**APÊNDICE II – MATRIZ DE PLANEJAMENTO**

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

| **QUESTÕES DE AUDITORIA** | **INFORMAÇÕES REQUERIDAS** | **FONTES DE INFORMAÇÃO** | **PROCEDIMENTOS DE COLETA DE DADOS** | **PROCEDIMENTOS DE ANÁLISE DE DADOS** | **O QUE A ANÁLISE VAI PERMITIR DIZER (CONCLUSÕES A CHEGAR)** | |
| --- | --- | --- | --- | --- | --- | --- |
| **1. AMBIENTE**  Nesta dimensão, o objetivo da equipe de auditoria é avaliar as capacidades existentes na organização, em termos de **liderança**, **políticas & estratégias** e preparo das **pessoas**, incluindo aspectos relacionados com a *cultura*, a *governança de riscos* e a *consideração do risco na definição da estratégia e dos objetivos* em todos os níveis, para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento da missão institucional na geração de valor para as partes interessadas. | | | | | | |
| **1.1. – Liderança**[[1]](#footnote-1)  Em que medida os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos e cultura? | | | | | A análise das subquestões 1.1.1 a 1.1.3 deve permitir à equipe concluir se os responsáveis pela governança e a alta administração assumem um compromisso forte e sustentado e exercem supervisão para obter comprometimento com a gestão de riscos em todos os níveis da organização, promovendo-a e dando suporte, de modo que possam ter uma expectativa razoável de que no cumprimento da missão institucional, a organização entende e é capaz de gerenciar os riscos associados à sua estratégia para atingir seus objetivos de gerar valor para as partes interessadas, tendo o cidadão e a sociedade como vetores principais. | |
| **Cultura**  1.1.1. A alta administração e os responsáveis pela governança reconhecem a importância da cultura, da integridade, dos valores éticos e da consciência de riscos como aspectos-chaves para o reforço da *accountability*? |  | Estes campos devem ser preenchidos pela equipe de auditoria, seguindo as orientações constantes do tópico **Elaboração da Matriz de Planejamento** do Roteiro. |  |  | * Se a alta administração e os responsáveis pela governança fornecem normas, orientações e supervisionam as questões afetas a cultura, integridade, valores éticos e consciência de riscos. * Se as questões relacionadas a cultura, integridade, valores éticos e consciência de riscos integram o conteúdo de cursos e programas voltados para o desenvolvimento de gestores. * Se a alta administração e os responsáveis pela governança reforçam o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização. * Se estão instituídos programas, políticas ou outras medidas que definem os padrões de comportamento desejáveis, tais como códigos de ética e de conduta, canais de denúncia e de comunicação para cima, ouvidoria, avaliações de aderência aos padrões de integridade e valores éticos. | |
| **Governança de riscos**  1.1.2. Existem estruturas e processos definidos para apoiar as responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão? |  |  |  |  | * Se existem instâncias internas de apoio à governança de riscos, tais como comitês de governança, riscos e controles; auditoria interna; coordenação central da gestão corporativa de riscos. * Se as instâncias internas de apoio à governança de riscos exercem suas atribuições mediante uma abordagem planejada, sistemática e disciplinada. * Se a gestão de riscos é integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades[[2]](#footnote-2) relevantes para o alcance dos objetivos-chaves da organização. | |
| **Supervisão da Governança e da alta administração**  1.1.3. Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos? |  |  |  |  | * Se os processos de governança e gestão incorporam explicitamente indicadores-chaves de risco e indicadores-chaves de desempenho, monitorados regularmente. * Se o órgão de governança e a alta administração são notificados de modo regular e oportuno sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos. * Se o órgão de governança faz uma revisão sistemática da visão de portfólio dos riscos em contraste com o apetite a riscos, fornecendo direção clara para gerenciamento dos riscos. * Se o órgão de governança e a alta administração utilizam os serviços da auditoria interna e de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controles. * Se o órgão de governança definiu um nível de maturidade almejado para a gestão de riscos e monitora o progresso das ações para atingir ou manter-se no nível definido. | |
| **1.2. – Políticas e estratégias**  Em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática? | | | | | A análise das subquestões 1.2.1 a 1.2.7 deve permitir à equipe concluir se a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira que o risco seja considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e gerenciado nas operações, funções e atividades relevantes das diversas partes da organização. | |
