivos que possam comprometer a fidedignidade dos resultados.

3. REQUISITOS DE MATURIDADE

Apresentamos, a seguir, cada um dos 24 requisitos de maturidade, por agrupamento, destacando que cada requisito reflete um conjunto de condições, comportamentos e evidências esperados para que a gestão de riscos seja efetiva e integrada à governança.

3.1 Agrupamento: Liderança e Envolvimento

A liderança é fundamental para a evolução da maturidade em gestão de riscos, pois é ela quem define o tom e a cultura organizacional em relação ao tema. Quando a alta administração demonstra um compromisso claro com a gestão de riscos, definindo diretrizes estratégicas e se envolvendo ativamente no processo de gerenciamento de riscos estratégicos, cria-se um ambiente onde a gestão de riscos é priorizada e valorizada em todos os níveis da organização.

• **Requisito de maturidade 01:** Existe diretriz estratégica para assegurar que o gerenciamento de riscos seja realizado nos PRINCIPAIS níveis hierárquicos do órgão/entidade.

- **Referência:** Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que a gestão de riscos esteja integrada em todas as atividades da organização, e convém que demonstrem liderança e comprometimento por: personalizar e implementar todos os componentes da estrutura; emitir uma declaração ou política que estabeleça uma abordagem, plano ou curso de ação da gestão de riscos; assegurar que os recursos necessários sejam alocados para gerenciar riscos; atribuir autoridades, responsabilidades e responsabilização nos níveis apropriados dentro da organização. (ISO 31000:2018, seção 5.2)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Formalizar diretrizes estratégicas claras que definam a necessidade de realização do gerenciamento de riscos em diferentes níveis hierárquicos (ex: estratégico, tático e operacional), assegurando que as diretrizes sejam revisadas periodicamente.

b. Definir responsabilidades específicas no modelo de governança para cada nível do órgão/entidade. (ex: Gestor dos Riscos, Unidade de Controle Interno, Comitê de Governança). Correlacionar os eventos de riscos identificados aos respectivos objetivos estratégicos.

c. Incorporar o gerenciamento de riscos nas rotinas e instrumentos de planejamento e tomada de decisão em todos os níveis (ex: planos de ação, planos de integridade, projetos estratégicos).

d. Incluir diretrizes de gestão de riscos, em todos os níveis, nos documentos estratégicos já publicados que ainda não contenham essa informação.

- **Evidências:** Documentos estratégicos da UG, como política de gestão de riscos, com seções específicas sobre responsabilidades por nível hierárquico, manuais, plano estratégico contendo diretrizes sobre gestão de riscos em diferentes níveis organizacionais, código de conduta mencionando a importância da gestão de riscos em todos os níveis e descrevendo como ela deve ser realizada, etc.

Saiba Mais!

Todas as iniciativas a serem implementadas dependem do patrocínio da alta gestão, é o chamado “tom do topo”. Com a gestão de riscos não é diferente, pois se não houver apoio dos dirigentes máximos, a utilização da metodologia pode ficar restrita a alguns setores, não cumprindo o papel de proporcionar uma visão geral dos principais riscos que podem prejudicar os objetivos organizacionais.

Exemplos:

Portaria SCGE 013.2021 – Institui o Comitê de Gestão de Riscos, Política de Gestão de Riscos da SCGE, Anexo Único da Política Geral de Riscos nas Contratações Públicas, etc.

- **Requisito de maturidade 02:** O **Gerenciamento dos Riscos Estratégicos** é implementado no órgão/entidade.

- **Referência:** Gerenciamento de Riscos Corporativos - Integrado com a Estratégia e Performance realça a importância do gerenciamento de riscos corporativos no planejamento estratégico e da sua incorporação em toda a organização - porque o risco influencia e alinha estratégia e performance em todos os departamentos e funções. (Um Framework orientado - COSO ERM 2017)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Relacionar os objetivos estratégicos do órgão/entidade que constam no seu planejamento estratégico.
  b. Realizar o gerenciamento de riscos estratégicos e documentar através do mapa de riscos validado pela alta gestão.
  c. Correlacionar os eventos de riscos identificados aos respectivos objetivos estratégicos
- **Evidências:** Mapa de Riscos dos objetivos estratégicos correlacionando os riscos aos respectivos objetivos com a devida ciência da alta gestão.

Saiba Mais!

Avaliar os riscos dos objetivos estratégicos auxilia na prevenção de eventos indesejados e aumenta as chances de atingi-los de maneira eficaz, além de ajudar a preservar a reputação do órgão. Assim como o gerenciamento dos demais riscos, é possível realizar o gerenciamento de riscos estratégicos através de planilha modelo semelhante à disponibilizada pela SCGE em seu sítio eletrônico https://www.scge.pe.gov.br/wp-content/uploads/2024/01/Mapa-de-Riscos-Modelo-pdf.pdf. ou modelo de mapa de riscos de preferência do órgão. O campo de “etapa” é substituído pelo objetivo estratégico e relacionam-se os riscos identificados. O gerenciamento de riscos estratégicos deve conter evidência de participação e anuência da alta gestão.

Figura 3: Modelo de Mapa de Riscos dos Objetivos Estratégicos da SCGE

MAPA DE RISCOS								
Nº	OBJETIVO ESTRATÉGICO	RISCO			NÍVEL DE RISCO	MEDIDAS DE TRATAMENTO		RESPONSÁVEL
		CAUSAS	EVENTO	CONSEQUÊNCIAS		MEDIDAS PREVENTIVAS	MEDIDAS CORRETIVAS	

Fonte: Elaboração própria

Atenção gestores!!! É de grande importância que os riscos documentados estejam sendo verdadeiramente acompanhados pela alta administração porque, caso venham a se materializar, e não tenham sido implementadas as medidas preventivas, a administração poderá ser considerada omissa, uma vez que estava ciente dos riscos, mas não tomou nenhuma providência.

3.2 Agrupamento: Estrutura

Refere-se aos alicerces necessários para o desenvolvimento eficaz e regular do processo de Gestão de Riscos. Este grupo traz práticas de planejamento estratégico, de definição de metas e indicadores, e do uso de sistemas informatizados para gerenciar e monitorar riscos. Também aborda a importância da existência de uma política formal de gestão de riscos aprovada e comunicada.

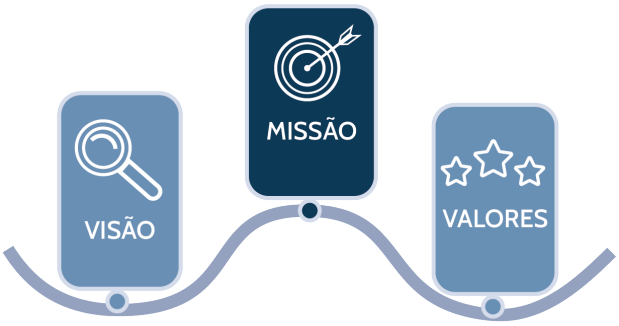
- **Requisito de maturidade 03:** O órgão/entidade possui planejamento estratégico (atualizado) contendo, dentre outras informações indispensáveis, as definições de missão, visão e objetivos.

- **Referência:** Gerenciamento de riscos corporativos - Integrado com Estratégia e Performance realça a importância do gerenciamento de riscos corporativos no planejamento estratégico e da sua incorporação em toda organização - porque o risco influencia e alinha estratégia e performance em todos os departamentos e funções. (COSO ERM 2017).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Elaborar e publicar no sítio eletrônico do órgão/entidade o planejamento estratégico do órgão/entidade em consonância com o planejamento do governo do estado. Vide Planejamento Estratégico da SCGE: (https://www.scge.pe.gov.br/planejamento-estrategico-2/).
- **Evidências:** Documento que formaliza o planejamento estratégico publicado no sítio eletrônico do órgão.

Saiba Mais!

Neste documento demonstraremos uma estrutura básica para elaboração de um planejamento estratégico, com o objetivo de auxiliar os órgãos que ainda não o possuem. Destaca-se que é um conteúdo meramente exemplificativo.

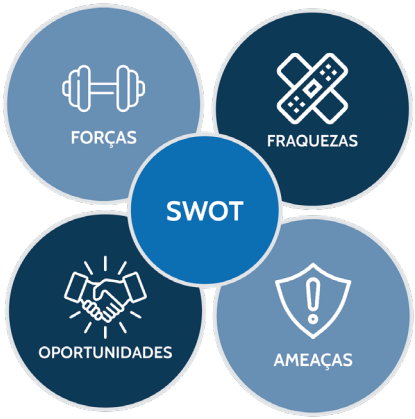
O Estado possui um planejamento contemplando todas as propostas do Governo ao longo da gestão. Em consonância com essas diretrizes gerais, cada órgão deve elaborar seu planejamento de acordo com sua natureza de atuação.



O primeiro passo é a definição da Missão, Visão e Valores. É impossível o órgão definir objetivos sem entender qual a sua razão de existir, qual a sua contribuição para a sociedade (Missão) e onde quer chegar nos próximos anos (Visão). Adicionalmente, é necessário determinar os princípios norteadores da atuação (Valores).

Exemplo: Missão, Visão e Valores do Google

Nossa Missão é "organizar as informações do mundo para que sejam universalmente acessíveis e úteis para todos", isso se dá por meio da Visão de "criar um futuro mais inteligente, no qual a tecnologia melhore a vida das pessoas" utilizando os seguintes Valores: foco no usuário, inovação, ética, transparência e responsabilidade



Posteriormente, realiza-se a "Análise ou Matriz SWOT", que é uma técnica para identificação das forças e fraquezas, oportunidades e ameaças de uma organização. É um método para entender de forma direta o que pode contribuir e o que pode atrapalhar no atingimento dos objetivos organizacionais. Para mais informações consulte o vídeo do Conselho Regional de Administração de São Paulo (CRA-SP): https://www.youtube.com/watch?v=bwo7lONcsyM.

Em seguida, é realizada a definição dos objetivos, que devem ser específicos e mensuráveis e, principalmente, estarem alinhados com a Missão, Visão e Valores do órgão. Devem funcionar como degraus que levam o órgão onde ele quer chegar.

Na etapa seguinte têm-se a formulação de estratégia, quando são definidas as técnicas e processos para atingimento dos objetivos. Essa etapa é seguida pela implementação, quando as estratégias são transformadas em ações concretas, com definição de responsabilidades, recursos e prazos para cada ação definida.

Por fim, há duas etapas de grande importância que muitas vezes são negligenciadas, o monitoramento e a comunicação. Em relação ao monitoramento, é preciso definir métricas de acompanhamento do progresso em relação aos objetivos definidos. Ressalta-se também que o planejamento não deve ser uma peça estática, uma vez que o ambiente está em constante mudança, então é preciso realizar revisões periódicas para verificar as necessidades de adequação. Com relação à comunicação, é necessário que o planejamento estratégico seja de conhecimento de todos os servidores, não devendo ficar restrito à alta gestão. O engajamento de todos é essencial para o sucesso da implementação.

- **Requisito de maturidade 04:** O órgão/entidade estabeleceu e comunicou adequadamente **metas** e **indicadores** dos projetos e processos para monitorar seu **desempenho.**

- **Referência:** Estabelecer a estratégia engloba: (...) b)Definir a estratégia da organização. Consiste em fazer escolhas e estabelecer prioridades, a partir de evidências. Essas escolhas e prioridades devem suportar a missão, a visão e os valores fundamentais da organização, compreendendo objetivos, indicadores e metas de desempenho. (Referencial Básico de Governança Organizacional Aplicável a Órgãos e Entidades da Administração Pública. 3. ed. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2020.)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Implantar a gestão de desempenho através do uso de indicadores.
  b. Definir metas claras e mensuráveis para os principais projetos e processos institucionais.
  c. Estabelecer indicadores de desempenho (KPIs) alinhados aos objetivos estratégicos e operacionais.
  d. Garantir a comunicação adequada dessas metas e indicadores a todos os níveis da organização, especialmente às equipes diretamente envolvidas nos projetos/processos.
  e. Integrar o monitoramento desses indicadores nos ciclos de gestão, como reuniões gerenciais, relatórios periódicos e painéis de controle (dashboards).
  f. Revisar periodicamente os indicadores e metas, ajustando-os conforme mudanças no ambiente interno ou externo.
- **Evidências:** Planos contendo metas e indicadores vinculados a projetos e processos, planilhas, dashboards ou sistemas de monitoramento com os indicadores utilizados, relatórios gerenciais ou de desempenho contendo a análise periódica dos resultados, atas de reuniões que demonstrem a discussão sobre metas e desempenho, comunicados internos ou apresentações utilizadas para divulgar os indicadores às equipes, etc.

Saiba Mais!

Checklist inicial:

- Mapear os objetivos estratégicos, projetos e processos críticos da organização;
- Verificar se já existem indicadores informais ou não estruturados;
- Verificar se os indicadores estão alinhados ao planejamento estratégico.

