

ANÁLISE DO CONTROLE INTERNO SOB O FOCO DE GERENCIAMENTOS DE RISCOS E DA PREVENÇÃO À CORRUPÇÃO - SUGESTÃO DE ROTEIRO DE AUDITORIA.

Objetivo:

O presente documento tem objetivo de descrever práticas de análise do Controle Interno sob o foco do gerenciamento de riscos, bem como práticas de prevenção à corrupção através das recomendações mais reconhecidas na atualidade nacionalmente e internacionalmente. A finalidade é servir como roteiro de auditoria a fim de avaliar o grau de maturidade do controle interno e orientar aos órgãos da administração direta e indireta para formação na direção um controle interno voltado à mitigação de riscos.

Autor: Leonardo Castro

Sumário

1. Introdução e contextualização	4
2. Metodologia	6
3. Práticas anticorrupção sob a perspectiva do controle interno	8
3.1. Código de Conduta	8
3.2. Gerenciamento dos Recursos Humanos sobre perspectiva da prevenção à corrupção	12
3.2.1. Treinamentos	12
3.2.2. Rotação de funções	13
3.2.3. Gestão de recursos Humanos baseado em mérito	16
3.2.4. Modelo de gestão e envolvimento dos colaboradores.....	18
3.3. Princípio da conferência cruzada (Quatro olhos).....	21
3.4. Segregação de funções.....	25
3.5. Supervisão adequada	29
3.6. Questões diversas de avaliação de controle interno:	29
3.7. Outras medidas anticorrupção.....	31
4. Metodologia de análise e gerenciamento do risco de riscos	34
4.1. Ambiente de Controle	40
4.1.1. Integridade na organização (Programa de integridade)	40
4.1.2. Compromisso com a competência.....	42
4.1.3. Tom no topo e estrutura organizacional.....	43
4.1.3.1. Apoio ao controle interno e estrutura organizacional.....	44
4.1.4. Política de gerenciamento de recursos humanos	52
4.1.5. Definição de responsabilidades	52
4.2. Avaliação dos riscos.....	53
4.2.1. Tratamento dos riscos.....	62
4.3. Atividades de Controle	64
4.4. Informação e comunicação	68
4.5. Atividade de monitoramento.....	71
5. Auditoria – Resumo de procedimentos de avaliação do controle interno sob ótica da prevenção da corrupção	72
5.1. Avaliação do ambiente de controle, código de conduta e sistema de gerenciamento de riscos	76
5.2. Avaliação do controle interno com orientação de boas práticas de prevenção da corrupção	84

6. Referência bibliográfica	93
7. ANEXO I - Exemplo de Mapa de Riscos	96
8. ANEXO II – Lista exemplificativa de possíveis riscos do Tribunal de Contas Federal da Alemanha	97

1. Introdução e contextualização

Este documento tem como proposta de aplicação para possível uso do Tribunal de Contas do Município de São Paulo sobre o papel do controle externo no gerenciamento de riscos e prevenção à corrupção na Administração Pública. Trata-se da compilação de diversos documentos e práticas internacionais a partir da análise do controle interno da administração pública, utilizando-se as metodologias sobre controle interno orientadas à mitigação de fraudes e riscos.

A auditoria com foco à mitigação à riscos e prevenção da corrupção não se caracteriza propriamente como uma auditoria de regularidade. Tem dessa maneira características de auditoria operacional¹ na medida que tem função de aconselhamento aos órgãos auditados para boas práticas. O trabalho de convencimento (à Origem) pela equipe de auditoria é essencial nesse aspecto.

Este documento aborda estruturas e procedimentos de gerenciamento de riscos e práticas anticorrupção dentro da ótica controle interno encontradas em diversas publicações.

Uma das chaves à prevenção à corrupção, que é conhecida por cientistas dedicados ao tema da corrupção sob aspecto sociológico² e comportamental, é que é necessárias mudanças no comportamento dos agentes econômicos, o qual inclui naturalmente os agentes públicos, através da criação de uma forte cultura integridade nas instituições, não bastando a mera normatização de regras. Torna-se em certa medida um desafio menos tangencial do ponto da auditoria clássica, visto que o comportamento e a cultura dos órgãos e instituições da administração pública não costuma ser objeto de auditoria, mas sendo possível de análise e avaliação, principalmente com ajuda de questionários junto aos funcionários das entidades públicas para se levantar percepções.

Há duas vertentes neste documento: A primeira vertente é orientada à mitigação de riscos em geral, utilizando-se práticas de criação de ambiente de

¹ ISSAI 5700, linhas 7-8.

² Para tais se pode se citar Donald R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*.

controle, análise de riscos, reação aos riscos e criação de controles como resposta, comunicação devida e monitoramento. Estes serão tratados no capítulo 4, sendo a base para a construção de um controle interno consistente.

Uma segunda vertente é colocada em relação aos possíveis métodos anticorrupção em rotina de trabalho das instituições públicas. Tais práticas englobam o tratamento devido de um código de conduta com a correspondente conscientização e treinamento dos funcionários (será utilizada a palavra funcionário ao longo deste trabalho, independente do regime de contratação³), a delimitação/segregações de funções, a rotação de funcionários, uma unidade de auditoria interna, informatização de sistemas, entre outros, que serão tratadas no capítulo 0.

Frisa-se que a segunda vertente (práticas anticorrupção) é uma parte da primeira vertente (controle interno voltado ao gerenciamento de riscos), isto é, a segunda é englobada pela primeira. Contudo, serão tratadas primeiramente as práticas anticorrupção ao invés da base teórica, vez que a familiarização destas, principalmente sobre o papel do código de conduta, deixará mais fluída a teoria sobre a construção de sistema de controle com a ótica de gerenciamento de riscos.

Atenta-se que este documento não aborda técnicas de investigação de corrupção, vez que o controle externo não é legalmente responsável para conduzir investigações que envolvam ilícitos criminais, cabendo tal atribuição ao Ministério Público e polícia federal (ou estadual). Assim, de imediato não se deve confundir prevenção com investigação. Não serão tratados aspectos de investigação no presente documento, nem sobre o tratamento correspondente previsto no código criminal e em diversas leis específicas que tipificam o crime de corrupção e outros crimes conexos.

³ A palavra funcionário pode ser imprópria do ponto de vista do direito administrativo visto que há servidores públicos estatutários, comissionados em cargos públicos, celetistas em emprego público, entre outros. Contudo, apenas para facilitar a leitura, todos os que exercem alguma atividade na administração pública serão denominados de funcionários no presente trabalho.

Embora a legislação tenha definições jurídicas sobre corrupção e crimes conexos⁴, será adotada uma definição mais ampla, sendo definido como o abuso da função pública para ganho privado⁵ com prejuízo da finalidade pública.

2. Metodologia

O capítulo 3 do presente documento trata diretamente de práticas de prevenção da corrupção e tem sua base primária na tradução e adaptação necessária da ISSAI 5700⁶. Tal ISSAI é denominada “Diretrizes para auditoria de prevenção à corrupção” de autoria de grupo de trabalho específico temático da INTOSAI – *International Organization of Superior Auditing Institutions*. A razão é que a ISSAI 5700 é um documento elaborado pela INTOSAI, portanto com aceitação de diversos órgãos de controle no mundo e especificamente direcionada à atividade de auditoria externa sobre a avaliação e recomendações de práticas de prevenção da corrupção. Também foram utilizadas nos questionários planilhas de avaliação do controle interno e riscos do Tribunal de Contas de Portugal e materiais obtidos em âmbito de pesquisa⁷.

No capítulo 4, que tratam dos modelos controle interno sob ótica de gerenciamento de riscos, foram utilizadas diversas outras fontes, com as traduções livres necessárias (vide capítulo 6 Referência Bibliográfica), as quais cita-se:

- ✓ INTOSAI GOV 9100;
- ✓ Roteiro de Auditoria de Gestão de Riscos da Secretaria de Métodos e Suporte do TCU;
- ✓ Convenção das nações unidas contra corrupção⁸;
- ✓ Planilhas de avaliação do controle interno e riscos do Tribunal de Contas de Portugal;

⁴ Para as diversas definições sobre corrupção, recomenda-se a leitura do artigo denominado “Definição do Conceito de Corrupção no Direito Administrativo Brasileiro” de Rafaela Barranco Bastos . Disponível em https://rafaelabasso.jusbrasil.com.br/artigos/555254522/definicao-do-conceito-de-corrupcao-no-direito-administrativo-brasileiro#_ftn6

⁵ Definição dada pela organização Transparency International. <https://www.transparency.org/what-is-corruption#define>

⁶ http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm

⁷ Como Documentos da Organização Transparency International e palestras de simpósio de combate à corrupção na universidade de Kehl e em Suttgart.

⁸ https://www.unodc.org/documents/lpo-brazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf

- ✓ Modelos de avaliação de gerenciamento de riscos e controles dos Tribunais de Contas da Alemanha e da Áustria.
- ✓ Guias do Committee of Sponsoring Organizations of the Treadway Commission – COSO;
- ✓ Manual para implementação de programas de integridade da CGU;
- ✓ Roteiro de Auditoria de Gestão de Riscos do TCU.
- ✓ Regulamentos da Alemanha como exemplos de boas práticas.

Por fim, o capítulo 5 condensa as sugestões de como auditar o controle interno sob a perspectiva do gerenciamento de riscos e boas práticas à prevenção da corrupção.

3. Práticas anticorrupção sob a perspectiva do controle interno

A base teórica de um sistema de controle interno estruturado a partir das metodologias internacionalmente mais reconhecidas na atualidade é primordial, mas irá ser tratada posteriormente no capítulo 4. Assim, inicialmente, irão ser tratadas diretamente algumas das práticas anticorrupção como parte do controle interno de uma entidade pública. A finalidade de primeiro se proceder a prática neste capítulo, e depois à teoria, é deixar menos abstrata a teoria da formação de um controle interno robusto (capítulo 4).

Cabe aqui a observação que as palavras organização, instituição ou entidade serão utilizadas *lato sensu* em referência aos órgãos da administração direta, tais como secretarias e departamentos especializados subordinados às secretarias, bem como da administração indireta como autarquias, empresas públicas, sociedades de economia mistas e fundações públicas, bem como a palavra funcionário, em sentido *lato*, servindo para servidores concursados, admitidos, comissionados e outros regimes de contratação.

3.1. Código de Conduta

Um código de ética (ou código de conduta) é um conjunto de princípios comuns que vinculam qualquer pessoa, desde o nível gerencial até um nível operacional, para se comportar adequadamente de acordo com a expectativa das partes interessadas (*stakeholders*), especialmente expectativas da sociedade civil. O código de ética é uma orientação moral a ser obedecida por todos os administradores e funcionários de uma organização para manter a credibilidade individual e organizacional.

A função do código de conduta não deve ser negligenciada como mera formalidade. Ela é base prática sobre um programa/plano de integridade e o correspondente ambiente de controle, que será tratado no capítulo 4.

Destaca-se que o código de conduta é o elo essencial do aspecto comportamental para quebra da chamada “auto justificção” do triângulo da fraude

de Cressey⁹, pois este tem a finalidade de criar uma cultura de integridade dentro de uma organização e alterar a percepção que os funcionários tem sobre a própria organização, atuando como barreira preventiva à corrupção.

Contudo, o código de conduta não deve ser apenas uma mera regra normativa formal. É necessário conscientização e sensibilização dentro da instituição junto aos funcionários através de treinamentos (INTOSAI, 2016¹⁰). A prevenção eficaz contra a corrupção pode ser alcançada se toda a administração e equipe entenderem corretamente o código de conduta da instituição. Um bom entendimento do código de ética de uma instituição pode ser alcançado por meio de uma disseminação regular e eficaz do código para todos os níveis da organização. A intenção dessa disseminação é melhorar ou alterar a cultura dentro de uma organização pública estabelecendo padrões de comportamentos esperados, e não somente prever punições em caso de infrações ao próprio código.

A este respeito, a Convenção das Nações Unidas contra a Corrupção (ONU, 2004) estabelece no Artigo 8 que¹¹:

“Artigo 8 Códigos de conduta para funcionários públicos

1. Com o objetivo de combater a corrupção, cada Estado Parte, em conformidade com os princípios fundamentais de seu ordenamento jurídico, promoverá, entre outras coisas, a integridade, a honestidade e a responsabilidade entre seus funcionários públicos.

2. Em particular, cada Estado Parte procurará aplicar, em seus próprios ordenamentos institucionais e jurídicos, códigos ou normas de conduta para o correto, honroso e devido cumprimento das funções públicas..”

Nesse sentido, é válido observar que na PMSP já foi instituído um código de ética em 26.05.15, através do Decreto Nº 56.130/15. Tal Decreto estabelece “no âmbito do Poder Executivo, o Código de Conduta Funcional dos Agentes Públicos e da Alta Administração Municipal, compreendendo normas de conduta funcional,

⁹ Other People's Money: A Study in the Social Psychology of Embezzlement (1953)

¹⁰ Every public institution should disseminate the code of ethics as an integrated part of corruption prevention. ISSAI 5700, pág 29, linha 10 e 11.