| **Direcionamento estratégico**  1.2.1. A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico? |  |  |  |  | * Se alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico traduzido nos objetivos-chaves, na missão, na visão e valores fundamentais da organização. * Se o direcionamento estratégico é alinhado com as finalidades e competências legais da entidade. * Se o direcionamento estratégico fornece uma base suficiente para a definição da estratégia e a fixação dos objetivos estratégicos e de negócios, traduzindo uma expressão inicial do risco aceitável (apetite a risco) para o gerenciamento dos riscos relacionados. | |
| 1.2.2. A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o *apetite a risco*? |  |  |  |  | * Se a alta administração, com a supervisão e a concordância do órgão de governança, define, comunica, monitora e revisa o apetite a risco na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas. * Se a expressão do apetite a risco fornece uma base consistente para orientar a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco. | |
| **Integração da gestão de riscos ao processo de planejamento**  1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos? |  |  |  |  | * Se os objetivos estratégicos de alto nível são alinhados e dão suporte à missão, à visão e aos propósitos da organização, e se são estabelecidos em consistência com o direcionamento estratégico e o apetite a risco definidos (subquestões 1.2.1 e 1.2.2), de modo a fornecer uma base consistente para a definição dos objetivos de negócios em todos os níveis da organização. * Se são consideradas as várias alternativas de cenários e os riscos associados na definição dos objetivos estratégicos e na seleção das estratégias para atingi-los. * Se os objetivos de negócios específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho) são definidos alinhados aos objetivos estratégicos e ao apetite a risco. | |
| 1.2.4. A administração define e comunica os objetivos e as respectivas medidas de desempenho em termos específicos e mensuráveis? |  |  |  |  | * Se a administração define os objetivos de negócios de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, explicitando-os com clareza suficiente, em termos específicos e mensuráveis. * Se a administração define as medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho) para todos os objetivos definidos. * Se os objetivos e as medidas de desempenho são comunicados aos responsáveis, em todos os níveis, de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização. * Se o modo como os objetivos são definidos, explicitados e comunicados permite a identificação e avaliação dos riscos que possam ter impacto no desempenho e no alcance dos objetivos. | |
| **Política de gestão de riscos**  1.2.5. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, apropriadamente comunicada, abordando todos os aspectos relevantes? |  |  |  |  | * Se a alta administração aprovou a política de gestão de riscos e assumiu a liderança no compromisso com a sua implementação. * Se a política de gestão de riscos é apropriadamente comunicada e está disponível para acesso a todos, dentro e fora da organização. * Se a política de gestão de riscos estabelece os princípios e objetivos relevantes da gestão de riscos na organização e as ligações entre os objetivos e políticas da organização com a política de gestão de riscos. * Se a política de gestão de riscos estabelece as diretrizes para a integração da gestão de riscos a todos os processos organizacionais, incluindo o planejamento estratégico, os projetos, as políticas de gestão em todos os níveis da organização e as parcerias com outras organizações. | |
| **Política de gestão de riscos**  (Continuação da questão 1.2.5). |  |  |  |  | * Se a política de gestão de riscos contém uma definição clara de responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas (unidades, departamentos, divisões, processos e atividades), incluindo a implementação e manutenção do processo de gestão de riscos e a asseguração da suficiência, eficácia e eficiência de quaisquer controles. * Se a política de gestão de riscos estabelece diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados, por meio de um plano de implementação do processo de gestão de riscos, em todos os níveis, funções e processos relevantes da organização. * Se a política de gestão de riscos estabelece diretrizes sobre como o desempenho da gestão de riscos, a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política de gestão de riscos, serão medidos e reportados. | |
| **Política de gestão de riscos**  (Continuação da questão 1.2.5). |  |  |  |  | * Se a política de gestão de riscos estabelece atribuição clara de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como diretrizes sobre a forma e a periodicidade como as alterações devem ser efetivadas. | |
