# 10 Gestão de riscos

Este capítulo fornece um comentário sobre o princípio da gestão de riscos contido na Recomendação do Conselho da OCDE sobre Integridade Pública. Tanto da perspectiva governamental quanto da institucional, o capítulo explora como as organizações do setor público podem adaptar políticas e práticas para gerenciar efetivamente os riscos de integridade, conduzir avaliações de risco e manter um ambiente de controle que preserve a integridade pública. Também enfatiza a necessidade de procedimentos coerentes para responder a possíveis fraudes ou corrupção, incluindo protocolos para denúncias, acompanhamento e investigações. O capítulo também considera o papel crítico das funções de auditoria interna em relação aos gestores públicos , com foco em seu valor agregado de garantirindependência e objetividade na gestão de riscos para a integridade. O capítulo destaca os principais desafios e práticas de liderança, como a articulação de políticas de controle interno orientadas a geração de valor, a realização de avaliações periódicas de riscos vinculadas aos objetivos estratégicos e a criação de ciclos de feedback para monitoramento e avaliação das atividades.

## 10.1. Por que gestão de risco?

Nas organizações do setor público, ter um sistema de controle interno e uma estrutura de gestão de risco é essencial para qualquer estratégia de integridade pública. Políticas e processos eficazes de controle interno e gestão de risco reduzem a vulnerabilidade das organizações do setor público à fraude e à corrupção, ao mesmo tempo em que garantem que a administração opere de maneira ideal para oferecer políticas públicas que beneficiem os cidadãos. Além disso, essas políticas e processos ajudam a garantir a relação custo-benefício e facilitam a tomada de decisões. Firmemente estabelecidos, eles ajudam os órgãos e entidades a equilibrar um modelo focado na fiscalização com abordagens mais preventivas e baseadas em riscos.

O controle interno e a gestão de riscos abrangem uma série de medidas para prevenir, detectar e combater à fraude e à corrupção. Isso inclui políticas, práticas e procedimentos que orientam a administração e os órgãos e entidades a cumprir suas funções na preservação da integridade, avaliando adequadamente os riscos e desenvolvendo controles baseados em riscos. Mecanismos de resposta a casos de corrupção e quebra de padrões de integridade também são medidas críticas adotadas em um sistema integrado de controle interno.

À luz disso, a Recomendação da OCDE sobre Integridade Pública exorta os aderentes a “aplicar um quadro de controle interno e gestão de risco parapreservar a integridade nas organizações do setor público, em particular através de:

a. assegurar um ambiente de controle com objetivos claros que demonstrem o compromisso dos gestores com a integridade pública e os valores do serviço público, e que forneça um nível razoável de garantia da eficiência, desempenho e conformidade de uma organização com as leis e práticas;
b. assegurar uma abordagem estratégica à gestão de riscos que inclua a avaliação dos riscos para a integridade pública, abordando as deficiências de controle (incluindo a construção de sinais de alerta em processos críticos), bem como o estabelecimento de um mecanismo eficiente de monitoramento e garantia de qualidade para o sistema de gestão de risco;
c. assegurar que os mecanismos de controle sejam coerentes e incluam procedimentos claros para responder a suspeitasde violação de leis e regulamentos e facilitar a denúncia às autoridades competentes sem medo de represálias” (OECD, 2017[1]).

## 10.2. O que é gestão de risco?

O controle interno e a gestão de risco apoiam os órgão e entidades do setor público no alcance de metas e objetivos. O princípio de gestão de riscos concentra-se em aspectos de controle interno e gestão de riscos no contexto da preservação da integridade e combate à corrupção no setor público. Órgãos e entidades devem, em última análise, adaptar sua abordagem aos seus respectivos contextos legais, regulatórios e culturais. Isso envolve a incorporação de objetivos de integridade em políticas e práticas de controle interno e gestão de risco existentes. Também envolve a adaptação de padrões e conceitos internacionais de controle interno e gestão de riscos às realidades locais e do setor público, incluindo padrões e orientações produzidos pelo Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO), a Organização Internacional para Padronização, o Instituto de Auditores Internos (por exemplo, o modelo “Três Linhas de Defesa”) e a Organização Internacional de Instituições Superiores de Auditoria (INTOSAI).

Um sistema de controle interno é um componente integrador das operações de uma organização do setor público. Do ponto de vista da integridade pública, o controle interno e a gestão de riscos consistem nas políticas, processos e ações para gerenciar os riscos de fraude, corrupção e abuso (doravante denominados coletivamente como riscos de integridade). A seguir estão os componentes críticos de um sistema de controle interno projetado para preservar a integridade:

- um ambiente de controle eficaz[1] e de gestão de riscos para a integridade.
- uma abordagem adaptada para a gestão de riscos e para a avaliação de riscos de integridade.
- monitoramento e avaliação da gestão do risco de integridade .
- procedimentos coerentes e responsivos dentro da estrutura de controle interno e gestão de risco.
- uma função de auditoria interna que fornece avaliação e consultoria independente e objetiva para fortalecer o controle interno e a gestão de risco para a integridade.

Esses componentes dependem de uma série de atores nos níveis governamental, institucional e individual para uma implementação efetiva. Por exemplo, para organizações do setor público, o legislador pode garantir que as políticas de controle interno e gestão de risco em toda Administração Pública sejam coerentes e harmonizadas, conforme discutido abaixo. No nível institucional, as políticas e processos de controle interno e gestão de riscos fornecem garantia razoável à administração de que a organização está atingindo seus objetivos de integridade e gerenciando seus riscos de forma eficaz. Os componentes de controle interno e gestão de risco também estão presentes em um nível individual: muitos padrões exigem o compromisso pessoal dos agentes públicos com a integridade e a adesão aos códigos de conduta.

### *10.2.1. Um ambiente de controle eficaz e de gestão de riscos para a integridade*

Nas organizações do setor público, o ambiente de controle atende a uma ampla gama de objetivos financeiros, orçamentários e de desempenho. Consiste em um conjunto de padrões, processos e estruturas de controle interno em uma entidade (Committee of Sponsoring Organizations of the Treadway Commission, 2013[2]). Além de garantir o cumprimento da legislação, normas e outros requisitos, o ambiente de controle e os processos que o compõem contribuem para a boa governança e ajudam órgãos e entidades do setor público a entregar resultados aos cidadãos de forma eficaz e eficiente. No contexto do princípio de gestão de riscos, o ambiente de controle reflete os objetivos, políticas e pessoas que ajudam a institucionalizar um sistema de integridade, de tomada de decisão e de gestão de riscos.

#### *Considerações governamentais para um ambiente de controle orientado à integridade*

Diversas organizações do setor público compartilham a responsabilidade pela implementação do controle interno e da gestão de riscos em toda Administração Pública. Essas organizações incluem o Governo Federal , instituições de auditoria, e órgãos que atuam no combate á corrupção. Em particular, eles: 1) definem e harmonizam padrões e políticas de controle interno, 2) fornecem orientação e ferramentas, 3) avaliam os esforços de todos os órgãos e entidades para preservar a integridade e 4) coordenam e padronizam práticas para lidar com suspeitas de violação de integridade no setor público como um todo. Por exemplo, nos Estados Unidos, a instituição suprema de auditoria, o Escritório de Contabilidade do Governo , lidera o processo de definição de padrões para controle interno e gestão de riscos em colaboração com um conselho de especialistas, e publica as Normas para Controle Interno no Governo Federal (U.S. Government Accountability Office, 2014[3]) bem como uma estrutura de práticas líderes para a gestão de riscos de fraude no governo (U.S. Government Accountability Office, 2015[4]). O Escritório de Gestão e Orçamento (OMB) complementa o trabalho do Escritório de Contabilidade com políticas e orientações para implementação. Isso inclui um documento (Circular OMB nº A-123) que descreve a responsabilidade da administração e os requisitos relacionados ao controle interno e à gestão de riscos no governo federal, com referência explícita à avaliação de riscos de fraude (U.S. Office of Management of Budget (OMB), 2016[5]). Na França, todas as entidades públicas (administrações públicas, autoridades

locais, instituições públicas e empresas semipúblicas) são legalmente obrigadas a realizar avaliações de risco, independentemente do seu tamanho. Como tal, as entidades públicas devem listar todos os processos relacionados com as suas atividades, tais como recrutamento e contratação pública, e avaliar os riscos de integridade associados (Quadro 10.1).

### Quadro 10.1. Controlo interno nos Estados-Membros da União Europeia

Dois princípios fundamentais das normas de controlo interno público entre os Estados-Membros europeus são: 1) o controlo interno público baseia-se no Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO) e na Organização Internacional das Instituições Superiores de Auditoria (INTOSAI), e 2) todos os países-membros devem ter uma função dentro do governo de coordenação e harmonização de controle interno e auditoria para todas as entidades públicas. Assim, embora haja uma variedade de sistemas de controle interno nos Estados-Membros, todos eles têm uma organização governamental que desempenha o papel de harmonização central de controle interno.