¹¹https://www.unodc.org/documents/lpo-brazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf

de educação ética e de prevenção à corrupção.”¹². Conforme artigo 2º do referido código, são objetivos do Código de Conduta Funcional dos Agentes Públicos e da Alta Administração Municipal:

- I - estabelecer, no campo ético, normas específicas de conduta funcional;
- II - orientar e difundir os princípios éticos, prevenindo condutas disfuncionais e ampliando a confiança da sociedade na integridade das atividades desenvolvidas pela Administração Pública Municipal;
- III - reforçar um ambiente de trabalho ético que estimule o respeito mútuo entre os servidores e a qualidade dos serviços públicos;

Este código cumpre com recomendações da ISSAI 5700¹³, na medida em que possuem as seguintes características ali aconselhadas¹⁴, tais como os seguintes exemplos (sugere-se a leitura completa do referido Decreto):

- ✓ Conduzir os trabalhos de maneira ética, íntegra e com boa-fé (Artigo 4º e 5º);
- ✓ Agir de forma neutra e imparcial (Artigo 4º);
- ✓ Evitar conflito de interesses (Artigos 11º a 16º);
- ✓ Agir com firmeza na implementação de princípios, normas e decisões
- ✓ Resistir às pressões de superiores hierárquicos, de contratantes, interessados e outros que visem obter quaisquer favores, benesses ou vantagens indevidas em decorrência de ações imorais, ilegais ou antiéticas, denunciando-as às autoridades competentes (Artigo 5º);
- ✓ Regulação sobre recebimento de presentes, benefícios ou vantagens (Artigo 13º);

¹² <https://leismunicipais.com.br/a/sp/s/sao-paulo/decreto/2015/5613/56130/decreto-n-56130-2015-institui-no-ambito-do-poder-executivo-o-codigo-de-conduta-funcional-dos-agentes-publicos-e-da-alta-administracao-municipal?q=56.130>

¹³ ISSAI 5700, página 30.

¹⁴ O código de conduta da PMSP tem normatização similares ao código de conduta do estado alemão de Baden-Württemberg denominado “Verwaltungsvorschrift der Landesregierung und der Ministerien zur Verhütung unrechtmäßiger und unläuterer Einwirkungen auf das Verwaltungshandeln und zur Verfolgung damit zusammenhängender Straftaten und Dienstvergehen (VwV Korruptionsverhütung und -bekämpfung)”.

- ✓ Fazer uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio ou de outrem, salvo em defesa de direito (Artigo 6º);

SUGESTÃO DE ITEM DE AUDITORIA

Inicialmente, frisa-se que no presente documento, as sugestões de auditoria, que irão surgindo conforme a apresentação dos tópicos, mas irão ser compiladas no capítulo 5.

Recomenda-se à equipe de auditoria analisar como é dado o tratamento este Código de Conduta de fato nas secretárias, autarquias e empresas públicas da PMSP tendo a planilha abaixo como guia¹⁵, mas com a seguinte pergunta como norte principal: Como é valorizado o código de conduta dentro da organização?

Avaliação da aplicação do código de Conduta	Sim	Não	N.A	Descrição / OBS
A gestão é pro ativa no sentido de encorajar e apoiar procedimentos éticos e o cumprimento da legislação e do código de conduta em vigor?				
Há treinamentos/sensibilização periódicos a servidores sobre o código de conduta (anual, bianual, etc..) ou sobre valores éticos e de integridade?				
Há divulgação do código de ética na intranet? É mencionado com alguma frequência?				
Existe evidências sobre a valorização do código de ética?				
Há treinamento a novos servidores ingressantes a respeito do código?				
Ele é mencionado nos documentos internos?				
Os servidores/funcionários encontram-se de uma forma geral cientes das suas responsabilidades, dos limites de sua autoridade e das práticas da atividade do órgão/entidade como um todo?				

¹⁵ Planilha elaborada a partir de perguntas mencionadas na ISSAI 5700, bem como nas planilhas de avaliação ao risco do Tribunal de Contas de Portugal (uso interno).

É dada importância ao código pela alta gerência/administração? A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos, e da consciência de riscos?				
--	--	--	--	--

Em referência à última pergunta da tabela acima, a fim de evidenciar a relevância do código de conduta em um determinado órgão, sugere-se realizar a aplicação de um questionário a funcionários e/ou gestores para avaliar o grau de conhecimento sobre o código de conduta.

Além da transmissão do código de ética, uma unidade ou comitê específico deve estabelecido para assegurar que o código de ética seja utilizado adequadamente, e para impor eventuais punição à violação do código de ética, havendo como exemplos, unidades de correição, corregedoria ou Comitê de Ética¹⁶.

3.2. Gerenciamento dos Recursos Humanos sobre perspectiva da prevenção à corrupção

O gerenciamento correto dos recursos humanos é parte fundamental na prevenção à corrupção (ISSAI 5700).

Três elementos devem ser considerados:

- ✓ Treinamentos
- ✓ Rotação de funções
- ✓ Gestão de recursos Humanos baseado em mérito

3.2.1. Treinamentos

Todas as instituições públicas devem organizar um programa de treinamento para aumentar a conscientização dos funcionários sobre os problemas da corrupção dentro de uma instituição, principalmente quanto à perda de

¹⁶ A ISSAI 5700, pág 29, linhas 25-27, recomenda, no caso de um comitê, que seja composto por representantes da alta gerência, divisão jurídica, divisão de auditor interno e uma parte independente.

credibilidade da organização junto aos cidadãos. Um programa de treinamento é necessário para acelerar a compreensão do perigo da corrupção, aumentando assim os esforços de prevenção da corrupção. O treinamento deve ser repetido periodicamente. Funcionários recém-ingressados podem passar por um treinamento específico anticorrupção a ser documentado no arquivo pessoal. Esforços devem ser feitos pela organização para garantir uma compreensão clara do código e seus princípios foram alcançados pela equipe após o treinamento.

Os treinamentos também a intenção de mudar o aspecto comportamental dentro de uma instituição, no sentido de aumentar a percepção interna dos próprios funcionários de que a integridade é levada a sério dentro da instituição, o que reduz a fator da racionalização ou auto justificativa quando alguém é exposto a uma oportunidade de corrupção¹⁷.

3.2.2. Rotação de funções

Rotação de trabalho (ou funções) é uma prática de gerenciamento de recursos humanos que atribui sistematicamente empregados a várias atividades e departamentos em um período de alguns anos. O objetivo é expor os funcionários a experiências diferentes e a uma variedade maior de habilidades para aumentar a satisfação no trabalho e treiná-las de forma cruzada. Além de ser um mecanismo de aprendizado, a rotação de tarefas também pode ser usada como uma ferramenta para evitar a corrupção. No entanto, há efeitos positivos e negativos envolvidos na rotação dos trabalhos que precisam ser levados em consideração.

A rotação de trabalho é uma prática bem-sucedida, mas que é frequentemente ignorada pelos gestores de alta posição (ISSAI 5700). Vale atentar que a rotação de trabalhos para servidores/funcionários públicos é mencionada expressamente na Convenção das Nações Unidas contra a Corrupção (UNCAC) adotada em

¹⁷ Sobre estudos de comportamento e corrupção: Donald Cressey, "Other People's Money"; Dan Areily, "the honest truth about dishonesty".

2003¹⁸. A rotação de trabalhos pode oferecer benefícios tanto para funcionários quanto para a instituição, considerando os seguintes aspectos:

Minimizar riscos de corrupção: A rotação dos servidores/funcionários diminui os riscos de corrupção. A razão é podem existir conexões corruptas entre as empresas e funcionários específicos. A simples troca de pessoas e funções desfaz as conexões antigas¹⁹.

Muitas vezes, algumas funções só podem ser exercidas por certos profissionais designados legalmente, como as funções de fiscalização, que exigem fé pública dando competência somente às pessoas concursadas para um cargo específico. Nestes casos, como não é possível que pessoas com cargos distintos aos que a Lei especifica exerçam funções de fiscalização, pode-se rotacionar os funcionários dentro do próprio departamento, como alocar em fiscalização de locais diferentes ou estabelecer sorteios de fiscalização.

Aumentar o conhecimento dos funcionários: a rotatividade entre departamentos permite que os funcionários aprendam diferentes aspectos das atividades de um órgão, passando a compreender a atividade como um todo. Assim, há a oportunidade de aprender habilidades necessárias que podem ajudar a progredir dentro da organização. Isso também pode aumentar sua moral e automotivação. Além disso, quando há vários funcionários com conhecimentos sobre diferentes tarefas em um sistema de rotação, no caso de um funcionário decidir deixar a instituição, um outro poderia seu lugar sem muito esforço necessário.

¹⁸ A Convenção da ONU contra corrupção, no Artigo 7º, estabelece diretrizes nesse sentido como:

“1. Cada Estado Parte, quando for apropriado e de conformidade com os princípios fundamentais de seu ordenamento jurídico, procurará adotar sistemas de convocação, contratação, retenção, promoção e aposentadoria de funcionários públicos e, quando proceder, de outros funcionários públicos não empossados, ou manter e fortalecer tais sistemas. Estes:

(..)

b) Incluirão procedimentos adequados de seleção e formação dos titulares e cargos públicos que se considerem especialmente vulneráveis à corrupção, assim como, quando proceder, a rotação dessas pessoas em outros cargos;“

¹⁹ Fonte: Palestra na Faculdade de Administração Pública de Kehl denominada “Elementos principais da Administração Pública na Administração de Baden-Württemberg. Palestrante: Julian Würtenberger; ISSAI 5700, página 32.

Desenvolver na carreira: a rotatividade de trabalhos pode ser vista como um meio para desenvolver a carreira de um funcionário e movê-lo ascendentemente, vez que há posições que requerem mais conhecimento em diferentes departamentos ou atividades da organização.

Efeitos negativos da rotação de pessoas:

Existem alguns atributos negativos associados à rotação de trabalhos. Algumas posições dentro de uma organização podem não ser elegíveis para rotação devido à necessidade de especialização especial. Essas posições podem não se encaixar no perfil de oportunidades de rotatividade devido às regras e regulamentos sobre competência, e também aos custos envolvidos para treinar os funcionários. Contudo, caso haja funções especializadas, uma alternativa seria rotacionar as pessoas dentro do próprio departamento/unidade.

Outro problema enfrentado vezes pelas organizações é a possibilidade de compensar o pessoal pela cooperação na implementação da rotação de empregos, pois isso pode levar à desigualdade salarial interna.

Conclusão

A decisão de utilizar a rotação de trabalho precisa ser avaliada com base nos aspectos positivos e negativos que uma organização pode enfrentar. Contudo, com exceção onde há obstáculos a rotação, essa prática tem se mostrado resultados positivos (ISSAI 5700). Mais importante, a organização também deve avaliar o risco de corrupção associado a cada uma das tarefas/atividades.

SUGESTÃO DE ITEM DE AUDITORIA

A avaliação da prática de rotação de funcionários pode ser orientada às seguintes perguntas²⁰. Vale atentar que tal medida é discricionária, mas pode ser recomendada como boa prática:

²⁰ Fonte: ISSAI 5700, páginas 34-35

Rotação de funções	Sim	Não	N.A	Descrição / OBS
A entidade tem alguma política em relação à rotação de trabalho?				
Se existir, como é implementada? Com qual frequência? A política de rotação é baseada em análise de risco?				
A política está sendo implementada? Se não, por quê?				
Quem toma decisões em relação à rotação de tarefas?				
Quem é elegível para a rotação de trabalho?				
Uma política de rotação existente é revisada? Com que frequência?				
Caso não exista política de rotação de funcionários: há áreas que a equipe de auditoria identifica e recomenda possibilidade de rotação?				

Fonte: ISSAI 5700, pág 34/35.

Atenta-se que para adotar uma política de rotatividade de trabalhos para reduzir o risco de corrupção dentro da organização, ideal é que a instituição faça uma avaliação completa do risco em cada uma das áreas que a compõem, considerando que há áreas mais vulneráveis à corrupção e outras menos. Só então um sistema de controles internos relacionados à rotação de tarefas pode ser projetado para lidar com esses riscos específicos.

Para mapeamento das áreas mais vulneráveis aos riscos de corrupção, pode-se recomendar a criação de um Plano de gerenciamento de riscos e de integridade que pode ser elaborado pela própria instituição, cuja metodologia será explorada no item 4.2.

3.2.3. Gestão de recursos Humanos baseado em mérito

A ISSAI 5700 estabelece a respeito da gestão de recursos humanos:

“A gestão de recursos humanos baseada em mérito é um elemento-chave na luta contra a corrupção. Para evitar a influência indevida dos processos de gestão de recursos humanos do setor público, os critérios e procedimentos de

seleção e promoção precisam ser justos, predefinidos e claramente documentados, para que a margem de discricção e arbitragem seja limitada. As estruturas e os mecanismos de recurso também precisam estar em vigor para garantir a correção efetiva. A gestão eficaz de recursos humanos pode reduzir os riscos potenciais e controlar os pontos fracos através da nomeação de pessoal competente para implementar procedimentos e controles. Isso inclui também o pagamento de uma remuneração adequada e justa a todos os funcionários públicos, para que eles não se tornem envolvidos na corrupção.

O pessoal de áreas especialmente vulneráveis à corrupção deve ser recrutado com especial cuidado. Para cargos executivos ou gerenciais, a necessidade de concluir os treinamentos anticorrupção deve ser um pré-requisito para a nomeação, promoção e sucessão.”

A este respeito, considerando que a seleção de pessoal é definida em Lei, cabe análise apenas das políticas de promoção com base em mérito nos órgãos da PMSP. Um estudo sobre as remunerações também é possível, visto que remunerações muito baixas levam a insatisfação e vulnerabilidades maiores a corrupção²¹. Contudo, deve-se atentar a fatos de discricionarieidade e disponibilidade orçamentária da PMSP.²².

