APÊNDICE B - Matriz de planejamento e possíveis achados relacionados às práticas de governança pública organizacional – ESTRATÉGIA

|  |
| --- |
| PRÁTICA 2110: A organização gerencia riscos?\*\*Observação: outras dimensões e métodos mais detalhados de avaliação da maturidade em gestão de riscos podem ser encontrados no Roteiro de Auditoria de Gestão de Riscos, publicado em 2017 pelo TCU, e no Guia “Gestão de Riscos: avaliação da maturidade”, publicado pelo TCU em 2018. |
| Conteúdo da prática |
| Esclarecimentos  | Consulte a página 71 do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | Consulte as questões da prática 2110 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |

|  |
| --- |
| Subquestão 2111: A estrutura da gestão de riscos está definida? |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. existência de política(s) institucional(ais) de gestão de riscos e nível de aprovação
 | Política de gestão de riscos; atas de reunião da liderança, assinatura no próprio documento |
| 1. Formas de comunicação da(s) política(s) de gestão de riscos
 | Política de gestão de riscos; site da organização, intranet, e-mails, informativos internos, guias, cartazes e vídeos de campanhas institucionais, disponibilização de links para acesso ao documento |
| 1. Designação das instâncias responsáveis pelo sistema de gestão de riscos, inclusive coordenador, comitê ou unidade com responsabilidades formalmente definidas para coordenar a implementação da estratégia, do plano ou do programa de gestão de riscos abrangendo toda a organização
 | Portarias ou atos de designação de colaboradores e gestores para gerenciar riscos |
| 1. Estratégia de implantação do processo de gestão de riscos na organização (mapeamento de processos prioritários; alocação de recursos)
 | Norma, guia ou Manual de gestão de riscos |
| 1. Processo de gestão de riscos formalizado
 | Norma, guia ou Manual de gestão de riscos |
| 1. Critérios de análise e avaliação de riscos
 | Norma, guia ou Manual de gestão de riscos |
| 1. Orientações sobre encaminhamento de assuntos relacionados a riscos para instâncias decisórias adequadas
 | Norma, guia ou Manual de gestão de riscos |
| 1. Níveis de exposição a risco definidos, formas de divulgação interna e periodicidade de revisão
 | Última declaração de apetite a risco |
| 1. Percepção dos gestores acerca das suas responsabilidades com respeito à gestão de riscos
 | Gestores |
| Procedimentos | 1. Verificar se o conselho ou a alta administração aprovou a(s) política(s) institucionais de gestão de riscos;
2. Analisar se a(s) política(s) foi(ram) comunicada(s) e está(ão) disponível(eis) para os públicos interno e externo;
3. Analisar se os aspectos abordados na(s) política(s) incluem: princípios e objetivos da gestão de riscos; diretrizes para a integração do processo de gestão de riscos aos processos organizacionais, incluindo o processo de planejamento estratégico; comprometimento com a disponibilização de recursos (pessoas, métodos, ferramentas, sistemas de informação, necessidades de treinamento);
4. Verificar se há definição clara das responsabilidades para gerir riscos na organização, incluindo as atividades de identificação e avaliação, tomada de decisões sobre respostas a riscos; monitoramento; assessoramento e coordenação; estabelecimento de fluxos de comunicação para compartilhar informações e decisões acerca de gestão de riscos interna e externamente;
5. Aplicar questionário de percepção aos gestores formalmente designados, para avaliar se possuem entendimento acerca das suas responsabilidades com respeito à gestão de riscos;
6. Analisar se há estratégia para integração da gestão de riscos aos processos organizacionais e se contempla alocação de recursos como plano de treinamento, solução tecnológica, metodologias;
7. Verificar se há processo definido para gestão de riscos, com etapas de identificação, análise, avaliação, avaliação de controles, resposta, monitoramento e comunicação, e ainda critérios para análise e avaliação de riscos (como probabilidade e impacto são medidos; outras medidas a serem utilizadas para obter o nível de risco; nível em que o risco se torna aceitável; como avaliar interdependências e intercorrelações);
8. Verificar se a organização declarou seu apetite a risco. Podem ser adotadas diversas abordagens, como definir apetite por categorias de objetivos de negócio ou por categorias de risco. A declaração pode ser precisa, utilizando métodos quantitativos e qualitativos, ou menos precisa, utilizando termos mais gerais;
9. Verificar se está definida a forma de divulgação do apetite a risco e os destinatários, bem como a periodicidade de revisão do apetite;
10. Comparar o grau de aderência a prática declarado com o evidenciado:
	1. inexpressivo - não há abordagem padronizada para definir nível aceitável de riscos; não há política; não há processo definido; não há plano de alocação de recursos; não há atribuição de responsabilidades em gestão de riscos.
	2. inicial - não há abordagem padronizada para definir nível aceitável de riscos; política e processo não estão aprovados ou não abordam aspectos mínimos necessários à implementação; não estão comunicados de forma consistente para toda a organização; não há plano de alocação de recursos, informações e relatórios podem existir somente por exigências externas; treinamentos pontuais começaram a ser realizados; as funções de segunda linha não estão formalizadas ou exercem suas atividades individualmente, não integradas a direcionamento estratégico; não há medidas para avaliação de desempenho.
	3. intermediário – há abordagem padronizada para definir nível aceitável de riscos, há apetite a risco definido, há política e processo definidos e comunicados, há estratégia de integração, há plano de alocação de recursos, há responsabilidades atribuídas, há indicadores e metas de monitoramento definidos.
	4. aprimorado - utiliza abordagem padronizada para definir apetite e tolerância a riscos; a política estabelece diretrizes sobre como e com qual periodicidade as etapas do processo serão realizadas, há plano de implementação do processo de gestão de riscos em toda a organização; há processo definido e comunicado; protocolos claros de comunicação existem e foram comunicados por toda a organização; há indicadores e metas de monitoramento definidos e modelos de reporte; há definição clara de responsabilidades para gerir riscos em todas as áreas organizacionais; foram atribuídas as responsabilidades pelo monitoramento e melhoria contínua; há diretrizes acerca das alterações nos política e procedimentos de acordo com mudanças na estratégia.
 |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Se a organização dispõe de política de gestão de riscos estabelecida e aprovada pelo conselho ou pela alta administração, disponível às partes interessadas, e que aborda aspectos necessários ao direcionamento da gestão de riscos;
* Se há estratégia para integração da gestão de riscos aos processos organizacionais;
* Se há comprometimento da alta administração com a alocação de recursos para a gestão de riscos e plano de alocação;
* Se foram definidas as instâncias responsáveis pela gestão de riscos e foram atribuídas as respectivas responsabilidades;
* Se a organização dispõe de um de processo formal de gestão de riscos, com etapas, fluxos de comunicação e critérios definidos;
* Se foi definido o apetite a riscos da organização, com periodicidade de revisão e formas de comunicação
 |
| Possíveis achados |
| Eventos de risco  | * Falta de clareza entre os respectivos papéis desempenhados por todos aqueles que contribuem para a estrutura geral de gerenciamento e controle de riscos;
* Falta de padronização de reporte para questões de gestão de riscos;
* Falta de abordagem padronizada para definição de nível de riscos;
* Alocação de recursos para a gestão de riscos inapropriada ou insuficiente;
* Processo de planejamento estratégico não orientado a riscos;
* Não há parâmetros de apetite a risco, ou não são comunicados de forma eficaz;
* Tomadores de decisão desconhecem os níveis de risco em que devem operar.