Além disso, os Estados-Membros e suas instituições públicas compartilham padrões consistentes derivados das mesmas práticas internacionais de controle interno e gestão de riscos. As normas contêm disposições explícitas relativas ao controlo interno e à gestão do risco contra a fraude na gestão dos fundos da UE.

Fonte: (European Commission, 2015[6]).

A falta de clareza do nível estratégico sobre como institucionalizar o controle interno e a gestão de riscos pode levar a uma percepção de que os objetivos de integridade e as atividades de controle interno e gestão de riscos que os apoiam são separados de outros objetivos estratégicos e operacionais. O governo federal, assim como outros órgãos com responsabilidades em toda a administração pública, pode desempenhar um papel fundamental para ajudar as organizações do setor público a superar esse desafio, fornecendo padrões, políticas e orientações unificadas. Eles também podem ajudar a aumentar a conscientização sobre o valor do controle interno e da gestão de riscos para a tomada de decisões e o alcance das metas organizacionais.

#### *Considerações institucionais e individuais para um ambiente de controle orientado à integridade*

Em uma organização, todos os indivíduos têm funções e responsabilidades na gestão de riscos e no combate à corrupção (Committee of Sponsoring Organizations of the Treadway Commission, 2016[7]). Isso pode ser reconhecido em políticas organizacionais, procedimentos e orientações para controle interno e gestão de riscos, ou pode ser articulado como uma política de integridade independente. Quer sejam articuladas em diferentes políticas ou dentro de uma política de integridade independente, tais políticas não devem servir como uma lista de verificação para cumprir os padrões mínimos. Eles devem ser abrangentes e adaptados a cada organização, com relevância para os riscos de integridade atuais e emergentes. Elementos essenciais das políticas para promover um ambiente de controle eficaz nas organizações do setor público podem incluir:

- referência aos valores e princípios de integridade, bem como aos padrões de conduta pessoal que sustentam a organização, e ao que eles significam na prática
- declaração dos objetivos antifraude e anticorrupção da organização, com ligação explícita a como o controle interno e as atividades de gestão de risco atendem a esses objetivos
- descrição do alinhamento entre os objetivos de integridade e outras políticas e ferramentas da organização (ou seja , código de conduta, código de ética)

- definição de fraude e corrupção, com exemplos ilustrativos de ações consideradas corruptas ou fraudulentas
- identificação do público-alvo a quem a política se aplica, levando em consideração o pessoal temporário e os voluntários
- funções e responsabilidades claramente definidas para o controle interno e gestão de riscos relacionados a fraude, corrupção, desperdício e abuso
- comunicação aos agentes públicos sobre como denunciar suspeitas de irregularidades, os canais internos e de denúncia disponíveis para eles e os procedimentos a serem seguidos
- identificação das medidas de fiscalização e descrição de como as ações suspeitas de irregularidades serão investigadas .

A administração tem a responsabilidade primária de criar e manter um ambiente de controle que enfatize a integridade e estabeleça um tom positivo. Além disso, o compromisso de alto nível ajuda a aumentar a conscientização sobre os riscos para a integridade e ajuda a melhorar a implementação das atividades de controle. A administração pode incluir os líderes ou grupos (por exemplo, conselhos ou comitês) responsáveis pelo desenho, implementação e monitoramento das políticas e práticas de controle interno e gestão de risco. Além disso, a administração deve demonstrar seu compromisso individual com a integridade (para mais informações, consulte os Capítulos 1 e 6). Por meio de códigos de conduta e códigos de ética, a administração pode comunicar suas expectativas em relação à conduta de integridade, bem como os valores organizacionais que permitem que os indivíduos demonstrem pessoalmente o comportamento ético. Esses códigos definem os padrões básicos de comportamento dos agentes públicos e podem ser a base para a administração avaliar a adesão aos códigos de ética e aplicá-los por meio de medidas disciplinares, se necessário (para mais informações, consulte o Capítulo 4).

Algumas organizações do setor público designam uma unidade para gerenciar riscos de integridade. A unidade pode ser um comitê, uma equipe ou um indivíduo, dependendo das necessidades. Por exemplo, em algumas organizações, a unidade é um comitê que ajuda a supervisionar, coordenar, monitorar e avaliar as atividades de gestão de risco em toda a organização. Em outros casos, as organizações nomeiam gerentes de riscos de integridade ou estabelecem forças-tarefa responsáveis por cumprir os objetivos de integridade dentro do ambiente de controle. A competência e o tamanho da organização (incluindo o número de programas e agentes e os recursos) e a complexidade dos riscos ajudam a determinar se uma unidade dedicada seria benéfica. Independentemente da abordagem, é essencial que a unidade tenha linhas diretas de reporte à alta administração, dada a responsabilidade geral desta última pela gestão dos riscos de integridade.

### *10.2.2. Uma abordagem adaptada para a gestão de riscos e para a avaliação de riscos de integridade*

Adaptar as atividades de gestão de risco às condições únicas de uma organização do setor público envolve a implementação de avaliações e controles de risco adequados à sua finalidade. Os riscos de integridade variam de acordo com os setores e organizações e, portanto, é fundamental que os órgãos e entidades do setor público ajustem suas orientações, ferramentas e abordagens para seus objetivos, ambientes e contextos específicos. Isso é crucial, uma vez que muitos dos padrões de controle interno e de gestão de riscos do setor público foram originalmente desenvolvidos no setor privado. O governo federal, os ministériose os órgãos e entidades responsáveis pela gestão de riscos desempenham um papel neste processo de adaptação, que é refletido abaixo nas discussões tanto da perspectiva governamental quanto institucional.

### *Apoio governamental orientado para a gestão e avaliações de risco para a integridade*

Orientações e ferramentas direcionadas podem apoiar os órgãos e entidades na condução de suas atividades de controle interno e gestão de riscos para a integridade, vinculando essas atividades a objetivos programáticos mais amplos. Eles também podem apoiar estratégias de comunicação que garantem que o controle interno e a gestão de riscos vão além do controle financeiro e das verificações de conformidade. Por exemplo, em 2010, a Secretaria do Conselho do Tesouro no Canadá desenvolveu uma estrutura para a gestão de risco para orientar os chefes adjuntos de departamentos governamentais na implementação de práticas de gestão de risco em todos os níveis de sua organização. A Agência Anticorrupção Francesa (AFA) publicou diretrizes para ajudar as entidades jurídicas públicas e privadas a cumprir certos requisitos anticorrupção e de integridade, incluindo a realização de avaliações de risco. A AFA também desenvolveu guias técnicos especializados, por exemplo, para agentes encarregados de compras públicas. Além dessas diretrizes gerais, a AFA oferece suporte personalizado a atores públicos ou privados que desejam otimizar seus procedimentos de gestão de riscos para a integridade. A orientação específica do setor, com foco em áreas de alto risco, como compras ou saúde, juntamente com mecanismos de coordenação e ferramentas de comucicação relevantes, pode ajudar a superar as lacunas de conhecimento (Quadro 10.2).

#### Quadro 10.2. O caso da Estônia:uma abordagem holística para a integridade e o o foco em áreas de alto risco

Na Estônia, a Estratégia Anticorrupção 2013-2020 do governo reconhece deficiências na prevenção da corrupção em domínios específicos e na mitigação de riscos e fornece ações para remediar esses desafios. Ele estipula que o ministério responsável pela área específica em questão (por exemplo, saúde ou meio ambiente) também deve ser responsável pela implementação de medidas específicas de prevenção da corrupção. Para atingir áreas de alto risco, o governo da Estônia estabeleceu redes anticorrupção específicas de domínio. Cada ministério tem um coordenador de prevenção da corrupção que deve gerenciar a implementação da política anticorrupção no ministério e sua área de governo. Os coordenadores formam a rede anticorrupção – a rede se reúne anualmente cerca de quatro a cinco vezes. A rede também inclui representantes da polícia, sociedade civil, parlamento, auditoria do estado e outras partes interessadas que são convidadas, dependendo do tema escolhido. Há também uma rede de autoridades de saúde para discutir os desenvolvimentos em suas respectivas áreas, bem como questões a serem resolvidas.

Fonte: (Estonian Ministry of Justice, 2013[8]).

### *Gestão e avaliação institucional de riscos de integridade*

As políticas, processos e ferramentas para realizar avaliações de risco de integridade variam de acordo com a organização e dependem do seu tamanho, do investimento que recebe e se a organização funciona dentro de um setor de alto risco (ou seja, saúde, infraestrutura). Por exemplo, um orgãodo setor público pode realizar uma avaliação independente de riscos de integridade ou incorporar objetivos de integridade em suas avaliações de risco para promover a eficiência. No entanto, as políticas de gestão de risco e os processos de avaliação compartilham características semelhantes entre entre órgãos e etidades. As políticas de gestão de risco devem estar vinculadas a objetivos e incluir, entre outras coisas, medidas de tratamentos do risco , destinação de de recursos, responsabilidades, medidas de desempenho e avaliação e monitoramento (Crime and Corruption Commission, 2018[9]). Além disso, conforme descrito abaixo, a gestão e as avaliações de risco geralmente envolvem um processo iterativo de várias etapas para estabelecer o contexto, avaliar e tratar os riscos e garantir monitoramento, comunicação e consulta contínuos (International Organization for Standardization, 2018[10]).