SUGESTÃO DE ITEM DE AUDITORIA

Uma avaliação sobre se a organização segue um modelo de promoção baseado em mérito pode ser feita através de elaboração de questionários on-line junto a funcionários, questionando sobre a política da organização e suas

²¹ A Convenção da ONU contra corrupção, no Artigo 7º, item 1 “c”, estabelece diretriz no sentido de haver remuneração adequada. A razão é que níveis muito baixos de salário podem propiciar corrupção.

²² A Convenção da ONU contra corrupção, no Artigo 7º, estabelece diretrizes nesse sentido como:

“1. Cada Estado Parte, quando for apropriado e de conformidade com os princípios fundamentais de seu ordenamento jurídico, procurará adotar sistemas de convocação, contratação, retenção, promoção e aposentadoria de funcionários públicos e, quando proceder, de outros funcionários públicos não empossados, ou manter e fortalecer tais sistemas. Estes:

a) Estarão baseados em princípios de eficiência e transparência e em critérios objetivos como o mérito, a equidade e a aptidão;

b) Incluirão procedimentos adequados de seleção e formação dos titulares e cargos públicos que se considerem especialmente vulneráveis à corrupção, assim como, quando proceder, a rotação dessas pessoas em outros cargos;

c) Fomentarão uma remuneração adequada e escalas de soldo equitativas, tendo em conta o nível de desenvolvimento econômico do Estado Parte;”

percepções. Abaixo, segue um possível modelo, utilizando-se uma avaliação de escala de 0 a 5 denominada Likert, útil para se avaliar percepção.

Avaliação sobre ambiente e envolvimento de trabalho - Escala Likert de 1 a 5 -1 - Discordo Totalmente, 2 – Discordo, 3 - Nem Concordo nem Discordo, 4 – Concordo, 5 - Concordo Totalmente	Discorda totalmente/ Discorda	Concorda totalmente / Concorda	Sem opinião
Os funcionários do órgão são avaliados de forma justa e responsabilizados pelo trabalho que desenvolvem			
O órgão consegue atrair e reter os melhores profissionais			
Vejo o órgão como o local certo para desenvolver uma carreira de médio/longo prazo			
Estou satisfeito em ser funcionário do órgão			
As promoções para chefia são baseadas em mérito			
Os critérios para promoções são justos			
A minha remuneração é a adequada às minhas funções e responsabilidades			
Obtenho informação regular, positiva ou negativa, sobre o meu desempenho			

Abaixo seguem dois exemplos de como os resultados poderiam ser apresentados utilizando-se a escala Likert (proceder com zoom para visualização):

Questões relativas à concordância com afirmações (escala Likert 1 a 5)		Discorda totalmente	Discorda	Concorda	Concorda totalmente	S/opinião
Obtenho informação regular, positiva ou negativa, sobre o meu desempenho	CHSJ	13%	21%	38%	11%	17%
	CHLN	12%	23%	18%	5%	35%
Os colaboradores do CH são avaliados de forma justa e responsabilizados pelo trabalho que desenvolvem	CHSJ	13%	36%	13%	4%	34%
	CHLN	12%	30%	17%	2%	35%

3.2.4. Modelo de gestão e envolvimento dos colaboradores

Uma boa integração dos funcionários com as estratégias da alta direção de um órgão pode evitar casos de corrupção. Assim, estrutura hierárquica menos vertical, em que os funcionários têm capacidade para se de certa maneira participarem de algumas decisões, é menos propícia à corrupção²³. Estruturas mais verticalizadas onde a comunicação dos gerentes de nível operacional para o topo

²³ Vide tese de doutora do Cientista Social Português Antônio João Maia, membro do Conselho de Combate a “Corrupção, Fatores Organizacionais: Explicativos da Corrupção”, Universidade de Lisboa, 2015.

da gestão (botton-up) é pouco usual, tendem a levar maior insatisfação aos funcionários e maior propensão a corrupção.

Do contrário, quando existe abertura da gestão de topo a propostas de mudança para melhorar o funcionamento do órgão, em que a estratégia do órgão, as suas políticas e os seus objetivos são comunicados com clareza aos funcionários, em que estes têm a possibilidade de alguma maneira participar na definição dos objetivos da área ou unidade em que está locado, tendem a ter maior motivação e menor vulnerabilidade.

SUGESTÃO DE ITEM DE AUDITORIA

Para uma análise da estrutura de gestão pode-se aplicar, como sugestão, o seguinte questionário junto aos funcionários. Para tal, utiliza-se um questionário de graduação de notas sobre afirmações de um a cinco para cada questionamento (escala Likert). Posteriormente, nas questões onde há discordância com das afirmações, em etapa seguinte a equipe de auditoria poderia proceder a uma investigação mais a fundo para se extrair as causas de problemas, utilizando-se questionários de perguntas abertas aos funcionários ou gestores de nível intermediário, abrindo-se a possibilidade de a auditoria realizar recomendações aos gestores:

Avaliação sobre ambiente e envolvimento de trabalho	Discorda totalmente / Discorda	Concorda totalmente / Concorda	Sem opinião
A estratégia do órgão que trabalho, as suas políticas e os seus objetivos são comunicados com clareza aos funcionários			
A forma como os serviços e níveis hierárquicos do órgão estão organizados é adequada e contribui para o seu bom funcionamento			
Existe abertura da gestão de topo a propostas de mudança para melhorar o funcionamento do órgão			

É dado a mim conhecimento adequado das mudanças ocorridas e em curso no órgão			
A comunicação entre os Serviços/ Áreas/ Direções é aberta e produtiva			
Existe boa comunicação e cooperação entre diferentes áreas			
Reconheço capacidade de liderança nos meus superiores na estrutura de gestão			
Reconheço competência e dedicação nos meus pares da estrutura de gestão			
O órgão/instituição tem os meios físicos e humanos adequados ao exercício da sua atividade, para poder corresponder aos objetivos definidos			
O Serviço/ Área/ Direção em que trabalho tem os meios físicos e humanos adequados ao exercício da sua atividade, para poder corresponder aos objetivos definidos			
Conheço os objetivos anuais definidos para o órgão em termos de atividade / produção			
Conheço os objetivos do Serviço/ Área/ Direção em que trabalho			
Participo na definição dos objetivos do Serviço/ Área/ Direção em que trabalho			
O meu papel no órgão, as minhas tarefas e as minhas responsabilidades estão claramente definidas e são do meu conhecimento			
Por vezes recebo ou tenho acesso a informação contraditória sobre o mesmo assunto (por exemplo, produção mensal, indicadores de qualidade, recursos humanos, consumos, etc)			
Tenho a autonomia adequada ao exercício das minhas funções			
Existe uma boa colaboração entre os dirigentes/ gestores/ administradores da área clínica e os da área de gestão			
Participo na tomada de decisões importantes que dizem respeito ao órgão como um todo			

Participo na tomada de decisões importantes que afetam ou dizem diretamente respeito ao Serviço/Área/Direção em que trabalho			
O órgão tem-me proporcionado formação profissional adequada às minhas funções e responsabilidades			
A formação disponibilizada pelo órgão corresponde às necessidades dos funcionários do Serviço/Área/Direção em que trabalho			
Estou satisfeito em pertencer ao Serviço/Área/ Direção em que trabalho			
O órgão é visto pelos cidadãos como a referência de qualidade no Serviço que presta			
O órgão presta um serviço de qualidade aos usuários na minha opinião dentro de suas possibilidades e limitações de recursos, independente de como os cidadãos percebam o serviço			
O órgão encontra-se num processo de melhoria contínua			

OBS – Utilizar escala Likert de 1 a 5 -1 - Discordo Totalmente, 2 – Discordo, 3 – Nem Concordo nem Discordo, 4 – Concordo, 5 - Concordo Totalmente.

Fontes: Planilha de Avaliação do Risco Global e Avaliação do Sistema de Controlo Interno Global do Tribunal de Contas de Portugal ²⁴;e Relatório de Auditoria às práticas de gestão no Centro Hospitalar Lisboa Norte, EPE, e no Centro Hospitalar de São João EPE²⁵.

3.3. Princípio da conferência cruzada (Quatro olhos)

O conceito do princípio da conferência cruzada (quatro olhos) é uma exigência de que dois indivíduos aprovem alguma ação antes que ela possa ser tomada, como por exemplo: autorizar pagamentos, atestar medições em obras complexas, decidir sobre resultados em certames, analisar o escopo e adequabilidade quanto questões da descrição do objeto de uma licitação, conceber licenciamentos. Sempre que possível, deve-se a responsabilidade duas ou mais pessoas, idealmente de departamentos distintos ou de pouco contato entre elas. A

²⁴ Planilhas coletas em âmbito de pesquisa. Sem publicação externa.

²⁵ https://www.tcontas.pt/pt/actos/rel_auditoria/2018/2s/rel012-2018-2s.pdf

denominação quatro olhos²⁶ vem dessa ideia: duas pessoas envolvidas, uma executa, a segunda confere.

Esse princípio leva a ideia que decisões importantes ou ações críticas não devem ser tomadas por uma única pessoa individualmente. Há dois objetivos neste princípio: o primeiro é simplesmente reduzir o risco de erros, visto que muitas das operações que não observam estritamente à lei simplesmente ocorrem simplesmente por falha humana. Trata-se de um sistema de conferência, onde uma segunda pessoa confere os trabalhos ou atos de uma pessoa que realiza o ato.

A simples conferência ou assinatura por uma segunda pessoa dificulta a ilegalidade ou prática antieconômica contra a administração. Como situação ideal, a melhor prática seria rotacionar os pares de conferência. Um sistema de sorteio poderia ser implementado.

Exemplo do princípio dos quatro olhos na Alemanha

Esse princípio, embora simples, é utilizado na Administração pública alemã como um mecanismo de diminuição de erros, e gera um efeito de dificultar situações que propiciam oportunidades à corrupção, na medida que quando há duas ou mais pessoas envolvidas para realizar algum tipo de decisão, torna-se mais difícil oportunidades suscetíveis a corrupção, uma vez que uma pessoa fiscaliza seu colega, e vice-versa.

O princípio dos quatro olhos é mencionado expressamente em regulamento de prevenção a corrupção e luta contra corrupção do Estado de Baden-Württemberg²⁷ (*VwV Korruptionsverhütung und –bekämpfung*), da seguinte forma:

“(2) A direção superior assegura que sejam verificadas periodicamente em áreas onde existe um risco de corrupção, se nos processos de trabalho especialmente em licitações de aquisição e serviços:

²⁶ O nome literal que esse princípio recebe em alemão é Vier-Augen-Prinzip, cuja a tradução literal é princípio dos quatro olhos, inclusive havendo menção na legislação sobre esse princípio com esse estranho nome.

²⁷ Nome do regulamento: *Verwaltungsvorschrift der Landesregierung und der Ministerien zur Verhütung unrechtmäßiger und unlauterer Einwirkungen auf das Verwaltungshandeln und zur Verfolgung damit zusammenhängender Straftaten und Dienstvergehen*. Disponível em http://www.gewerbeaufsicht.baden-wuerttemberg.de/servlet/is/16499/4_02.pdf

- o princípio dos quatro olhos é respeitado e

- *A transparência é assegurada pela tomada de decisões compreensíveis e documentadas em processos.*”

O seguinte exemplo revela uma possível forma de controle por “quatro olhos”. Em licitações voltuosas ou complexas, sempre é um ponto de risco que as especificações do certame possam ser restritivas²⁸, não intencionalmente ou com intenção, de forma que as especificações técnicas do Edital levem a só a um possível fornecedor, através de exigências restritivas na qual uma só empresa consiga atender o que é exigido em Edital.

Supondo um departamento “X” de um certo órgão qualquer que elabore os requisitos de atestados técnicos para os licitantes participarem, tanto quanto em relação a quais atestados e quantidades que irá ser exigido, como os detalhes dos “Termos de Referência”, estes documentos ainda em fase interna da licitação serão encaminhadas ao um outro departamento “Y”, que também possua conhecimento técnico, para que este se pronuncie antes da publicação do Edital. O departamento “Y” se pronuncia sobre questões como restritividade e adequabilidade das exigências técnicas. Dessa maneira, o gestor público responsável pode desconstruir pontos restritivos antes da publicação de um Edital com base no avaliação e conferência do departamento “Y”, ampliando a concorrência.

Ponto negativo: O princípio de quatro olhos é de certa forma eficaz contra corrupção, mas ao mesmo tempo custoso, tendo em vista a necessidade de alocar um segundo funcionário para a conferência dos trabalhos de um funcionário executor principal. Deve-se sopesar a utilização dessa ferramenta de controle interno nas áreas mais vulneráveis ao risco de corrupção quando envolvem fiscalização, concessão de autorizações (alvarás, permissões e licenciamentos), ateste de pagamentos de alto volume, projetos de grandes licitações, decidem sobre proibições ou restringem atividades comerciais de particulares.

SUGESTÃO DE ITEM DE AUDITORIA

²⁸ Na Alemanha, usam-se os termos como “limitação de competição” (Wettbewerbsbeschränkungen) e não discriminação (Nichtdiskriminierung) para se referir a aspectos de restritividade.

Analisar se princípio do quatro olhos é utilizado nas áreas vulneráveis ao risco. Caso não seja utilizado, sugerir à área auditada o uso dessa prática.

Especificamente sobre licitações, em âmbito de Análise de Editais ou acompanhamentos de Editais, observar regras específicas da Lei 8.666/93 em que já está presente o princípio dos quatro olhos a partir da formação de comissão de licitação, a saber:

Art 15. (...)