| **Comprometimento da gestão**  1.2.6. Toda a gestão da organização é comprometida com a gestão de riscos? |  |  |  |  | * Se a alta administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade. | |
| **Alocação de recursos**  1.2.7. A administração aloca recursos suficientes e apropriados para a gestão riscos? |  |  |  |  | * Se a administração aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas de TI, métodos, treinamento e ferramentas) para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chaves, bem como com a natureza e o nível dos riscos. | |
| **1.3. – Pessoas**  Em que medida as pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los? | | | | | A análise das subquestões 1.3.1 a 1.3.2 deve permitir à equipe concluir se as pessoas na organização estão informadas, habilitadas e autorizadas para exercer os seus papéis e as suas responsabilidades no gerenciamento de riscos e controles; entendem esses papéis e os limites de suas responsabilidades, e como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização. | |
| **Reforço da *accountability***  1.3.1. A gestão transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gerenciamento riscos e o pessoal recebe orientação e capacitação suficiente para exercer essas responsabilidades? |  |  |  |  | * Se todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de cumprir suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes. * Se o pessoal designado para atividades de identificação, avaliação e tratamento de riscos recebe capacitação suficiente para executá-las, inclusive no que diz respeito à identificação de oportunidades e à inovação. | |
| **Estrutura de gerenciamento de riscos e controles**  1.3.2. Os grupos de pessoas que integram as *três linhas de defesa* na estrutura de gerenciamento de riscos e controles por toda a organização têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização? |  |  |  |  | * Se os gestores, que integram a *primeira linha de defesa*:  1. têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e 2. são regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.  * Se o pessoal da *segunda linha de defesa*, que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização:  1. apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade; | |
| **Estrutura de gerenciamento de riscos e controles**  (Continuação da questão 1.3.2). |  |  |  |  | 1. fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos; 2. define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização; 3. estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos; 4. orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la; 5. comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização.  * Se o pessoal da auditoria interna, que integra a *terceira linha de defesa*, especialmente o dirigente dessa função: | |
| **Estrutura de gerenciamento de riscos e controles**  (Continuação da questão 1.3.2). |  |  |  |  | 1. tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, conforme previsto na Declaração de Posicionamento do IIA: *“O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo”*, e de fato os exerce em conformidade. 2. tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com essas prioridades da organização; 3. detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança. | |
| **2. PROCESSOS**  Nesta dimensão, o objetivo da equipe de auditoria é examinar os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida a organização dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas. | | | | | | |
| **2.1. – Identificação e análise de riscos**  Em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente a todas operações, funções e atividades relevantes da organização (unidades, departamentos, divisões, processos e atividades que são críticos para a realização dos objetivos-chaves da organização)? | | | | | A análise das subquestões 2.1.1 a 2.1.4 deve permitir à equipe concluir se a identificação e análise de riscos é realizada de forma consistente em relação a todas operações, funções e atividades relevantes para a realização dos objetivos-chaves da organização, de modo a priorizar os riscos significativos identificados para as atividades subsequentes de avaliação e resposta a riscos. | |
| **Estabelecimento do contexto**  2.1.1. A identificação de riscos é precedida de uma etapa de estabelecimento do contexto? |  |  |  |  | * Se previamente ao processo de identificação de riscos, todos os participantes desse processo obtêm entendimento da organização e dos seus objetivos-chaves, bem como do ambiente no qual esses objetivos são buscados, a fim de obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização para atingir seus objetivos. | |