### Estabelecendo o contexto para gerenciar riscos de integridade

Compreender o contexto interno e externo é um passo fundamental para os agentes públicos ao avaliarem pela primeira vez os impulsionadores e os potenciais impedimentos para alcançar os objetivos de integridade. O contexto interno inclui – mas não se limita a – objetivos estratégicos, estrutura de governança, funções, conjuntos de habilidades dos agentes, ferramentas operacionais (por exemplo, sistemas de dados e informações), cultura e diretrizes internas. O contexto externo pode incluir estruturas legais e políticas, partes externas interessadas e realidades políticas, sociais e econômicas que evidenciam tipos específicos de riscos de integridade ou mecanismos de resposta. Este contexto é a base para desenhar e melhorar as políticas, estratégias e objetivos de gestão e avaliação dos riscos para a integridade, uma vez que as configurações internas e externas não são estáticas.

Várias ferramentas de planejamento estratégico podem ser pontos de partida úteis para avaliar o contexto e definir o escopo do processo de avaliação de risco. Por exemplo, ferramentas como árvore de decisão e diagramas de "espinha de peixe", mapas de processo e influência, e o método "PESTLE" (Fatores Políticos, Econômicos, Sociais, Tecnológicos, Jurídicos e Ambientais) pode facilitar a análise ao mesmo tempo em que promove o engajamento entre as partes interessadas. Os registros de risco em nível de governo ou departamento podem ser uma entrada útil para estabelecer o contexto, conforme ilustrado no Quadro 10.3.

#### Quadro 10.3. Desenvolvimento e gestão de registros de riscos – Exemplo do Sistema de Saúde Irlandês (Health Service Executive - HSE)

O Health Service Executive desenvolve registros de riscos para gerenciar seus riscos e obter uma visão geral de alta qualidade do status de risco dos serviços em um determinado momento. Uma ferramenta poderosa para rastreamento de riscos, o registro de riscos descreve o sistema geral de riscos e o status das ações de mitigação de riscos.

Cada gerente de linha é responsável por desenvolver um registro de risco em sua área de responsabilidade. Uma vez concluído, o cadastro é compartilhado com todos os funcionários da entidade de forma clara e compreensível, levando em consideração seu nível de formação, conhecimento e experiência. Um plano de ação é a parte crítica de um registro de risco. Isso aborda os controles adicionais necessários para reduzir o risco a um nível satisfatório. Os controles suplementares que não podem ser gerenciados no nível de serviço devem ser transferidos para o próximo nível de gestão.

A HSE reconhece que, por várias razões, nem todos os riscos podem ser eliminados. Consequentemente, em qualquer fase do processo pode-se decidir "conviver" ou aceitar um certo nível de risco. Quando um risco não pode ser totalmente eliminado, ele deve ser registrado no registro de riscos juntamente com uma lista de controles visando reduzi-lo a um nível aceitável. Esses riscos serão monitorados regularmente. Quatro elementos foram identificados como pré-requisitos para o desenvolvimento de um registro de risco sólido:

1. *Disponibilidade de experiência em riscos* – A equipe que apoia o processo precisa de treinamento e educação adequados.
2. *Uso de materiais e ferramentas de apoio aprovados* – Para garantir a consistência em todo o processo, vários documentos e ferramentas aprovados devem ser usados ao desenvolver um registro.
3. *Compromisso e propriedade* – Compromisso visível da alta administração, que pode promover a adesão entre as partes interessadas para garantir qualidade e sustentabilidade.
4. *Disponibilidade de suporte no local* – O suporte administrativo é necessário para a organização de workshops e coordenação geral.

Como as avaliações de risco envolvem um processo dinâmico, os riscos e suas medidas de controle devem ser continuamente verificados, monitorados e revisados quando necessário.

Fonte: (Irish Health Service Executive, 2018[11]).

Estabelecer o contexto também requer identificar funções e responsabilidades e estabelecer uma equipe para avaliar os riscos de integridade em toda a organização. Embora existam indicações de cargos e funções para lidar com os riscos de integridade nos órgãos e entidades, a gestão de riscos requer o envolvimento de vários atores. Por exemplo, gerentes de linha, gerentes de risco e auditores internos (ou seja, a primeira, segunda e terceira linhas de defesa,[2] respectivamente) desempenham papéis críticos para garantir que a gestão de riscos e o controle interno avancem nas metas e objetivos organizacionais.

Ao longo de todo o processo, deve haver mecanismos para garantir a coleta de todos s insumos relevantes e a comunicação das conclusões e resultados. Com eles, as organizações podem integrar melhor a gestão de riscos em suas operações e apropriar-se do processo de avaliação de riscos. Na Lituânia, por exemplo, a lei sobre prevenção da corrupção inclui uma metodologia para análise de risco de corrupção. A metodologia especifica que várias fontes devem ser consultadas ao realizar a análise, incluindo resultados de auditorias e pesquisas sociais e de pessoal (OECD, 2015[12]).

O alcance da integração da gestão de riscos na organização é outra característica crítica do contexto interno. As políticas e práticas de controle interno e gestão de riscos são mais eficazes quando fazem parte da estratégia geral da organização e das operações em apoio a metas e objetivos concretos. A forma precisa como essa integração ocorre varia de acordo com a organização. No entanto, o processo pode incluir a criação de vínculos entre a gestão de riscos e as políticas e processos de planejamento estratégico, atividades de monitoramento e avaliação. Por exemplo, no Reino Unido, a HM Revenue and Customs usa seu relatório de desempenho mensal para medir o progresso em relação aos objetivos e identificar áreas de desempenho que requerem ação adicional. Um Comitê de Desempenho, juntamente com “Hubs de Desempenho”, discute dados relevantes e considera os principais riscos para o alcance das metas. Especificamente, eles revisam os registros de riscos de vários departamentos e integram informações e insights sobre riscos em sua avaliação do desempenho atual e do desempenho existente (National Audit Office, 2011[13]).

### Identificando e analisando riscos de integridade

As avaliações de riscos são processos iterativos que permitem que uma organização entenda os facilitadores e as barreiras aos seus objetivos, com base na análise dos[3] riscos inerentes e residuais.[4] Uma ligação clara com os objetivos é fundamental para orientar os envolvidos na definição do escopo da avaliação de risco e garantir que eles não sobrecarreguem de informações o processo e os registros de risco. Em última análise, os resultados da avaliação de risco devem ser úteis para a tomada de decisões, e vincular objetivos específicos aos riscos (em vez do contrário) pode ajudar as organizações a manter o foco nos riscos que importam. As avaliações de risco de corrupção e fraude podem ser exercícios autônomos ou incorporados às atividades de avaliação de risco de uma organização, reconhecendo as interligações entre as diferentes categorias de risco, como riscos estratégicos, operacionais, financeiros, de conformidade e de reputação.[5]

Não existe uma abordagem universal para conduzir avaliações de risco de integridade e, de fato, adaptá-las às necessidades de uma organização é fundamental. Em geral, as organizações podem avaliar riscos específicos, fatores de risco[6] ou uma combinação de ambos. Os riscos específicos são os esquemas de corrupção ou fraude relevantes que podem ter impacto nos objetivos organizacionais. A avaliação de tais riscos é discutida em mais detalhes abaixo. Os fatores de risco também estão vinculados aos objetivos, mas referem-se às características das políticas, procedimentos ou atividades da organização que, quando avaliadas e pontuadas, podem destacar áreas de operações de alto risco e, posteriormente, definir

prioridades. Por exemplo, a complexidade dos procedimentos pode ser um fator de risco que pode tornar mais difícil para uma organização realizar uma supervisão eficaz e prevenir fraudes ou corrupção.

Outro exemplo de fator de risco é o grau de dependência de subcontratados ou terceiros, uma vez que muitos órgãos e entidades contratam terceiros para adquirir bens e serviços. Cada fator de risco pode ser ponderado de acordo com as prioridades da organização e pontuado de acordo com critérios pré-determinados. Por exemplo, uma organização pode pontuar o fator de risco de dependência de terceiros, conforme mostrado na Tabela 10.1 abaixo. Também é possível desenvolver critérios para outros fatores de risco, como tamanho do orçamento, extensão do impacto do programa para as partes interessadas, suscetibilidade à fraude ou volume e tipo de recomendações de auditoria recebidas.

### Tabela 10.1. Exemplo de critérios para o fator de risco de terceiros

| Pontuação | Critério |
|---|---|
| 5 | Os processos críticos são completamente terceirizados |
| 4 | Processos importantes são altamente dependentes de terceiros |
| 3 | Os processos são moderadamente dependentes de terceiros |
| 2 | Terceiros realizam algumas atividades que têm impacto nos objetivos |
| 1 | Terceiros não são usados ou realizam atividades que não são críticas para os objetivos |

Nota: 5 = alto risco; 1 = baixo risco.
Fonte: Adaptado de (Wright Jr., 2013[14]).