A partir desse diagnóstico inicial deve-se selecionar os objetivos estratégicos, projetos ou processos que terão os desempenhos acompanhados através de indicadores.

Em seguida, deve-se avaliar "O que medir?"(ex.: qualidade, produtividade, prazos, custo, satisfação) e "Por que medir? (qual decisão será apoiada?).

Por fim, é necessário definir, de forma clara, o nome do indicador e a respectiva descrição, a unidade de medida, a polaridade, a frequência de apuração, o setor responsável, a fórmula de cálculo, a fonte de dados e o mecanismo de apuração.

Um exemplo de indicador de desempenho conhecido de todas as Unidades de Controle Interno é o Indicador de Adequação ao Sistema de Controle Interno - IAS. A seguir, apresenta-se informações básicas de estruturação do referido indicador:

Tabela 2: Modelo de ficha de indicador

Nome do indicador:	Indicador de Adequação ao Sistema de Controle Interno - IAS
Descrição:	Mensurar o grau de adequação das Unidades de Controle Interno ao Decreto Estadual nº 47.087/19, à Portaria SCGE nº 24/2025 e às orientações técnicas repassadas pela SCGE, a partir de pontos de controle estabelecidos por esta Secretaria
Unidade de medida:	%
Polaridade:	Maior melhor
Frequência de apuração:	Quadrimestral
Setor responsável:	Diretoria de Governança e Risco (DIGR)/ Coordenadoria de Governança (CGO)
Fórmula de cálculo:	A fórmula de apuração do IAS está normatizada no § 6º, Art. 2º da Portaria SCGE nº 24/2025 § 6º O Indicador de Adequação ao Sistema de Controle Interno - IAS será obtido da divisão entre a pontuação atingida e a pontuação total possível de ser alcançada, descontados os pontos não aplicáveis, conforme demonstrado na fórmula a seguir: IAS = (Pontuação Atingida) ÷ (Pontuação Total - Pontuação N/A).
Fonte de dados:	Planilha de apuração do IAS.
Mecanismo de apuração:	O mecanismo de apuração do IAS está regulamentado na Portaria SCGE º 24/2025 que estabelece as diretrizes a serem seguidas, no âmbito do Poder Executivo Estadual, para apuração do Indicador de Adequação ao Sistema de Controle Interno pela Secretaria da Controladoria-Geral do Estado - SCGE.

Fonte: Elaboração própria

Para aprofundamento dos conhecimentos nesta temática, recomenda-se a capacitação "Elaboração de Indicadores de Desempenho Institucional" (https://www.escolavirtual.gov.br/curso/604), oferecida pela Escola Nacional de Administração Pública - ENAP.

- **Requisito de maturidade 05:** Os dados do gerenciamento de riscos são processados através de **sistema informatizado** que permite uma visão abrangente dos riscos da organização e a manutenção do histórico das análises realizadas.

◆ **Referência:** A Alta Direção é responsabilizada por gerenciar riscos, enquanto os órgãos de supervisão são responsabilizados por supervisionar a gestão de riscos. Com frequência, é requerido ou esperado que os órgãos de supervisão: — assegurem que os riscos sejam adequadamente considerados no estabelecimento dos objetivos da organização; — compreendam os riscos aos quais a organização está exposta na busca de seus objetivos; — **assegurem que sistemas para gerenciar estes riscos estejam implementados e operem eficazmente**; — assegurem que estes riscos sejam apropriados no contexto dos objetivos da organização; — assegurem que a informação sobre estes riscos e sua gestão seja apropriadamente comunicada.(ISO 31000:2018, seção 5.2)

◆ **Prescrição:** O uso de sistemas de informação, apesar de não ser condição necessária para a realização da gestão de riscos, é altamente recomendável. O uso do sistema facilita a identificação, análise, tratamento e monitoramento dos riscos, tornando o processo mais eficiente e eficaz, além de facilitar o fluxo de informações para a tomada de decisão. Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Utilizar Sistema de Gestão de Riscos que permita uma visão abrangente dos riscos da organização e a manutenção do histórico das análises realizadas.

Obs.: O órgão/entidade poderá adotar o Sistema de Gestão de Riscos disponibilizado pela SCGE ou utilizar sistema próprio.

◆ **Evidências:** Registros de uso do sistema, manuais do sistema, relatórios extraídos.

Saiba Mais!

Ainda que seja altamente recomendável o uso de um sistema para gestão de riscos, é possível realizar o gerenciamento de riscos sem contratar um sistema. Seguem algumas dicas para auxiliar neste desafio:

- **Centralizar os registros**
  - Crie uma planilha única (Excel ou Google Sheets) para consolidar todos os riscos da organização.
  - Estruture campos como: descrição do risco, causa, efeito, controles existentes, responsável, nível de risco, status, data da última análise. Para este tópico, recomenda-se utilizar a planilha modelo disponibilizada pela SCGE.

- **Garantir o histórico**
  - Mantenha uma aba para cada ciclo de avaliação (ex.: 2023, 2024, 2025) ou crie colunas de versão/atualização.
  - Nunca sobrescreva dados antigos: registre as análises em novas linhas, garantindo o histórico.
- **Automatizar o acompanhamento**
  - Use recursos simples como filtros, tabelas dinâmicas ou gráficos para gerar visões consolidadas.
  - Isso permitirá enxergar riscos por área, categoria ou nível de criticidade.
- **Controlar acessos e versões**
  - Armazene a planilha em local corporativo (intranet, drive institucional, etc.) com controle de acesso.
  - Se possível, use ferramentas online para evitar múltiplas versões circulando por e-mail.
- **Integrar com indicadores estratégicos**
  - Relacione cada risco a um objetivo estratégico/metas.
  - Dessa forma, o relatório consolidado de riscos já mostrará seu impacto sobre a estratégia.
- **Formalizar o processo**
  - Elabore um procedimento interno (manual ou instrução) descrevendo como a planilha será atualizada, por quem e com qual periodicidade.
  - Isso dá legitimidade ao método e demonstra conformidade com o requisito.

É importante garantir três pontos-chave:

1. Visão abrangente de todos os riscos (planilha consolidada).
2. Histórico mantido das análises realizadas (não sobrescrever dados).
3. Uso efetivo das informações pela gestão (relatórios apresentados à alta direção).

Ressalta-se, entretanto, que o requisito só será atendido se o órgão/entidade utilizar um sistema informatizado para o gerenciamento de riscos.

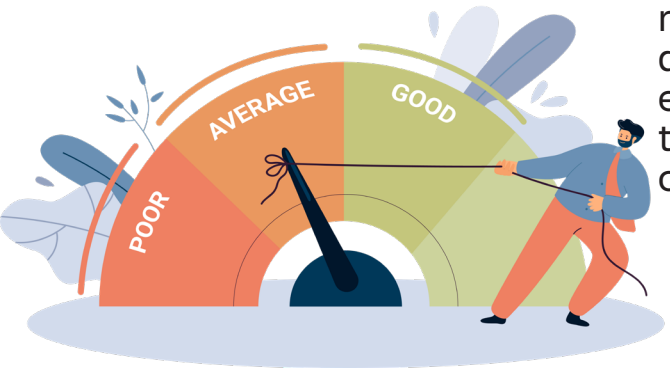
• **Requisito de maturidade 06:** O órgão/entidade dispõe de uma política de gestão de riscos aprovada pela alta administração, comunicada e disponível às partes interessadas.

- **Referência:** Estabelecer uma estrutura de gestão de riscos, bem como monitorá-la e avaliá-la, são boas práticas que contribuem para a eficácia e melhoria do desempenho organizacional. Para que esse fim seja alcançado, recomenda-se: definir papéis e responsabilidades relacionados à gestão de riscos; definir estratégia e diretrizes para gestão de riscos; definir critérios de classificação de risco e grau de tolerância a risco; definir e implantar política de gestão de riscos; definir e implantar processo de gestão de riscos; identificar, avaliar, analisar, tratar e monitorar riscos críticos; identificar e implantar controles internos para tratar riscos críticos; definir e implantar plano de continuidade; monitorar e avaliar a estrutura de gestão de riscos; bem como, aprimorar continuamente a estrutura de gestão de riscos. (Referencial Básico de Gestão de Riscos. TCU, 2018).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Elaborar e aprovar formalmente uma Política de Gestão de Riscos (PGR), com a participação da alta administração e do(s) comitê(s) de governança, se houver.
  b. Realizar ações de divulgação da Política de Gestão de Riscos de forma ampla, clara e acessível às partes interessadas
  c. Disponibilizar a Política de Gestão de Riscos no sítio eletrônico do órgão/entidade.
- **Evidências:** Documento oficial da Política de Gestão de Riscos, com assinatura ou aprovação formal da alta administração e publicação em meio oficial (site institucional, boletim interno, intranet), comunicados internos ou externos anunciando a política e incentivando sua aplicação, material de capacitação ou sensibilização que contenham ou citem a política, etc.

Saiba Mais!

Inicialmente, é importante estabelecer o contexto, definindo claramente os objetivos da política de gestão de riscos e o escopo de sua aplicação dentro da organização, bem como identificar as partes interessadas e suas responsabilidades no processo de gestão de riscos .

A política deve contemplar também como será a operacionalização do gerenciamento de riscos, incluindo a avaliação dos riscos através das análises qualitativas e quantitativas e o tratamento do risco, contendo as estratégias de resposta aos riscos e os planos de ação.



Assim como o planejamento, a gestão de riscos também não é estática; por isso, é necessário um plano de monitoramento e melhoria contínua, cuja existência deve estar prevista na Política de Gestão de Riscos.

Por fim, para garantir que as partes interessadas no processo de gestão de riscos tenham informações e possam supervisionar e tomar as decisões de forma eficiente é importante que haja um plano de comunicação que também deve deve ser delineado na política.

Apenas em caráter exemplificativo, pode ser consultada a Política de Gestão de Riscos da SCGE, disponível em seu sítio eletrônico.

3.3 Agrupamento: Conhecimento e Cultura

Conhecimento e cultura organizacional abordam as pessoas como elemento central no aprimoramento da gestão de riscos e dos controles internos. Este grupo enfatiza o nível de conhecimento e a consciência dos gestores quanto às suas responsabilidades na identificação e gestão de riscos, a existência de documentos e manuais relacionados ao tema, além da qualificação dos membros da Unidade de Controle Interno.

• **Requisito de maturidade 07:** Os gestores da **primeira linha** têm consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes.

- **Referência:** Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização, e convém que enfatizem que a gestão de riscos é uma responsabilidade principal; identifiquem indivíduos que possuam responsabilização e tenham autoridade para gerenciar riscos (proprietários dos riscos). (ISO 31000:2018, seção 5.4.3)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Os gestores da primeira linha devem realizar o gerenciamento dos riscos e manter o plano de tratamento monitorado
  b. Atribuir formalmente a responsabilidade pela gestão de riscos aos gestores da primeira linha (gestores operacionais), incluindo isso em normativos, manuais ou matrizes de responsabilidade.
  c. Capacitar e sensibilizar os gestores sobre sua responsabilidade pela identificação, avaliação, tratamento e monitoramento dos riscos relacionados às suas áreas
  d. Assegurar que esses gestores compreendam e operem os controles internos, mantendo-os eficazes e atualizados.
  e. Estabelecer rotinas de reporte e monitoramento que envolvam a primeira linha de forma ativa no processo de gestão de riscos.
- **Evidências:** Manuais ou políticas internas que definem as responsabilidades da primeira linha na gestão de riscos, atas de reuniões ou comunicados internos evidenciando a orientação sobre a responsabilidade da primeira linha, mapa de riscos assinado pelo gestor do processo (primeira linha), planos de ação ou controles internos implementados e acompanhados pelos gestores responsáveis, etc

Saiba Mais!

É necessário que os gestores tenham ciência dos seus papéis e responsabilidades na gestão de riscos. Dessa forma, recomenda-se que sejam realizadas ações de conscientização e treinamento, bem como facilitação do processo de gerenciamento de riscos. A seguir, serão demonstradas as responsabilidades relacionadas aos gestores da primeira linha:

Compromissos dos Gestores:

1. **Identificação de Riscos:**
   - Reconhecer e documentar os riscos potenciais relacionados às suas áreas de responsabilidade.
   - Utilizar técnicas adequadas para a identificação de riscos, tais como brainstorming, análise SWOT e consulta a partes interessadas.
2. **Avaliação de Riscos:**
   - Avaliar a probabilidade e o impacto dos riscos identificados.
   - Priorizar os riscos com base na sua criticidade e potencial de afetar os objetivos estratégicos.
3. **Mitigação de Riscos:**
   - Desenvolver e implementar planos de ação para mitigar os riscos prioritários.
   - Alocar recursos adequados para a implementação das medidas de mitigação.
4. **Monitoramento de Riscos:**
   - Monitorar continuamente os riscos e a eficácia das ações de mitigação.
   - Atualizar periodicamente a avaliação dos riscos com base em novas informações e mudanças no ambiente interno e externo.
5. **Comunicação de Riscos:**
   - Reportar regularmente o status dos riscos e das ações de mitigação à alta administração.
   - Garantir a transparência e a clareza na comunicação sobre riscos com todos as partes interessadas relevantes.
6. **Conformidade e Melhoria Contínua:**
   - Assegurar a conformidade com políticas internas, regulamentações e normas aplicáveis à gestão de riscos.
   - Promover uma cultura de melhoria contínua na gestão de riscos, buscando sempre aprimorar processos e práticas.