§ 8º O recebimento de material de valor superior ao limite estabelecido no art. 23 desta Lei, para a modalidade de convite, deverá ser confiado a uma comissão de, no mínimo, 3 (três) membros.

Art. 38. O procedimento da licitação será iniciado com a abertura de processo administrativo, devidamente autuado, protocolado e numerado, contendo a autorização respectiva, a indicação sucinta de seu objeto e do recurso próprio para a despesa, e ao qual serão juntados oportunamente:

II - ato de designação da comissão de licitação, do leiloeiro administrativo ou oficial, ou do responsável pelo convite;

Art. 51. A habilitação preliminar, a inscrição em registro cadastral, a sua alteração ou cancelamento, e as propostas serão processadas e julgadas por comissão permanente ou especial de, no mínimo, 3 (três) membros, sendo pelo menos 2 (dois) deles servidores qualificados pertencentes aos quadros permanentes dos órgãos da Administração responsáveis pela licitação.

§ 1º No caso de convite, a Comissão de licitação, excepcionalmente, nas pequenas unidades administrativas e em face da exigüidade de pessoal disponível, poderá ser substituída por servidor formalmente designado pela autoridade competente.

§ 2º A Comissão para julgamento dos pedidos de inscrição em registro cadastral, sua alteração ou cancelamento, será integrada por profissionais legalmente habilitados no caso de obras, serviços ou aquisição de equipamentos.

§ 3º Os membros das Comissões de licitação responderão solidariamente por todos os atos praticados pela Comissão, salvo se posição individual divergente estiver devidamente fundamentada e registrada em ata lavrada na reunião em que tiver sido tomada a decisão.

§ 4º A investidura dos membros das Comissões permanentes não excederá a 1 (um) ano, vedada a recondução da totalidade de seus membros para a mesma comissão no período subsequente.

§ 5º *No caso de concurso, o julgamento será feito por uma comissão especial integrada por pessoas de reputação ilibada e reconhecido conhecimento da matéria em exame, servidores públicos ou não.*

(...)

Art. 53. O leilão pode ser cometido a leiloeiro oficial ou a servidor designado pela Administração, procedendo-se na forma da legislação pertinente”

Ressalva-se, contudo, que o princípio dos quatro olhos pode ser aplicado a diversas atividades administrativas, e não só a licitações.

3.4. Segregação de funções

Um dos objetivos de um sistema de controle bem estruturado é eliminar a possibilidade de dissimulação de erros e fraudes. Considerando este aspecto, os procedimentos destinados a detectar erros ou fraudes devem ser realizados por funcionários que não estejam em posição de praticá-los, em outras palavras, deve haver uma adequada segregação de funções.

De uma maneira geral, o sistema de controle interno deve prever segregação entre as funções de autorização, execução, atesto/aprovação, registro e revisão ou fiscalização, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer atividade administrativa.

Abaixo segue exemplos de ações que, se exercidas, de forma cumulativa, por determinados setores da Administração Pública, comprometem o princípio da segregação de funções²⁹:

a) compras e almoxarifado (recebimentos de bens): Mesmo servidor pode ser responsável por realizar processo licitatório (ou compra direta via adiantamento) e realizar registro em sistemas de compras e de almoxarifado. Nesse caso, pode resultar, no registro da entrada de um bem inexistente.

b) recebimento de bens e contas a pagar: incluir documento falso no sistema para, posteriormente, liberá-lo para pagamento, em benefício do próprio servidor responsável.

²⁹ Fonte: <http://wdwww.etecnico.com.br/paginas/mef22868.htm>

c) contabilidade e contas a pagar: contabilizar uma nota fiscal ou documento inidôneo no sistema e, posteriormente, emitir uma nota de empenho e receber o seu valor correspondente no setor financeiro.

d) contabilidade e controle interno: lançar determinado evento contábil e, posteriormente, emitir parecer sobre o mesmo.

e) contabilidade e administração financeira da administração: informar senhas pessoais, que são de uso restrito, a outros usuários, para alterar ou excluir registros que possam interferir em resultados e comprometer tomadas de decisões.

Portanto, é coerente segregar funções nos casos em que possa existir possibilidade riscos de corrupção ou fraude quando um servidor desempenha múltiplas atividades, mas essas são passíveis de ser manipuladas pelo acúmulo de funções incompatíveis³⁰, evitando-se ou diminuindo-se, dessa forma, a possibilidade de lesivos à Administração Pública. Um mapeamento dos processos e atividades, com uso de fluxograma, elucidando se há atividades que deveriam ser segregadas.

Licitações

É importante observar a aplicação da segregação de função aos processos de contratação, pois trata-se de um ato composto, vez que envolvem diversos atos e atividades durante a execução, sendo impróprio os mesmos servidores participarem em fases posteriores³¹. Tais atividades são: preencher a requisição ou elaborar projeto básico, pesquisar (estimar) o preço de mercado, elaborar o edital de licitação, publicar o aviso de licitação, conduzir o certame, responder aos questionamentos e aos recursos impetrados (caso ocorram), publicar o resultado do julgamento, empenhar, liquidar (atestar) e receber o objeto licitado.

³⁰ Mas atividades compatíveis podem ser acumuladas por questões de economia na administração pública.

³¹ Conforme texto de Magno Antônio da Silva intitulado O princípio da segregação de funções e sua aplicação no controle processual das despesas: uma abordagem analítica pela ótica das licitações públicas e das contratações administrativas. Disponível em <https://jus.com.br/artigos/59608/mecanismos-de-controle-interno-da-licitacao-e-o-principio-da-segregacao-das-funcoes>

O Tribunal de Contas da União ³² nesse sentido determinou a um órgão que não designasse “... para compor comissão de licitação o servidor ocupante de cargo com atuação na fase interna do procedimento licitatório, em atenção ao princípio da segregação de funções.”. Em fase de execução do contrato, idealmente, a possibilidade de um mesmo servidor atuar como fiscal e executor em um mesmo contrato também deve ser evitada.

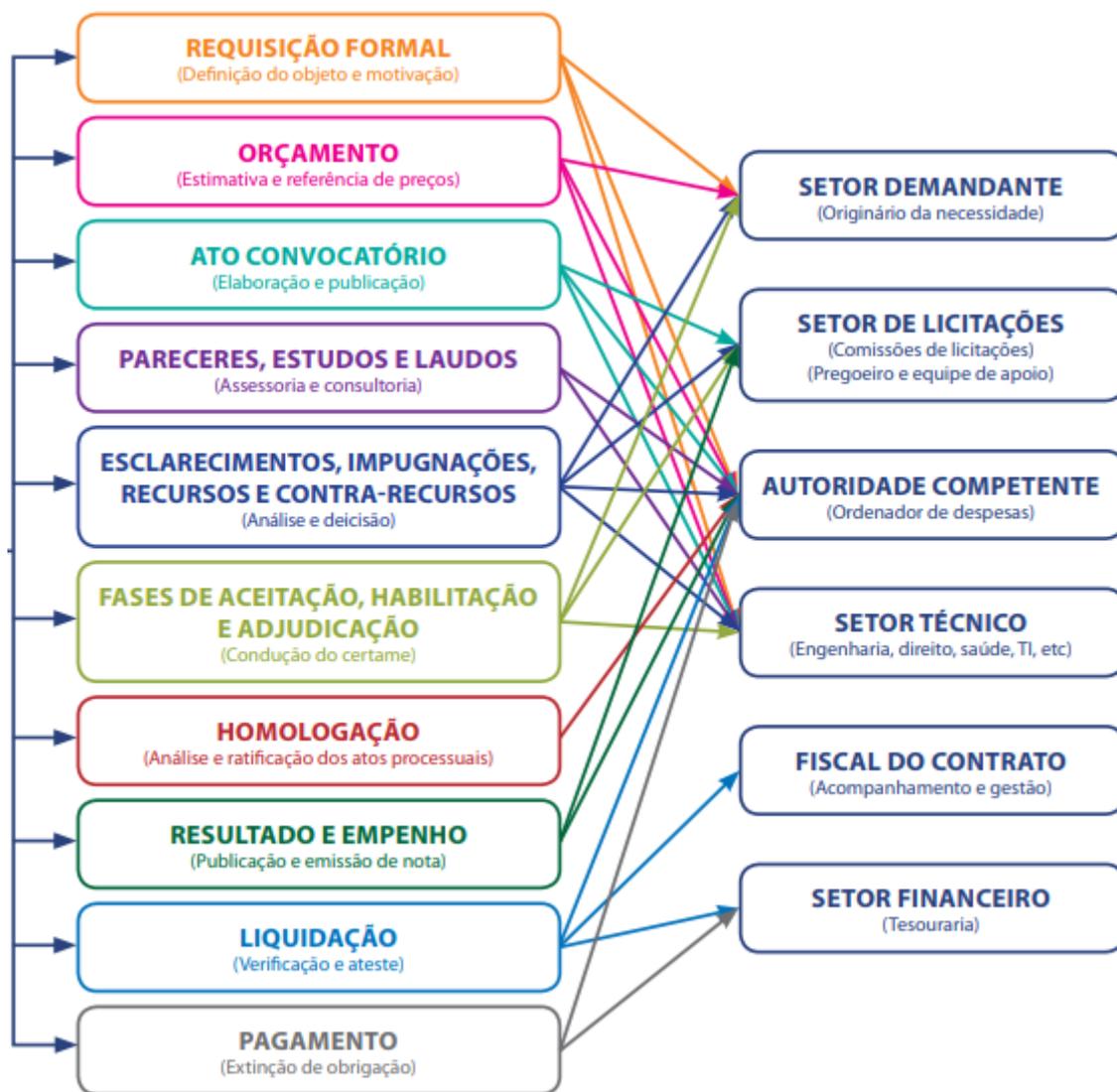
Como sugestão, é passível de verificação pela equipe de auditoria se o Artigo 9º especificamente da Lei 8.666/93 está sendo observado, pois este artigo já embutem a noção da segregação de funções. A Lei de licitações, a partir deste artigo, não permite:

a) que servidor que elaborou o projeto básico ou executivo (autor do projeto) participe da fase da licitação (recebimento e julgamento das propostas, habilitação, decisão de recursos);

b) que o servidor ou dirigente de órgão ou entidade contratante ou responsável pela licitação participe da execução de obra ou serviço e do fornecimento de bens nas seguintes condições

Abaixo segue uma figura esquematizada da decomposição da segregação de funções sob a perspectiva das licitações públicas e das contratações administrativas. As colunas da esquerda são os atos administrativos de uma licitação, enquanto à direita são os servidores ou agentes encarregados pelos atos. Nota-se que distintos servidores participam e agem em diferentes fases, mas nenhum servidor ou agente público deve ser o responsável sozinho pelo processo todo em sua totalidade. Nessa figura, um mesmo “ator” participa de vários atos ou “papéis” em momentos sequenciais diferentes. Contudo, nenhum ato deve ser realizado por menos de dois agentes ou servidores públicos (exceto homologação). Também se nota que não há atores com atos incompatíveis, como por exemplo, alguém do setor demandante ou do setor de licitações sendo o fiscal do contrato.

³² (Acórdão nº 686/2011 – Plenário)



Fonte: Magno Antônio da Silva em artigo intitulado O princípio da segregação de funções e sua aplicação no controle processual das despesas: uma abordagem analítica pela ótica das licitações públicas e das contratações administrativas

SUGESTÃO DE ITEM DE AUDITORIA

Inicialmente, deve-se verificar se a instituição tem uma política clara com relação à segregação de funções.

Dependendo do tempo disponível para consecução da auditoria, a equipe pode buscar tarefas em que há riscos de manipulação por serem exercidas por mesma pessoa, através da análise de cada uma das atividades e serviços que a entidade audita realiza. Para isso, pode-se elaborar um mapa de processos para clarificar

cada etapa e estágio das atividades de uma entidade, pois um mapa de processos (fluxo de trabalho), contendo os respectivos responsáveis em cada etapa do fluxo facilitar esclarecer se cada se está ocorrendo sobreposição indevida de funções.

Quanto a segregação de funções obrigatória do Artigo 9º da Lei 8.666/93, pode-se verificar uma amostra aleatória de alguns processos administrativos de contratação, examinado especificamente este requisito do Art. 9º, mas sem realizar uma análise formal a cada, pois demandaria tempo em excesso.

3.5. Supervisão adequada

Além do princípio dos quatro olhos, uma supervisão adequada quantos às chefias com relação aos seus subordinados é essencial. Por vezes, as chefias são sobrecarregadas em muitos afazeres, e podem a ter pouco tempo disponível para supervisão. As seguintes perguntas orientam possíveis avaliações nestes aspectos, podendo ser levantadas por entrevistas:

- ✓ Há evidências que as chefias efetivamente conferem os trabalhos de seus subordinados?
- ✓ Como são estabelecidas as rotinas de conferências (caso existente)? Quais aspectos são de fato conferidos? Com que frequência e como as conferências ocorrem? É realizada conferência cada uma das transações/tarefas concluídas?
- ✓ A relação chefe/quantidade de funcionários é adequada, de forma que possa haver tempo suficiente para supervisionar os trabalhos de seus subordinados?