| **Estabelecimento do contexto**  (Continuação da questão 2.1.1). |  |  |  |  | * Se a identificação dos objetivos-chaves da atividade, do processo ou do projeto objeto da identificação e análise de riscos é realizada considerando o contexto dos objetivos-chaves da organização como um todo, de modo a assegurar que os riscos significativos do objeto sejam apropriadamente identificados. * Se é realizada a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta. * Se é realizada comunicação e consulta com partes interessadas (internas e externas) para assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos. | |
| **Documentação do estabelecimento do contexto**  2.1.2. A documentação da etapa de estabelecimento do contexto inclui elementos essenciais para viabilizar um processo de avaliação de riscos consistente? |  |  |  |  | * Se a documentação da etapa de estabelecimento do contexto inclui pelo menos:  1. a descrição concisa dos objetivos-chaves e dos fatores críticos para que se tenha êxito (ou fatores críticos para o sucesso) e uma análise dos fatores do ambiente interno e externo (por exemplo, análise SWOT); 2. a análise de partes interessadas e seus interesses (por exemplo, análise de *stakeholder*, análise RECI, matriz de responsabilidades); 3. os critérios com base nos quais os riscos serão analisados, avaliados e priorizados (como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados). | |
| **Identificação e análise dos riscos**  2.1.3. Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos? |  |  |  |  | * Se nos processos de identificação de riscos são envolvidas pessoas com conhecimento adequado, bem como os gestores das áreas. * Se são utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de riscos. * Se o processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos. * Se o processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução daqueles objetivos identificados na etapa de estabelecimento do contexto. * Se a seleção de iniciativas estratégicas, novos projetos e atividades também têm os riscos identificados e analisados, incorporando-se ao processo de gestão de riscos. * Se são analisados o impacto e a probabilidade dos riscos. | |
| **Documentação da identificação e análise dos riscos**  2.1.4. No registro de riscos (sistema, planilhas ou matrizes de avaliação de riscos), a documentação da identificação e análise dos riscos contém elementos suficientes para apoiar um adequado gerenciamento dos riscos? |  |  |  |  | * Se há registro dos riscos identificados e analisados em sistema, planilhas ou matrizes de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto. * Se no registro de riscos da organização, a documentação das atividades de identificação e análise de riscos inclui pelo menos:  1. o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise; 2. os participantes das atividades de identificação e análise de riscos; 3. a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas; | |
| **Identificação e análise dos riscos**  (Continuação da questão 2.1.4). |  |  |  |  | 1. a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos; 2. os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco; 3. a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e 4. o risco residual. | |
| **2.2. – Avaliação e resposta a riscos**  Em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos? | | | | | A análise das subquestões 2.2.1 a 2.2.5 deve permitir à equipe concluir se a avaliação de riscos e a seleção de respostas aos riscos identificados e analisados como significativos é realizada de forma consistente, para assegurar que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como significativos, e para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento. | |
| **Critérios para priorização de riscos**  2.2.1. Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por toda a organização? |  |  |  |  | * Se existem critérios estabelecidos para orientar as decisões sobre riscos em relação a todas as operações, funções e atividades relevantes da organização. * Se os critérios estabelecidos levam em conta fatores como a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, critérios de comunicação a instâncias competentes, o tempo de resposta requerido. * Se os critérios estabelecidos são adequados para orientar decisões quanto a se:  1. um determinado risco precisa de tratamento e a prioridade para isso; 2. uma atividade deve ser realizada, reduzida ou descontinuada; 3. controles devem ser implementados, modificados ou apenas mantidos. | |
| **Avaliação e seleção das respostas a riscos**  2.2.2. A seleção de respostas para tratar riscos considera todas as opções de tratamento e o seu custo-benefício?  2.2.3. Os responsáveis pelo tratamento de riscos são envolvidos no processo de avaliação e seleção das respostas e são formalmente comunicados das ações de tratamento decididas?  **Planos e medidas de contingência**  2.2.4. Os elementos críticos da atuação da organização estão identificados e têm definidos planos e medidas de contingência? |  |  |  |  | * Se a avaliação e a seleção das respostas a serem adotadas para reduzir a exposição aos riscos identificados considera a relação custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas, além de controles internos, para mitigar os riscos. * Se todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento, bem como são formalmente comunicados das ações de tratamento decididas para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas. * Se todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização têm identificados os elementos críticos de sua atuação e têm definidos planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres. | |