• **Requisito de maturidade 08:** O órgão/entidade dispõe de **um manual de gestão de riscos, ou documento similar**, aprovado pela alta administração, disponível e comunicado às partes interessadas.

- **Referência:** A estrutura de gestão de riscos é a maneira como a entidade se organiza para gerenciar os riscos do seu 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 através de toda a organização. Inclui a política de gestão de riscos, os manuais e guias, os recursos, a definição de objetivos e de papéis e responsabilidades que permitirão incorporar a gestão de riscos em todos os níveis da organização (Referencial Básico de Gestão de Riscos do TCU, 2018).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Elaborar um manual, ou documento similar, que descreva de forma clara os conceitos, princípios e diretrizes da gestão de riscos adotados pela organização; as etapas do processo de gestão de riscos: contexto, identificação, análise, avaliação, tratamento, monitoramento e comunicação; os papéis e responsabilidades dos envolvidos, entre outros.
  b. Aprovar o documento pela alta administração;
  c. Disponibilizar o documento no sítio eletrônico do órgão/entidade;
  d. Dar ampla divulgação do documento aos servidores do órgão/entidade, promovendo ações de sensibilização, com o objetivo de garantir o conhecimento e a correta aplicação das diretrizes pelos envolvidos.
- **Evidências:** Manual de Gestão de Riscos, ou documento similar, com assinatura ou aprovação formal da alta administração, publicação em meio oficial (site institucional, boletim interno, intranet), comunicados institucionais informando e divulgando o documento, registros de treinamentos, oficinas ou eventos de disseminação do conteúdo do manual, etc.

Saiba Mais!

A elaboração de um manual de gestão de riscos possibilita a disseminação dos conceitos de gestão de riscos que precisam ser internalizados pelos gestores. Ter um guia levando em consideração a realidade de cada unidade gestora fortalece o conhecimento do órgão na temática e permite maior autonomia e capacitação aos servidores, sendo uma fonte de consulta permanente.

Esse documento integra o conjunto de instrumentos necessários para a implementação e operacionalização da gestão de riscos.

Figura 4: Guia prático de gerenciamento de riscos da SCG

Fonte: Elaboração própria

Cabe destacar que o manual, ou documento similar, deve ser elaborado a partir da política de gestão de riscos dos órgãos, sendo instrumentos correlatos, representando uma ferramenta para sua implementação. Outros requisitos, listados neste Guia, podem ser formalizados no Manual de GR, tais como definição de instâncias e responsabilidades, atuação das Unidades de Controle Interno, por exemplo.

Vide modelos de manual de gestão de riscos nos sítios eletrônicos a seguir:

https://www.scge.pe.gov.br/wp-content/uploads/2022/03/Guia-Pratico-de-Gerenciamento-de-Riscos-1.pdf

https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/

https://www.gov.br/ans/pt-br/arquivos/acesso-a-informacao/transparencia-institucional/gestao-de-riscos/manual-de-gestao-de-riscos-da-ans.pdf

• **Requisito de maturidade 09:** Os membros da Unidade de Controle Interno (Segunda Linha) possuem conhecimento suficiente para conduzir e orientar a gestão de riscos em seu órgão/entidade.

- **Referência:** A responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da primeira e segunda linhas. Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. Os papéis de segunda linha fornecem assistência no gerenciamento de riscos.

  Os papéis de primeira e segunda linha podem ser combinados ou separados. Alguns papéis de segunda linha podem ser atribuídos a especialistas, para fornecer conhecimentos complementares, apoio, monitoramento e questionamento àqueles com papéis de primeira linha. Os papéis de segunda linha podem se concentrar em objetivos específicos do gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade. Como alternativa, os papéis de segunda linha podem abranger uma responsabilidade mais ampla pelo gerenciamento de riscos, como o gerenciamento de riscos corporativos (enterprise risk management – ERM). No entanto, a responsabilidade pelo gerenciamento de riscos segue fazendo parte dos papéis de primeira linha e dentro do escopo da gestão
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

  a. Assegurar que os membros da Unidade de Controle Interno possuam conhecimento técnico e capacitação específica em Gestão de Riscos (normas ISO, COSO, metodologia institucional) e Controles internos;

  b. Assegurar que a unidade esteja preparada para orientar metodologicamente as áreas operacionais na aplicação dos processos de gestão de riscos e apoiar na elaboração e revisão de documentos normativos relacionados a riscos (política, manual, matrizes).Disponibilizar o documento no sítio eletrônico do órgão/entidade;

- **Evidências:** Certificados de participação em cursos, seminários ou eventos sobre gestão de riscos, plano de capacitação institucional que contemple a segunda linha, registros de reuniões ou notas técnicas da unidade orientando a primeira linha na gestão de riscos, procedimentos internos que descrevam as atribuições da unidade em relação ao apoio à gestão de riscos, etc.

Saiba Mais!

A SCGE disponibiliza, periodicamente, cursos de capacitação em gestão de riscos através da Escola de Controle Interno Prof. Francisco Ribeiro (ECI/SCGE). As capacitações são oferecidas em diferentes formatos, incluindo turmas presenciais e cursos a distância (EAD) ao vivo. Além disso, os órgãos e entidades da administração pública estadual podem solicitar a realização de turmas fechadas voltadas especificamente para as suas unidades gestoras.

Adicionalmente, é possível buscar em outras instituições, como a Escola Nacional de Administração Pública (ENAP), Escolas de Governo dos Tribunais de Contas, Instituto Serzedello Corrêa do Tribunal de Contas da União, etc., cursos na temática de gestão de riscos.

3.4 Agrupamento: Processo

O processo refere-se às etapas do gerenciamento de riscos. E para que elas funcionem corretamente, é importante a participação dos principais atores da primeira e da segunda linha nesse processo, resultando numa lista de riscos e controles relevantes, evidenciados com os principais documentos que dão suporte às análises e definições.

- **Requisito de maturidade 10:** O gerenciamento dos riscos é realizado por pessoas designadas que têm responsabilidade, autoridade e experiência nas atividades objeto de análise.

- **Referência:** Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, assegurem que as autoridades, responsabilidades e responsabilizações para os papéis pertinentes à gestão de riscos sejam atribuídas e comunicadas a todos os níveis da organização, e convém que: — enfatizem que a gestão de riscos é uma responsabilidade principal; — identifiquem indivíduos que possuam responsabilização e tenham autoridade para gerenciar riscos (proprietários dos riscos). (ISO 31000:2018, seção 5.4.3)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Definir responsabilidades, autoridades e experiências necessárias para gerenciar os riscos e registrar nos documentos organizacionais, como políticas, manuais ou descrições de cargos;
  b. Assegurar que a responsabilidade pela gestão de riscos esteja incorporada às atribuições funcionais dos gestores e servidores, especialmente em cargos de direção e coordenação.
- **Evidências:** Documentos organizacionais, como políticas, manuais ou descrições de cargos, que identifique claramente quem são os responsáveis pela gestão de riscos. Esses documentos devem conter as responsabilidades, autoridades e experiências necessárias para gerenciar os riscos; Documentos que comprovem que os responsáveis pela gestão de riscos estão efetivamente envolvidos nas atividades relacionadas.

Saiba Mais!

Inicialmente, é necessário checar se há responsáveis pelo gerenciamento de riscos e se os papéis exercidos estão em conformidade com o Modelo das Três Linhas. Nos casos em que há pessoas designadas, verificar se há formalização da responsabilidade e autoridade claramente definidas em documentos oficiais, como portarias,

organograma, políticas e procedimentos e manuais, por exemplo. Esses documentos devem ser acessíveis e de conhecimento de todos os envolvidos no processo.

Em um segundo momento, é preciso verificar as competências e experiências dos profissionais. É importante que os gestores de riscos sejam capacitados, uma vez que é uma temática sensível e não deve ser designada para qualquer pessoa.

Por fim, é importante também verificar se os gestores de riscos participam ativamente do processo de gerenciamento de riscos (identificação, análise, avaliação e tratamento) e se possuem autonomia para tomar decisões e implementar ações corretivas quando necessário. Essas análises podem ser realizadas através de relatórios de identificação de riscos, planos de tratamento e registros de incidentes. É importante destacar que esses documentos devem ser revisados periodicamente e precisam refletir a realidade de riscos do momento.

• **Requisito de maturidade 11:** A Unidade de Controle Interno (Segunda Linha) apoia o processo de gerenciamento de riscos, fornecendo metodologias e ferramentas às áreas, com a finalidade de identificar e avaliar riscos.

- **Referência:** Funções que supervisionam riscos: a segunda linha de defesa é constituída por funções – unidades, comitês ou outras estruturas organizacionais – estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão 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, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional, apoiar a definição de metas de exposição a risco, monitorar riscos específicos (de compliance, por exemplo), bem como ajudar a definir controles e/ ou monitorar riscos e controles da primeira linha de defesa. (Referencial Básico de Gestão de Riscos do TCU, 2018)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Fornecer metodologia, formulários, orientações técnicas e ferramentas para aplicação do processo de gestão de riscos (ex.: manuais, cartilhas, planilhas);
  b. Atuar como facilitadora nos processos de gerenciamento de riscos, apontando melhorias ou inconsistências, não substituindo a primeira linha, mas atuando como suporte e referência técnica;
  c. Ministrar treinamentos sobre as metodologias e ferramentas de gerenciamento de riscos para garantir que todos compreendam e saibam usar essas ferramentas adequadamente.
- **Evidências:** Documentos que descrevem as metodologias; Ferramentas e orientações técnicas disponibilizadas pela segunda linha para gerenciamento de risco, devendo esses materiais ser comunicados amplamente para todas as áreas da organização; Registro das facilitações realizadas; Comprovação da promoção de treinamentos e programas de capacitação sobre as metodologias e ferramentas de gerenciamento de riscos ministrados pela UCI, incluindo workshops, seminários ou cursos para garantir que todos compreendam e saibam usar essas ferramentas adequadamente.

Saiba Mais!

Um dos grandes desafios enfrentados pela segunda linha é saber de que forma pode se dar a sua atuação como facilitadora do processo de gerenciamento de riscos. Aqui estão algumas formas pelas quais a segunda linha pode desempenhar seus trabalhos:

- Desenvolvimento de Manuais, Políticas e Procedimentos com o objetivo de assegurar que todos na organização compreendam como gerenciar riscos de forma eficaz.
- Treinamento e Capacitação - Atuar como multiplicador de conhecimento, organizando e conduzindo programas de treinamentos contínuos, facilitando workshops e seminários.
- Monitoramento e Relatórios - Realizar monitoramento contínuo dos riscos e controles e preparar relatórios regulares sobre o gerenciamento de riscos e as ações de mitigação para que a alta gestão tenha ciência do andamento das ações.
- Suporte e Orientação - Fornecer orientação sobre a aplicação de políticas de risco e ajudando na identificação e avaliação de riscos.
- Avaliação e melhoria contínua - Conduzir revisões periódicas dos processos de gerenciamento de riscos para identificar áreas de melhoria e assegurar que as práticas estejam alinhadas com os objetivos estratégicos da organização. Além de propor e implementar melhorias nos processos de gerenciamento de riscos com base nas lições aprendidas e nas mudanças no ambiente de risco.
- Integração e Coordenação - Assegurar que as atividades de gerenciamento de riscos estejam integradas com outras funções de controle interno, promovendo uma abordagem coesa e coordenada.

• **Requisito de maturidade 12:** O processo de gerenciamento de riscos produz uma lista de riscos RELEVANTES e controles APROPRIADOS, através da utilização de metodologia consolidada, como às do COSO ou ISO.

- **Referência:** A identificação de riscos é o processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e apoiando-se na comunicação e consulta com as partes interessadas internas e externas (ABNT, 2009). O objetivo é produzir uma lista abrangente de riscos, incluindo fontes e eventos de risco que possam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto (Referencial Básico de Gestão de Riscos. TCU, 2018).

  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. (Referencial Básico de Gestão de Riscos. TCU, 2018).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

  a. Aplicar a metodologia de gerenciamento de riscos, assegurando que: os riscos identificados sejam relevantes e significativos, considerando o contexto, os objetivos e o ambiente da organização; que sejam descritos os controles internos já existentes (controles preventivos ou corretivos); e, quando identificadas lacunas ou fragilidades, devem ser propostos novos controles ou melhorias nos já existentes, de modo a fortalecer a capacidade da organização de prevenir, detectar ou responder aos eventos de risco, garantindo maior robustez e efetividade do processo de gestão.
- **Evidências:** Mapas de riscos elaborados a partir da metodologia oficial do órgão/entidade; Planilhas de riscos, contendo todos os campos exigidos pela metodologia (risco, causas, consequências, análise, avaliação, controles); Documentação gerada através de sistemas informatizados utilizados para o registro e acompanhamento dos riscos (se houver).