3.6. Questões diversas de avaliação de controle interno:

As seguintes questões, elaboradas e utilizadas internamente pelo Tribunal de Contas de Portugal, supletivamente podem ser utilizadas pela equipe de auditoria para avaliação do controle interno. Deve-se observar que a equipe de auditoria há de avaliar quais questões serão respondidas, pois algumas necessitam de certo tempo de avaliação ou mesmo uso de questionários específicos para tal, e assim, as respostas dependerão do tempo de auditoria:

Aspetos relacionados com a Gestão e atividade da entidade	Sim	Não	N.A	Descrição / OBS
Existem funcionários cuja sarda teria um impacto negativo material sobre a entidade ou sobre as suas operações?				
São elaboradas periodicamente informações para apoio às decisões da gestão?				
Existem alterações frequentes e significativas nos administradores, gerentes e diretores, nos sistemas contabilísticos ou na natureza das transações que tenham elevado o risco de ocorrerem erros ou omissões?				
Estão os serviços adequadamente dotados de pessoal em número e conhecimentos, de forma a desempenhar adequadamente as suas funções?				
Há frequentes alterações na(s) atividade(s) da entidade?				
Verificam-se com frequência mudanças da administração, incluindo a saída dos principais administradores?				
Existe uma estrutura hierárquica e uma adequada subdivisão de funções definida para a entidade?				
A entidade está inserida em um setor/Secretaria onde existe um forte peso ao nível das decisões políticas ou outras tomadas?				
A entidade está dependente de um reduzido n.º de fornecedores/empresas?				

As seguintes questões são relacionadas aos sistemas de Tecnologia de Informação – TI:

Aspetos relacionados com os sistemas de informação –TI	Sim	Não	N.A	Descrição / OBS
Foram introduzidos novos sistemas de informação com significância para o trabalho de auditoria ou os existentes sofreram modificações?				
Há atividades que existem oportunidades de automação?				

Quais os sistemas de informação de que a entidade dispõe? Existe articulação entre os vários sistemas de informação?				
O tipo de software utilizado apresenta-se adequado face às necessidades da entidade e providencia outputs de forma prática com informação relevante, em um formato adequado e para cada área significativa da entidade?				
Encontram-se previstas adequadas políticas e procedimentos de segurança por forma a evitar acessos não autorizados a equipamentos informáticos, software ou outras informações armazenadas nos sistemas de informação?				
Existe evidência de ter existido alguma ruptura ou falha nos sistemas de informação durante o período em análise?				

Em uma questão relevante por ser um ponto de possível fragilidade, deve-se atentar para política dos sistemas (softwares) e o nível de permissão dos usuários. Sugere-se analisar a política de senhas e permissão de autorização de uso na entidade e quem efetivamente as detêm, onde apenas as pessoas devidas devem ter acesso e permissão onde haja possibilidade de alteração, exclusão ou inclusão de registros.

Um estudo aprofundado das políticas de registro e permissão de dados visando detectar pontos de fragilidade que podem ser burlados pode ser realizado. Pode ser apropriado fazer um conjunto de testes em verificação dos registros a fim de se detectar eventuais pontos de fragilidade. Para tal, a equipe de auditoria necessita aprofundar-se dos meandros de como é estabelecido a política de segurança. Um corpo de prova de testes no local pode ser verificado. Contudo, o órgão auditado deve, como boa prática, manter uma rotina de verificação permanente por alguém que seja responsável em fazer verificações de rotina com corpo de prova.

3.7. Outras medidas anticorrupção

O processo de informatização dos serviços do governo, ou governo eletrônico (e-gov) pode ser usado como uma medida específica de corrupção e como parte da prestação de eficiente de serviços e procedimentos, na medida que

despersonaliza e padroniza a prestação de serviços. Assim, oportunidades de automação do serviço final podem ser sugeridas pela equipe de auditoria.

Detecção de Corrupção

Os gestores de nível intermediário e chefias têm a missão de monitorar constantemente suas operações e tomar medidas imediatas e responsivas sobre irregularidades, operações não econômicas, ineficientes e ineficazes. As ações de monitoramento são imprescindíveis para garantir os resultados desejáveis. Com frequência, verificou-se que sem o necessário entendimento e monitoramento, é uma tendência das pessoas não seguirem práticas de controle estabelecidas.

Os seguintes instrumentos para a detecção de corrupção podem ser considerados:

Mecanismos de Denúncia

Um mecanismo de denúncia de irregularidades é um meio formal de comunicação estabelecido pela instituição para que os funcionários públicos e qualquer terceiro interessado possam fornecer informações sobre possíveis ações ou transgressões corruptas que tenham acontecido no passado ou estejam acontecendo atualmente. Esse mecanismo pode ser composto de caixas de correio, linhas telefônicas, e-mails ou sites criados para receber as denúncias acima mencionadas.

Mecanismos de denúncia de irregularidades são meios fundamentais para prevenir, detectar e impedir ações corruptas, violações de integridade e comportamento inadequado contra o código de conduta.

Segundo recomendações da ISSAI 5700, *“Estudos especializados indicaram que os mecanismos de denúncia de irregularidades têm sido tradicionalmente a maneira mais eficaz de descobrir ações corruptas, fraudes e outros comportamentos irregulares, superando de longe outros controles de corrupção, como auditorias externas e internas e verificações de gestão.*

Esses mecanismos também são importantes elementos dissuasivos, pois transmitem a mensagem de que ações contrárias à política de integridade podem

ser facilmente relatadas e tratadas. Da mesma forma, quando esse mecanismo é adequadamente adaptado às necessidades da instituição e implementado, ele reduz significativamente a quantidade de corrupção real que ocorre e a quantidade de perdas que a instituição enfrenta devido à detecção antecipada.

A implementação correta de um mecanismo de denúncia de irregularidades requer, entre outras coisas, que a política seja devidamente comunicada dentro da instituição em todos os níveis. A política também deve garantir que os denunciantes possam informar sobre irregularidades de forma anônima, confidencial e livre de consequências.

O mecanismo deve incluir um sistema de rastreamento que registre os relatórios e que garanta que seja sejam acompanhados adequadamente. A unidade anticorrupção da instituição, ou equivalente, deve supervisionar a eficácia do cumprimento do mecanismo.

A alta administração deve periodicamente promover que qualquer atividade suspeita seja relatada em tempo hábil e enfatizar o anonimato dos denunciantes e a falta de represálias para eles.”

4. Metodologia de análise e gerenciamento do risco de riscos

Este capítulo apresenta as características básicas dos principais sistemas de controle interno, tanto na área pública como na área privada, para implementar e avaliar uma gestão de riscos de forma consistente e sistematizada. Serão assim tratados aspectos do controle interno sob a ótica de gestão de riscos e prevenção da corrupção.

A ideia do controle interno tem aceção vasta, e carrega certa abstração, tendo em vista que se depende muito do fator humano, e mesmo comportamental. De acordo com publicação da INTOSAI intitulada “ISSAI GOV 9100-Diretrizes para padrões do controle interno na Administração Pública” (*Guidelines for Internal Control Standards for the Public Sector*), controle interno é definido como³³:

“O controle interno é um processo integral que é efetuado pela administração e pelo pessoal de uma entidade e é projetado para tratar dos riscos e fornecer uma garantia razoável de que, em cumprimento da missão da entidade, os seguintes objetivos gerais estão sendo alcançados:

- *Executar operações de maneira ordenada, ética, econômica, eficiente e eficaz;*
- *Cumprir com as obrigações de prestação de contas (accountability)³⁴;*
- *Cumprir as leis e regulamentos aplicáveis;*
- *Salvaguardar recursos contra perda, uso indevido e danos”.*

Ainda, sobre controles internos, é interessante algumas observações que a ISSAI 9100 faz, no sentido de que *“As pessoas são o que faz o controle interno funcionar. É realizado por indivíduos dentro de uma organização, pelo que eles fazem e dizem. Consequentemente, o controle interno é efetuado pelas pessoas.*

³³ Internal control is an integral process that is effected by an entity’s management and personnel and is designed to address risks and to provide reasonable assurance that in pursuit of the entity’s mission, the following general objectives are being achieved:

- executing orderly, ethical, economical, efficient and effective operations;
- fulfilling accountability obligations;
- complying with applicable laws and regulations;
- safeguarding resources against loss, misuse and damage.

³⁴ A palavra original é era accountability, de tradução imprecisa.

As pessoas devem conhecer seus papéis e responsabilidades e limites de autoridade.”

Os controles são um dos meios para que organização atinja seus objetivos de forma eficiente. Idealmente, os controles internos são desenhados a partir de modelos de gerenciamento de risco, os quais passarão a ser descritos.

Modelos de gestão de riscos

Riscos são todos eventos que, se ocorrer, afetará negativamente e de forma significativa a capacidade que tem a organização de atingir seus objetivos estratégicos. Para lidar com riscos e aumentar a chance de alcançar objetivos, as entidades públicas devem adotar desde abordagens informais até abordagens altamente estruturadas baseadas em modelos de gestão de riscos, dependendo do seu porte e da complexidade de suas atividades. Contudo, é importante que a organização se apoie em modelos reconhecidos.

Geralmente, as metodologias atualmente mais reconhecidas são baseadas ou tem influência nos modelos da organização norte americana chamada COSO – Comitê das Organizações Patrocinadoras (*Committe Of Sponsoring Organizations of the Treadway Commission*)³⁵.

No início dos anos 90, devido a fraudes em balanços em anos anteriores, as bases para conhecidas gestão de risco foram criadas. A publicação da COSO em 1992 acabou se tornado referência mundial no tema, recebendo o nome atualmente de COSO I. O guia *Internal Control - Integrated Framework* (COSO I, consolidou a ideia de gestão de risco corporativo e apresentou um conjunto de princípios e boas práticas de gestão e controle interno.

³⁵ Sobre o COSO (Fonte: wikipedia):

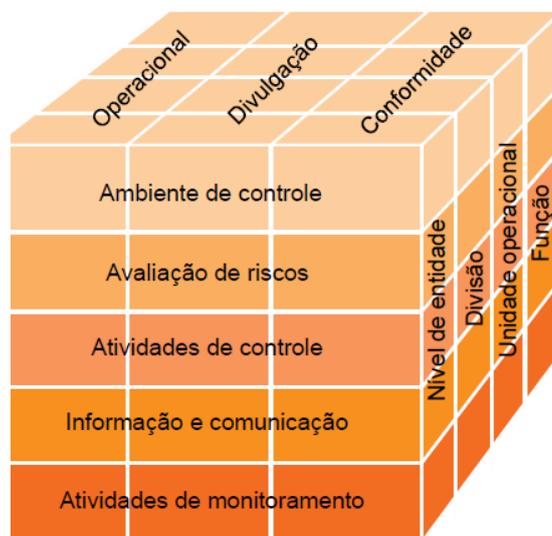
A missão do COSO é fornecer uma liderança ponderada por meio do desenvolvimento de estruturas abrangentes e orientação sobre gerenciamento de riscos corporativos, controle interno e redução de fraude destinados a melhorar o desempenho organizacional e a governança e reduzir a extensão das fraudes nas organizações.

O COSO é formado por representantes da American Accounting Association, American Institute of Certified Public Accountants, Financial Executives International, Institute of Managements Accountants e pelo Institute of Internal Auditors, ao qual está ligado a AUDIBRA – Instituto dos Auditores Internos do Brasil, através da FLAI – Federação latino-americana de Auditores Internos.

Em 2004, devido novamente a escândalos de fraude em balanço novamente de grandes empresas americanas³⁶, o COSO publicou o *Enterprise Risk Management - Integrated Framework*, que recebe o nome COSO-ERM ou COSO II.

O modelo da COSO I, bem como na ISSAI 9100 que é baseada nesse primeiro modelo, tem uma versão simplificada em cinco componentes chaves, sendo seu núcleo baseado nos seguintes âmbitos que são representados em um formato de um cubo:

- ✓ Ambiente de Controle
- ✓ Avaliação dos riscos
- ✓ Atividades de Controle
- ✓ Informação e comunicação
- ✓ Atividade de monitoramento



Fonte: COSO, Executive Summary (2013).

A ISSAI 9100 (INTOSAI, 2004) segue uma estrutura semelhante a esta versão do COSO I. No presente documento, serão tratados conjuntamente alguns dos componentes da ISSAI 5700 (INTOSAI, 2016) de maneira agrupa com os cinco componentes da ISSAI 9100 e COSO em sua primeira versão.

³⁶ Como o caso da empresa Eron.