 |
| Causas | * Cultura organizacional inibe o avanço da maturidade em riscos;
* Falta de supervisão por parte da instância superior de governança. Instância superior de governança não atua junto a alta administração para determinar se a gestão de riscos foi projetada adequadamente;
* Instância superior de governança não possui coletivamente as habilidades, experiências e conhecimentos de negócio necessários para a supervisão eficaz da gestão de riscos e não faz uso de consultoria independente;
* A alta administração teme a exposição ao risco;
* Cultura focada na atribuição de culpa e não de responsabilidade e melhoria.
 |
| Efeitos | * Aumento do nível de incerteza associado ao alcance dos objetivos da organização;
* Estratégia desvinculada da Missão, Visão e Valores da Organização
* Não cumprimento da estratégia
* Perda de confiança das partes interessadas na organização;
* Baixa capacidade de resiliência da organização;
* Danos à reputação da organização;
* Baixo nível de colaboração, confiança e compartilhamento de informações relacionadas a riscos na organização;
* Impossibilidade de definir limites de tolerância a riscos na implementação da estratégia.
* Gestão de riscos ad hoc ou personalíssima.
 |
| Subquestão 2112: Atividades típicas de segunda linha estão estabelecidas? |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Designação das funções de segunda linha (responsáveis por facilitação, apoio e monitoramento das atividades de gestão de riscos)
 | Política de gestão de riscos; portarias ou atos de designação de colaboradores e gestores para gerenciar riscos; resultados da análise da subquestão 2111 |
| 1. Atividades formalmente atribuídas às funções típicas de segunda linha (ou salvaguardas formalizadas para o caso de haver sobreposição entre segunda linha e auditoria interna)
 | Política de gestão de riscos; portarias ou atos de designação de colaboradores e gestores para gerenciar riscos; resultados da análise da subquestão 2111 |
| 1. Protocolos de comunicação definidos para compartilhamento de informações entra as instâncias de segunda linha, terceira linha, gestores e alta administração
 | Política de gestão de riscos |
| 1. Lista das atividades realizadas pela segunda linha nos dois últimos anos (p. ex.: publicação de manuais, relatórios enviados à liderança, atividades de facilitação, reavaliações de registros de riscos, revisões de reportes de risco, supervisão de autoavaliações de riscos e controles internos, outros).
 | Funções de segunda linha |
| Procedimentos | 1. Analisar a política de gestão de riscos e normativos internos relacionados para verificar se há atribuição de papéis de segunda linha e ainda se foram definidos fluxos de comunicação sobre riscos e controles entre os agentes que executam atividades de segunda linha, os gerentes de áreas (primeira linha) e a alta administração. O Modelo das Três Linhas do IIA 2020 prevê que “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”.
2. Verificar se atribuições da segunda linha incluem:
	1. o monitoramento da integridade e precisão dos reportes de gestão de riscos;
	2. fornecimento de metodologias, ferramentas e orientações para que os gestores (primeira linha) identifiquem e avaliem riscos;
	3. suporte aos gestores (primeira linha) na implementação e monitoramento contínuo dos controles internos destinados a mitigar os riscos identificados;
	4. apoio às atividades de auditoria interna (terceira linha), no acompanhamento e auxílio da interlocução com as áreas auditadas;
	5. alertar a gerência operacional (primeira linha) para questões emergentes e para as mudanças no cenário regulatório e de riscos;
3. (se a auditoria interna estiver exercendo as atividades da segunda linha, as seguintes salvaguardas devem ter sido previamente discutidas com o conselho e alta administração e também documentadas: definição clara das atribuições em que as atividades de segunda e terceira linha se sobrepõem, impacto na independência da auditoria, aceitação e propriedade dos riscos por parte da alta administração, determinação se a sobreposição é temporária ou de longo prazo, plano de transição para o caso de ser temporária – ver guia prático do IIA “A auditoria interna e a segunda linha de defesa”).
4. Selecionar amostra da lista de atividades realizadas e solicitar comprovação;
5. Confrontar as informações obtidas para avaliar se as atribuições e atividades realizadas pela segunda linha contemplam os requisitos mínimos explicitados na questão 2112.
 |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Se as instâncias responsáveis pela facilitação, apoio e monitoramento das atividades de gestão de riscos estão definidas;
* Se estão previstos os fluxos de comunicação sobre riscos e controles entre segunda linha, os gerentes de áreas (primeira linha), a auditoria interna (terceira linha) e a alta administração;
* Se as atribuições da segunda linha contemplam requisitos mínimos necessários ao monitoramento e facilitação das atividades de gestão de riscos.
 |
| Possíveis achados |
| Eventos de risco  | * Sobreposição de atividades de segunda e terceira linhas sem a formalização das salvaguardas;
* Segunda linha opera pontualmente, em áreas onde ocorreram incidentes de riscos ou para cumprimento de obrigações regulatórias;
* Falta de clareza acerca das funções de segunda linha na organização;
* Falta de clareza dos papéis desempenhados pela segunda linha;
* Ausência de orientações para adoção de abordagem padronizada nas atividades de identificação, análise e avaliação dos riscos organizacionais;
* Ausência de padrões de reporte acerca de riscos;
* Ausência de protocolos de comunicação entre primeira e segunda linhas, auditoria interna e alta administração.
 |
| Causas | * Cultura organizacional inibe o avanço da maturidade em riscos;
* Falta de supervisão por parte da instância superior de governança. Não atua junto a alta administração para determinar se a gestão de riscos foi projetada adequadamente;
* A alocação de recursos para a gestão de riscos é inapropriada ou insuficiente.
 |
| Efeitos | * Perda de independência da atividade de auditoria interna;
* Sobreposições e lacunas na cobertura de riscos organizacionais;
* Desconhecimento acerca da adequação e eficácia do gerenciamento de riscos;
* Falta de alinhamento entre as instâncias que operam como segunda linha;
* Falta de alinhamento entre a Governança e os níveis tático e operacional da organização;
* Critérios e métodos utilizados nas etapas do processo de gestão de riscos diferem entre as diversas unidades organizacionais;
* As linguagens e termos utilizados nas etapas do processo de gestão de riscos diferem entre as diversas unidades organizacionais;
* Fragilidade na identificação de riscos emergentes;
* Fragilidade na identificação de mudanças no perfil de riscos organizacional;
* Falhas no compartilhamento de informações acerca de incidentes de riscos e lições aprendidas.