Saiba Mais!

A SCGE disponibiliza em seu sítio eletrônico um modelo de planilha para realização do gerenciamento de riscos, conforme metodologia estabelecida pela SCGE e registrada em seu Guia Prático de Gerenciamento de Riscos. Os documentos estão disponíveis no campo Documentos de Orienta-

ção no link https://www.scge.pe.gov.br/gestao-de-riscos/.

A unidade gestora define quais os processos estratégicos e inicia a identificação dos riscos, buscando as causas e consequências, bem como as medidas que podem ser adotadas para mitigar os riscos e as medidas que podem ser adotadas caso o risco se materialize.

O gerenciamento de riscos será materializado no documento mapa de riscos, conforme modelo a seguir, também disponível no sítio eletrônico da SCGE:

Figura 5: Modelo de mapa de riscos da SCGE

MAPA DE RISCOS									
Nº	ETAPA		RISCO			NÍVEL DE RISCO	MEDIDAS DE TRATAMENTO		RESPONSÁVEL
	SUBPROCESSO	ATIVIDADE	CAUSAS	EVENTO	CONSEQUÊNCIAS		MEDIDAS PREVENTIVAS	MEDIDAS CORRETIVAS	

Fonte: Elaboração própria

• **Requisito de maturidade 13:** O órgão/entidade realiza o **registro sistemático das evidências** que suportam a identificação, análise e avaliação dos riscos, a proposição de controles e a avaliação da eficácia desses controles.

◆ **Referência:** Convém que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. O registro e o relato visam: — comunicar atividades e resultados de gestão de riscos em toda a organização; — fornecer informações para a tomada de decisão; — melhorar as atividades de gestão de riscos; — auxiliar a interação com as partes interessadas, incluindo aquelas com responsabilidade e com responsabilização por atividades de gestão de riscos. (ISO 31000:2018, seção 6.7)

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Inserir na Política de Gestão de Riscos e/ou Manual de Gestão de Riscos a obrigatoriedade de registro das evidências que sustentam cada etapa do processo;

b. Manter registros formais e sistemáticos de todas as etapas do processo de gestão de riscos, assegurando a confiabilidade e rastreabilidade das informações

c. Manter registros formais e sistemáticos das evidências, incluindo:

- Documentos que comprovam a existência de controles: normativos, fluxogramas de processos, relatórios de sistema, prints de telas, registros contábeis/financeiros, checklists de execução, relatórios de auditoria, notas técnicas, etc.
- Documentos que embasam a análise do risco: relatórios de falhas anteriores, ocorrências registradas, estatísticas, indicadores, ofícios recebidos, pareceres técnicos.
- Documentos que demonstram a eficácia dos controles: resultados de testes de controles, evidências de monitoramento, relatórios de conformidade, atas de reuniões em que problemas/controles foram discutidos.

d. Garantir que esses registros sejam:

- Organizados de forma padronizada (ex.: planilhas, sistemas, formulários);
- Acessíveis às partes interessadas;
- Atualizados periodicamente, refletindo a situação real dos riscos e controles.

◆ **Evidências:** Documentação formal que define metodologia, responsabilidades e exigência de registro das evidências, Atas de comitês ou grupos que discutem riscos e decisões fundamentadas, documentação que registra o gerenciamento de riscos, evidências da implementação dos controles, evidências de atualizações periódicas das informações (datas de revisão, histórico de alterações, versões anteriores).

Saiba Mais!

Para atender a essa prática de maturidade, o órgão/entidade deve iniciar pela organização e padronização do registro das informações relacionadas à gestão de riscos. Isso significa estruturar um processo que permita documentar, de forma clara e consistente, todas as etapas da identificação, análise, avaliação e tratamento dos riscos.

Um bom ponto de partida é:

1. **Estabelecer um fluxo de trabalho claro:**

   Defina quem são os responsáveis por preencher, revisar e validar os registros. Isso pode incluir gestores das áreas (primeira linha) e a unidade de controle interno (segunda linha) como apoio metodológico.

2. **Capacitar os envolvidos:**

   Promova orientação ou capacitação básica para as equipes sobre como preencher corretamente os registros de riscos, reforçando a importância da qualidade das informações.

3. **Documentar também as revisões e atualizações:**

   Além de registrar os riscos e controles, mantenha histórico das revisões, com datas, responsáveis e as principais alterações realizadas.

4. **Dar atenção especial à avaliação dos controles existentes:**

   Inclua no processo o hábito de avaliar se os controles internos já existentes são realmente eficazes para reduzir a probabilidade ou o impacto dos riscos.

- **Requisito de maturidade 14:** O tratamento dos riscos é registrado em **plano de ação e comunicado formalmente** aos responsáveis pela sua implementação, assegurando que compreendam, assumam compromissos e sejam responsáveis por essas ações.

- **Referência:** O propósito dos planos de tratamento de riscos é especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado. Convém que o plano de tratamento identifique claramente a ordem em que o tratamento de riscos será implementado. (ISO 31000:2018, seção 6.5.3)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Elaborar plano de tratamento com a ciência/assinatura dos responsáveis pela implementação da resposta ao risco.
- **Evidências:** Planos de tratamento com a devida assinatura dos responsáveis pela implementação da resposta ao risco.

Saiba Mais!

Para iniciar, é preciso definir um modelo padrão de plano de ação vinculado ao mapa de riscos e incluir o plano de ação como etapa obrigatória da metodologia de gestão de riscos, sempre que o risco for classificado no nível acima do apetite de riscos do órgão/entidade.

A SCGE disponibiliza em seu sítio eletrônico um modelo de planilha para realização do gerenciamento dos riscos, que contém o plano de tratamento. Os documentos estão disponíveis no campo Documentos de Orientação no link https://www.scge.pe.gov.br/gestao-de-riscos/.

Importante destacar que, muitas vezes, os participantes da elaboração do plano de tratamento são representantes de um determinado setor, mas não é necessariamente a pessoa que será responsável pela ação de tratamento. Neste sentido, é essencial que as pessoas que estejam citadas como responsáveis pelas ações do plano conheçam o que é necessário ser realizado e qual o prazo acordado.

O plano de tratamento deverá conter a descrição da ação corretiva, preventiva ou de mitigação a ser executada, o prazo inicial e final para implementação, o responsável pela implementação (pessoa e setor) e o status das ações.

3.5 Agrupamento: Resultado

Este grupo avalia se a gestão de riscos gera resultados tangíveis. Em um primeiro momento, a avaliação se concentra no nível de implementação dos controles propostos. Em um segundo, o foco recai sobre o impacto desses controles no atingimento dos objetivos organizacionais.

- **Requisito de maturidade 15:** As **respostas aos riscos** identificados (controles) são implementadas.

- **Referência:** Para todos os riscos identificados, a administração seleciona e implementa uma resposta ao risco. A administração considera a severidade e a priorização do risco, bem como o contexto de negócios e os respectivos objetivos de negócio. Em última análise, a resposta ao risco também é responsável pelas metas de performance da organização. (COSO ERM 2017, Princípio 13: Implementa respostas aos riscos)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Definir e aprovar planos de tratamento de risco, com responsáveis, prazos e recursos;
  b. Executar os controles previstos (ações de mitigação, planos de contingência, etc.);
  c. Acompanhar a implementação dos controles, com evidências de execução;
  d. Atualizar o mapa de riscos com o status das respostas;
  e. Avaliar se os controles são eficazes, revisando-os quando necessário.
- **Evidências:** Plano de tratamento (documento com estratégias de resposta, responsáveis, prazos e recursos), registros de execução dos controles (relatórios, atas, checklists, evidências de implantação - ex: instalação de software, treinamento realizado, normas revisadas).

Saiba Mais!

O primeiro passo para atender a este requisito é formalizar os planos de tratamento por meio de um sistema ou planilha. Para cada risco, devem ser definidos a estratégia de resposta, as ações a serem executadas, os responsáveis, os prazos e os recursos necessários. Em seguida, é preciso atribuir responsabilidades, envolvendo as áreas gestoras dos riscos e formalizando os responsáveis por cada ação.

Após essa etapa, os controles devem ser implementados mediante a execução das ações planejadas, como revisão de normas, realização de treinamentos, mudanças de processos ou aquisição de tecnologias. Em cada fase, é fundamental registrar e arquivar as evidências, mantendo a documentação das ações executadas com datas e validações adequadas. Por fim, deve-se estabelecer rotinas de monitoramento e revisão dos planos de tratamento, garantindo também o devido registro dessa etapa.

- **Requisito de maturidade 16:** A gestão de riscos no órgão/entidade está contribuindo para o alcance dos seus principais objetivos.

◆ **Referência:** O gerenciamento de riscos corporativos destaca a escolha da estratégia. A definição de uma estratégia demanda um processo decisório estruturado que analise os riscos e alinhe os recursos com a missão e a visão da organização (COSO ERM 2017, O papel do risco na definição da estratégia).

- O propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos (ISO 31000:2018, seção 4)

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Realizar monitoramento de métricas de desempenho que demonstrem o impacto das medidas de tratamento no alcance dos objetivos;

b. Elaborar relatórios de progresso que demonstrem como a gestão de riscos agrega valor à estratégia institucional e aos resultados de desempenho, utilizando indicadores que evidenciem seu impacto. Acompanhar a implementação dos controles, com evidências de execução;

◆ **Evidências:** Documento de monitoramento das métricas de desempenho antes e depois da implementação das estratégias de gerenciamento de riscos, incluindo o registro das ações que impactaram positivamente a realização dos objetivos estratégicos; Relatório de progresso que evidencie não apenas os riscos identificados, mas também a forma como as estratégias de mitigação têm contribuído para o avanço em direção aos objetivos estratégicos.

Saiba Mais!

O objetivo da gestão de riscos é identificar, avaliar, monitorar e mitigar os riscos que podem afetar uma organização, para assegurar a realização dos seus objetivos. Dessa forma, não adianta implementar a metodologia de gestão de riscos apenas para cumprir obrigações, é necessário acompanhar os atingimentos dos objetivos, através do monitoramento de indicadores, da análise das ações que impactaram positivamente à consecução das metas, e da análise dos incidentes ocorridos que foram minimizados pelos controles implementados.

3.6 Agrupamento: Monitoramento

Este grupo contempla (i) as práticas de revisão periódica dos riscos identificados, das respectivas avaliações e das respostas aos riscos (controles), (ii) da análise da existência de novos riscos, (iii) o estabelecimento de indicadores que permitam avaliar a efetividade dessas respostas, (iv) a atuação da Unidade de Controle Interno (UCI) como facilitadora e supervisora no processo de monitoramento e a (v) existência de mecanismos para avaliação e registro dos problemas ocorridos.

• **Requisito de maturidade 17:** Existe monitoramento e revisão periódica dos riscos e das respectivas respostas (controles), visando avaliar se permanecem adequadas.

◆ **Referência:** Ainda que cuidadosamente concebido e implementado, o tratamento de riscos pode não produzir os resultados esperados e pode produzir consequências não pretendidas. Monitoramento e análise crítica precisam ser parte integrante da implementação do tratamento de riscos, para assegurar que as diferentes formas de tratamento se tornam e permanecem eficazes. O tratamento de riscos também pode introduzir novos riscos que precisam ser gerenciados. Se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, convém que este seja registrado e mantido sob análise crítica contínua. Convém que os tomadores de decisão e outras partes interessadas estejam conscientes da natureza e extensão do risco remanescente após o tratamento de riscos. Convém que o risco remanescente seja documentado e submetido a monitoramento, análise crítica e, onde apropriado, tratamento adicional. (ISO 31000:2018, seção 6.5.2)

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Estabelecer processo contínuo de monitoramento dos riscos, controles e planos de tratamento, garantindo o acompanhamento da implementação das ações definidas para mitigação dos riscos;

b. Acompanhar a execução dos planos de ação vinculados aos riscos, avaliando: se as ações estão sendo implementadas nos prazos acordados; se os responsáveis designados estão atuando conforme o previsto; se os resultados obtidos são eficazes para reduzir a probabilidade ou impacto dos riscos.

c. Realizar revisões periódicas dos controles existentes vinculados aos riscos mapeados, com o objetivo de verificar: se os controles ainda estão sendo aplicados corretamente, se continuam sendo eficazes para mitigar o risco, se são suficientes diante de mudanças no processo ou no ambiente

d. Estabelecer uma frequência mínima para essa revisão (ex.: semestral ou anual), conforme o perfil do risco e a criticidade do processo, assegurando a rastreabilidade das revisões;

e. Formalizar e comunicar os resultados do monitoramento, registrando: situação atual das ações do plano de tratamento (em andamento, concluídas, atrasadas, canceladas); ajustes necessários em prazos, responsáveis ou medidas de tratamento; evolução da exposição ao risco em função das ações implementadas

f. Formalizar os resultados da revisão, registrando: controles mantidos, controles que precisam ser ajustados ou substituídos, novos controles recomendados

- **Evidências:** (i) Relatórios de acompanhamento dos planos de tratamento, contendo status (concluído, em andamento, atrasado), prazos e responsáveis; ii) Painéis ou dashboards de acompanhamento, mostrando a execução dos planos de tratamento, indicadores de progresso e níveis de risco residual; iii) Relatórios ou formulários de revisão dos riscos e controles internos, indicando data, responsável e conclusão da análise; iv) Registros de atualizações nos mapas de riscos e controles, com histórico de alterações; v) vi) Atas de reuniões de monitoramento de riscos, com registro das decisões sobre atualização ou revisão de controles.