Ao avaliar riscos específicos em oposição a fatores de risco, as avaliações geralmente distinguem entre riscos inerentes e residuais. Para tais avaliações, uma organização deve primeiro analisar os riscos inerentes, ou seja, os riscos avaliados na ausência de medidas de controle. Por exemplo, como passo inicial, um órgão avaliaria a probabilidade e o impacto de todos os esquemas de fraude em potencial relacionados ao uso de cartões de crédito ou de viagem a serviço público. A organização pode usar pontuações numéricas (por exemplo, 1 a 5) para avaliar a probabilidade e o impacto, ou pode usar classificações (por exemplo, baixo, médio e alto). Tanto as pontuações de probabilidade quanto de impacto podem ser vinculadas a critérios específicos para facilitar a avaliação. Por exemplo, uma organização que avalia os riscos de aquisição pode usar valores ou frequência do contrato para medir o impacto e categorizar riscos muito altos (pontuação 5) versus riscos muito baixos (pontuação 1). Ao passar pelo processo de avaliação de risco, as organizações repetiriam esse processo de pontuação para avaliar os riscos residuais.

O risco residual refere-se à exposição ao risco após a aplicação de medidas de mitigação. No exemplo anterior, isso incluiria uma segunda fase de análise dos riscos inerentes identificados, incluindo uma determinação revisada da probabilidade e impacto dos riscos de fraude mediante medidas de controle, como procedimentos de limites colocados nos cartões de crédito. Conforme discutido na próxima seção, a organização então levaria em consideração seu risco residual relativo aos critérios de risco (ou seja, tolerâncias),[7] antes de determinar se deve fazer mudanças nas atividades de controle. Ao analisar os riscos inerentes e residuais, é importante que as organizações evitem a armadilha comum de identificar e analisar controles ou consequências em vez de riscos que possam prejudicar o alcance dos objetivos.

Para apoiar formas qualitativas de análise de risco, as organizações podem recorrer a uma variedade de fontes. Analisar resultados de auditoria, entrevistar funcionários, realizar avaliações de risco de controle e conduzir análises de lacunas de Forças, Fraquezas, Oportunidades e Ameaças (SWOT) são métodos comuns para identificar riscos potenciais. Outras técnicas podem incluir consultar o registro de risco do país ou do órgão e entidade, se houver, para identificar tendências ou esquemas em andamento que sejam indicativos de atividade fraudulenta ou corrupta. Além disso, as avaliações de risco são um esforço de equipe. Pode ser útil envolver os funcionários em toda a organização para fornecer diferentes perspectivas, bem como validar os resultados. Gestores e agentes da linha de frente – aqueles que são

diretamente responsáveis pelas operações ou prestação de serviços, como um fiscal de contrato em contato direto com fornecedores ou um agente de saúde que interage com os beneficiários – podem ter percepções diferentes sobre a probabilidade e o impacto dos riscos. Os agentes da linha de frente podem estar em uma posição melhor do que os gerentes para identificar riscos emergentes.

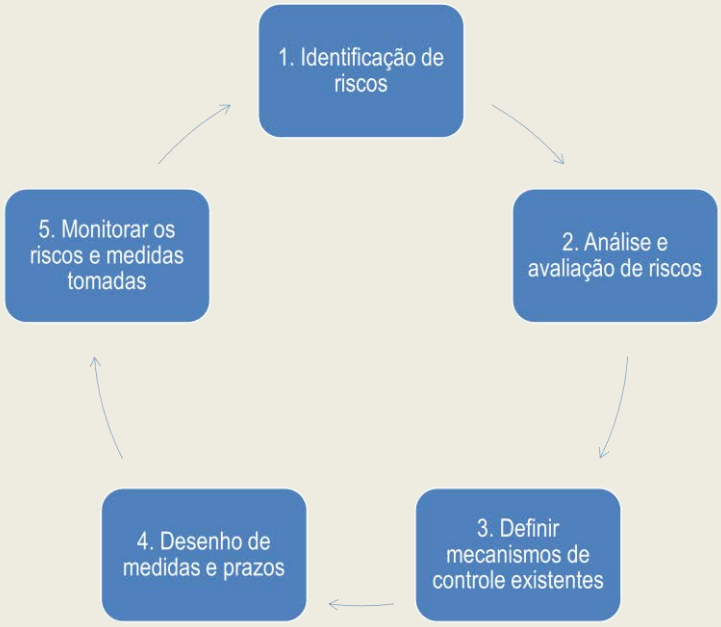
O uso de técnicas quantitativas e análise de dados também pode ajudar a identificar possíveis fraudes e corrupção em diversas áreas onde os órgãos e entidades tendem a coletar dados confiáveis e válidos. Isso inclui projetos de obras públicas, compras, folha de pagamento, serviços sociais, benefícios de saúde e emprego. No entanto, as abordagens quantitativas podem consumir muitos recursos e, muitas vezes, exigem habilidades especializadas e investimentos em infraestrutura de TI, software e treinamento. Antes de investir fortemente em abordagens quantitativas ou baseadas em dados para avaliar riscos, as instituições podem considerar análises de custo-benefício e oportunidades para testar novas abordagens.

As organizações que avaliam efetivamente os riscos adaptam o processo ao seu próprio ambiente e realizam avaliações regularmente, embora a frequência com que diferentes entidades realizam avaliações de risco varie. Quadro 10.4 ilustra como as autoridades da República Eslovaca realizam análises de risco de fraude e corrupção.

### Quadro 10.4. O processo de avaliação de risco para as autoridades da República Eslovaca que implementaram os Fundos Estruturais e de Investimento Europeus (FEI)

Na República Eslovaca, as autoridades responsáveis pela execução dos programas operacionais (PO) têm procedimentos de gestão de risco específicos que constituem a base para a avaliação dos riscos. De acordo com os procedimentos, a gestão de risco é composta por cinco fases interligadas, entre as quais se inclui a avaliação de risco (ver Figura 10.1). Um elemento importante desse processo é o ciclo de feedback, ilustrando a natureza iterativa das avaliações de risco e o aprendizado contínuo das atividades de monitoramento.

### Figura 10.1. O processo de avaliação de risco na República Eslovaca



A primeira fase é identificar os riscos potenciais que podem afetar negativamente o cumprimento dos objetivos do programa operacional (PO); estes são classificados em um catálogo de riscos abrangente ou selecionado. Estão incluídos os riscos de fraude e corrupção. Os riscos são então analisados e avaliados com base em sua significância e probabilidade de ocorrência usando matrizes de risco, que ajudam a determinar o nível geral de risco. Os riscos de fraude e corrupção com um nível de risco geral superior a 4 são designados pela equipe de avaliação de risco como significativos e críticos. Posteriormente, os riscos são classificados em seus respectivos catálogos de riscos, onde uma lista restrita é elaborada para riscos críticos. Os procedimentos de gestão de risco para cada PO estabelecem o tratamento de risco adequado após a identificação e avaliação.

Fonte: Apresentado por representantes do Ministério do Meio Ambiente da República Eslovaca em Bratislava, fevereiro de 2019.

**Avaliação de risco e uma estratégia de mitigação**

Depois de identificar e avaliar os riscos de integridade, incluindo riscos inerentes e residuais, o próximo passo é determinar se e como responder. Esta fase envolve avaliar os resultados da análise de risco em relação a critérios de risco específicos (ou seja, tolerâncias) e, em seguida, refinar a estratégia da organização para mitigar os riscos. “Apetite a risco” refere-se ao nível de risco que uma organização está disposta a aceitar. Com efeito, as tolerâncias são critérios que atuam como limites para facilitar a tomada de decisões e garantir que os controles sejam eficazes e proporcionais.

Os gerentes devem determinar esses critérios antecipadamente antes de realizar avaliações de risco. Conselhos, comitês de auditoria e liderança gerencial podem ser envolvidos na definição dos critérios de risco para garantir que sejam definidos da forma mais objetiva possível e alinhados com as políticas, regulamentos e objetivos organizacionais. A “tolerância zero” para corrupção e fraude não é um critério de risco útil. É certo que esta mensagem pode servir como um princípio orientador e ajudar a promover uma cultura consciente do risco. No entanto, entre outras consequências imprevistas , também pode ter um efeito desencorajador no processo de avaliação de risco se a cultura de tolerância zero criar uma resistência entre os gerentes em fornecer informações francas sobre os riscos percebidos em sua área de atuação. Ao contrário das declarações de tolerância zero, os critérios de risco específicos do contexto têm implicações mais práticas para avaliar e adaptar as atividades de controle.