* Governança não recebe informações sobre os níveis tático e operacional da organização para qualificar decisões estratégicas.
 |
| Subquestão 2113: O processo de gestão de riscos da organização está implantado? |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Respostas da organização às questões 2111 (especialmente a letra f) e 2113
 | Painel de indicadores do iGG |
| 1. Estrutura organizacional
 | Organograma |
| 1. Instâncias responsáveis pela gestão de riscos
 | Política de gestão de riscos |
| 1. Relatórios dos últimos dois anos de autoavaliação ou emitidos por auditores externos, reguladores e auditoria interna que abordem a adequação do processo de gestão de riscos organizacional ou de áreas/funções organizacionais.
 | segunda linha, auditoria interna, gestores, auditoria externa, site da organização, site de entes reguladores |
| 1. Incidentes de riscos relevantes nos últimos dois anos
 | Registro de incidentes de risco; segunda linha; auditoria interna; gestores; auditoria externa; OGS; site da organização; site de entes reguladores; mídia; pesquisa integrada do TCU |
| 1. Onde e com que frequência as avaliações de riscos são conduzidas em toda a organização
 | Política de gestão de riscos; sistema de informação utilizado pela gestão de riscos; instância responsável pela coordenação da gestão de riscos; estratégia de integração da gestão de riscos nas atividades organizacionais |
| 1. Inventário ou registro de riscos organizacionais/corporativos (o escopo para essa matriz não contempla riscos financeiros e pode ser delimitado de acordo com o porte da organização e a análise dos relatórios de prestadores internos e externos de serviços de avaliação)
 | Documentação da etapa de identificação de riscos |
| 1. Técnicas e ferramentas utilizadas na etapa de identificação
 | Manual de gestão de riscos da organização; documentação da etapa de identificação de riscos |
| 1. Método de análise utilizado, descrição dos controles existentes
 | Manual de gestão de riscos da organização; documentação da etapa de análise de riscos |
| 1. Planos de tratamento dos riscos
 | Instância responsável pela coordenação da gestão de riscos; documentação da etapa de avaliação de riscos |
| 1. Formas de participação dos responsáveis pelo tratamento dos riscos no processo de escolha das respostas aos riscos
 | Documentação da etapa de avaliação de riscos |
| 1. Diretrizes e protocolos de comunicação estabelecidos para viabilizar o compartilhamento de informações sobre os riscos identificados
 | Política de gestão de riscos; sistema de informação utilizado pela gestão de riscos; instância responsável pela coordenação da gestão de riscos |
| 1. Percepção de membros de funções de segunda linha; e gerentes operacionais acerca do funcionamento do processo de gestão de riscos
 | Membros de funções de segunda linha; gerentes operacionais |
| 1. Sistema de informação que apoia a gestão de riscos, se houver
 | Política de gestão de riscos; sistema de informação utilizado pela gestão de riscos; instância responsável pela coordenação da gestão de riscos |
| Procedimentos | 1. Verificar as respostas da organização às questões 2111 letra f e 2113. Se a organização estiver no nível inexpressivo ou inicial na 2113 e/ou 2111 e/ou se não tiver marcado a letra f da 2111, não se justifica aprofundar a análise da 2113.
2. Analisar os relatórios dos dois últimos anos dos prestadores internos e externos de serviços de avaliação para levantamento preliminar do funcionamento da gestão de riscos;
3. Aplicar roteiro de entrevista em amostra de membros de conselho/comitê de riscos, chefes de outras instâncias responsáveis pela segunda linha; e gerências de grupos/divisões para coletar informações acerca do funcionamento do processo de gestão de riscos;
4. Realizar pesquisa de percepção ou grupo focal com amostra de gerentes operacionais sobre o funcionamento do processo de gestão de riscos (modelo pode ser encontrado na instrução do TC 020.372/2014-0);
5. Analisar a política e manual de gestão de riscos, se houver, para verificar se foram definidos: estratégia de implementação da gestão de riscos na organização; métodos de identificação de riscos; critérios de análise e de avaliação. Podem ser utilizados os resultados da avaliação da questão 2111;
6. Verificar se a organização possui registro de riscos identificados (seja por matrizes, sistema, planilhas) com descrição das causas, eventos e efeitos, níveis de risco calculados. Avaliar quais áreas foram cobertas no registro;
7. Analisar se os controles existentes foram considerados para cálculo de níveis residuais. Essa análise pode ajudar a identificar riscos residuais acima do tolerável, controles excessivos ou ineficazes ou a ausência de avaliação dos controles mantidos pela organização;
8. Verificar se foram definidos requisitos de reporte das informações;
9. Verificar se para os riscos avaliados para medidas de tratamento há planos de tratamento, com identificação de proprietários, ações propostas e responsáveis pela implementação;
10. Confrontar as informações obtidas com as entrevistas, pesquisas e análise documental para avaliar o nível de implementação da gestão de riscos na organização:
	1. Inexpressivo - não foram definidos métodos e critérios para identificação, análise e avaliação de riscos; não há direcionamento da alta administração; não há processo definido, não há registro de riscos.
	2. Inicial - métodos e critérios para identificação, análise e avaliação de riscos estão em fase piloto ou no início da implementação; processos ainda não foram mapeados; não foram identificados objetivos e elementos (processos, produtos, atividades, ativos) prioritários ou relevantes; não há protocolos de comunicação definidos; não há registro de riscos ou as etapas do processo começaram a ser realizadas em pequena parte da organização, de forma separada ou sob demanda; informações e relatórios são direcionados por exigências externas.
	3. Intermediário – há abordagem padronizada para identificação, análise e avaliação de riscos; objetivos e elementos (processos, produtos, atividades, ativos) prioritários ou relevantes foram identificados; há protocolos de comunicação definidos; registro de riscos abrange apenas parte da organização; há documentação das etapas do processo mas ainda não é completa, por exemplo, não há completa descrição dos riscos, ou não são explicitadas as razões de escolha das respostas, responsáveis pelo plano de tratamento não participam da seleção das respostas, dentre outros; indicadores e metas de desempenho estão definidos mas ainda não monitorados.
	4. Aprimorado - há abordagem padronizada para identificação, análise e avaliação de riscos; o processo é executado de forma sistemática em nível organizacional e está integrado ao planejamento estratégico; tecnologia integrada é empregada nos processos de gestão de riscos; o processo produz registro abrangente de riscos, incluindo causas, fontes, efeitos, controles existentes, níveis inerentes e residuais; os responsáveis pelo tratamento são envolvidos no processo de avaliação; os planos de tratamento especificam ordem de prioridade, responsáveis, cronogramas e medidas de desempenho; os protocolos de comunicação estão definidos e aplicados de forma sistemática; metas e indicadores de desempenho são monitorados.