Saiba Mais!

É importante sempre lembrar que o gerenciamento de riscos não deve se restringir à elaboração de um documento, sendo algo que necessita ser constantemente monitorado e atualizado para que venha trazer os benefícios esperados.

Assim sendo, é necessário estabelecer uma periodicidade de acompanhamento dos riscos e da eficácia das ações de mitigação, bem como atualizar a avaliação dos riscos com base em novas informações e mudanças no ambiente interno e externo. Cada unidade gestora deve se organizar de acordo com as peculiaridades de sua organização.

- **Requisito de maturidade 18:** São estabelecidos **indicadores** que permitam monitorar os riscos e avaliar a efetividade das respostas aos riscos (controles).

◆ **Referência:** Para avaliar a eficácia da estrutura de gestão de riscos, convém que a organização: — mensure periodicamente o desempenho da estrutura de gestão de riscos em relação ao seu propósito, planos de implementação, indicadores e comportamento esperado; — determine se permanece adequada para apoiar o alcance dos objetivos da organização. (ISO 31000:2018, seção 5.6)

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Definir indicadores que permitam monitorar os riscos (KRI, ou Key Risk Indicator);

b. Definir indicadores específicos que permitam avaliar se os controles estão funcionando conforme esperado (KPI, ou Key Performance Indicators), com base nos riscos mapeados;

c. Estabelecer metas ou limites aceitáveis para os indicadores, de forma que seja possível identificar quando o controle está falhando;

d. Monitorar os indicadores com regularidade, integrando-os ao processo de acompanhamento dos riscos;

e. Integrar os indicadores de risco/controle ao painel de monitoramento institucional (quando houver).

◆ **Evidências:** Ficha de Indicadores de risco ou controle e relatório de acompanhamento dos indicadores.

Saiba Mais!

Selecionar indicadores de risco (KRI) e indicadores de desempenho (KPI) diretamente ligados aos objetivos definidos é essencial para uma gestão de riscos eficaz e orientada a resultados. Os KRIs são métricas utilizadas para monitorar sinais de alerta antecipado relacionados à probabilidade ou impacto de um risco. Eles devem ser capazes de demonstrar tendências ou variações que indiquem aumento da exposição ao risco, permitindo a adoção de ações preventivas antes que eventos adversos ocorram. Os KPIs são métricas que refletem a eficácia das respostas aos riscos e dos controles implementados, evidenciando se os objetivos e metas da organização estão sendo alcançados conforme o esperado. Para auxiliar as unidades gestoras na seleção dos indicadores, podem ser citados alguns exemplos:

- **KRI:** número de incidentes de segurança da informação; percentual de não conformidades em auditorias; taxa de rotatividade de pessoal em áreas críticas; variação de custos acima de determinado limite; frequência de interrupções em processos essenciais.
- **KPI:** percentual de implementação de planos de ação de tratamento de riscos; tempo médio de resposta a incidentes; redução percentual no impacto financeiro de riscos ocorridos; nível de aderência a prazos de monitoramento e revisão dos riscos.

É importante que esses indicadores sejam compartilhados com as partes interessadas com o objetivo de demonstrar os resultados alcançados e fortalecer a cultura de riscos, além de possibilitar melhorias contínuas.

O gestor deve estar preparado para ajustar as estratégias de resposta aos riscos e os próprios indicadores com base nos resultados e nas mudanças no ambiente de risco.

• **Requisito de maturidade 19:** A Unidade de Controle Interno (Segunda Linha) atua como responsável pelo monitoramento da Gestão de Riscos, verificando se a construção, implementação e resultados do processo de gestão de riscos se concretizam conforme o esperado e comunicando ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos das áreas máximo e aos gestores executivos o andamento do gerenciamento de riscos das áreas.

◆ **Referência:** O propósito do monitoramento e análise crítica é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo. Convém que o monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas. (ISO 31000:2018, seção 6.6)

Papéis da segunda linha • Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo: o Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidade. • O atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade. • Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno) (MODELO DAS TRÊS LINHAS DO IIA 2020, Papéis da segunda linha)

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Acompanhar a aplicação da metodologia de riscos;
b. Monitorar a implementação das ações previstas nos planos de ação;
c. Consolidar relatórios gerenciais com o status da gestão de riscos por setor/processo;
d. Elaborar documento contendo as ações de monitoramento realizadas e encaminhar para a alta gestão, destacando:
    1. Riscos críticos e não tratados;
    2. Falhas em controles relevantes;
    3. Atrasos ou ineficiência na implementação de planos de ação;
    4. Sugestões de melhoria no processo de gestão de riscos;
e. Estabelecer um ciclo de monitoramento formal, com periodicidade definida (por exemplo, semestral), podendo ser apresentado em comitês, reuniões gerenciais ou por meio de painéis institucionais.

- **Evidências:** Documento de formalização do monitoramento efetuado pela segunda linha, bem como os devidos encaminhamentos para a alta gestão; Relatórios ou dashboards consolidados com visão geral da situação dos riscos e planos de ação nas áreas; Registros de reuniões em que a UCI apresentou ou discutiu o status da gestão de riscos com dirigentes ou gestores estratégicos.

Saiba Mais!

Para dar início à atividade de monitoramento da gestão de riscos, recomenda-se começar com a elaboração de relatórios simples que consolidem informações essenciais. Esses relatórios devem indicar, de forma objetiva, quais setores já realizaram o mapeamento de riscos, qual é a situação atual dos respectivos planos de ação (em andamento, concluídos ou não iniciados) e identificar os riscos classificados como críticos que ainda não possuem tratamento definido.

Paralelamente, é fundamental estabelecer um cronograma regular de reporte à alta administração, com periodicidade previamente definida (trimestral ou semestral, por exemplo), assegurando que as informações sobre riscos e suas respostas cheguem tempestivamente aos tomadores de decisão. Para isso, devem-se definir também os canais de comunicação mais adequados, como reuniões executivas ou relatórios formais da Unidade de Controle Interno.

Além disso, é importante promover reuniões periódicas com as áreas responsáveis e com a direção da organização para apresentar os achados obtidos durante o monitoramento. Essas interações contribuem para fortalecer o papel da UCI como parceira estratégica, reforçando a gestão de riscos como uma ferramenta de governança essencial ao alcance dos objetivos institucionais e à prevenção de falhas ou perdas relevantes

• **Requisito de maturidade 20:** A gestão avalia e registra os problemas ocorridos em **documento específico (Ex.: Planilha de Registro de incidentes)**, realizando a devida atualização no gerenciamento de riscos, quando necessário.

- **Referência:** O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade: (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar 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) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009).(Referencial Básico de Gestão de Riscos. TCU, 2018).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Estabelecer um procedimento formal para registro e análise de incidentes, falhas operacionais, eventos adversos ou desvios relevantes nos processos.
  b. Orientar as áreas a reportar formalmente os incidentes relevantes;
  c. Utilizar documento ou sistema específico (ex. planilha de registro de incidentes, formulário eletrônico, sistema de ocorrências), contendo os seguintes campos: data e descrição do evento, área envolvida, causa provável, impactos observados e ações corretivas adotadas.
  d. Realizar análise crítica dos eventos registrados, verificando se estão relacionados a riscos já mapeados, se os controles falharam ou se é necessário atualizar a matriz de riscos.
- **Evidências:** Planilha ou sistema de registro de incidentes operacionais, preenchida e atualizada; Mapa de riscos revisado após a ocorrência de eventos relevantes; Registros de reuniões que discutiram os eventos ou falhas operacionais.

Saiba Mais!

Um dos documentos que a segunda linha pode apresentar à primeira linha quando da capacitação sobre a temática de gestão de riscos é o registro de incidentes. Esse documento permite que todas as ocorrências sejam registradas, proporcionando uma base de dados que pode ser analisada posteriormente.

A utilização dessa base facilita o rastreamento de incidentes desde a sua ocorrência até a sua resolução, garantindo que nenhum detalhe importan-

te seja perdido. Adicionalmente, permite a análise detalhada das causas dos incidentes, ajudando a identificar padrões e tendências que podem indicar problemas sistêmicos, além de contribuir para a implementação de medidas corretivas e preventivas que abordem as causas subjacentes dos incidentes.

Esse instrumento contribui com o monitoramento contínuo, ajudando a identificar novos riscos ou mudanças nos riscos existentes e ajuda a priorizar os riscos com base na frequência e gravidade dos incidentes registrados.

Vide exemplo de planilha de registro de incidentes elaborada pela SCGE:

Figura 6: Modelo de planilha de registro de incidentes da SCGE

GESTÃO DE RISCOS (GR) - INVENTÁRIO DE CONCRETIZAÇÃO DE RISCOS							
Qual o problema ocorrido?	O risco estava contemplado no Gerenciamento de Riscos?	Qual o evento de Risco relacionado?	Existia Medida de Tratamento para o Risco?	O plano de tratamento funcionou?	A análise da probabilidade de impacto foi correta?	Data de ocorrrência	Sugestão Medidas Tratamento

Fonte: Elaboração própria

3.7 Agrupamento: Comunicação

A comunicação busca promover a conscientização e o entendimento do risco, bem como a existência de mecanismos para informar tempestivamente sobre o processo e a eficácia da gestão de riscos. Um processo de gestão de riscos que utilize comunicação adequada reduz as chances de que a alta Administração só tome ciência de um risco depois que ele já se transformou em crise.

• **Requisito de maturidade 21:** O órgão/entidade realiza campanhas, palestras e/ou outros atos de sensibilização sobre a importância de gerenciar riscos.

- **Referência:** Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, demonstrem e articulem o seu comprometimento contínuo com a gestão de riscos por meio de uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização. (ISO 31000:2018, seção 5.4.2)
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Realizar ações contínuas de sensibilização para promover e fortalecer a cultura de gestão de riscos na unidade, podendo ser articuladas com outras iniciativas de governança, como integridade, ética e inovação;
  b. Manter a participação ativa da alta gestão em eventos da temática de gestão de riscos
  c. Elaborar material institucional sobre a temática
  d. Elaborar programas de treinamentos periódicos
  e. Utilizar a intranet, sítio eletrônico institucional e email para disseminar informações
- **Evidências:** Registro da participação da alta gestão em eventos na temática de gestão de riscos; Registro das campanhas de incentivo à implementação e monitoramento da gestão de riscos; material institucional divulgado.

Saiba Mais!

Para iniciar a sensibilização sobre a importância da gestão de riscos, é recomendável adotar ações simples, estratégicas e adaptadas à realidade de cada órgão/entidade. O primeiro passo é elaborar uma apresentação breve e didática que explique, de forma clara, o que é a gestão de riscos, quais seus objetivos e por que ela é relevante para o alcance dos resultados e a prevenção de falhas no órgão. Essa apresentação deve ser utilizada como base para ações de comunicação e engajamento.

Em seguida, é importante realizar um evento-piloto, como uma palestra

ou uma roda de conversa, envolvendo diferentes áreas da instituição. Sempre que possível, essa atividade pode ser inserida em momentos já previstos no calendário institucional, como reuniões de equipe, semanas de planejamento ou outros eventos internos, o que facilita a adesão e reduz resistências.

A produção de materiais de apoio complementares também fortalece a iniciativa. Cards informativos, vídeos curtos, e-mails com mensagens-chave ou cartazes com linguagem acessível ajudam a disseminar a cultura da gestão de riscos de forma leve e contínua, especialmente quando vinculados à identidade institucional.