| **Documentação da avaliação e seleção das respostas a riscos**  2.2.5. A documentação da avaliação e seleção de respostas a riscos inclui elementos suficientes para permitir o gerenciamento adequado da implementação das respostas? |  |  |  |  | * Se a documentação da avaliação e seleção de respostas aos riscos inclui pelo menos:  1. o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos, identificando claramente os riscos que requerem tratamento, suas respectivas classificações (probabilidade, impacto, níveis de risco etc.), a ordem de prioridade para cada tratamento; 2. as respostas a riscos selecionadas e as razões para a seleção, incluindo justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados; 3. as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; 4. a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las. | |
| **2.3. – Monitoramento e comunicação**  Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização? | | | | | A análise das subquestões 2.3.1 a 2.3.8 deve permitir à equipe concluir se as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente, para garantir que a gestão de riscos e os controles sejam eficazes e eficientes no desenho e na operação. | |
| **Informação e comunicação**  2.3.1. Diretrizes e protocolos de informação e comunicação estão estabelecidos e são efetivamente aplicados em todas as fases do processo de gestão de riscos? |  |  |  |  | * Se diretrizes e protocolos estão estabelecidos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito da organização, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos. * Se há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos. | |
| **Sistema de informação**  2.3.2. A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado? |  |  |  |  | * Se há um registro de riscos ou sistema de informação apoia a gestão de riscos da organização e facilita a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação; * Se o registro de riscos ou sistema de informação é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas na sequência), pelo menos quanto aos seus resultados e com referências para a documentação original completa. | |
| **Monitoramento contínuo e autoavaliações**  2.3.3. Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (primeira linha de defesa) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade? |  |  |  |  | * Se os gestores com propriedade sobre os riscos e como primeira linha de defesa monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade:  1. de modo contínuo, ou pelo menos frequente, por meio de indicadores-chaves de risco, indicadores-chaves de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho; 2. por meio de autoavaliações periódicas de riscos e controles *(Control and Risk Self Assessment – CRSA)*, que constam de um ciclo de revisão periódica estabelecido; e 3. a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança. | |
| **Monitoramento contínuo e autoavaliações**  (Continuação).  2.3.4. As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa) exercem suas atribuições de modo efetivo? |  |  |  |  | * Se as funções que supervisionam riscos ou coordenam atividades de gestão de riscos exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa. * Se essas funções fornecem orientação e facilitação para a condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém a sua documentação e comunica os seus resultados às instâncias apropriadas da administração e da governança. | |
| **Monitoramento periódico e avaliações independentes**  2.3.5. A função de auditoria interna auxilia a organização a realizar seus objetivos aplicando abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança? |  |  |  |  | * Se a função de auditoria interna estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança. | |
| **Monitoramento periódico e avaliações independentes**  (Continuação da questão 2.3.5). |  |  |  |  | * Se a função de auditoria interna utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos, o que implica a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável. * Se a função de auditoria interna fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização. | |
| 2.3.6. Há planos e medidas de contingência definidos para os elementos críticos da atuação da organização e estes são periodicamente testados e revisados? |  |  |  |  | * Se os planos e as medidas de contingência definidos para os elementos críticos da atuação da entidade, em todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização * Se os planos e as medidas de contingência são periodicamente testados e revisados. | |