É impossível identificar e agir em todos os riscos de fraude e corrupção. Os critérios de risco devem ser definidos em um nível em que uma organização queira entender completamente um problema e garantir que medidas de mitigação estejam em vigor (Fountain, 2015[15]). O apetite a risco ajuda os gerentes a decidir se aceitam, evitam, reduzem ou compartilham o risco. Se as medidas de controle forem eficazes para manter o risco dentro ou abaixo do limite estabelecido pelos critérios de risco (por exemplo, processos em que os riscos de fraude interna são inferiores a um valor financeiro especificado), então aceitar o risco residual pode ser o mais eficaz e eficiente em termos de recursos. Se for determinado que as atividades de controle não conseguem mitigar os riscos ao nível aceitável, os gerentes devem evitar, reduzir ou compartilhar o risco.

Evitar o risco envolve cessar a política ou as operações a ele vinculadas. Por exemplo, uma instituição pode decidir proibir os funcionários de aceitar pequenos presentes de parceiros do projeto ou pode encerrar seu relacionamento com um fornecedor de alto risco, eliminando totalmente o risco. Alguns riscos são inevitáveis, como o risco de atestados médicos falsificados ou o risco de solicitações fraudulentas para serviços públicos A redução desses riscos envolve a adaptação de procedimentos e atividades de controle para diminuir sua probabilidade e impacto. Por fim, o compartilhamento do risco é mais comum no contexto empresarial, mas também pode ocorrer no setor público. Normalmente envolve a tomada de alguma ação para transferir o risco para um terceiro, como uma seguradora, que pode cobrir as perdas no caso de o risco se materializar.

Matrizes de risco, registros de risco ou tabelas simples do Excel podem ser ferramentas úteis para documentar os resultados das avaliações de risco, bem como avaliar as interligações entre riscos e controles. Por exemplo, a Figura 10.2 ilustra uma maneira de categorizar as pontuações de risco e comunicar as ações necessárias, bem como as funções e responsabilidades dos gerentes de riscos. Independentemente de como eles são documentados, é fundamental que os resultados das avaliações de risco reflitam o nível aceitável de risco com base em critérios predeterminados. Mapas de calor[8] ou outras ferramentas que transmitem pontuação da probabilidade e impacto dos riscos sem também mostrar o nível de gestão de risco considerado aceitável têm pouco valor para a tomada de decisão ou adaptação de medidas de mitigação.

## Figura 10.2. Exemplo de categorias para critérios de risco

| Classificação de risco e pontuação | Tolerância ao risco | Nível de responsabilidade | Resposta a riscos |
|---|---|---|---|
| **Extremo (16-20)** | Inaceitável | Alta administração | Reporte imediato à cúpula e às partes interessadas, com um plano detalhado de resposta a riscos. Adapte os controles, que podem incluir o fortalecimento de medidas existentes e a adição de novas. Monitorar riscos e controles continuamente. |
| **Alto (11-15)** | Inaceitável | Líder do projeto ou equipe | Reporte imediato ao supervisor e às partes interessadas, com um plano detalhado de resposta a riscos. Provavelmente serão necessárias atividades de controle adicionais, considerando tanto os controles flexíveis quanto os rígidos. Monitorar os riscos e controles regularmente. |
| **Moderado (6-10)** | Aceitável | Líder do projeto ou equipe | Reporte imediato ao supervisor, com um plano de resposta detalhado. Aumente, mantenha ou reduza os controles, dependendo da pontuação e das tendências no ambiente de risco. Monitorar riscos e controles regularmente. |
| **Baixo (1-5)** | Aceitável | Gerente do projeto | Ação imediata não é necessária. Reduza os controles se forem considerados muito rigorosos e, portanto, de risco não proporcional. Monitorar os riscos e controles periodicamente. |

Nota: isto é apenas para fins ilustrativos.

As matrizes de risco são uma das várias ferramentas para classificação de risco residual. Uma organização também pode usar classificações absolutas, nas quais prioriza os riscos com base em suas pontuações numéricas. Seja qual for a abordagem, é fundamental que as organizações estejam cientes dos vieses que podem afetar o processo de pontuação da avaliação de risco e implementem processos de controle de qualidade sobre o próprio processo de avaliação de risco. De fato, os gerentes podem ter incentivos para minimizar a percepção de que as atividades que supervisionam são vulneráveis a riscos de corrupção e fraude. Alternativamente, também podem exagerar os riscos para justificar mais investimentos em atividades de controle, ferramentas, treinamentos e outros recursos. Os processos de validação integrados à avaliação de risco podem ajudar a minimizar a influência de vieses.

A documentação e a comunicação dos resultados da avaliação de risco variam de acordo com a organização; no entanto, existem considerações comuns, independentemente do contexto. Primeiro, os registros de riscos ou ferramentas semelhantes podem ser úteis para garantir a capacidade de uma organização de rastrear os riscos ao longo do tempo, melhorar o processo de avaliação de riscos e aprimorar as estratégias de integridade. Painéis baseados na Web que retratam e animam visualmente os riscos também podem ser ferramentas poderosas para facilitar a tomada de decisões sobre medidas de mitigação. Em segundo lugar, embora uma avaliação detalhada possa ser uma ferramenta útil para gerentes e auditores, no contexto de avaliações de risco de integridade, ela também pode consolidar informações confidenciais sobre vulnerabilidades institucionais à fraude e corrupção. Como parte do processo de planejamento de avaliação de risco, as organizações podem considerar e comunicar claramente os controles sobre o próprio processo, incluindo políticas e procedimentos para segurança da informação, anonimato das partes interessadas e uso dos resultados. Isso pode ajudar a aumentar o nível de conforto dos envolvidos e promover o engajamento ativo no processo de avaliação de risco.

### *10.2.3. Monitoramento e avaliação da gestão de risco para a integridade*

O processo de monitoramento e avaliação é um componente-chave de uma estrutura geral de gestão de risco que pode ajudar órgãos e entidades a avaliar políticas e práticas para gerenciar riscos de integridade e fazer alterações conforme necessário. Essa atividade pode ocorrer em nível governamental, com foco em questões sistêmicas, ou dentro de uma organização do setor público para aprimorar a gestão de risco institucional.

#### *Monitoramento e avaliação sistêmica*

Avaliar os padrões, políticas e procedimentos de controle interno e de gestão de riscos da Administração Pública é uma função crítica para as organizações. Órgãos de auditoria interna e externa, órgãos de combate à corrupção e órgãos reguladores geralmente realizam essas avaliações mas essa competência pode variar de acordo com o país. Avaliações externas independentes e abrangentes avaliam as características críticas das políticas de controle interno e gestão de riscos, incluindo até que ponto as normas, políticas e procedimentos abordam os riscos para a integridade e a harmonização de políticas e clareza de papéis e responsabilidades para gerenciar riscos para a integridade. Por exemplo, o Tribunal de Contas da Áustria (ACA) realiza auditorias dos sistemas de prevenção de corrupção das entidades, o que inclui avaliar se uma entidade tem ou não provisões suficientes para mitigar os riscos para a integridade. Essas avaliações podem destacar deficiências em todo o sistema, permitindo que o governo melhore as estruturas de controle interno e gestão de risco por meio de uma abordagem coordenada em todo o governo.

#### *Monitoramento e feedback específicos da organização*

Para lidar com os riscos, mudanças operacionais, regulatórias, tecnológicas e inúmeras outras podem influenciar a eficácia das medidas de controle de fraude e corrupção de uma organização. Portanto, os controles internos individuais, as atividades de gestão de risco e o sistema de controle interno como um todo devem ser monitorados regularmente para garantir que a estrutura esteja funcionando corretamente e os controles sejam ideais. Nesse sentido, as atividades de monitoramento auxiliam as organizações na melhoria contínua dos processos de gestão e controle de riscos: se as atividades de monitoramento descobrirem deficiências, a alta administração (Committee of Sponsoring Organizations of the Treadway Commission, 2013[2]). No contexto da integridade pública, o monitoramento ativo da estrutura de controle interno e gestão de riscos pode ajudar a melhorar a prevenção e a detecção de casos potenciais ou suspeitos de fraude, corrupção ou abuso.

De acordo com a legislação, órgãos específicos podem determinar como as atividades de monitoramento serão realizadas e com que frequência. Avaliações contínuas são processos rotineiros que monitoram as atividades de controle em tempo real, enquanto avaliações separadas podem ser realizadas periodicamente por auditores internos ou partes externas. Ao aplicar uma abordagem baseada em avaliação de risco , as informações coletadas sobre esquemas de fraude e corrupção e áreas de alto risco podem servir como base para atividades demonitoramento.