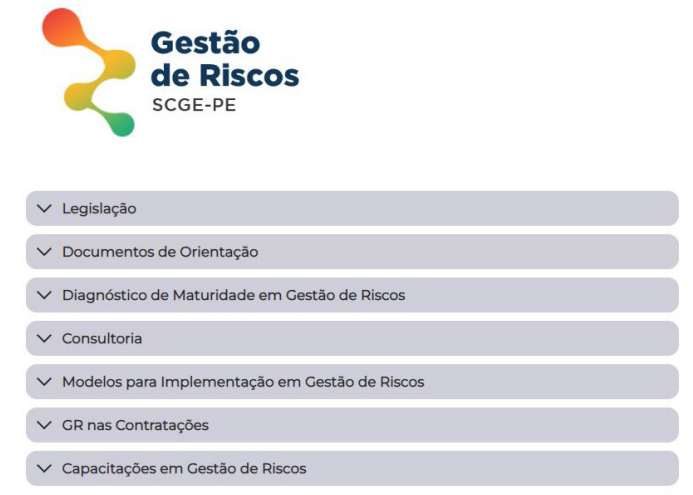
Outro fator essencial é o engajamento dos gestores. Convidá-los a falar sobre a importância da prática em suas áreas reforça o compromisso da alta direção e legitima o tema como prioridade de governança. Aproveitar datas estratégicas, como o Dia da Integridade Pública ou o início do exercício orçamentário, também é uma boa oportunidade para incluir a pauta de riscos nas ações internas, conectando-a a momentos de maior atenção institucional.

Por fim, é fundamental documentar todas as ações realizadas, registrando conteúdos, listas de presença, comunicações e materiais produzidos. Esses registros servirão como evidências institucionais, fortalecendo a memória organizacional e criando base para o aprimoramento e continuidade das ações no futuro

Figura 7: Sugestões de ações de sensibilização

Fonte: Elaboração própria

Figura 8: Material institucional sobre a temática de gestão de riscos no sítio eletrônico do órgão.



Fonte: Elaboração própria

- **Requisito de maturidade 22:** Existem mecanismos de comunicação formalizados através de plano de comunicação e em execução que garantam que as partes interessadas recebam informações **tempestivas, claras e relevantes** sobre o processo de gestão de riscos e a sua eficácia no órgão/entidade.

◆ **Referência:** Convém que a comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas (ISO 31000:2018, seção 6.7).

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Elaborar o plano de comunicação, com fluxos, periodicidade, responsáveis e canais definidos;

b. Executar o plano de forma eficiente

◆ **Evidências:** i. Plano de comunicação; ii. comunicados emitidos para as partes interessadas sobre o status dos riscos críticos, percentual de planos de ação concluídos, mudanças nos controles, eventos registrados, lições aprendidas, melhorias, etc. e iii. registro da formalização dos encaminhamentos (processo SEI, e-mail, intranet, etc.).

Saiba Mais!

O Plano de Comunicação tem como principal objetivo garantir que as partes interessadas no processo de gestão de riscos tenham informações e possam supervisionar e tomar as decisões de forma eficiente. Deve ser composto pelos seguintes elementos:

- Atividade do processo de gestão de riscos;
- Produto associado à atividade;
- Objetivo da Comunicação;
- Tipo de informação a ser comunicada;
- Comunicador;
- Destinatários;
- Meio de Comunicação;
- Sistema a ser utilizado para envio da comunicação;
- Frequência.

O plano poderá prever um conjunto de medidas para incentivar o engajamento e ampliar o conhecimento dos colaboradores sobre a gestão de riscos, por meio de ações de conscientização e esclarecimento quanto ao que é, seus objetivos, benefícios e público-alvo, bem como pela disseminação de informações relevantes sobre o plano de gestão de riscos, incluindo atividades realizadas e resultados obtidos.

Se o órgão ainda não possui mecanismos estruturados de comunicação sobre riscos, pode começar assim:

- Mapeie quem são as partes interessadas em saber sobre o processo de gestão de riscos (ex: alta administração, gestores, UCI, servidores de áreas críticas).
- Defina que tipo de informação será comunicada (ex: status dos riscos críticos, percentual de planos de ação concluídos, mudanças nos controles, eventos registrados).
- Escolha canais simples e acessíveis, como e-mails periódicos, comunicados internos, inserções em reuniões estratégicas, quadros ou páginas da intranet.
- Elabore um cronograma básico com frequência e responsáveis pela comunicação (ex: relatório trimestral da UCI aos gestores; e-mail semestral à alta direção).
- Crie modelos-padrão de relatório ou mensagem, para manter clareza e objetividade das informações transmitidas.
- Documente o fluxo de comunicação, mesmo que simples, e registre todas as comunicações realizadas, para fins de comprovação e melhoria contínua.

3.8 Agrupamento: Integração

Reforça a importância de integrar a gestão de riscos em todos os processos organizacionais, desde a tomada de decisão até a execução. Este grupo trata da integração entre a gestão de riscos e o planejamento e da abrangência de setores da organização que conhecem os seus riscos críticos.

- **Requisito de maturidade 23:** O monitoramento dos riscos e controles é realizado de forma integrada com o monitoramento dos objetivos estratégicos, metas e indicadores da organização.

◆ **Referência:** A integração da gestão de riscos apoia-se em uma compreensão das estruturas e do contexto organizacional. Estruturas diferem, dependendo do propósito, metas e complexidade da organização. O risco é gerenciado em todas as partes da estrutura da organização. Todos na organização têm responsabilidade por gerenciar riscos (ISO 31000:2018, seção 5.3).

◆ **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:

a. Estabelecer procedimento formal que integre o acompanhamento dos riscos e controles ao processo de monitoramento dos objetivos estratégicos, metas e indicadores.

b. Garantir que o sistema de gestão de desempenho (painéis, relatórios, reuniões de acompanhamento) inclua informações sobre riscos e efetividade dos controles relacionados a cada objetivo/metas.

c. Assegurar que a periodicidade de monitoramento de riscos e controles esteja alinhada à periodicidade de monitoramento dos indicadores estratégicos

d. Consolidar e apresentar relatórios integrados, permitindo à alta administração visualizar, para cada objetivo estratégico, os riscos associados, controles implementados, indicadores de desempenho e ações corretivas.

e. Prever responsabilidades claras para coleta, consolidação e análise das informações, assegurando coerência e atualização contínua

◆ **Evidências:** Documento que descreva o processo integrado de monitoramento de riscos, controles, objetivos e indicadores; relatórios de desempenho que apresentem indicadores, metas, riscos e controles relacionados de forma conjunta; atas ou registros de reuniões de acompanhamento estratégico onde constem discussões sobre riscos e controles vinculados aos objetivos/metas; painéis ou dashboards de gestão que integrem dados de desempenho com informações sobre riscos e controles; evidências de atualização periódica dessas informações (planilhas, registros em sistemas corporativos, logs de atualização).

Saiba Mais!

Para estruturar este requisito o ideal é seguir um caminho gradual e estruturado. Segue um roteiro prático em cinco passos:

1. Revisar e alinhar o planejamento estratégico

- **O que fazer:** Revise o planejamento estratégico e liste todos os objetivos estratégicos, metas e indicadores já definidos.
- **Por que:** Você precisa ter clareza sobre o "alvo" antes de associar riscos e controles.
- **Dica prática:** Crie uma tabela com colunas: Objetivo Estratégico, Meta, Indicador.

2. Mapear riscos e controles relacionados

- **O que fazer:** Para cada objetivo, identifique os riscos que podem comprometer seu alcance e os controles existentes para mitigá-los.
- **Por que:** Isso cria o vínculo direto entre estratégia e gestão de riscos.
- **Dica prática:** Use oficinas, entrevistas ou reuniões com gestores de áreas-chave para levantar essas informações.

3. Definir como será o monitoramento integrado

- **O que fazer:** Decida se vai integrar as informações em relatórios já existentes (como balanços de desempenho) ou criar um painel/dashboards específicos.
- **Por que:** A integração não precisa "reinventar a roda" — ela pode aproveitar canais já consolidados de monitoramento estratégico.
- **Dica prática:** Utilize o mesmo calendário das reuniões de acompanhamento estratégico para atualizar também riscos e controles.

4. Criar um fluxo de coleta e consolidação

- **O que fazer:** Documente quem será responsável por fornecer, analisar e consolidar dados de indicadores, riscos e controles.
- **Por que:** A integração depende de responsabilidades claras e periodicidade definida.
- **Dica prática:** Estabeleça um checklist mensal/trimestral com todos os dados que precisam ser atualizados.

5. Comunicar e treinar

- **O que fazer:** Apresente o processo às áreas envolvidas, mostrando como riscos e controles estarão no mesmo radar que objetivos e metas.
- **Por que:** Sem alinhamento, o risco é que cada área monitore de forma isolada.
- **Dica prática:** Mostre exemplos concretos de como a visão integrada ajuda na tomada de decisão.

SUGESTÃO DE PRIMEIRO PASSO IMEDIATO:

A partir do relatório ou painel de acompanhamento dos objetivos estratégicos do seu órgão/entidade e, para cada objetivo, adicione uma coluna de "Riscos Associados" e outra de "Controles Existentes". Esse é o ponto de partida para a integração.

• **Requisito de maturidade 24:** As principais áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) têm identificados os riscos críticos de sua atuação para a realização dos principais objetivos da organização.

- **Referência:** Identificação e gestão do risco na entidade como um todo: toda a entidade está sujeita a vários tipos de riscos, que podem afetar diversas partes da organização. Às vezes, um risco pode ser originário de uma parte da entidade, mas impactar outra parte. Dessa forma, a administração identifica e gerencia os riscos na entidade como um todo para manter e melhorar a performance (COSO ERM 2017, Benefícios do efetivo gerenciamento de riscos corporativos).
- **Prescrição:** Para que a questão seja atendida de forma satisfatória, o órgão/entidade deve:
  a. Definir critérios organizacionais para a identificação dos riscos críticos, alinhados ao contexto estratégico e operacional da organização.
  b. Garantir que todas as áreas relevantes realizem o mapeamento de riscos relacionados às suas atividades, processos, projetos e objetivos.
  c. Estabelecer procedimentos formais para consolidar e integrar os riscos identificados em nível organizacional, considerando interdependências e impactos cruzados entre áreas.
  d. Promover a validação dos riscos críticos junto à alta administração, assegurando o alinhamento com os objetivos estratégicos..
  e. Manter os riscos críticos registrados e atualizados no inventário ou matriz de riscos corporativa, com indicação de responsáveis, causas, impactos e medidas de tratamento.
  f. Assegurar que a gestão dos riscos críticos seja monitorada periodicamente e comunicada às partes interessadas relevantes.
- **Evidências:** Inventário ou matriz de riscos corporativa atualizada, contendo a identificação dos riscos críticos por área/unidade, registros ou relatórios de workshops, reuniões ou entrevistas realizados para identificação e validação dos riscos críticos, procedimentos, manuais ou políticas internas que definam critérios e responsabilidades para identificação e integração dos riscos críticos, atas de reuniões da alta administração ou comitês de risco aprovando ou revisando a lista de riscos críticos, relatórios consolidados que demonstrem a integração dos riscos críticos de diferentes áreas e a análise de interdependências.

Saiba Mais!

É importante entender inicialmente que os riscos críticos são aqueles que, independentemente de serem estratégicos, táticos ou operacionais, foram avaliados como os mais relevantes para o órgão/entidade, porque apresentam alto impacto e/ou alta probabilidade de ocorrência.

Ou seja, “crítico” é um grau de prioridade e não um tipo de risco, um risco estratégico, por exemplo, pode ser crítico ou não dependendo da avaliação da probabilidade x impacto.

Nesse sentido, uma falha no sistema de folha de pagamento que paralise o pagamento dos servidores, embora seja um risco operacional, é considerada um risco crítico, pois pode gerar alto impacto caso se materialize.

4. CONCLUSÃO

A gestão de riscos, quando tratada de forma estruturada e integrada, fortalece a capacidade do órgão/entidade em alcançar seus objetivos estratégicos, gerar valor público e assegurar maior transparência e confiabilidade em sua atuação.

Este guia de maturidade foi elaborado para apoiar os gestores públicos no diagnóstico, monitoramento e evolução contínua da prática de gestão de riscos, oferecendo requisitos claros, referências normativas e instrumentos de comprovação.

Mais do que uma ferramenta de avaliação, trata-se de um instrumento de aprendizagem institucional, que permite identificar lacunas, consolidar boas práticas e direcionar esforços para a evolução dos níveis de maturidade.

O sucesso na aplicação deste guia depende do engajamento da alta administração, do compromisso das áreas envolvidas e do uso sistemático das evidências levantadas para subsidiar melhorias.

Por fim, alcançar níveis superiores de maturidade não é um fim em si mesmo, mas sim um meio para fortalecer a governança, apoiar a tomada de decisão e gerar resultados, contribuindo para que a gestão de riscos se torne parte da cultura organizacional e esteja presente em todas as instâncias de planejamento, execução e monitoramento.