| **Monitoramento de mudanças significativas**  2.3.7. A organização monitora as mudanças que podem aumentar sua exposição a riscos ter impacto nos seus objetivos? |  |  |  |  | * Se existem procedimentos e protocolos estabelecidos e em funcionamento para monitorar e comunicar mudanças significativas nas condições que possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos da organização. | |
| **Correção de deficiências e melhoria contínua**  2.3.8. São tomadas as medidas necessárias para a correção de deficiências e a melhoria contínua do desempenho da gestão de riscos em função dos resultados das atividades de monitoramento? |  |  |  |  | * Se os resultados das atividades de monitoramento são comunicados às instâncias apropriados da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias. * Se são elaborados e devidamente acompanhados planos de ação para corrigir as deficiências identificadas nas atividades de monitoramento e para melhorar o desempenho da gestão de riscos. | |
| **3. PARCERIAS**  Nesta dimensão, o objetivo da equipe de auditoria é examinar os aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhadas (quando o alcance de objetivos comuns de um setor estatal ou de uma política pública envolve parcerias com outras organizações públicas ou privadas), procurando avaliar em que medida a organização estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento. | | | | | | |
| **3.1. – Gestão de riscos em parcerias**  Em que medida a organização estabelece arranjos com clareza para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito das parcerias? | | | | | A análise das subquestões 3.1.1 a 3.1.6 deve permitir à equipe concluir se a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão gerenciados adequadamente e os objetivos alcançados. | |
| **Avaliação da capacidade de gestão de riscos das entidades parceiras**  3.1.1. A capacidade das potenciais organizações parceiras para gerenciar os riscos das políticas de gestão compartilhadas é avaliada antes da realização das parcerias? |  |  |  |  | * Se o compartilhamento dos riscos com potenciais organizações parceiras é precedido de avaliação fundamentada e documentada da capacidade da organização para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado das políticas de gestão compartilhadas. | |
| **Definição de responsabilidades, informação e comunicação**  3.1.2. Existe clara e adequada designação de responsáveis pelo gerenciamento de riscos nas parcerias e de protocolos de informação e comunicação entre eles? |  |  |  |  | * Se são designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou resultado esperado das políticas de gestão compartilhadas por meio de parcerias. * Se são definidas em quais condições e para quem cada responsável deve fornecer informações relacionadas a risco e desempenho. | |
| **Processo de gestão de riscos em parcerias**  3.1.3. O processo de gestão de riscos é aplicado no âmbito das parcerias? |  |  |  |  | * Se o processo de gestão de riscos é aplicado para identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas. | |
| 3.1.4. A identificação e avaliação de riscos em parcerias envolve as pessoas apropriadas das organizações parceiras e outras partes interessadas? |  |  |  |  | * Se pessoas de todas as áreas, funções ou setores com envolvimento na parceria, de ambas organizações parceiras, e outras partes interessadas no seu objeto participam do processo de identificação e avaliação dos riscos relacionados a cada objetivo, meta ou resultado esperado das parcerias. | |
| 3.1.5. A gestão de riscos nas parcerias é apoiada por um registro de riscos único ou sistema de informação efetivo e atualizado? |  |  |  |  | * Se um registro de riscos único é elaborado na identificação e avaliação dos riscos e é atualizado conjuntamente pelas organizações parceiras em função das atividades de tratamento e monitoramento de riscos. | |
| 3.1.6. Os riscos e o desempenho das parecerias são monitorados mediante troca regular de informação confiável? |  |  |  |  | * Se há informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado das parcerias. | |
| **3.2. – Planos de medidas de contingência**  Em que medida são estabelecidos planos ou medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas? | | | | | A análise das subquestões 3.2.1 deve permitir à equipe concluir se a organização estabelece, em conjunto com as entidades parceiras, planos e medidas de contingência para garantir a recuperação e a continuidade da prestação de serviços em caso de incidentes. | |