As instituições devem delinear claramente as atividades de monitoramento e avaliação em sua política de gestão de risco para a integridade, incluindo funções e responsabilidades. Por exemplo, nos Países Baixos, o Escritório para a Promoção da Integridade do Setor Público (BIOS), o Escritório de Integridade do Município de Amsterdã e o Tribunal de Contas dos Países Baixosdesenvolveram conjuntamente o IntoSAINT. Essa ferramenta de autoavaliação de integridade permite que organizações do setor público avaliem sua vulnerabilidade e resiliência a violações de integridade e fornece recomendações sobre como melhorar a gestão de integridade. Os participantes do IntoSAINT selecionam os processos mais vulneráveis com base em um inventário dos processos primários e de suporte da organização avaliada, identificando os riscos de integridade mais significativos entre os selecionados. Estes são combinados com uma avaliação de fatores culturais – como a sensibilização e o papel da gestão – e a adequação das medidas do sistema, ou seja, medidas destinadas a incorporar e consolidar políticas de integridade. Os resultados, que vêm na forma de um relatório, fornecem informações sobre o funcionamento do sistema de integridade existente. Os resultados podem ser utilizados pelas entidades para atualizar suas políticas de integridade ou como ponto de partida para a aplicação de outras medidas de análise de risco mais aprofundadas. Reconhecendo a funcionalidade desta ferramenta, a Polônia desenvolveu uma auto-avaliação de integridade semelhante que é distribuída aos ministérios setoriais.

Outro exemplo demonstra como a Política de Controle de Fraude e Corrupção do Departamento de Justiça e Procurador-Geral (DJAG) de Queensland, Austrália, atribui a um Diretor de Controle de Fraude (FCO) - colocado na Unidade de Governança Corporativa do Departamento - a responsabilidade de melhorar ativamente a estrutura de risco de fraude e corrupção do departamento. O FCO preside o Grupo Operacional de Risco de Fraude, que, entre outras responsabilidades, monitora a estrutura supervisionando as revisões de políticas, questões relacionadas à auditoria, reclamações, treinamento e conformidade, e garante que a estrutura de controle de fraude e corrupção seja submetida a uma revisão a cada dois anos ou com maior frequência, se necessário (Department of Justice and Attorney-General, 2017[16]).

### *10.2.4. Procedimentos coerentes e responsivos dentro da estrutura de controle interno e gestão de risco*

O controle interno dentro dos órgãos e entidades do setor público deve conter procedimentos claros para responder a suspeitas de violações da lei, de processos ou a ocorrência de violações de integridade. Embora a ação necessária possa variar entre as organizações e depender do tamanho, função e arranjos de governança, a administração pública pode desempenhar um papel essencial na coordenação de relatórios e respostas a suspeitas de violações de integridade nas organizações do setor público.

#### *Garantir a coerência na forma como as organizações respondem a violações de integridade*

O Governo Federalpode estabelecer protocolos e mecanismos padrão para relatar e responder a suspeitas de violações de integridade. Essa abordagem pode garantir que todas as organizações do setor público tenham disposições suficientes para responder à corrupção e violações de integridade dentro de sua estratégia geral de integridade. Também reduz a duplicação e minimiza as lacunas em relação à estrutura de controle interno e gestão de risco em organizações do setor público. O governo federal ou outro órgão responsável pode garantir que procedimentos e critérios comuns sejam usados para que os

agentes públicos e o público em geral possam denunciar suspeitas de violações sem medo de represálias. Por exemplo, o governo federal pode desenvolver disposições que exijam que organizações do setor público estabeleçam linhas de comunicação separadas, como linhas diretas. Canais de denúncia claros e a existência de mecanismos de denúncia coerentes são características-chave de um sistema de controle interno eficaz.

#### *Respondendo a violações de integridade dentro de uma organização*

Embora as políticas e orientações fornecidas pelo governo federal apoiem a coerência, elas nem sempre refletem o contexto institucional de todas as organizações do setor público. Como tal, mecanismos claros podem apoiar essas organizações na resposta a possíveis violações de integridade ou violações da lei.

A principal maneira de detectar possíveis violações de integridade ou violações da lei é por meio dos funcionários. As organizações do setor público podem criar uma cultura na qual os agentes públicos se sintam seguros para denunciar se souberem de suspeitas de violação de integridade (para mais informações, consulte o Capítulo 9). Deve haver canais de denúncia internos e externos claros para agentes públicos, e os denunciates devem receber proteção suficiente ao relatar suspeitas de corrupção ou fraude. Diretrizes devem estar em vigor dentro da organização que estipulem quais procedimentos devem ser seguidos no caso de um funcionário relatar uma suposta má conduta e quais opções estão disponíveis para eles. Os agentes públicos podem relatar suspeitas de violações a seus líderes, pessoal de recursos humanos, unidade de auditoria interna da organização ou outro unidade designada. Muitas organizações do setor público têm linhas diretas para facilitar denúncias anônimas. Independentemente da forma, divulgar claramente os meios e canais de denúncia facilita a implementação de mecanismos de comunicação.

Quando uma suspeita de fraude ou corrupção é identificada dentro de uma organização, os processos precisam estar aptospara desencadear uma resposta apropriada. Esses processos dependerão da natureza e gravidade da suposta conduta. Por exemplo, reclamações podem ser tratadas pela administração, enquanto casos mais graves, particularmente aqueles em que a conduta alegada pode constituir uma ofensa criminal, podem justificar uma resposta investigativa completa. Os objetivos de qualquer investigação precisam ser claramente definidos na política de integridade, e esses objetivos devem ser seguidos durante toda a investigação interna. Além disso, as investigações devem garantir o cumprimento da legislação vigente (criminal e trabalhista) e dos procedimentos investigativos.

Uma vez que uma investigação tenha sido realizada, as descobertas precisam ser transmitidas à administração. As organizações devem então determinar a ação a ser tomada em resposta aos resultados. Se uma ocorrência de fraude ou corrupção realmente ocorreu, as ações corretivas podem variar de ação disciplinar a encaminhamento criminal. No caso de denúncias criminais, quaisquer obrigações de denúncia externa devem ser estabelecidas na política de integridade da organização. Além disso, a administração pode adotar uma abordagem de “lições aprendidas” para casos de fraude e corrupção após uma investigação.

### *10.2.5. Uma função de auditoria interna que garanta consultoria independente e objetiva para fortalecer o controle interno e a gestão de riscos para a integridade*

#### *O valor agregado da auditoria interna*

A função de auditoria interna examina a adequação e eficácia dos sistemas de controle interno das organizações do setor público, procedimentos, estruturas de governança, processos de gestão de risco e desempenho das operações (The Institute of Internal Auditors, 2016[17]). Espera-se, portanto, que o papel da auditoria interna se estenda além das abordagens orientadas para a conformidade e baseadas em regras para avaliar os controles. Essa visão contemporânea da auditoria interna captura o valor mais amplo que a função pode agregar a uma organização. A auditoria interna pode contribuir não apenas para o alcance dos

objetivos financeiros e controle de recursos, mas também para melhorar a tomada de decisões e a gestão de riscos em apoio aos objetivos estratégicos, táticos operacionais.

Os auditores internos dos órgãos e entidades do setor público desempenham um papel importante ao fornecer avaliações independentes e objetivas sobre se os recursos públicos estão sendo gerenciados de forma eficaz para alcançar os resultados pretendidos. Evidências, objetivos e insights , baseados em valor, podem ajudar as organizações do setor público a gerenciar e avaliar melhor os riscos de integridade. Espera-se que os auditores avaliem o potencial de fraude e como a organização gerencia o risco de fraude (The Institute of Internal Auditors, 2016[17]). Na prática, isso envolve identificar os fatores de risco de integridade no decorrer do trabalho de auditoria interna e avaliar se esses riscos estão sendo gerenciados de forma eficaz, mesmo que a organização do setor público não tenha programas formais de gestão de risco para a integridade implementados. Por exemplo, os auditores internos podem sinalizar áreas de alto risco para violações de integridade, como relacionamentos com terceiros, atividades terceirizadas ou compras. As recomendações de auditoria, para melhorar o ambiente de controle nessas áreas operacionais de alto risco, podem impulsionar os esforços da organização para prevenir e detectar fraudes e corrupção.

No entanto, não se espera que os auditores internos sejam investigadores. Na verdade, os mesmos padrões reconhecem que, embora os auditores internos devam ter conhecimento suficiente para avaliar os fatores de risco de fraude e a gestão de riscos de fraude dentro da organização, os auditores não precisam ter conhecimento ou experiência para assumir um papel investigativo. O papel da auditoria interna em relação às investigações de suspeitas de violação de integridade depende de vários fatores, como a estrutura da organização e a disponibilidade de recursos. Por exemplo, a Agência de Auditoria Interna do Governo (GIAA) no Reino Unido oferece uma linha de serviço distinta que aconselha as organizações do setor público sobre estratégias antifraude e como investigar suspeitas de fraude interna ou de fornecedores. Este serviço especializado é adicional às atividades principais de auditoria interna que o GIAA oferece. Em seu relatório anual 2018-19, o GIAA indicou que o trabalho da unidade antifraude e investigações levou à detecção de 1 milhão de libras esterlinas desviadas e evitou a perda de mais de 1 milhão de libras nas organizações do setor público que contrataram seus serviços.