ANEXO

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Liderança e Envolvimento	1. Existe diretriz estratégica para assegurar que o gerenciamento de riscos seja realizado nos PRINCIPAIS níveis hierárquicos do órgão/ entidade.	0 - Inexistente - Não há diretriz estratégica estabelecida para garantir que o gerenciamento de riscos seja realizada nos principais níveis hierárquicos.
		1 - Inicial - Existe alguma diretriz estratégica, mas ela é insuficiente ou não abrange de forma adequada os principais níveis hierárquicos do órgão/entidade.
		2 - Parcial - Há diretrizes estratégicas, mas a aplicação nos principais níveis hierárquicos é limitada ou precisa de melhorias.
		3 - Estabelecida - A diretriz estratégica está estabelecida e cobre os principais níveis hierárquicos da entidade, mas pode haver lacunas em sua execução.
		4 - Integrada - Existe uma diretriz estratégica sólida, bem estabelecida e plenamente implementada, assegurando que o gerenciamento de riscos seja realizada eficazmente nos principais níveis hierárquicos.
Liderança e Envolvimento	2. O Gerenciamento dos Riscos Estratégicos é implementado no órgão/ entidade.	0 - Inexistente - O gerenciamento dos riscos estratégicos não é implementado na organização.
		1 - Inicial - O gerenciamento dos riscos estratégicos é implementado de forma limitada ou inconsistente, sem uma abordagem estruturada.
		2 - Parcial - O gerenciamento dos riscos estratégicos está parcialmente implementado, mas sua aplicação é inconsistente ou precisa de melhorias.
		3 - Estabelecida - O gerenciamento dos riscos estratégicos está implementado de forma estruturada e consistente, mas há espaço para aperfeiçoamento.
		4 - Integrada - O gerenciamento dos riscos estratégicos é totalmente implementado na organização, com uma abordagem eficaz e bem estruturada.
Estrutura	3. O órgão/entidade possui planejamento estratégico (atualizado) contendo, dentre outras informações indispensáveis, as definições de missão, visão e objetivos.	0 - Inexistente - O órgão/entidade não possui um planejamento estratégico formal ou atualizado, e não há definições claras de missão, visão e objetivos.
		1 - Inicial - O órgão/entidade tem um planejamento estratégico, mas ele está desatualizado ou incompleto, faltando definições claras de missão, visão ou objetivos.
		2 - Parcial - O órgão/entidade possui um planejamento estratégico, mas há dúvidas quanto à sua atualização ou clareza nas definições de missão, visão e objetivos.
		3 - Estabelecida - O órgão/entidade possui um planejamento estratégico atualizado, com definições de missão, visão e objetivos, mas pode haver espaço para melhorias.
		4 - Integrada - O órgão/entidade tem um planejamento estratégico atualizado e completo, com definições claras e bem estabelecidas de missão, visão e objetivos.
Estrutura	4. O órgão/entidade estabeleceu e comunicou adequadamente metas e indicadores dos projetos e processos para monitorar seu desempenho.	0 - Inexistente - O órgão/entidade não estabeleceu metas e indicadores de desempenho para os projetos e processos.
		1 - Inicial - O órgão/entidade estabeleceu algumas metas e indicadores, mas a comunicação é falha ou insuficiente, e o monitoramento do desempenho é inadequado.
		2 - Parcial - O órgão/entidade tem metas e indicadores, mas a comunicação e o monitoramento de desempenho são inconsistentes ou precisam ser aprimorados.
		3 - Estabelecida - O órgão/entidade estabeleceu metas e indicadores e os comunicou adequadamente; o desempenho é monitorado regularmente, mas pode haver oportunidades de melhoria.
		4 - Integrada - O órgão/entidade estabeleceu metas e indicadores claros, comunicou-os de forma eficaz e realiza um monitoramento de desempenho completo e contínuo.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Estrutura	5. Os dados do gerenciamento de riscos são processados através de sistema informatizado que permite uma visão abrangente dos riscos da organização e a manutenção do histórico das análises realizadas.	0 - Inexistente - Os dados do gerenciamento de riscos não são processados através de um sistema informatizado.
		1 - Inicial - Existe um sistema informatizado, mas ele não proporciona uma visão abrangente dos riscos ou não mantém o histórico das análises de forma adequada.
		2 - Parcial - Há um sistema informatizado para o gerenciamento de riscos, mas a visão abrangente dos riscos e a manutenção do histórico das análises são apenas parcialmente atendidas ou precisam de melhorias.
		3 - Estabelecida - O sistema informatizado permite uma visão geral dos riscos e mantém o histórico das análises, mas pode haver algumas áreas que poderiam ser aprimoradas.
		4 - Integrada - O sistema informatizado processa os dados do gerenciamento de riscos de maneira eficaz, oferecendo uma visão abrangente dos riscos da organização e mantendo um histórico completo e acessível das análises realizadas.
Estrutura	6. O órgão/entidade dispõe de uma política de gestão de riscos aprovada pela alta administração, comunicada e disponível às partes interessadas.	0 - Inexistente - A entidade não possui uma política de gestão de riscos.
		1 - Inicial - A entidade possui uma política de gestão de riscos, mas ela não foi aprovada pela alta administração ou não é adequadamente comunicada e disponibilizada às partes interessadas.
		2 - Parcial - A política de gestão de riscos foi aprovada pela alta administração e está disponível, mas a comunicação e o acesso às partes interessadas podem ser limitados ou precisar de melhorias.
		3 - Estabelecida - A política de gestão de riscos é aprovada pela alta administração, comunicada e disponibilizada às partes interessadas, mas pode haver áreas para melhorar a efetividade da comunicação ou o acesso.
		4 - Integrada - A política de gestão de riscos é aprovada pela alta administração, amplamente comunicada e prontamente disponível às partes interessadas, com uma comunicação eficaz e acessível.
Conhecimento e Cultura	7. Os gestores da primeira linha têm consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes.	0 - Inexistente - Os gestores da primeira linha não têm consciência de sua responsabilidade sobre os riscos e a manutenção de controles internos eficazes.
		1 - Inicial - Os gestores da primeira linha têm alguma consciência, mas a compreensão de sua responsabilidade pela identificação e gerenciamento dos riscos e pela manutenção de controles internos é limitada.
		2 - Parcial - Os gestores da primeira linha estão parcialmente cientes de suas responsabilidades, mas a consciência sobre a propriedade dos riscos e a manutenção de controles internos pode ser inconsistente ou precisar de melhorias.
		3 - Estabelecida - Os gestores da primeira linha têm uma boa consciência de sua responsabilidade pelos riscos e pela manutenção de controles internos, embora haja espaço para reforçar essa compreensão.
		4 - Integrada - Os gestores da primeira linha têm plena consciência de sua responsabilidade sobre os riscos, com um entendimento claro da identificação, gerenciamento e manutenção de controles internos eficazes.
Conhecimento e Cultura	8. O órgão/entidade dispõe de um manual de gestão de riscos, ou documento similar, aprovado pela alta administração, disponível e comunicado às partes interessadas.	0 - Inexistente - A entidade não possui um manual de gestão de riscos ou documento similar aprovado pela alta administração.
		1 - Inicial - Existe um manual de gestão de riscos ou documento similar, mas não foi aprovado pela alta administração ou não está suficientemente disponível às partes interessadas.
		2 - Parcial - O manual de gestão de riscos ou documento similar foi aprovado pela alta administração e está disponível, mas a comunicação e o acesso às partes interessadas são limitados ou podem ser aprimorados.
		3 - Estabelecida - O manual de gestão de riscos ou documento similar está aprovado pela alta administração e é disponibilizado às partes interessadas, com uma comunicação e acessibilidade adequadas, mas pode haver oportunidades de melhoria.
		4 - Integrada - A entidade possui um manual de gestão de riscos ou documento similar, aprovado pela alta administração, que é amplamente disponibilizado e facilmente acessível às partes interessadas, com uma comunicação clara e eficaz.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Conhecimento e Cultura	9. Os membros da Unidade de Controle Interno (Segunda Linha) possuem conhecimento suficiente para conduzir e orientar a gestão de riscos em seu órgão/entidade.	0 - Inexistente - Os gestores da Unidade de Controle Interno (Segunda Linha) não possuem conhecimento suficiente para conduzir e orientar a gestão de riscos em seu órgão/entidade.
		1 - Inicial - Os gestores da Unidade de Controle Interno (Segunda Linha) têm algum conhecimento sobre gestão de riscos, mas não é suficiente para conduzir e orientar efetivamente em seu órgão/entidade.
		2 - Parcial - Os gestores da Unidade de Controle Interno (Segunda Linha) possuem conhecimento moderado sobre gestão de riscos, mas podem precisar de mais treinamento ou recursos para conduzir e orientar de forma mais eficaz.
		3 - Estabelecida - Os gestores da Unidade de Controle Interno (Segunda Linha) possuem conhecimento adequado para conduzir e orientar a gestão de riscos em seu órgão/entidade, embora haja espaço para aprofundamento ou atualização.
		4 - Integrada - Os gestores da Unidade de Controle Interno (Segunda Linha) têm conhecimento completo e suficiente para conduzir e orientar a gestão de riscos em seu órgão/entidade, demonstrando competência e segurança na prática.
Processo	10. O gerenciamento dos riscos é realizado por pessoas designadas que têm responsabilidade, autoridade e experiência nas atividades objeto de análise.	0 - Inexistente - O gerenciamento de riscos não é realizado por pessoas com a devida responsabilidade, autoridade ou experiência nas atividades objeto de análise.
		1 - Inicial - O gerenciamento de riscos é realizado por algumas pessoas com responsabilidade e autoridade, mas elas carecem da experiência necessária nas atividades objeto de análise.
		2 - Parcial - O gerenciamento de riscos é realizado por pessoas com responsabilidade, autoridade e alguma experiência, mas pode haver lacunas em relação à expertise ou à clareza de papéis.
		3 - Estabelecida - O gerenciamento de riscos é realizado por pessoas com a devida responsabilidade, autoridade e experiência, mas ainda pode haver espaço para melhorar a especialização em alguns casos.
		4 - Integrada - O gerenciamento de riscos é realizado por pessoas plenamente qualificadas, com a responsabilidade, autoridade e experiência necessárias nas atividades objeto de análise, garantindo um processo de gestão eficaz.
Processo	11. A Unidade de Controle Interno (Segunda Linha) atua como facilitadora do processo de gerenciamento de riscos, fornecendo metodologias e ferramentas às áreas, com a finalidade de identificar e avaliar riscos.	0 - Inexistente - A Unidade de Controle Interno (Segunda Linha) não atua como facilitadora do processo de gerenciamento de riscos, nem fornece metodologias ou ferramentas às áreas para identificar e avaliar riscos.
		1 - Inicial - A Unidade de Controle Interno (Segunda Linha) atua parcialmente como facilitadora, mas a oferta de metodologias e ferramentas é insuficiente ou pouco eficaz para ajudar as áreas a identificar e avaliar riscos.
		2 - Parcial - A Unidade de Controle Interno (Segunda Linha) facilita o processo de gerenciamento de riscos em parte, fornecendo algumas metodologias e ferramentas, mas o apoio é limitado ou pode ser aprimorado.
		3 - Estabelecida - A Unidade de Controle Interno (Segunda Linha) atua como facilitadora do processo de gerenciamento de riscos, fornecendo metodologias e ferramentas adequadas, mas há espaço para melhorar a eficácia ou o alcance desse suporte.
		4 - Integrada - A Unidade de Controle Interno (Segunda Linha) desempenha plenamente seu papel de facilitadora, fornecendo metodologias e ferramentas eficazes e acessíveis.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Processo	12. O processo de gerenciamento de riscos produz uma lista de riscos RELEVANTES e controles APROPRIADOS, através da utilização de metodologia consolidada, como às do COSO ou ISO.	0 - Inexistente - O processo de gerenciamento de riscos não utiliza uma metodologia consolidada (como COSO ou ISO) e não produz uma lista de riscos relevantes ou controles apropriados.
		1 - Inicial - O processo de gerenciamento de riscos utiliza uma metodologia consolidada de forma limitada ou inadequada, resultando em uma lista de riscos e controles que não são suficientemente relevantes ou apropriados.
		2 - Parcial - O processo de gerenciamento de riscos utiliza uma metodologia consolidada, mas a lista de riscos relevantes e controles apropriados é incompleta ou precisa de melhorias.
		3 - Estabelecida - O processo de gerenciamento de riscos segue uma metodologia consolidada, como COSO ou ISO, produzindo uma lista de riscos relevantes e controles apropriados, com espaço para aperfeiçoamento.
		4 - Integrada - O processo de gerenciamento de riscos utiliza plenamente uma metodologia consolidada (COSO, ISO etc.), gerando uma lista abrangente de riscos relevantes e controles adequados, com resultados altamente eficazes.
Processo	13. O órgão/entidade realiza o registro sistemático das evidências que suportam a identificação, análise, avaliação dos riscos, a proposição de controles e a avaliação da eficácia desses controles.	0 - Inexistente - O órgão/entidade não realiza o registro sistemático das evidências que suportam a identificação, análise, avaliação dos riscos e a proposição e avaliação dos controles.