11. Comparar o grau de aderência a prática declarado com o evidenciado;
12. Levantar incidentes de riscos relevantes ocorridos nos últimos dois anos evidenciados em relatórios ou expostos na mídia. Para identificar os efeitos, como incidentes de riscos, podem ser necessárias pesquisas adicionais.
 |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Em que medida a as atividades de identificação, análise e avaliação de riscos são aplicadas às atividades da organização;
* Se há abordagem padronizada para execução das etapas do processo;
* Em que medida são selecionadas e implementadas opções para tratar os riscos, considerando-se parâmetros definidos, e a relação custo-benefício das respostas consideradas;
* Se a organização conta com sistema de informação para apoiar a execução do processo e viabilizar o fluxo de informações sobre exposição a riscos.
 |
| Possíveis achados |
| Eventos de risco  | * Criação e/ou manutenção de controles desnecessários, redundantes, excessivos;
* Criação e/ou manutenção de controles internos ineficazes;
* Processo decisório não orientado a riscos;
* Manutenção de riscos acima do nível aceitável;
* A identificação, análise e avaliação de riscos é executada de maneira assistemática ou sob demanda;
* Prioridades e estratégias organizacionais não são estabelecidas com a conscientização dos riscos que envolvem cada curso de ação;
* Desconhecimento acerca dos riscos a que a organização está exposta (operacionais, de imagem, legais, orçamentários, etc.);
* Ocorrência de eventos de riscos evitáveis;
* Perda ou mau aproveitamento de oportunidades.
 |
| Causas | * Implementação de controles internos não fundamentada em gestão de riscos;
* As informações acerca de riscos não são encaminhadas às instâncias decisórias adequadas;
* Não há abordagem padronizada para definir o nível aceitável de riscos;
* O risco é visto como de propriedade das funções de auditoria interna e controle interno;
* A alocação de recursos para a gestão de riscos é inapropriada ou insuficiente, pois faltam: pessoas capacitadas; procedimentos documentados; sistema de gestão da informação; métodos e ferramentas para gerir riscos;
* Processos organizacionais não estão mapeados;
* Cultura organizacional inibe o avanço da maturidade em riscos;
* Deficiência na atuação da auditoria interna.
 |
| Efeitos | * Altos custos de manutenção de controles sem os benefícios esperados;
* Multas, sanções regulatórias, perda de ativos;
* Danos à imagem institucional;
* Perda de confiança das partes interessadas;
* Aumento do nível de incerteza associado ao alcance dos objetivos da organização;
* Baixa capacidade de resiliência da organização.
* Assunção de postura meramente reativa ao ambiente organizacional
 |
| Subquestão 2114: Os riscos considerados críticos para a organização são geridos? |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Respostas da organização às questões 2111 (especialmente a letra f) e 2113
 | Painel de indicadores do iGG |
| 1. Relatórios de auditoria interna resultantes de trabalhos de avaliação e de consultoria, nos últimos dois anos, que abordem a gestão e reporte de riscos críticos da organização
 | Auditoria interna |
| 1. Incidentes de riscos relevantes nos últimos dois anos
 | Registro de incidentes de risco; segunda linha; auditoria interna; gestores; auditoria externa; OGS; site da organização; site de entes reguladores; mídia; pesquisa integrada do TCU |
| 1. Lista de riscos analisados como críticos (alto nível inerente, alto potencial de impacto nas operações e nos resultados). (obs: o escopo para essa matriz não contempla riscos financeiros e pode ser delimitado de acordo com o porte da organização e a análise da questão 2113);
 | Registro de riscos organizacionais/corporativos (o escopo não contempla riscos financeiros e pode ser delimitado de acordo com o porte da organização) |
| 1. Método de análise utilizado, descrição dos controles existentes
 | Manual de gestão de riscos da organização; documentação da etapa de análise e avaliação de riscos |
| 1. Gestores dos riscos analisados como críticos, respostas selecionadas e responsáveis pela implementação e pelo monitoramento, forma e periodicidade de reporte
 | Planos de tratamento dos riscos críticos  |
| 1. Forma de participação dos responsáveis pelo tratamento dos riscos no processo de escolha das respostas aos riscos
 | Política e manual de gestão de riscos |
| 1. Reportes acerca de riscos críticos emitidos no último ano
 | Relatórios de riscos críticos apresentados à alta administração e/ou conselho ou colegiado superior no último ano; atas das reuniões da alta administração e/ou conselho ou colegiado superior nas quais os riscos críticos foram discutidos |
| Procedimentos | 1. Verificar as respostas da organização às questões 2111 e 2113. Se a organização estiver no nível inexpressivo ou inicial na 2111 e/ou na 2113, não se justifica aprofundar a análise da 2114, pois não haverá confiabilidade de que o sistema de gestão de riscos consegue identificar e gerenciar riscos críticos;
2. Analisar os relatórios dos dois últimos anos de auditoria interna resultantes de trabalhos de avaliação e de consultoria relacionados à gestão e reporte de riscos críticos da organização, para levantamento de informações;
3. Verificar se há registro dos riscos prioritários, aqueles com alto grau de severidade, com alto impacto potencial nas operações e nos resultados, com descrição das causas, eventos e efeitos, níveis calculados;
4. Analisar se os controles existentes foram considerados para cálculo de níveis;
5. Verificar se nos registros há riscos críticos que permanecem com alto nível residual;
6. Analisar a documentação da etapa de avaliação para identificar se há justificativa das respostas escolhidas, e se os responsáveis pelo tratamento participam do processo de escolha;
7. Verificar se há planos de tratamento, com identificação de gestores, ações propostas e responsáveis pela implementação e formas de monitoramento;
8. Verificar se foram definidos requisitos de reporte das informações acerca de riscos críticos;
9. Analisar atas de reuniões do conselho e reportes de riscos críticos, para verificar se a alta administração e o conselho recebem relatórios periódicos acerca da gestão de riscos críticos.
10. Levantar incidentes de riscos relevantes ocorridos nos últimos dois anos evidenciados em relatórios ou expostos na mídia. Para identificar os efeitos, como incidentes de riscos, podem ser necessárias pesquisas adicionais.
 |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Se há registro abrangente de riscos críticos da organização;
* Se há plano de tratamento para riscos críticos contendo elementos necessários à implementação e monitoramento;
* Se a alta administração e o conselho recebem relatórios periódicos acerca da gestão de riscos críticos.
 |
| Possíveis achados |
| Eventos de risco  | * Ausência de informações claras, confiáveis e relevantes sobre os riscos mais significativos e como eles estão sendo gerenciados;
* Planos de tratamento de riscos críticos sem os elementos necessários à eficácia da implementação e ao monitoramento;
* Deficiência de reporte dos riscos críticos;
* Interrupção ou descontinuidade das atividades organizacionais;
* Recorrência de incidentes de risco;
* Tomada de decisões críticas não orientadas a riscos;
* Perfil de risco mantido fora da capacidade de risco da organização.
 |
| Causas | * Processo de gestão de riscos não implementado;
* Excesso de riscos classificados como críticos;
* Gerenciamento de riscos voltado apenas aos riscos operacionais ou da área meio;
* Falta de padronização de reporte para questões de gestão de riscos ou excesso de informações nos reportes;
* Falta de abordagem padronizada para definir o nível aceitável de riscos ou simplificação excessiva do método de cálculo;
* A alocação de recursos para a gestão de riscos é inapropriada ou insuficiente, pois faltam: pessoas capacitadas; procedimentos documentados; sistema de gestão da informação; métodos e ferramentas para gerir riscos;
* Processos e projetos relevantes não estão identificados e/ou não são rotineiramente avaliados quanto a risco;
* Cultura organizacional inibe o avanço da maturidade em riscos;
* Deficiência na atuação da auditoria interna.
 |
| Efeitos | * Danos à imagem institucional e perda de ativos;
* Aumento do nível de incerteza associado ao alcance dos objetivos estratégicos da organização;
* Baixa capacidade de resiliência da organização.