A versão de COSO (2013) enumera 17 princípios associados a cada um dos cinco componentes chaves:

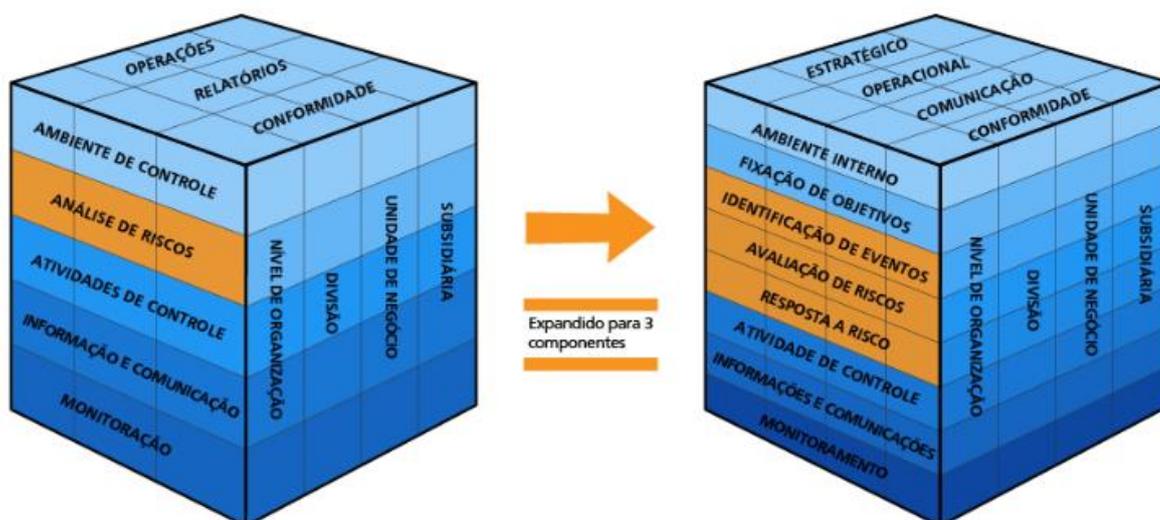
Componente-chave	Princípios
Ambiente de controle	1. Demonstrar compromisso com a integridade e os valores éticos
	2. Exercer a responsabilidade pela supervisão
	3. Definir a estrutura, autoridade e responsabilidade
	4. Demonstrar compromisso com a competência
	5. Aplicar a prestação de contas
Avaliação dos riscos	6. Especificar os objetivos adequados
	7. Identificar e analisar os riscos
	8. Avaliar o risco de fraude
	9. Identificar e analisar alterações significativas
Atividades de controle	10. Selecionar e realizar atividades de controle
	11. Selecionar e realizar o controle geral da tecnologia
	12. Aplicar através de políticas e procedimentos
Informação e comunicação	13. Utilizar informações pertinentes
	14. Comunicar internamente
	15. Comunicar para o exterior
Acompanhamento	16. Efetuar avaliações em curso e/ou separadas
	17. Avaliar e comunicar as deficiências

Já nas versões do COSO II, é encontrada um desdobramento em 8 componentes:



Fonte: COSO – Executive Summary (2013)

A mudança principal está no desdobramento da análise de risco, em que a que a figura abaixo faz esta comparação:



Fonte: Portal do TCU³⁷.

Vale também comentar que a ISSAI 5700 traz um modelo próprio de controle interno, mas voltado na abordagem da prevenção a corrupção. Ela aborda com sete componentes chaves de gestão identificados, sendo os que seguem:

1. Cultura Organizacional Anticorrupção
2. Objetivos / Estratégia
3. Responsabilidade Organizacional
4. Gestão de Risco
5. Módulos de Prevenção da Corrupção (programa anticorrupção)
6. Comunicação e Informação
7. Monitoramento e Modificação.

Tais elementos, contudo são próximos aos encontrados na metodologia da Edição “Gerenciamento de Riscos – Estrutura Integrada” (COSO, 2013).

Há ainda que se mencionar outro modelo de gestão de riscos consubstanciada na norma NBR ISSO 31000 - Gestão de Riscos: Princípios e diretrizes. Esta

³⁷ <https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/politica-de-gestao-de-riscos/modelos-de-referencia.htm>

fornece princípios e diretrizes para gerenciar qualquer tipo de risco em toda ou em parte de qualquer organização. Trata-se de uma norma geral e não concorre com outras normas sobre gestão de riscos em áreas específicas. Seus objetivos são servir como guia mestre em matéria de gestão de riscos e harmonizar os processos de gestão de riscos, fornecendo uma abordagem comum, que pode ser aplicada a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos (ABNT, 2009). Tal norma pode ser indicada às unidades auditadas como alternativa de modelo de gestão de risco.

Os itens que passarão a ser abordados são itens de maneira comuns entre as os referências de modelos citados anteriormente e têm de objetivo de fornecer à equipe de auditoria um panorama geral, mas não completamente aprofundado, sobre estes sistemas. A finalidade é criar um bom referencial para um parâmetro de respeito de um sistema de controle baseado em gerenciamento de riscos. Vale atentar que estes sistemas podem ser combinados, não sendo exclusivos, inclusive com as medidas de controle voltadas à prevenção da corrupção, pois a corrupção e fraude, na verdade, é um tipo específico de risco.

Deve-se ressaltar neste momento que a implementação desses sistemas deve ser conduzida pelo órgão auditado, cabendo ao controle externo fazer apenas recomendações e avaliar a maturidade do sistema de controle da unidade auditada, conforme será detalhado no capítulo 5.

A partir desses sistemas, o órgão ou entidade pública pode elaborar um plano de ação escrito e documentado para gerenciamentos de riscos e prevenção da corrupção. A razão de se ter um Plano escrito é para que a entidade atinja um maior grau de maturidade dos controles, a fim de que esses sejam padronizados, rastreáveis (documentados) com atribuições de responsabilidades claras (Rechnungshof, 2016³⁸).

³⁸ Página 28, „Wesentliche Elemente der Beurteilung des IKS sind:
1. Bewusstsein der Führung für Risiken und Kontrollnotwendigkeiten,
2. Standardisierte, nachvollziehbare (dokumentierte) Prozesse mit klaren Verantwortlichkeiten, in die Kontrollen integriert sind,

Os seguintes elementos costumam ser comuns aos modelos de gerenciamento de riscos e estruturas de controles.

4.1. Ambiente de Controle

O ambiente de controle define o tom de uma organização, influenciando a consciência de controle de sua equipe. É a base para todos os outros componentes do controle interno, proporcionando disciplina e estrutura (ISSAI 9100³⁹).

Os elementos do ambiente de controle citados pela ISSAI 9100 são:

(1) a integridade pessoal e profissional e valores éticos de gestão e pessoal, incluindo uma atitude de apoio ao controle interno em todos os momentos da organização;

(2) compromisso com a competência;

(3) o “tom no topo” (filosofia e estilo operacional da alta administração);

(4) estrutura organizacional;

(5) políticas e práticas de recursos humanos.

Os cinco pontos acima serão comentados nas linhas seguintes, alguns agrupados em conjunto.

4.1.1. Integridade na organização (Programa de integridade)

A concepção e implementação de um sistema eficaz de prevenção anticorrupção e de gestão de riscos em relação ao ambiente é um desafio para todas os órgãos e requer a participação ativa de todos os funcionários e gestores para que constitua mais do que um conjunto inercial de etapas destinadas a cumprir políticas e procedimentos específicos (ISSAI 5700).

Neste contexto, o modelo de gestão de todos os níveis hierárquicos é essencial para um sistema eficiente de prevenção da corrupção. Sem haver um “tom no topo” e o total comprometimento da alta administração (secretários municipais,

(...)
³⁹ Página 17

presidentes de empresas/autarquias) com uma abordagem abrangente para o combate à corrupção, medidas preventivas são ineficientes.

Possíveis indicadores para um clima organizacional anticorrupção desejável e bom ambiente de podem ser (ISSAI 5700):

1. A organização demonstra um compromisso com a integridade e valores éticos.
2. O órgão encarregado pela supervisão interna, idealmente um gabinete de auditoria interna, deve supervisionar o sistema de controle interno da entidade.
3. A administração estabelece, estruturas, relatórios gerenciais, delega autoridades e responsabilidades apropriadas na busca de objetivos.
4. A organização demonstra um compromisso para atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos, e possui compromisso com a competência.

Do ponto de vista da prevenção a corrupção, um ponto é o estabelecimento de objetivos estratégicos ou prioridades. A partir de uma declaração ou visão de missão, o gerenciamento de uma organização deve definir objetivos ou prioridades organizacionais de longo prazo. Tais objetivos devem lidar com a melhoria da integridade organizacional, o fortalecimento dos sistemas de prevenção da corrupção ou a melhoria da eficácia e eficiência do sistema de integridade. Assim, deve-se definir objetivos anticorrupção, destacando o compromisso da administração no esforço para conter a corrupção dentro de uma organização (ISSAI 5700, página 19).

Um comprometimento da alta administração pode ser indicado através de um Plano de Integridade, ou alternativamente, um Plano de Gerenciamento de riscos que incluía pautas de melhoramento do sistema de integridade e governança em seu conteúdo. Cabe ressaltar que tais planos, embora desejados, não são obrigatórios do ponto de vista legal, isto é, são discricionários, cabendo apenas realizar recomendações dessas práticas.

Sugestão de auditoria: Caso a entidade não disponha de um programa de integridade, recomenda-se a elaboração de um plano de gerenciamento de riscos, que pode também englobar um Plano de integridade. O “Manual para implementação de Programas de Integridade: Orientações para o setor público”⁴⁰ da Controladoria Geral da União utilizada em âmbito federal pode ser recomendado como referências, mas sendo necessária as devidas adaptações a realidade da legislação da PMSP. Pode-se utilizar também como referência o “Manual de Gestão de Integridade, Riscos e Controle Interno de Gestão” do Ministério de Planejamento, Desenvolvimento e Gestão⁴¹. Os seguintes exemplos servem como referências de planos de integridade, cabendo, contudo, observar a adequabilidade a órgãos de pequena dimensão:

CGU	http://www.cgu.gov.br/sobre/governanca/programa-de-integridade-da-cgu/arquivos/plano-de-integridade-cgu.pdf/view
ANVISA	http://portal.anvisa.gov.br/documents/33756/4115433/Plano+de+Integridade+2018+2019/4d05ef4a-3876-4867-8463-ec2c31c630a2
Banco do Nordeste	https://www.bnb.gov.br/documents/50268/2244856/Relat%C3%B3rio_Integridade_BNB_2017.pdf/83bcb55e-fb7e-df46-6df3-72f7183bb126
Ministério da Fazenda	https://www.fazenda.gov.br/pmimf/frentes-de-atuacao/gestao-de-riscos/download-de-arquivos/2018-07-03-plano-de-integridade-mf-anexo-res-cgrci-04.pdf

Cabe a ressalva, contudo, que um Plano de Integridade deve ser recomendado como uma orientação de boa prática, visto que não há obrigação legal na PMSP em estabelecer Planos de Integridade. Um plano de integridade também poderia ser realizado de maneira conjunta com um plano de gerenciamento de riscos.

4.1.2. Compromisso com a competência

A Organização deve reter e manter pessoas competentes para garantir que as atividades sejam economia, eficientes e eficazes, que tenham um bom

⁴⁰ Disponível em http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual_profip.pdf

⁴¹ http://www.planejamento.gov.br/assuntos/gestao/controle-interno/170609_manual-de-girc_v1-2.pdf

desempenho, bem como uma boa compreensão das responsabilidades individuais com respeito ao controle interno (ISSAI 9100).

Os administradores e suas equipes devem, portanto, manter e demonstrar um nível de habilidade necessário para avaliar o risco e ajudar a garantir um desempenho eficaz e eficiente, e uma compreensão do controle interno suficiente para efetivamente cumprir suas responsabilidades.

Treinamentos, programas de educação continuada e reciclagens, por exemplo, pode aumentar a conscientização dos servidores públicos sobre os objetivos do controle interno.

Sugestão de auditoria: Os pontos deste tópico estão descritos nos itens 3.2.1 e 3.2.3.

4.1.3. Tom no topo e estrutura organizacional

Segundo a ISSAI 9100⁴², o “tom no topo” (isto é, a filosofia e operação da gerência e seu estilo) deve idealmente refletir uma atitude de apoio ao controle interno em todos os momentos com suporte a sua independência e amplo acesso dentro da organização, por exemplo.

A atitude estabelecida pela alta administração se reflete em todos os aspectos das ações da administração. O compromisso, o envolvimento e o apoio de altos funcionários do governo e legisladores na definição do “tom no topo” promovem uma atitude positiva e são fundamentais para manter uma atitude positiva e de apoio em relação ao controle interno de uma organização.

Se a alta administração acredita que o controle interno é importante, os outros membros da organização perceberão isso e responderão respeitando conscientemente os controles estabelecidos. Por exemplo, a criação de uma unidade de auditoria interna como parte do sistema de controle interno é um sinal forte da administração de que o controle interno é importante.

⁴² Páginas 18-19.

Por outro lado, se os membros da organização percebem que o controle não é uma preocupação importante para a alta administração e o controle é visto como mero discurso em vez de apoio significativo, é quase certo que os objetivos de controle da organização não serão efetivamente alcançados.

Conseqüentemente, a demonstração e a insistência na conduta ética da administração são de importância vital para os objetivos de controle interno. Ao desempenhar seu papel, a administração deve dar um bom exemplo por meio de suas próprias ações, e sua conduta deve refletir o que é apropriado, e não o que é aceitável ou conveniente. Em particular, as políticas, procedimentos e práticas da administração devem promover uma conduta ordenada, ética, econômica, eficiente e efetiva.

A integridade dos gerentes e suas equipes é, no entanto, influenciada por muitos elementos. Portanto, os funcionários devem ser periodicamente lembrados de suas obrigações sob um código de conduta.

SUGESTÃO DE ITEM DE AUDITORIA

Um dos pontos referentes à avaliação no tom no topo é sobre o tratamento dado pela alta administração para o código de conduta. Assim, reporta-se a forma de verificação descrita item 3.1 (página **Erro! Indicador não definido.**).

Mas o tratamento do “Tom no topo” não se restringe apenas ao código de conduta. Pode-se avaliar se a filosofia da gestão, observando se ela menciona a integridade e ética em sua pauta ou objetivos estratégicos, em seus planos, documentos, comunicações interna, eventos, pronunciamentos, entre outros.

4.1.3.1. Apoio ao controle interno e estrutura organizacional

O órgão encarregado pela supervisão interna deve supervisionar o sistema de controle interno da entidade. A alta administração deve demonstrar apoio a uma unidade de controle interno (ISSAI 9100, página 19).