		1 - Inicial - O órgão/entidade realiza o registro das evidências de forma parcial ou inconsistente, deixando lacunas na documentação dos processos de gerenciamento de riscos e controles.
		2 - Parcial - O órgão/entidade realiza o registro das evidências de forma razoável, mas o processo é incompleto ou necessita de melhorias para garantir uma documentação mais consistente e sistemática.
		3 - Estabelecida - O órgão/entidade realiza o registro sistemático das evidências de maneira adequada, cobrindo as etapas de identificação, análise, avaliação dos riscos e controle, mas ainda pode melhorar em termos de detalhamento ou rigor.
		4 - Integrada - O órgão/entidade realiza o registro sistemático e completo das evidências que suportam todas as etapas do gerenciamento de riscos, incluindo a avaliação da eficácia dos controles, garantindo um processo bem documentado e robusto.
Processo	14. O tratamento dos riscos é registrado em plano de ação e comunicado formalmente aos responsáveis pela sua implementação, assegurando que compreendam, assumam compromissos e sejam responsáveis por essas ações.	0 - Inexistente - O tratamento dos riscos não é registrado em plano de ação formal.
		1 - Inicial - O tratamento dos riscos é registrado em um plano de ação, mas a comunicação com os responsáveis é falha, e os compromissos e responsabilidades não são claramente definidos ou assumidos.
		2 - Parcial - O tratamento dos riscos é registrado e comunicado, mas a compreensão, o compromisso e a responsabilidade dos responsáveis podem ser inconsistentes ou precisar de melhorias.
		3 - Estabelecida - O tratamento dos riscos é adequadamente registrado em um plano de ação e formalmente comunicado, com os responsáveis compreendendo e assumindo seus compromissos, embora possam existir áreas de aperfeiçoamento.
		4 - Integrada - O tratamento dos riscos é registrado em um plano de ação claro e formal, comunicado de maneira eficaz aos responsáveis, garantindo plena compreensão, compromisso e responsabilidade por parte de todos os envolvidos.
Resultado	15. As respostas aos riscos identificados (controles) são implementadas.	0 - Inexistente - As respostas aos riscos identificados não são implementadas.
		1 - Inicial - Algumas respostas aos riscos são implementadas, mas a implementação é incompleta ou inadequada para a maioria dos riscos identificados.
		2 - Parcial - As respostas aos riscos identificados são implementadas, mas de forma parcial ou com falhas, e melhorias podem ser necessárias para assegurar uma implementação completa e eficaz.
		3 - Estabelecida - As respostas aos riscos identificados são implementadas adequadamente, mas há espaço para aprimorar a eficácia ou a abrangência da implementação.
		4 - Integrada - As respostas aos riscos identificados são plenamente implementadas, de maneira eficaz e completa, garantindo a mitigação dos riscos.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Resultado	16. A gestão de riscos no órgão/entidade está contribuindo para o alcance dos seus principais objetivos.	0 - Inexistente - A gestão de riscos na entidade não está contribuindo para o alcance dos principais objetivos do órgão/entidade.
		1 - Inicial - A gestão de riscos tem alguma contribuição, mas é insuficiente ou limitada para impactar de maneira significativa o alcance dos principais objetivos do órgão/entidade.
		2 - Parcial - A gestão de riscos contribui para o alcance dos principais objetivos da entidade em certa medida, mas a eficácia pode variar e há espaço para melhorias.
		3 - Estabelecida - A gestão de riscos está contribuindo de maneira adequada para o alcance dos principais objetivos do órgão/entidade, embora haja oportunidades para aprimorar ainda mais sua eficácia.
		4 - Integrada - A gestão de riscos está efetivamente contribuindo para o alcance dos principais objetivos do órgão/entidade., com impacto claro e significativo na realização desses objetivos.
Monitoramento	17. Existe revisão periódica das respostas ao risco (controles), visando avaliar se permanecem adequadas.	0 - Inexistente - Não há revisão periódica das respostas ao risco, ou essa prática não é realizada de forma adequada.
		1 - Inicial - Existe alguma revisão das respostas ao risco, mas ela é esporádica e insuficiente para garantir que permaneçam adequadas.
		2 - Parcial - A revisão das respostas ao risco é realizada de maneira periódica, mas pode ser mais frequente ou mais profunda para garantir a adequação contínua.
		3 - Estabelecida - A revisão periódica das respostas ao risco é realizada de forma adequada, com ajustes quando necessário, mas ainda pode ser aprimorada em alguns aspectos.
		4 - Integrada - A revisão periódica das respostas ao risco é realizada de maneira consistente e eficaz, garantindo que as respostas permaneçam sempre adequadas e alinhadas com as necessidades da organização.
Monitoramento	18. São estabelecidos indicadores que permitam avaliar a efetividade das respostas aos riscos (controles).	0 - Inexistente - Não são estabelecidos indicadores para avaliar a efetividade das respostas aos riscos.
		1 - Inicial - Alguns indicadores são estabelecidos, mas eles são insuficientes ou inadequados para avaliar a efetividade das respostas aos riscos.
		2 - Parcial - Existem indicadores para avaliar a efetividade das respostas aos riscos, mas eles são limitados em escopo ou precisão, e melhorias podem ser necessárias.
		3 - Estabelecida - Indicadores adequados são estabelecidos e permitem avaliar de maneira eficaz a efetividade das respostas aos riscos, embora haja espaço para aprimorar sua abrangência ou detalhamento.
		4 - Integrada - Indicadores claros e completos são estabelecidos e são eficazes para avaliar a efetividade das respostas aos riscos de maneira contínua e precisa.
Monitoramento	19. A Unidade de Controle Interno (Segunda Linha) atua como responsável pelo monitoramento da Gestão de Riscos, verificando se a construção, implementação e resultados do processo de gestão de riscos se concretizam conforme o esperado e comunicando ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos das áreas.	0 - Inexistente - A UCI não exerce um papel claro no monitoramento da gestão de riscos. Falta um processo definido para acompanhar, verificar ou comunicar o progresso da gestão de riscos às partes envolvidas, resultando em ausência de supervisão sistemática e transparente do processo de gestão de riscos.
		1 - Inicial - A UCI realiza apenas um monitoramento pontual e reativo, com lacunas no acompanhamento e na comunicação sobre o andamento da gestão de riscos. A comunicação com os gestores e o dirigente máximo ocorre raramente ou em resposta a eventos específicos, e não há uma rotina de verificação.
		2 - Parcial - A UCI atua no monitoramento da gestão de riscos de maneira limitada e pouco estruturada. As verificações e a comunicação sobre os resultados do processo ocorrem ocasionalmente, sem uma abordagem sistemática. Há um nível básico de acompanhamento, mas ainda não consolidado.
		3 - Estabelecida - A UCI realiza o monitoramento da gestão de riscos, mas algumas práticas, como a comunicação regular aos dirigentes e gestores, ocorrem de forma menos estruturada ou apresentam pontos de melhoria. Em geral, acompanha o processo, mas pode não cobrir todas as áreas ou aspectos conforme o esperado.
		4 - Integrada - A UCI monitora de forma sistemática e proativa todos os aspectos da gestão de riscos, desde a construção e implementação até a obtenção de resultados. Realiza verificações contínuas, comunica de maneira regular e estruturada aos dirigentes e gestores executivos sobre o status e as necessidades de ajustes, promovendo ações corretivas sempre que necessário.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Monitoramento	20. A gestão avalia e registra os problemas ocorridos em documento específico (Ex.: Planilha de Registro de incidentes), realizando a devida atualização no gerenciamento de riscos, quando necessário.	0 - Inexistente - A gestão não avalia nem registra os problemas ocorridos
		1 - Inicial - A gestão avalia e registra alguns problemas, mas a atualização no gerenciamento de riscos é esporádica ou inadequada.
		2 - Parcial - A gestão avalia e registra problemas ocorridos e realiza atualizações no gerenciamento de riscos, mas o processo pode ser inconsistente ou precisar de melhorias para garantir que todas as atualizações sejam realizadas de forma completa e oportuna.
		3 - Estabelecida - A gestão avalia e registra de forma adequada os problemas ocorridos e realiza atualizações necessárias no gerenciamento de riscos, embora haja espaço para melhorar a consistência ou a rapidez das atualizações.
		4 - Integrada - A gestão avalia e registra de maneira eficaz todos os problemas ocorridos e realiza atualizações completas e oportunas no gerenciamento de riscos, garantindo que o processo de gerenciamento de riscos permaneça atualizado e relevante.
Comunicação	21. O órgão/entidade realiza campanhas, palestras e/ou outros atos de sensibilização sobre a importância de gerenciar riscos.	0 - Inexistente - O órgão/entidade não realiza campanhas, palestras ou outros atos de sensibilização sobre a importância de gerenciar riscos.
		1 - Inicial - O órgão/entidade realiza algumas atividades de sensibilização, mas são esporádicas ou de alcance limitado.
		2 - Parcial - O órgão/entidade realiza campanhas, palestras ou outros atos de sensibilização, mas a frequência e o impacto dessas atividades são variáveis ou precisam de melhorias.
		3 - Estabelecida - O órgão/entidade realiza regularmente campanhas, palestras e/ou outros atos de sensibilização sobre a importância de gerenciar riscos, com um impacto geral positivo.
		4 - Integrada - O órgão/entidade realiza campanhas, palestras e outros atos de sensibilização de forma consistente e eficaz, destacando a importância de gerenciar riscos e promovendo uma cultura robusta de gerenciamento de riscos.
Comunicação	22. Existem mecanismos de comunicação formalizados através de plano de comunicação e em execução que garantam que as partes interessadas recebam informações tempestivas, claras e relevantes sobre o processo de gestão de riscos e a sua eficácia no órgão/entidade.	0 - Inexistente - Não existe um plano de comunicação nem mecanismos de comunicação funcionando que garantam que as partes interessadas recebam informações tempestivas, claras e relevantes sobre a gestão de riscos, comprometendo a transparência e a eficácia.
		1 - Inicial - Embora não haja um plano de comunicação estruturado, existem alguns mecanismos em funcionamento. No entanto, eles não asseguram que as partes interessadas recebam informações de forma consistente, resultando em falhas na clareza e na tempestividade.
		2 - Parcial - Há um plano de comunicação e alguns mecanismos em funcionamento, mas a eficácia deles é inconsistente. Às vezes, as partes interessadas recebem informações adequadas, enquanto em outras situações, a comunicação é insuficiente.
		3 - Estabelecida - O plano de comunicação existe e os mecanismos permitem que as partes interessadas recebam informações sobre a gestão de riscos, mas ainda há necessidade de melhorias na rapidez e na clareza das comunicações.
		4 - Integrada - O plano de comunicação está em vigor e os mecanismos de comunicação garantem que as partes interessadas recebam informações tempestivas, sucintas e corretas sobre a gestão de riscos, promovendo transparência e eficácia.
Integração	23. O monitoramento dos riscos e controles é realizado de forma integrada com o monitoramento dos objetivos estratégicos, metas e indicadores da organização.	0 - Inexistente - O monitoramento dos riscos e controles não é integrado com o monitoramento dos objetivos estratégicos, metas e indicadores da organização.
		1 - Inicial - Existe algum nível de monitoramento, mas a integração entre o monitoramento dos riscos e controles e o monitoramento dos objetivos estratégicos, metas e indicadores é insuficiente ou irregular.
		2 - Parcial - O monitoramento de riscos e controles ocorre, mas sua integração com o monitoramento dos objetivos estratégicos, metas e indicadores é limitada ou precisa de melhorias.
		3 - Estabelecida - O monitoramento dos riscos e controles é integrado com o monitoramento dos objetivos estratégicos, metas e indicadores, mas ainda existem áreas que podem ser aperfeiçoadas.
		4 - Integrada - O monitoramento dos riscos e controles é plenamente integrado com o monitoramento dos objetivos estratégicos, metas e indicadores, funcionando de maneira eficaz e contínua.

Agrupamento	Requisito de Maturidade	Estágio de Maturidade
Integração	24. As principais áreas, funções e atividades relevantes (unidades, departamentos, divisões, processos, projetos) têm identificados os riscos críticos de sua atuação para a realização dos objetivos-chaves da organização.	0 - Inexistente - As principais áreas, funções e atividades relevantes não têm os riscos críticos de sua atuação identificados.
		1 - Inicial - Algumas áreas, funções e atividades relevantes identificam riscos críticos, mas a identificação é insuficiente ou incompleta.
		2 - Parcial - As principais áreas, funções e atividades relevantes têm alguns riscos críticos identificados, mas a cobertura pode ser inconsistente ou precisar de melhorias para abranger todos os riscos essenciais.
		3 - Estabelecida - As principais áreas, funções e atividades relevantes têm os riscos críticos identificados de forma adequada, mas pode haver oportunidades para aprimorar a abrangência ou a precisão das identificações.
		4 - Integrada - Todas as principais áreas, funções e atividades relevantes têm os riscos críticos identificados de maneira eficaz.