* Desperdício de recursos
* Antieconomicidade
* Sujeição a intempéries que poderiam ter sido previstas e evitadas
* Deficiências organizacionais persistentes ao longo do tempo
* Deficiências organizacionais já conhecidas sujeitam a organização a crises periódicas
 |
| Subquestão 2115: A organização executa processo de gestão de continuidade do negócio? |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Respostas da organização às questões 2111 (especialmente a letra f) e 2113
 | Painel de indicadores do iGG |
| 1. política institucional de gestão de continuidade do negócio (PGCN) e nível de aprovação
 | Comitê de gestão de risco, outras instâncias de segunda linha, área de gestão de TI  |
| 1. processo de gestão de continuidade do negócio formalizado
 | Comitê de gestão de risco, outras instâncias de segunda linha, área de gestão de TI |
| 1. plano de continuidade do negócio (PCN) e nível de aprovação
 | Comitê de gestão de risco, outras instâncias de segunda linha, área de gestão de TI |
| 1. análises de impacto sobre o negócio (Business Impact Analysis – BIA) realizadas sobre os processos organizacionais críticos
 | Documentação de análise e avaliação de riscos de processos críticos; registro de análises de impacto de negócio |
| 1. treinamentos realizados para execução dos planos de recuperação nos últimos dois anos (p. ex.: simulações; testes de comunicação; campanhas de conscientização)
 | Plano de continuidade do negócio; planos de treinamento; registros de treinamentos realizados; relatórios de treinamentos  |
| 1. há previsão de revisão periódica do PCN
 | Política institucional de gestão de continuidade do negócio; plano de continuidade do negócio |
| Procedimentos | 1. Verificar as respostas da organização às questões 2111 letra f e 2113. Se a organização estiver no nível inexpressivo ou inicial na 2113 e/ou 2111 e/ou se não tiver marcado a letra f da 2111, não se justifica aprofundar a análise da 2115, pois não há processo de gestão de riscos estabelecido.
2. Verificar se há política institucional de gestão de continuidade do negócio (PGCN) aprovada pela alta administração;
3. Verificar se a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo de gestão de continuidade de negócio; definiu papéis e atribuiu responsabilidades;
4. Verificar se há plano de continuidade do negócio (PCN) aprovado pela alta administração, se o documento prevê a realização de treinamentos anuais, e reflete a estrutura atual da organização;
5. Verificar se há previa análise de impacto sobre o negócio (Business Impact Analysis – BIA) realizadas sobre os processos organizacionais críticos. O IIA (Guia prático: gestão de continuidade de negócios, 2008) orienta que a BIA permite identificar processos de negócios que sejam essenciais para manter a unidade de negócios em funcionamento durante um desastre e determinar em quanto tempo esses processos integrais devem ser recuperados após um desastre e qual o nível satisfatório de recuperação;
6. Se há exercícios/treinamentos (ao menos uma vez ao ano) para preparação da equipe de recuperação.
 |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Se há diretrizes estabelecidas pela liderança da organização para orientar e patrocinar o processo de gestão de continuidade de negócios;
* Se o processo de gestão de continuidade de negócios foi implantado: definição de papeis e atribuição de responsabilidades; PCN atualizado, baseado em gestão de riscos e em análise de impacto; com revisão periódica; e as equipes envolvidas na execução do PCN são treinadas periodicamente.
 |
| Possíveis achados |
| Eventos de risco  | * Desconhecimento acerca do nível atual de risco de continuidade de negócio;
* Existência de risco inaceitável para a continuidade de negócios e não informado às partes interessadas;
* Perda de: vidas humanas; redes de abastecimento; sistemas de TI; instalações e equipamentos; linhas de comunicação;
* Recorrência de incidentes de risco.
 |
| Causas | * Processos e projetos críticos não estão identificados e/ou não são rotineiramente avaliados quanto a risco;
* Ausência ou deficiência de processo de gestão de riscos na organização;
* Deficiência na atuação da auditoria interna;
* Falta de apoio da liderança da organização ao programa de gestão de continuidade de negócios;
* A alocação de recursos para programa de gestão de continuidade de negócios é inapropriada ou insuficiente.
 |
| Efeitos | * Interrupção ou descontinuidade das atividades organizacionais;
* Incapacidade ou baixa capacidade de restaurar processos críticos de negócios impactados por eventos disruptivos (p. ex.: incêndios, pandemias, terremotos, inundações, terrorismo, falhas de serviços essenciais e na rede de abastecimento, greves trabalhistas).
* Danos à imagem institucional.
* Perda da agregação de valor para as partes interessadas dependentes das atividades organizacionais
 |

|  |
| --- |
| PRÁTICA 2120: A estratégia está estabelecida? |
| Conteúdo da prática |
| Esclarecimentos  | Consulte a página 77 do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | Consulte as questões da prática 2120 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências (questões 2121, 2122 e 2123)
 | Painel de indicadores do iGG |
| 1. Respostas da organização às questões 3122 e 4413 do questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Modelo de gestão da estratégia da organização
 | Normativos que tratam do planejamento estratégico; sistema corporativo; Unidade de Gestão Estratégica; Comitê de governança (Consultar as referências dessa prática, pois há regras de alinhamento para o Poder Executivo e Judiciário) |
| 1. Objetivos, indicadores e metas do plano estratégico
 | Plano estratégico organizacional |
| 1. Locais de publicação do plano estratégico organizacional e relatórios de acompanhamento da execução
 | Site da organização; site de órgãos governantes superiores; Unidade de Gestão Estratégica; Comitê de governança |
| 1. Objetivos, indicadores, metas, ações, programas e projetos do Plano Estratégico de TI, caso houver
 | Plano Estratégico de TI, caso houver |
| 1. Ações, projetos, indicadores e metas do plano diretor de tecnologia da informação (PDTI)
 | PDTI |
| 1. Políticas públicas de responsabilidade da organização ou nas quais a organização esteja envolvida
 | PPA; Planos setoriais; estratégias nacionais; site da organização; site de órgãos governantes superiores; Unidade de Gestão Estratégica; Comitê de governança (obs: nas referências dessa prática são citados alguns exemplos de políticas públicas do Poder Judiciário). |
| 1. Diretrizes de órgãos governantes superiores (OGS) para o planejamento estratégico organizacional
 | Planos setoriais; estratégias nacionais; guias; normativos; site de órgãos governantes superiores; Unidade de Gestão Estratégica; Comitê de governança (Consultar as referências dessa prática, pois há regras de alinhamento para o Poder Executivo e Judiciário) |
| Procedimentos | 1. Analisar as respostas da organização às questões 2121, 2122, 2123, 3122 e 4413 do questionário do iGG. Essas questões trazem as declarações da organização acerca da definição do modelo de gestão da estratégia, da estratégia e de metas de transformação digital; da publicação dos extratos dos planos e relatórios de acompanhamento na internet, e da consideração de orçamento na formulação da estratégia. As respostas a essas questões poderão corroborar as análises.