A este respeito, o COSO (2004) reporta que a estrutura organizacional de uma entidade deve prover o arcabouço para planejar, executar, controlar e monitorar as suas atividades. Uma estrutura organizacional relevante inclui a definição de áreas

fundamentais de autoridade e responsabilidade, bem como a definição de linhas apropriadas de comunicação. Por exemplo, uma função de auditoria interna deve ser estruturada a fim de poder alcançar objetividade organizacional e permitir acesso irrestrito à alta administração e ao comitê de auditoria do conselho de administração, devendo o executivo chefe de auditoria reportar-se a um nível da organização que permita à atividade de auditoria interna cumprir com as suas responsabilidades.

Sugere-se verificar se unidade auditada possui em sua declaração de missão, ou documentos recentes relacionados a metas e estratégias, podendo-se prever a criação de unidade de auditoria interna, unidade de revisão ou unidade de controle interno, ou caso existente, se efetivamente haja um suporte e importância. Uma auditoria interna ao órgão, e diretamente vinculada à alta direção, poderia vir fortalecer o controle interno neste sentido⁴³. Os seguintes pontos podem ser verificados:

Aspetos relacionados com auditoria interna ou área específica de controle interno	Sim	Não	N.A	Descrição / OBS
A entidade dispõe de Gabinete de Auditoria Interna, unidade de controle interno, unidade de revisão ou unidade de controle de qualidade?				
A unidade acima está diretamente ligada ao órgão do dirigente máximo?				
No caso de existirem relatórios efetuados pelos órgãos de controle interno ou auditoria interna, existem reuniões e as situações detectadas são acompanhadas?				
A nível do controle interno, os pontos fracos detectados são corrigidos?				
Foram efetuadas ações de controle à entidade, nos últimos três anos?				
A administração, auditoria interna ou unidade de controle interno identificou algum tipo de risco de fraude ou suspeita de alguma fraude em curso?				

⁴³ Neste sentido, a ISSAI 9100 (página 19) reflete que “Se a alta administração acredita que o controle interno é importante, os outros membros da organização perceberão isso e responderão respeitando conscientemente os controles estabelecidos. Por exemplo, a criação de uma unidade de auditoria interna como parte do sistema de controle interno é um sinal forte da administração de que o controle interno é importante.”

Observação sobre auditoria interna na PMSP:

Ressalta-se que a auditoria interna foi atribuída a Controladoria Geral do Município de São Paulo – CGM, conforme Artigo 118 e Artigo 119 da Lei 15.764. Considerando o papel da GCM, há que ser estudado se não há objeção legal de criação dentro de um órgão um gabinete de auditoria interna, uma vez que o Art. 113 da referida Lei prevê dentro da GCM a Coordenadoria de Auditoria Interna para “exercer as atividades de órgão central do Sistema de Auditorias do Poder Executivo Municipal”. Por outro lado, não há objeção na Lei, a princípio, para criação de um departamento interno ao órgão para auditoria interna descentralizada. Os seguintes estudos de caso sobre o sistema de Controle Interno do governo federal e de Portugal podem servir como referência, ou mesmo como base de recomendações de boas práticas para um sistema de controle interno com maior grau de maturidade.

Estudo de caso nº 1: Governo federal

No governo federal, o Decreto federal nº 9.203/2017 e a Instrução Normativa Conjunta IN-MP/CGU nº 01/2016 preveem a auditoria interna aos órgãos da administração pública de maneira descentralizada, como parte integrante do sistema de controle, concomitante com as funções da CGU. No referido decreto, destaca-se o papel da auditoria interna da forma abaixo:

Art. 18 A auditoria interna governamental deverá adicionar valor e melhorar as operações das organizações para o alcance de seus objetivos, mediante a abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, dos controles e da governança, por meio da:

I - realização de trabalhos de avaliação e consultoria de forma independente, segundo os padrões de auditoria e ética profissional reconhecidos internacionalmente;

II - adoção de abordagem baseada em risco para o planejamento de suas atividades e para a definição do escopo, da natureza, da época e da extensão dos procedimentos de auditoria; e

III - promoção à prevenção, à detecção e à investigação de fraudes praticadas por agentes públicos ou privados na utilização de recursos públicos federais.

No caso da IN-MP/CGU Nº 1/2016⁴⁴, o Artigo 7º prevê que “os controles internos da gestão tratados neste capítulo não devem ser confundidos com as atividades do Sistema de Controle Interno relacionadas no artigo 74 da Constituição federal de 1988, nem com as atribuições da auditoria interna, cuja finalidade específica é a medição e avaliação da eficácia e eficiência dos controles internos da gestão da organização.”

Estudo de Caso nº 2: Sistema de controle interno de Portugal

O sistema de controle interno em Portugal se encontra em fase mais desenvolvida quando comparada ao caso brasileiro, sendo definido seus pormenores legalmente. O Decreto-Lei n.º 166/98 instituiu o sistema de controle interno da administração Portuguesa, abreviando-se por SCI. O SCI tem a seguinte definição legal:

“Art. 2º

1 - O SCI compreende os domínios orçamental, económico, financeiro e patrimonial e visa assegurar o exercício coerente e articulado do controlo no âmbito da Administração Pública.

2 – O controlo interno consiste na verificação, acompanhamento, avaliação e informação sobre a legalidade, regularidade e boa gestão, relativamente a actividades, programas, projectos, ou operações de entidades de direito público ou privado, com interesse no âmbito da gestão ou da tutela governamental em matéria de finanças públicas, nacionais e comunitárias, bem como de outros interesses financeiros públicos nos termos da lei”.

O Sistema de Controle Interno em Portugal, criado pelo Decreto-Lei n.º 166/98 funciona vinculado ao Governo executivo.

⁴⁴ Há uma longa definição da auditoria interna no Artigo 2º da IN-MP/CGU Nº 1/2016:

“III – auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança. As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos). Compete às auditorias internas oferecer avaliações e assessoramento às organizações públicas, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de que os órgãos e entidades não alcancem seus objetivos;”

Este sistema é dividido e previsto no referido Decreto-Lei em três níveis chamados de controle: a) operacional, b) setorial e c) estratégico, havendo a cada sua característica própria e atuando de formas distintas. Há, portanto, três camadas de controle interno, como será explicado a seguir cada uma.

Segundo Paulo Costa (2014), “o *controle operacional é assegurado pelos órgãos e serviços de inspeção, auditoria ou fiscalização inseridos no âmbito da respetiva unidade executiva, centrando-se no controle das decisões dos órgãos de gestão dessas unidades*”, ou seja, trata-se nesse nível de controle interno descentralizado, não estando subordinado a um órgão criado para efetuar auditoria interna, mas sendo diretamente um setor ou departamento dentro de um ministério, secretária, autarquia ou empresa pública. Normalmente, este órgão é vinculado diretamente ao dirigente máximo do órgão, não estando subordinados aos demais departamentos, vez que isto comprometeria o alcance e eficácia das auditorias internas. Trata-se do modelo de auditoria interna descentralizada.

Já o controle setorial é exercido pelos órgãos setoriais e regionais de controle interno, traduzindo-se, fundamentalmente, na avaliação do controle operacional e no exame da adequação da inserção de cada unidade operativa, e respetivo sistema de gestão, nos planos globais de cada ministério ou região. Por exemplo, o ministério da saúde possui um órgão próprio de controle deste setor (saúde). Contudo, hospitais com personalidade jurídica própria podem ter uma unidade de auditoria interna (controle operacional), mas ainda assim ser auditada também pelo controle setorial.

Por fim o controle estratégico tem carácter horizontal relativamente a toda a administração financeira do Estado português. Este é exercido pela Inspeção-Geral de Finanças⁴⁵, Órgão similar à Controladoria Geral da União (CGU) e Controladoria Geral do Município de São Paulo (CGM); pela Direção-Geral do Orçamento; e pelo Instituto de Gestão Financeira da Segurança Social.

⁴⁵ Mais detalhes em <http://www.igf.gov.pt/institucional1/apresentacao111.aspx>

Este último nível de controle consiste na avaliação do controle operacional e do controle setorial, e na avaliação do grau de realização das metas traçadas nos Programas de Governo e o Orçamento do Estado.

Nota-se uma estrutura em que efetivamente há um sistema inteiro de controle interno, assegurando o controle em várias etapas.

Ainda, em ordem a assegurar que não haja redundância de controles pelos diversos níveis, nem existência de áreas não sujeitas a nenhum tipo de controle foi adicionalmente previsto pelo Decreto-Lei n.º 166/98 o denominado Conselho Coordenador do SCI. Este Conselho é “*composto por todos os inspetores-gerais, pelo diretor-geral do Orçamento, pelo presidente do conselho directivo do Instituto de Gestão Financeira da Segurança Social e pelos demais titulares de órgãos setoriais e regionais de controlo interno*”, sendo um órgão de consulta do governo (executivo) em matéria de controle interno, sendo presidido pelo Inspetor-Geral de Finanças. Compete ao referido conselho:

- a. Emitir pareceres sobre os projetos de leis orgânicas dos órgãos setoriais
- b. e regionais de controle;
- c. Emitir pareceres sobre os planos e relatórios setoriais de atividade;
- d. Elaborar o plano e relatório anuais do SCI;
- e. Estabelecer normas sobre metodologias de trabalho e aperfeiçoamento técnico-profissional dos recursos humanos afetos ao SCI.

Designação de um responsável por prevenção à corrupção como boa prática

Uma prática sugerida é designar uma unidade dentro da estrutura para projetar e supervisionar as atividades de controle interno podendo idealmente ser um gabinete de auditoria interna, conforme anteriormente descrito. Mas indo além, a responsabilidade organizacional pela prevenção da corrupção como um objetivo específico dentro da instituição pode ser claramente atribuída. Isso poderia ser organizado dentro da instituição, como uma unidade ou simplesmente uma pessoa específica designada de combate à corrupção⁴⁶, como a nomeação de um encarregado de prevenção à corrupção. Eles devem entender o programa de

⁴⁶ Na Alemanha, muitas vezes há uma determinada pessoa encarregada de combate à corrupção e que tratava as denúncias, chamada de *Korruptionsbeauftragte* ou *Korruptionsansprechpartner*.

integridade e suas operações, bem como os riscos e controles anticorrupção em todo o programa; ter responsabilidades definidas; e ser independente e ter o direito de se reportar diretamente ao administrador-chefe da organização (ISSAI 5700, página 20).

A unidade ou pessoa para a prevenção da corrupção deve ser estabelecida com base nas tarefas e tamanho da organização. Esta unidade ou pessoa pode ser encarregada das seguintes tarefas abrangendo todas as atividades organizacionais:

- ✓ Servir como um contato para o pessoal da organização e gerenciamento, se necessário sem ter que depender de canais oficiais, juntamente com pessoas particulares (a unidade / pessoa deve ter acesso direto e pode reportar ao nível de gerência superior (por exemplo, secretário municipal);
- ✓ Ser o repositório de conhecimento sobre riscos de corrupção e assessoria à gestão de organizações;
- ✓ Manter os funcionários informados (por exemplo, por meio de seminários, ferramentas de e-learning e apresentações regularmente);
- ✓ Ajudar na formação e ter acesso a todas as sessões de formação relacionadas com a corrupção;
- ✓ Gerenciando o processo de avaliação de risco;
- ✓ Monitorar e avaliar quaisquer indícios de corrupção;
- ✓ Ajudar a manter o público informado sobre as penalidades previstas na lei de serviço público e na lei criminal (efeito preventivo), respeitando os direitos de privacidade das pessoas envolvidas.

Se a unidade / pessoa tomar conhecimento de fatos que levem a uma suspeita razoável de que uma ocorrência de corrupção ou crime conexo, a alta administração da organização deve ser informada imediatamente e as recomendações devem ser feitas sobre:

- ✓ Realização de uma possível investigação interna;

- ✓ Informar as autoridades policiais ou ministério público (a administração da organização deve tomar as medidas necessárias para lidar com este assunto) e;
- ✓ Relatar deficiências nos sistemas existentes de prevenção à corrupção.

Segundo a recomendação da ISSAI 5700, a unidade / pessoa não deve ter autoridade para executar medidas disciplinares e não deve conduzir investigações em processos disciplinares por casos de corrupção, sendo apenas um contato para recepção de possíveis casos de corrupção ou fraude que leve ao conhecimento à alta administração se tiverem uma suspeita razoável de que uma ocorrência de corrupção foi cometida.

Ainda, sugere-se que unidade ou pessoa para a prevenção da corrupção deve ser formalmente nomeada. Esta nomeação deve ser anunciada na área de responsabilidade da pessoa.

Exemplo da Alemanha como estudo de caso:

Na esfera federal da Alemanha, o regulamento denominado “Guia para prevenção à corrupção no governo federal”⁴⁷ prevê que uma pessoa de contato para a prevenção da corrupção deve ser indicada (recebem o nome de *Ansprechperson für Korruptionsprävention* ou *beauftragter*), podendo ser atribuída as seguintes tarefas: a) pessoa de contato para funcionários e administração, mesmo sem a observância dos canais oficiais, bem como para os cidadãos; b) assessoria à administração sobre matérias de corrupção; c) treinamentos aos funcionários (por exemplo, através de eventos regulares de informação); d) observação e avaliação de sinais de corrupção; e) Participação na informação do público sobre penalidades civis e criminais (aspecto de prevenção).