| **Planos e medidas de contingência**  3.2.1. São definidos planos e medidas de contingência no âmbito das parcerias, periodicamente testados e revisados? |  |  |  |  | * Se as organizações parceiras definem planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços, em casos de desastres, ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público, quando uma ou outra parte falhar. * Se os planos e as medidas de contingência são periodicamente testados e revisados. | |
| **4. RESULTADOS**  Nesta dimensão, o objetivo da equipe de auditoria é examinar os efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos. | | | | | | |
| **4.1. – Melhoria dos processos de governança e gestão**  Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão? | | | | | A análise das subquestões 4.1.1 a 4.1.4 deve permitir à equipe concluir se a organização integra a gestão de riscos em seus processos de governança e gestão e isso tem sido eficaz para a sua melhoria. | |
| **Integração da gestão de riscos aos processos organizacionais**  4.1.1. Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização? |  |  |  |  | * Se os responsáveis pela governança e a alta administração sabem até que ponto a administração estabeleceu uma gestão de riscos eficaz, integrada e coordenada por todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, tendo consciência do nível de maturidade atual e do progresso das ações em curso para atingir o nível almejado. | |
| 4.1.2. Os objetivos-chaves da organização estão identificados e refletidos na sua cadeia de valor e nos seus demais instrumentos de direcionamento e comunicação da estratégia? |  |  |  |  | * Se os objetivos-chaves, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, na missão e visão e da organização e nos seus valores fundamentais, formando a base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios. | |
| 4.1.3. Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho? |  |  |  |  | * Se os objetivos estratégicos e de negócios estão estabelecidos, alinhados com o direcionamento estratégico (questão anterior), com as respectivas medidas de desempenho (metas, indicadores-chaves de desempenho, indicadores-chaves de risco e variações aceitáveis no desempenho), permitindo medir o progresso e monitorar o desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chaves. | |
| 4.1.4. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos? |  |  |  |  | * Se estão identificados, avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chaves da organização, com o desempenho sendo comunicado aos níveis apropriados da administração e da governança. | |
| **4.2. – Resultados-Chaves da gestão de riscos**  Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização? | | | | | A análise das subquestões 4.1.1 a 4.2.3 deve permitir à equipe concluir se os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos. | |
| **Entendimento dos objetivos, riscos, papéis e responsabilidades**  4.2.1. Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização? |  |  |  |  | * Se os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos. | |
| **Garantia proporcionada pela gestão de riscos**  4.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização? |  |  |  |  | * Se os responsáveis pela governança e a administração, com base nas informações resultantes da gestão de riscos, têm garantia razoável de que:  1. entendem até que ponto os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização; | |
| **Garantia proporcionada pela gestão de riscos**  (Continuação da questão 4.2.3). |  |  |  |  | 1. entendem até que ponto os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados; 2. a comunicação de informações por meio de relatórios, de mecanismos de transparência e prestação de contas é confiável; 3. as leis e os regulamentos aplicáveis estão sendo cumpridos. | |
| **Eficácia da gestão de riscos**  4.2.3. Os riscos da organização estão dentro dos seus critérios de risco? |  |  |  |  | * Se, de acordo com a documentação resultante do processo de gestão de riscos e os critérios de risco definidos pela alta administração com a supervisão e concordância dos responsáveis pela governança, (apetite a risco, tolerâncias a risco ou variações aceitáveis no desempenho), os riscos da organização estão dentro dos seus critérios de risco. | |
| Elaborado por: | | | | | | / / |
| Revisado por: | | | | | | / / |
| Supervisionado por: | | | | | | / / |

1. Quando a questão de auditoria se desdobrar em subquestões, como neste caso, a sua conclusão (o que a análise vai permitir dizer) é obtida mediante avaliação conjunta das evidências obtidas na execução dos procedimentos de análise das subquestões que a compõe. O nível de maturidade (ou pontuação) correspondente à questão será calculado conforme orientações constantes do tópico **Determinação do nível de maturidade**. [↑](#footnote-ref-1)
2. Áreas (por exemplo: unidades, departamentos, divisões), funções (por exemplo: finanças, aquisições, contabilidade, gestão de pessoas, TI), atividades (por exemplo: processos, projetos, sistemas). [↑](#footnote-ref-2)