2. Verificar se o normativo ou política que trata do modelo de gestão da estratégia da organização contempla:
3. as fases de formulação, monitoramento, avaliação e comunicação da estratégia;
4. integração do processo de gestão de riscos à formulação da estratégia;
5. obrigatoriedade de que sejam considerados, no processo de formulação, diretrizes dos órgãos governantes superiores e as políticas públicas de responsabilidade ou nas quais a organização esteja envolvida;
6. conteúdo mínimo do plano estratégico organizacional: objetivos, orçamentos, indicadores (com as linhas de base e as periodicidades de aferição) e metas quantificáveis; responsabilidades dos envolvidos na formulação e gestão da estratégia;
7. publicação dos extratos dos planos e dos extratos dos relatórios de acompanhamento na internet (ressalvados casos de sigilo)
8. Atenção: para as organizações do Poder Executivo federal, o planejamento estratégico organizacional deve conter, pelo menos, os seguintes elementos (Guia Técnico de Gestão Estratégica v1.0 – Governo Federal):
9. cadeia de valor e mapa estratégico da instituição;
10. definição da missão, da visão e dos valores da instituição;
11. objetivos estratégicos;
12. indicadores, com seus atributos: fórmula de cálculo, periodicidade de medição, linha de base e metas;
13. projetos estratégicos a serem desenvolvidos, com seus atributos: entregas, com prazos e unidade responsável.
14. Analisar se o plano estratégico organizacional é composto dos elementos mínimos: objetivos; responsáveis (pessoa ou unidade) por sua coordenação; responsabilidades das organizações ou unidades (internas ou externas) que contribuem para o alcance de cada objetivo; orçamentos relacionados aos objetivos; indicadores (com as linhas de base e as periodicidades de aferição); e metas quantificáveis.
15. Verificar se o plano e último relatório de acompanhamento está publicado na internet.
16. Levantar informações acerca das políticas públicas de responsabilidade da organização ou nas quais a organização esteja envolvida, e sobre diretrizes de OGS (p. ex. estratégias, guias, normativos. Ver referências dessa prática, pois há regras de alinhamento para o Poder Executivo e Judiciário). Confrontar com os objetivos estratégicos, para avaliar se a estratégia contempla as políticas públicas e mecanismos de articulação e coordenação das ações que envolvam outras organizações, além das prioridades definidas por OGS.
17. Verificar se o plano estratégico organizacional, o Plano Estratégico de TI ou o PDTI contemplam metas de transformação digital:
18. metas para a ampliação da oferta de serviços públicos prestados em meio digital;
19. quando aplicável, metas com vistas à eliminação da exigência de atestados, certidões ou outros documentos comprobatórios que constem em base de dados oficial da administração pública federal, como condição para a prestação de serviços;
20. quando aplicável, metas no sentido de reduzir a necessidade de atendimento presencial dos usuários;
21. metas voltadas à melhoria e ao incremento da atuação integrada e sistêmica com outros órgãos e entidades dos quais dependa ou com os quais interaja intensivamente na prestação dos serviços públicos;
22. metas com vistas a otimizar o uso de múltiplos canais de atendimento;

observação: as metas podem estar relacionadas num Plano Digital, documento que contêm a lista dos serviços prestados pela organização, o nível de digitalização de cada serviço e, nos casos de serviços parcial ou totalmente não digitais, decisão para a transformação, forma e previsão de implementação. |
| O que a análise vai permitir dizer | * Se o grau declarado (no questionário do iGG) acerca da adoção da prática na organização é real e as possíveis lacunas na implementação;
* Se há modelo de gestão da estratégia estabelecido para a organização;
* Se a estratégia da organização está definida e atualizada com as diretrizes e prioridades estabelecidas pelos órgãos governantes superiores e com os planos governamentais;
* Se a organização definiu metas de transformação digital.
 |
| Possíveis achados |
| Eventos de risco  | * Plano estratégico organizacional não contempla elementos mínimos necessários ao monitoramento e avaliação da implementação;
* Prioridades e estratégias organizacionais não são estabelecidas com a devida conscientização dos riscos e oportunidades;
* Estratégia desalinhada às diretrizes de Governo e de Estado (p. ex.: PPA 2020-2023, estratégias nacionais, setoriais e regionais; diretrizes dos órgãos governantes superiores);
* Estratégia não considera políticas públicas de responsabilidade da organização ou nas quais a organização esteja envolvida;
* Estratégia não comunicada às partes interessadas internas e externas;
* Estratégia desalinhada com a cadeia de valor e com a Missão, Visão e Valores da Organização
* A “transformação digital” é tratada em aspectos abstratos, mas o PDTI não prioriza projetos e ações para a efetiva “transformação digital” da organização.
 |
| Causas | * Modelo de gestão da estratégia não contempla as fases do planejamento estratégico e/ou os elementos mínimos preconizados nas boas práticas;
* Processo de gestão de riscos não definido e/ou não implementado;
* Cultura de baixa interação com outras organizações públicas;
* Processo de planejamento estratégico não contempla etapa de identificação de políticas públicas e de diretrizes superiores;
* Processo de planejamento estratégico visto como burocrático e sem utilidade prática;
* Desenvolvimento de cultura que inibe a transparência e participação social;
* Liderança não comprometida com a melhoria dos serviços prestados aos cidadãos;
* Ausência de envolvimento das partes interessadas na concepção da estratégia
 |
| Efeitos | * Impossibilidade de monitorar a execução da estratégia;
* Sobreposição de esforços e lacunas da atuação governamental;
* Emprego de recursos organizacionais em programas e projetos não prioritários;
* Restrição à *Accountability* e transparência da organização;
* Baixa capacidade de atender necessidades e expectativas dos cidadãos relacionadas com: ampliação de serviços públicos prestados em meio digital, diminuição da burocracia governamental (simplificação) e maior agilidade na prestação de serviços;
* Dano à imagem, reputação e credibilidade da organização.
 |

|  |
| --- |
| PRÁTICA 2130: A organização promove a gestão estratégica?\*\*Observação: as análises podem ser feitas também por área (TI, contratações e pessoas), basta acessar as matrizes que estão no grupo de cada área. |
| Conteúdo da prática |
| Esclarecimentos  | Consulte a página 81 do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | Consulte as questões da prática 2130 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências (questões 2131 a 2135)
 | Painel de indicadores do iGG |
| 1. Funções finalísticas e de suporte identificadas na organização
 | Normativos internos; cadeia de valor |
| 1. Nomes e contatos dos gestores das áreas finalísticas e de suporte
 | Área de gestão de pessoas; site da organização |
| 1. Diretrizes, papéis e responsabilidades para a gestão dos processos finalísticos
 | Normativos internos; políticas internas; planos diretores; comitês do conselho (pessoas, TI, gestão estratégia, governança) |
| 1. Diretrizes, papéis e responsabilidades da área de gestão de pessoas
 |
| 1. Diretrizes, papéis e responsabilidades da área de gestão de tecnologia da informação
 |
| 1. Diretrizes, papéis e responsabilidades da área de gestão de contratações
 |
| 1. Diretrizes, papéis e responsabilidades para a gestão orçamentária e financeira
 |
| 1. Diretrizes para o planejamento estratégico
 | Normas sobre o planejamento estratégico; normas sobre o planejamento das áreas de gestão; mapa do processo de planejamento estratégico |
| 1. objetivos, indicadores e metas para a gestão dos processos finalísticos
 | Plano estratégico organizacional; mapas estratégicos; planos estratégicos das áreas de gestão; painel de indicadores estratégicos; acordos de níveis de serviço entre as unidades de suporte e as unidades de negócio |
| 1. objetivos, indicadores e metas para a gestão de pessoas
 |
| 1. objetivos, indicadores e metas para a gestão de tecnologia da informação
 |
| 1. objetivos, indicadores e metas para a gestão de contratações
 |
| 1. objetivos, indicadores e metas para a gestão orçamentária e financeira
 |
| Procedimentos | 1. Verificar se estão identificadas as unidades ou funções finalísticas e as de suporte;
2. Verificar se há modelo de gestão, estabelecido pela alta administração, por meio políticas internas e/ou conjunto de normas que orientem a gestão das áreas finalísticas e de suporte (pode ser selecionada amostra não estatística), contemplando:
	1. diretrizes para o planejamento articulado com o planejamento das demais unidades e com o processo de planejamento organizacional;
	2. diretrizes para a integração do processo de gestão de riscos às áreas de gestão;
	3. papéis e responsabilidades das áreas de gestão;
	4. orientações acerca da tomada de decisões críticas (como p. ex.: as relacionadas a questões estratégicas; a início e descontinuidade de projetos; a investimentos e desinvestimentos, a definição de apetite a risco).