Os auditores internos também devem avaliar a eficácia dos objetivos e atividades da organização relacionados à ética e os processos para promover a ética e os valores. Isso pode incluir, por exemplo, avaliações da eficácia da estrutura de governança na promoção de uma cultura de integridade ou auditorias de processos de tratamento de denúncias. As avaliações periódicas dos riscos de integridade pela auditoria interna podem destacar áreas com maior exposição a violações de integridade, permitindo que a administração tome medidas corretivas prontamente. A Agência Anticorrupção Francesa (AFA) observou em sua pesquisa de 2018 sobre a prevenção da corrupção no governo local que, em algumas organizações do setor público, as atividades de prevenção da corrupção estão explicitamente incluídas no rol de competências de auditoria interna.

Além de suas contribuições para a avaliação dos fatores de risco de integridade, os auditores internos podem desempenhar um papel crítico avaliando se os controles internos para gerenciar os riscos de integridade estão operando de forma eficaz e eficiente e identificando áreas de melhoria. Isso pode assumir a forma de auditoria ou avaliação da eficácia dos componentes da gestão de risco para a integridade, como programas anticorrupção ou anti-suborno, ou avaliação de quão bem os componentes estão trabalhando juntos. A seleção de auditoria baseada em risco pode ajudar os auditores internos a determinar a melhor forma de identificar os riscos mais relevantes para os objetivos da organização e a tomar decisões sobre o que auditar com base em critérios de risco predeterminados. Essa abordagem, ao contrário das abordagens cíclicas ou baseadas em incidentes, pode ajudar os auditores a evitar as armadilhas das abordagens orientadas à conformidade e deixar de sobrecarregar os gestores com auditorias e controles.

Os resultados da atividade de auditoria interna podem, portanto, apoiar os gestores no alinhamento dos processos e controles de gestão de risco para a integridade com os objetivos organizacionais, para que esses processos ajudem a avançar nas metas estratégicas e subsidiem a tomada de decisões. Várias estruturas e orientações, gratuitas e pagas, estão disponíveis de forma on-line para apoiar os auditores internos na avaliação de medidas de integridade ou programas antifraude. Em geral, as estruturas e orientações fornecem ideias para aprimorar tanto os controles "rígidos" (ou seja, políticas, procedimentos, estrutura etc.), quanto os controles ''flexíveis'' (ou seja, cultura, gestão comportamental, alta administração etc.) reconhecendo, ao mesmo tempo, a necessidade de os auditores levarem em consideração o comportamento, motivação e atitudes humanas.

Os auditores internos podem desempenhar outras funções críticas para promover a integridade dentro de uma organização do setor público. Por exemplo, eles podem fornecer uma visão independente e objetiva dos riscos estratégicos, operacionais e de reputação internos e externos para aprimorar as avaliações de risco da própria administração. Além disso, a função de auditoria interna pode ser uma aliada da administração para promover uma cultura de integridade. Isso inclui a participação na conscientização sobre os riscos, apoio à capacitação (por exemplo, treinamento e workshops) e contribuição para mensagens baseadas em valores sobre integridade e boa governança.

### *Traçar uma linha entre a auditoria interna e a gestão de riscos*

É fundamental que os auditores internos mantenham sua independência das outras linhas de defesa, que incluem gerentes (primeira linha) e gerentes de risco (segunda linha). Essas linhas geralmente são confusas quando se trata de gestão de riscos para a integridade, em parte por causa dos padrões mencionados acima que definem explicitamente um papel para a auditoria interna na avaliação de riscos de integridade. No entanto, as organizações devem garantir que a auditoria interna não assuma todas as responsabilidades relacionadas a gestão de riscos para a integridade. Os gerentes de "segunda linha" em funções como controle financeiro, garantia de qualidade, conformidade e unidades de inspeção também têm um papel fundamental a desempenhar. Por exemplo, avanços em técnicas analíticas, como mineração de dados e software de correspondência, podem permitir que os gerentes de risco monitorem transações financeiras incomuns que possam sinalizar uma violação de integridade. Tabela 10.2 sugere maneiras de delinear as funções e responsabilidades específicas dos auditores internos para evitar duplicação ou sobreposição com outras linhas de defesa.

**Tabela 10.2. O papel de um auditor interno na gestão de risco para a integridade**

| | |
|---|---|
| *Funções essenciais* de auditoria interna | Fornecer independência que garanta eficácia e eficiência dos processos de gestão de risco |
| | Avaliar os processos de gestão de risco |
| | Avaliar o relato dos principais riscos |
| | Rever a gestão dos principais riscos |
| | Fazer recomendações para melhorar a gestão de riscos |
| Funções legítimas de auditoria interna *com ressalvas* | Facilitar a identificação e avaliação de riscos |
| | Gerir coaching na resposta a riscos |
| | Consolidar relatórios sobre riscos |
| | Desenvolver e atualizar a estrutura de gestão de risco |
| | Defender as práticas de gestão de risco |
| Funções que a auditoria interna *não deve assumir* | Definir critérios de risco |
| | Impor processos de gestão de risco |
| | Realizar avaliações de risco para gerentes |
| | Decidir como mitigar ou responder aos riscos |
| | Implementar medidas de mitigação de riscos para a gestão |

Fonte: Adaptado de (The Institute of Internal Auditors, 2009[18]).

O papel específico que a função de auditoria interna desempenhará em relação a gestão de riscos ou, de maneira mais geral, em relação à prevenção de fraude e corrupção, é específico do contexto. Tabela 10.2 oferece algumas diretrizes relativas a padrões e boas práticas; no entanto, em alguns países, as leis ou políticas oferecem poucos detalhes sobre o papel da auditoria interna com tanta especificidade ou, na pior das hipóteses, definem um papel aparentemente contraditório aos padrões e boas práticas internacionais. Isso pode ser remediado até certo ponto no nível institucional. O papel da auditoria interna no que diz respeito à prevenção de fraude e corrupção, ou gestão de risco para antegridade, precisa ser claramente definido em políticas ou em documentos e orientações estratégicas relevantes, como um estatuto de auditoria. Este documento pode definir claramente o papel da auditoria interna em relação à prevenção e detecção de fraude e corrupção, incluindo a avaliação da gestão de riscos para a integridade, conscientização, investigações e relatórios para a alta administração. Como sua competência geralmente abrange os processos e procedimentos da organização como um todo, a auditoria interna está bem posicionada para fornecer relatórios consolidados sobre a gestão de riscos para a integridade no nível institucional.

As funções de auditoria interna nos órgãos e entidades públicos geralmente contam com um número pequeno de agentes públicos e recursos limitados; a coordenação com outros órgãos, é, portanto, vital. Os auditores podem recorrer ao trabalho dos gerentes de “segunda linha”, como unidades, comitês ou outras unidades da estrutura organizacional, que também têm um papel na avaliação da eficácia das práticas de risco de integridade. Isso pode envolver o compartilhamento de conhecimento em uma base informal, coordenação no momento das atividades para minimizar o impacto na área sob revisão ou critérios formais para confiança no trabalho de cada um. No nível federal, uma abordagem coordenada para abordara gestão de riscos para a integridade pode ajudar a quebrar as barreiras entre órgãos e entidades do setor público, fornecer consistência nas medidas de mitigação de riscos e levar a uma melhor governança dos riscos de integridade em geral.

## 10.3. Desafios

Os desafios enfrentados por governos e organizações do setor público diferem até certo ponto quando se trata de implementar estruturas de controle interno e gestão de risco para a integridade. Os governos estão em diferentes estágios de maturidade a esse respeito e, portanto, enfrentam questões diferentes. No entanto, existem desafios comuns que surgem entre os países. Esta seção fornece uma visão geral de algumas das dificuldades que os países enfrentam e maneiras de superá-las para melhor preservar a integridade. As áreas de foco são:

- superar as lacunas de implementação, indo além das abordagens de verificação para a gestão de riscos;
- garantir que as avaliações e controles de riscos se adaptem a um ambiente de mudanças;
- coordenar a atuação dos órgãos policiais e de investigação para aprimorar os ciclos de feedback e melhorar as avaliações de riscos.