3. Verificar se objetivos das áreas de gestão estão relacionados aos estratégicos (pode ser selecionada amostra), se há indicadores (com linhas de base e periodicidade de aferição), metas quantificáveis para as áreas de gestão e responsáveis pelas rotinas de monitoramento, e se essas informações estão disponíveis em meio de comunicação eletrônico acessível às partes interessadas;
4. Aplicar questionário aos gestores de áreas finalísticas e de suporte para avaliar percepção acerca do propósito da unidade, seus objetivos e metas, e da correlação com as prioridades da organização.
 |
| O que a análise vai permitir dizer | * Se está estabelecido na organização um conjunto de diretrizes, princípios e regras claras quanto à gestão diária das operações;
* Se a há diretrizes para que o planejamento das áreas de gestão suporte a estratégia organizacional;
* Se foram estabelecidos os critérios para o monitoramento do desempenho das funções de gestão.
 |
| Possíveis achados |
| Eventos de risco  | * Operação diária dos processos de gestão realizada sem critérios claros e objetivos de qualidade, desempenho e otimização de riscos;
* Baixa articulação entre formulação e implementação da estratégia;
* Tomadas de decisão sobre alocação de recursos, projetos e ações das áreas de suporte não alinhadas às estratégias do negócio;
* Tomadas de decisão sobre alocação de recursos, projetos e ações das áreas de negócio não alinhadas à estratégia organizacional;
* Tomadas de decisão sobre alocação de recursos, projetos e ações das áreas de gestão dominada por gestores com maior “poder político”;
* Emprego de recursos organizacionais em ações e projetos não prioritários;
* Desperdício de recursos em contratações, projetos e ações que não atendem às necessidades organizacionais;
* Desmotivação dos gestores e dos colaboradores, que não compreendem como suas atividades contribuem para os resultados organizacionais.
 |
| Causas | * Processo de planejamento estratégico visto como burocrático e sem utilidade prática;
* Planejamento das áreas de gestão realizado de forma não controlada, ad hoc;
* Modelo de gestão estratégica da organização não estabelecido;
* Falta de clareza na codificação e na comunicação da estratégia organizacional;
* Cultura de baixa interação entre as unidades organizacionais.
 |
| Efeitos | * Impossibilidade de monitorar o desempenho das áreas de gestão;
* Estratégia meramente formal, sem impacto no dia-a-dia da organização, como o reconhecimento dos colaboradores com base nos valores organizacionais e a definição de projetos/atividades com base em diretrizes estratégicas;
* Baixa capacidade de identificar desvios na implementação da estratégia organizacional ou necessidades de mudança da estratégia;
* Sobreposição de esforços e existência de lacunas na atuação das unidades organizacionais;
* Incoerências entre os processos e atividades das unidades organizacionais;
* Baixa capacidade de atender as demandas das partes interessadas;
* Dano à imagem, reputação e credibilidade da organização.
 |

|  |
| --- |
| PRÁTICA 2140: Os resultados organizacionais são monitorados? |
| Conteúdo da prática |
| Esclarecimentos  | Consulte a página 83 do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | Consulte as questões da prática 2140 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Resposta da organização à questão 2120 do questionário do iGG
 |
| 1. Indicadores definidos para acompanhar o progresso dos objetivos estratégicos: descrição e finalidade; método de cálculo; fontes de dados; linha de base (quando aplicável); periodicidade da apuração; dimensão da avaliação (economicidade, eficiência, eficácia, efetividade); meta para o período; agente ou unidade responsável pela coleta dos dados e pelo cálculo do indicador.
 | Plano de monitoramento da estratégia; painéis de informação; outros sistemas informatizados para acompanhamento dos indicadores.  |
| 1. Rotinas, procedimentos e processos de trabalho estabelecidos para monitoramento contínuo da estratégia.
 | Unidade de Gestão Estratégica; plano de monitoramento da estratégia; painéis de informação; outros sistemas informatizados para acompanhamento dos indicadores |
| 1. Processo de trabalho estabelecido para avaliação da estratégia: periodicidade, participantes, formas de publicação e destinatários dos relatórios de avaliação.
 | Unidade de Gestão Estratégica (UGE); atas de reuniões de avaliação da estratégia; site da organização |
| Procedimentos | 1. Analisar a resposta da organização à questão 2120 do questionário do iGG. Essa questão trata da definição da estratégica, com indicadores e metas. É uma condição para que haja monitoramento da implementação da estratégia. Se a resposta a essa questão for negativa, é provável que a resposta à 2140 também seja. Basta então confirmar com a organização se a situação declarada persiste. Nesse caso, não há necessidade de aprofundar as análises
2. Verificar se:
	1. há indicadores de eficácia, eficiência e efetividade, com os requisitos de implementação;
	2. os indicadores estão implantados (há coleta e análise dos dados necessários à medição de desempenho);
	3. há rotinas, procedimentos ou processos estabelecidos para monitoramento e para a avaliação da estratégia, com indicação de periodicidade; formas de apresentação e comunicação dos resultados; responsáveis pela elaboração dos relatórios; destinatários da informação;
	4. os relatórios de avaliação estão disponíveis às partes interessadas internas e externas.
 |
| O que a análise vai permitir dizer | * Se os indicadores definidos possuem os requisitos mínimos para avaliar eficácia e efetividade da estratégia, e eficiência dos principais processos pelos quais a estratégia é implementada;
* Se os indicadores estão implantados;
* Se há rotinas, procedimentos ou processos estabelecidos para monitorar a implementação da estratégia organizacional;
* Se os resultados do monitoramento são utilizados para avaliar a estratégia;
* Se os relatórios de avaliação da estratégia estão disponíveis às partes interessadas internas e externas.
 |
| Possíveis achados |
| Eventos de risco  | * Ausência/deficiência de indicadores para medir o progresso do alcance dos objetivos estratégicos (não foram definidos os requisitos necessários à implantação desses indicadores);
* Indicadores foram definidos e possuem requisitos mínimos de implantação, mas não foram implantados (não há rotinas de monitoramento);
* Monitoramento da estratégia planejado e executado pela UGE, sem participação de representantes das demais unidades organizacionais;
* Informações do monitoramento não são comunicadas às instâncias competentes para viabilizar a correção de desvios ou não são comunicadas de forma tempestiva (p. ex.: Poder Executivo prevê relatórios gerenciais mensais aos níveis tático e operacional);
* Periodicidade das reuniões de avaliação da estratégia (RAEs) inadequada para o acompanhamento efetivo (p. ex.: Poder Executivo prevê reuniões trimestrais; Poder Judiciário prevê RAEs quadrimestrais);
* Relatórios de acompanhamento do plano estratégico organizacional não disponíveis às partes interessadas.
 |
| Causas | * Processo de planejamento estratégico visto como burocrático e sem utilidade prática;
* Baixo nível de automatização das rotinas de monitoramento;
* Falta de clareza na codificação e na comunicação da estratégia organizacional;
* Desenvolvimento de cultura que inibe a transparência e participação social;
* Baixo nível de engajamento da liderança e dos gestores com o processo de gestão estratégica.
 |
| Efeitos | * Baixa capacidade de identificar desvios na implementação da estratégia organizacional ou necessidades de mudança da estratégia;
* Desconhecimento acerca do desempenho organizacional;
* Restrição à *accountability* e transparência da organização;
* Baixa capacidade de entregar resultados pretendidos pelas partes interessadas;
* Dano à imagem, reputação e credibilidade da organização;
* Não identificação de necessidades de realocação de recursos para alcance dos resultados esperados.
 |

|  |
| --- |
| PRÁTICA 2150: A liderança monitora o desempenho das funções de gestão?\*Observação: as análises podem ser feitas também por área (TI, contratações e pessoas), basta acessar as matrizes que estão no grupo de cada área. |
| Conteúdo da prática |
| Esclarecimentos  | Consulte a página 86 do Referencial Básico de Governança Organizacional 3ª edição: ([LINK PARA O REFERENCIAL](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799)) |
| Aspectos avaliados | Consulte as questões da prática 2150 do questionário de governança: ([LINK PARA O QUESTIONÁRIO](https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E73726BD201742591477D595B)) |
| Glossário | Consulte, no glossário, os verbetes aplicáveis a esta prática: ([LINK PARA O GLOSSÁRIO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/)) |
| Relação com o Relatório de Gestão | Consulte o documento “Práticas x Conteúdo do relatório de gestão”: ([LINK PARA O DOCUMENTO](https://portal.tcu.gov.br/governanca/governancapublica/organizacional/auditoria-de-governanca/matrizes-de-auditoria.htm)) |
| Matriz de Planejamento |
| Critérios | [LINK PARA QRN](http://www.tcu.gov.br/govorganizacional/) |
| Informações requeridas e respectivas fontes | **Informações requeridas** | **Fontes de informação** |
| 1. Declaração de aderência à prática informada no questionário do iGG e evidências
 | Painel de indicadores do iGG |
| 1. Resposta da organização à questão 2130 do questionário do iGG
 |
| 1. Indicadores definidos para acompanhar o progresso dos objetivos dos processos de gestão: descrição e finalidade; método de cálculo; fontes de dados; linha de base (quando aplicável); periodicidade da apuração; dimensão da avaliação (economicidade, eficiência, eficácia, efetividade); meta para o período; agente ou unidade responsável pela coleta dos dados e pelo cálculo do indicador.
 | Unidade de Gestão Estratégica; plano de monitoramento da estratégia; painéis de informação; outros sistemas informatizados para acompanhamento dos indicadores |
| 1. Rotinas, procedimentos e processos de trabalho estabelecidos para monitoramento contínuo das estratégias de gestão.
 |
| 1. Último relatório de monitoramento, forma de divulgação, destinatários das informações.
 |
| 1. Ata de reunião das duas últimas reuniões de avaliação da estratégia (RAEs)
 | Unidade de Gestão Estratégica |
| Procedimentos | 1. Analisar a resposta da organização à questão 2130 do questionário do iGG. Essa questão trata do modelo de gestão estratégica. É uma condição para que haja monitoramento dos resultados da gestão. Se a resposta a essa questão for negativa, é provável que a resposta à 2150 também seja. Basta então confirmar com a organização se a situação declarada persiste. Nesse caso, não há necessidade de aprofundar as análises.
2. Verificar se:
	1. há rotinas, procedimentos ou processos estabelecidos para monitoramento do desempenho da gestão, com indicação de periodicidade; formas de apresentação e comunicação dos resultados; responsáveis pela elaboração dos relatórios; destinatários da informação; previsão para que os dados do monitoramento alimentem a avaliação da estratégia;
	2. os indicadores das estratégias de gestão estão implantados (pode ser selecionada amostra dos processos da cadeia de valor);
	3. os relatórios de monitoramento são elaborados com a periodicidade adequada e estão disponíveis aos dirigentes (o Poder Executivo prevê relatórios gerenciais mensais para os níveis tático e operacional);
	4. As RAEs utilizam os resultados do monitoramento contínuo como subsídio à avaliação da estratégia.
 |
| O que a análise vai permitir dizer | * Se os indicadores de medição de desempenho da gestão estão implementados;
* Se há rotinas, procedimentos ou processos estabelecidos para monitorar o desempenho da gestão;
* Se os relatórios de monitoramento estão disponíveis aos dirigentes;
* Se os resultados do monitoramento são utilizados para avaliar a estratégia.
 |
| Possíveis achados |
| Eventos de risco  | * Ausência/deficiência de indicadores para medir o progresso do alcance dos objetivos de gestão (não foram definidos os requisitos necessários à implantação desses indicadores);
* Indicadores foram definidos e possuem requisitos mínimos de implantação, mas não foram implantados (não há rotinas de monitoramento);
* Monitoramento da estratégia planejado e executado pela UGE, sem participação de representantes das demais unidades organizacionais;
* Informações do monitoramento não são comunicadas às instâncias competentes para viabilizar a correção de desvios ou não são comunicadas de forma tempestiva;
* Reuniões de avaliação da estratégia (RAEs) não consideram os resultados do monitoramento.
 |
| Causas | * Modelo de gestão estratégica não estabelecido (objetivos, indicadores e metas das unidades de negócio e de suporte não definidos);
* Processo de planejamento estratégico visto como burocrático e sem utilidade prática;
* Baixo nível de automatização das rotinas de monitoramento;
* Falta de clareza na codificação e na comunicação da estratégia organizacional;
* Baixo nível de engajamento da liderança e dos gestores com o processo de gestão estratégica.
 |
| Efeitos | * Baixa capacidade de identificar desvios na implementação da estratégia organizacional ou necessidades de mudança da estratégia;
* Desconhecimento acerca do desempenho das funções de gestão;
* Baixa capacidade de entregar resultados pretendidos pelas partes interessadas;
* Dano à imagem, reputação e credibilidade da organização.
 |