### *10.3.1. Superar as lacunas de implementação, indo além das abordagens de verificação check-the-box para a gestão de riscos*

Uma abordagem sistemática – pela qual a gestão de risco está claramente vinculada aos objetivos organizacionais, integrado aos processos existentes – é vital para uma governança eficaz dos riscos de integridade no setor público. Isso requer uma base legislativa forte, acompanhada de normas e políticas, que forneça a base para o controle interno e gestão de risco. Embora muitos países tenham essas disposições em vigor, muitas vezes há lacunas na forma como os governos e as organizações do setor público implementam os processos de gestão de risco. Por exemplo, alguns enxergam as avaliações de

risco como um exercício orientado para a conformidade ou verificações e, como tal, as realizam de forma ad hoc. Além disso, a alta administração e outros agentes podem perceber a gestão de risco para a integridade como uma função que está além de sua competência, preferindo a auditoria interna. Para superar esses desafios e fortalecer as práticas de controle interno e gestão de risco nas entidades do setor público, a administração pode fazer o seguinte:

- *Atribuir responsabilidades claras* – As políticas de integridade podem atribuir responsabilidades pela gestão de risco de corrupção, ou essas disposições podem ser incluídas em políticas de gestão de risco existentes como parte do ambiente de controle. De acordo com padrões e modelos internacionais (por exemplo, as Três Linhas de Defesa do Instituto de Auditores Internos), a administração deve ser responsável pela identificação e gestão de riscos, mas cada agente público contribui para o sucesso da gestão de riscos dentro de uma entidade. Juntamente com as funções de gestão de risco, os gestores são responsáveis pela gestão diária dos riscos de fraude e corrupção – o que inclui garantir que os controles internos estejam implementados e funcionando – e, de forma mais geral, pela prevenção e detecção de riscos de fraude e corrupção.
- *Aumentar a capacidade através da formação* – Programas de formação formalizados, regulares e contínuos permitem o desenvolvimento de competências e capacidades na gestão de riscos. Se os recursos forem limitados, as prioridades de treinamento devem visar principalmente o pessoal com responsabilidade direta pela identificação e mitigação dos riscos de fraude e corrupção. Os instrutores podem usar pesquisas de funcionários, padrões reconhecidos internacionalmente e grupos de consulta para identificar as necessidades de treinamento. Além disso, avaliações regulares de treinamento ajudam a garantir que os treinamentos de agentes públicos levem em consideração os riscos específicos de fraude e corrupção que ocorrem em diferentes entidades. Para saber mais, consulte o Capítulo 8.

### *10.3.2. Garantir que as avaliações e controles de risco se adaptem a um ambiente de mudança*

Os riscos de integridade sistêmica podem prosperar em entidades que não realizam avaliações regularmente, pois as atividades de controle podem se tornar ineficazes em relação a um ambiente de risco dinâmico. Os esquemas de corrupção e fraude evoluem constantemente, muitas vezes em resposta a mudanças nos controles. Além disso, nos casos mais flagrantes, um esforço ad hoc para gerenciar e avaliar os riscos de integridade pode ser resultado de controles e ferramentas de detecção que se sobrepõem à administração. Portanto, é fundamental que as políticas e estruturas para avaliar os riscos de integridade estipulem a avaliação em intervalos regulares para fornecer uma imagem abrangente e atual do perfil de risco da organização, bem como a eficácia dos controles.

As organizações do setor público precisam monitorar e testar controles selecionados, principalmente em áreas que enfrentam riscos mais altos, para verificar se estão funcionando de forma eficaz e são proporcionais aos riscos identificados. Dado o fato de que vários funcionários e vários departamentos estão envolvidos nas medidas de mitigação de risco, é preciso haver uma comunicação clara de como avaliar a eficácia dos controles nos procedimentos e orientações relevantes. O teste de qualidade de controle fornece evidências de como os controles mitigam os riscos e devem ser comunicados a todos os proprietários de risco.

### *10.3.3. Coordenar a atuação dos órgãos policiais e de investigação para aprimorar os ciclos de feedback e melhorar as avaliações de riscos*

Em toda Administração Pública, a coordenação entre órgãos e entidades é vital para o encaminhamento de casos suspeitos de fraude e corrupção às autoridades policiais e outros órgãos relevantes. No entanto, as organizações muitas vezes enfrentam dificuldades em relatar às autoridades os resultados dos incidentes de fraude e corrupção que tomam conhecimento. A falta de comunicação sobre os casos

processados representa um desafio significativo para as entidades ao revisar seus controles e tomar medidas corretivas.

Melhorar os ciclos de feedback em relação ao processo pode aprimorar as avaliações de risco, desestimular a fraude e a corrupção e permitir que as organizações lidem com vulnerabilidades de controle de forma mais eficaz, reduzindo o risco de ocorrências semelhantes no futuro. Uma maneira de conseguir isso é criar workshops de compartilhamento de informações com a participação de órgãos policiais e de investigação, com o objetivo de ajudar essas organizações a identificar tendências, padrões e modos de operação de fraude e corrupção.

## Referências


Committee of Sponsoring Organizations of the Treadway Commission (2016), *Fraud Risk Management Guide*, https://www.coso.org/Pages/Purchase-Guide.aspx (accessed on 17 February 2020). [7]

Committee of Sponsoring Organizations of the Treadway Commission (2013), *Internal Control - Integrated Framework*, https://www.coso.org/Pages/ic.aspx (accessed on 17 February 2020). [2]

Crime and Corruption Commission (2018), *Fraud and Corruption Control - Best Practice Guide*, https://www.ccc.qld.gov.au/publications/fraud-and-corruption-control-best-practice-guide (accessed on 17 February 2020). [9]

Department of Justice and Attorney-General (2017), *Fraud and corruption control policy*, https://www.justice.qld.gov.au/__data/assets/pdf_file/0020/534350/fraud-and-corruption-control-policy.pdf. [16]

Estonian Ministry of Justice (2013), *Anti-Corruption Strategy 2013-2020*, https://www.korruptsioon.ee/en/anti-corruption-activity/anti-corruption-strategy-2013-2020 (accessed on 24 January 2020). [8]

European Commission (2015), *Public Internal Control Systems in the European Union*, https://ec.europa.eu/budget/pic/lib/docs/2015/CD02PrinciplesofPIC-PositionPaper.pdf. [6]

Fountain, L. (2015), *Raise the Red Flag: An Internal Auditor's Guide to Detect and Prevent Fraud*, The Institute of Internal Auditors Research Foundation. [15]

International Organization for Standardization (2018), *ISO 31000:2018, Risk Management - Guidelines*, https://www.iso.org/iso-31000-risk-management.html. [10]

Irish Health Service Executive (2018), *Risk Management Support Tools*, https://www.hse.ie/eng/about/qavd/riskmanagement/risk-management-documentation/risk%20management%20support%20tools%20.html (accessed on 17 February 2020). [11]

National Audit Office (2011), *Managing risks in government*, https://www.nao.org.uk/report/managing-risks-in-government/ (accessed on 17 February 2020). [13]

OECD (2017), *OECD Recommendation of the Council on Public Integrity*, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0435 (accessed on 24 January 2020). [1]

OECD (2015), *Prevention of Corruption in the Public Sector in Eastern Europe and Central Asia*, OECD Anti-Corruption Network for Eastern Europe and Central Asia, OECD, Paris, http://www.oecd.org/investment/anti-bribery/ACN-Prevention-Corruption-Report.pdf. [12]

The Institute of Internal Auditors (2016), *International Professional Practices Framework (IPPF) – Standards and Guidance*, https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx. [17]

The Institute of Internal Auditors (2009), *The Role of Internal Auditing in Enterprise-Wide Risk Management*, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf. [18]

U.S. Government Accountability Office (2015), *A Framework for Managing Fraud Risks in Federal Programs*, https://www.gao.gov/assets/680/671664.pdf. [4]

U.S. Government Accountability Office (2014), *Standards for Internal Control in the Federal Government*, https://www.gao.gov/assets/670/665712.pdf. [3]

U.S. Office of Management of Budget (OMB) (2016), *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf. [5]

Wright Jr., R. (2013), *The Internal Auditors' Guide to Risk Assessment*, The Institute of Internal Auditors Research Foundation. [14]

## Notas

[1] O ambiente de controle consiste no conjunto de padrões, processos e estruturas que fornecem a base para realizar o controle interno em uma organização.

[2] No modelo das Três Linhas de Defesa, a primeira linha de defesa são os gerentes operacionais que possuem e gerenciam os riscos. A segunda linha de defesa são as funções que supervisionam os riscos, normalmente as funções de gestão de riscos e conformidade. A terceira linha de defesa são as funções de auditoria interna que fornecem garantia independente de que os processos de gestão de risco são eficazes.

[3] Riscos inerentes são riscos que são avaliados na ausência de medidas de controle, ou seja, antes que as medidas de controle tenham sido aplicadas.

[4] O risco residual é o nível de risco remanescente após a aplicação das medidas de mitigação.

[5] Os riscos estratégicos são a probabilidade de algo acontecer que pode afetar a capacidade de uma organização de alcançar os resultados pretendidos. Os riscos operacionais são a probabilidade de algo acontecer que afetará a capacidade de uma organização de atingir seus objetivos e produzir resultados. Os riscos de reputação referem-se ao potencial de publicidade negativa, percepção pública ou eventos incontroláveis que tenham um impacto adverso na reputação de uma organização.

[6] Fatores de risco são características do ambiente, políticas, procedimentos ou atividades de uma organização que estão associados a um alto risco.

[7] A tolerância ao risco é o nível de risco que os gerentes estão dispostos a aceitar após a implementação das atividades de controle. Definir a tolerância ao risco ajuda a orientar os agentesem suas decisões de aceitar, reduzir, evitar ou compartilhar riscos.

[8] Um mapa de calor é uma representação das avaliações quantitativas e quantitativas resultantes da probabilidade de ocorrência de risco e do impacto na organização no caso de um risco específico ocorrer.