No estado Alemão chamado de Baden-Württemberg, o Regulamento de prevenção e luta contra corrupção (*VwV Korruptionsverhütung und –bekämpfung*)

⁴⁷ http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_30072004_O4634140151.htm

prevê a criação de um departamento ou unidade para tratar assuntos de corrupção⁴⁸, como segue:

“3.1 Medidas nas autoridades da administração do estado

3.1.1 Alocação de atividades

(1) No caso das secretarias, todas as medidas para prevenir e combater a corrupção em toda a pasta são coordenadas em uma unidade organizacional. Esta deve coordenar as medidas sempre que necessários com os outros departamentos, dispõe que quaisquer indicações de suspeita de corrupção sejam acompanhadas.

(2) Para todas as outras unidades, essa atividade é de responsabilidade da alta administração, quando não estiver atribuída a uma unidade organizacional expressamente no plano de alocação de atividades.”

4.1.4. Política de gerenciamento de recursos humanos

Segundo a ISSAI 5700, as políticas e práticas de recursos humanos incluem a forma de contratação (ou seleção para ingresso no serviço público), orientação, treinamento (formal e em serviço) e de educação continuada, avaliação e aconselhamento, promoção e compensação e ações corretivas.

Um aspecto importante do controle interno é um corpo de pessoal qualificado, visto que para a organização atingir seus objetivos, necessita-se de funcionários bem treinados. Uma equipe competente e confiável é necessária para fornecer um controle efetivo. Portanto, os métodos pelos quais os servidores ingressam em carreira pública, bem como são treinados, avaliados, motivados e promovidos são uma parte importante do ambiente de controle. Tais pontos foram abordados nos itens 3.2.1 e 3.2.3, e 3.2.4, sugerindo-se a releitura dos detalhes nestes itens.

4.1.5. Definição de responsabilidades

Os papéis e as responsabilidades de cada grupo de profissionais e de unidades da organização devem ser claramente definidos para que todos entendam os limites de suas responsabilidades e como os seus cargos se encaixam na estrutura de gestão de riscos, permitindo que estejam informados, habilitados e autorizados a exercer seus papéis e as responsabilidades que foram

⁴⁸ <https://im.baden-wuerttemberg.de/de/sicherheit/polizei/praevention/korruptionsverhuetung-und-bekaempfung/>

delegadas no gerenciamento de riscos. Uma gestão de riscos mais madura define claramente quem vai ser responsável por gerenciar um determinado risco, bem como documenta esses procedimentos (Rechnungshof, 2016).

Na prática, a instância máxima de governança toma a decisão e delega a implantação e operação da gestão de riscos aos executivos da gestão, assumindo um papel de supervisão desses processos. Além disso, vale-se dos serviços de asseguração da auditoria interna para monitorar e avaliar a eficácia dos processos de gerenciamento de riscos e controles por toda a organização.

A administração é diretamente responsável pela concepção, estruturação e implementação da gestão de riscos. Em qualquer organização, o dirigente máximo é o depositário final dessa responsabilidade, cabendo-lhe assumir a iniciativa de delegar as responsabilidades⁴⁹. Contudo, enfatizando, esta delegação deve ser documentada, idealmente atribuindo as responsabilidades em um plano de gerenciamento de riscos, após a fase avaliação e mapeamento de riscos.

4.2. Avaliação dos riscos

Um passo seguinte à construção de um modelo de controle interno robusto condiz se a organização faz alguma política de avaliação, identificação e documentação de riscos. Neste sentido, vale notar que o Tribunal de Contas da União⁵⁰, Tribunal de Contas da Áustria⁵¹ bem como o Tribunal de Contas federal da Alemanha⁵² consideram que um controle interno passa ser no mínimo satisfatórios apenas quando a administração tem ciência da necessidade de gerenciamento de riscos e sistematiza seus controles em razão dos riscos identificados.

A ISSAI 9100 define que a avaliação de riscos é o processo de identificação e análise de riscos para a consecução dos objetivos da entidade e determinar a resposta apropriada. Segundo esse documento, isso implica:

(1) identificação de risco:

⁴⁹ TCU – Gestão de Riscos – Avaliação de Maturidade e Rechnungshof (2016).

⁵⁰ TCU 2018 - Gestão de Riscos – Avaliação de Maturidade.

⁵¹ Rechnungshof (2016), páginas 20 e 28.

⁵² Bundesrechnungshof (2018) -

- relacionado aos objetivos da entidade;
- relacionados a atividade ou tipo de serviço;
- deve incluir riscos devidos a fatores externos e internos, tanto na entidade e os níveis de atividade;

(2) avaliação de risco:

- estimar impacto que um risco pode ter caso ocorra (consequência de um risco, caso aconteça);
- avaliar a probabilidade de ocorrência do risco;

(3) avaliação do apetite de risco da organização;

(4) Desenvolver respostas para mitigar os riscos:

• quatro tipos de respostas ao risco devem ser considerados: transferência, tolerância (aceitação do risco), tratamento ou término da atividade. Destes, o tratamento (ou mitigação) de risco é o mais relevante para essas diretrizes, porque um controle interno eficaz é o principal mecanismo para tratar o risco;

• os controles apropriados envolvidos podem ser investigativos ou preventivos.

No aspecto tocante ao risco, é relevante citar nesse momento “Roteiro de Auditoria de Gestão de Riscos” da Secretaria de Métodos e Suporte ao Controle Externo do TCU que aborda uma metodologia própria as maneiras de se identificar e avaliar os riscos, os quais serão aqui tratados⁵³.

Identificação dos riscos

Identificação de riscos é o processo de busca, reconhecimento e descrição de riscos, tendo como base o contexto estabelecido e apoiado na comunicação e consulta com as partes interessadas, internas e externas. O objetivo é produzir uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter

⁵³ Mas cabe à unidade auditada implementar um programa de avaliação dos riscos.

um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto⁵⁴.

No contexto do sistema de controle interno voltado à prevenção da corrupção, a organização pode avaliar quais áreas são mais suscetíveis ao risco da corrupção e que possíveis medidas podem ser tomadas para minimizar tais riscos, levando-se em consideração que a corrupção é um tipo de risco específico.

Para produzir uma lista de riscos⁵⁵, deve-se analisar setor a setor e as correspondentes atividades que são realizadas, bem como a forma de sua realização. Mapas de processos ou fluxos de trabalhos (workflows) ajudam a clarificar cada uma das etapas.

Ao avaliar riscos, a administração leva em consideração eventos previstos e imprevistos. Muitos eventos são rotineiros e recorrentes e já foram abordados nos programas de gestão e orçamentos operacionais, enquanto que outros são imprevistos. A administração avalia os riscos em potencial de eventos imprevistos e, caso ainda não tenha feito essa avaliação, até os previstos que podem causar um impacto significativo na organização⁵⁶.

A administração leva em conta tanto o risco inerente quanto o residual. Risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Risco residual é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes. Após o desenvolvimento das respostas aos riscos, a administração passará a considerar os riscos residuais.⁵⁷

⁵⁴ Fonte: (TCU-SEGESEX, 2017).

⁵⁵ No Anexo II, encontra-se uma tradução exemplificativa do Tribunal de Contas da Alemanha sobre uma lista hipotética de riscos, guardada as considerações das estruturas administrativas e de realidade daquele país, que obviamente vezes diferem da brasileira. Contudo, prática melhor é buscar planos já constituídos na prática como exemplos.

⁵⁶ Fonte: (COSO, 2013).

⁵⁷ Fonte: (COSO, 2013)

A identificação de riscos pode se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, necessidades das partes interessadas. Convém que pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados. Envolver a equipe diretamente responsável pela execução do processo, do projeto ou da atividade que está tendo os riscos identificados também ajuda a criar a responsabilidade em relação ao processo de gestão de riscos e o comprometimento em relação ao tratamento dos riscos⁵⁸.

O risco depende da probabilidade e sua correspondente consequência na organização caso aconteça em termos da magnitude do impacto nos objetivos. Cabe ressaltar que esses os riscos são relacionados tanto simplesmente a erros na execução da entidade, como a casos de dolo relacionados à fraude. Como exemplo, pagamentos indevidos à fornecedores podem ocorrer tanto por erro, como por dolo. A questão seria, neste caso, avaliar qual é o risco de se cometer um pagamento indevido levando-se em consideração os controles já existentes, seu impacto caso aconteça, e posteriormente como tratar esse risco, criando-se algum tipo de controle preventivo adicional ou modificando a forma de controle existente.

O resultado final do processo de análise de riscos será o de atribuir, para cada risco identificado, uma classificação tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A ideia central é produzir uma lista de risco em um documento⁵⁹. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas e as fontes de risco, suas consequências positivas ou negativas, expressas em termos de impactos tangíveis ou intangíveis.

⁵⁸ Fonte: (TCU-SEGESEX, 2017)

⁵⁹ Na Alemanha se utiliza matrizes de risco (BUNDESRECHNUNGSHOF, 2018), enquanto em Portugal, se utiliza um “Mapa de riscos”, como no Anexo I. A essência, contudo, é produzir um catálogo documentado com riscos, em que haja a informação de sua descrição, sua probabilidade de ocorrer, sua consequência caso ocorra, e como será tratado, bem como quem será o responsável pelo tratamento do risco.

Os riscos sempre deverão ser avaliados entre sua consequência versus probabilidade. A avaliação da probabilidade e impacto é baseada no grau de experiência dos gestores. A seguinte fórmula mostra o risco em função da Probabilidade (P) versus seu Impacto (I):

$$\text{Riscos} = P \times I$$

O quadro abaixo serve como um exemplo guia para avaliação dos riscos na prática para uma posterior construção de uma matriz de riscos, a qual será tratada em seguida:

METODOLOGIA DE ANÁLISE DO RISCO		
ITINERÁRIO DE ANÁLISE	CRITÉRIOS DE ANÁLISE	QUESTÕES
Definição do contexto	Estratégico Operacional	- Quais as áreas de atividade e as características da organização? - Quais são as suas missões e objetivos?
Identificação do Risco	Data Área Descrição	- O que pode acontecer? - Como pode acontecer? - Quando pode acontecer? - Há oportunidade para aperfeiçoamento?
Análise do Risco	Probabilidade Gravidade da Consequência	- Quais as causas da ocorrência do risco? - Quais os efeitos caso o risco ocorra? - O risco é estratégico ou operacional? - Como podem estes efeitos ser reduzidos?
Avaliação do Risco	Elevado Moderado Fraco	- Quais as medidas de prevenção do risco? - Qual a eficiência operacional? - O que resulta da comparação dos custos e dos benefícios do risco?
Desenvolvimento, Tratamento e Controlo do Risco	Evitar Prevenir Transferir Aceitar	- A atividade geradora do risco deve ou não prosseguir? - Como reduzir/controlar as probabilidades e consequências da ocorrência? - Pode delegar-se num terceiro total ou parcialmente a atividade ou o efeito do risco, através de contratos, parcerias, seguros, etc. - O risco é aceitável face ao custo/benefício a que está associado? - Houve aperfeiçoamentos organizacionais?
Acompanhamento, Revisão e Atualização do Plano	Anual Semestral	- Qual a periodicidade do Acompanhamento do Impacto do Risco? - Qual a efetividade da Revisão do Risco? - Houve mudança no grau de prioridade do risco?

Fonte: Plano de prevenção de riscos da gestão da Direção Geral do Tribunal de Contas de Portugal.

Idealmente, os riscos podem ser visualizados para uma matriz de riscos, em que os avaliadores (do risco) devem, com base na sua experiência, estimar se a probabilidade de riscos é alta, média ou baixa para cada um dos riscos levantados sem se atribuir um número, ou seja, sem ser uma avaliação quantitativa. Segundo

a Norma de Gestão de Riscos⁶⁰ da Federação Europeia das Associações de Gerenciamento de Riscos FERMA (2003), as três categorias de probabilidade podem ser avaliadas tendo o seguinte guia:

Probabilidade	Descrição	Indicadores
Alta	Com possibilidade de ocorrência todos os anos ou hipótese de ocorrência superior a 25%.	Potencial para ocorrer diversas vezes dentro do período de tempo (por exemplo - dez anos). Ocorreu recentemente.
Média	Com possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 25%.	Pode ocorrer mais do que uma vez dentro do período de tempo (por exemplo - dez anos). Pode ser difícil de controlar devido a algumas influências externas. Existe um histórico de ocorrências?
Baixa	Sem possibilidade de ocorrência em cada dez anos ou hipótese de ocorrência inferior a 2%.	Não ocorreu. Improvável que ocorra

Da mesma forma, no caso do evento do risco aconteça, qual é sua consequência: Alta, média ou baixa. A simples associação de probabilidades e consequências para cada risco, sem se atribuir um número, forma uma matriz de risco do tipo qualitativa.

A matriz gerada é utilizada para avaliar em qual o grau de risco que um determinado risco apresenta, considerando probabilidade versus consequência. Uma possível matriz seria como a seguinte na página a seguir:

		IMPACTO		
		Baixa	Média	Alta
Probabilidade	Provável ou quase certo	Amarelo	Vermelho	Vermelho
	Possível	Ciano	Amarelo	Vermelho
	Raro	Ciano	Ciano	Amarelo

Fonte: Elaboração do autor

⁶⁰ FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS. Disponível em http://www.ifc-camboriu.edu.br/~nildo/si/Normas_GR.pdf

Os riscos em vermelho são os mais críticos e de alta prioridade para serem tratados (mitigados), os amarelos secundários, e os azuis possivelmente toleráveis.

É possível ampliar essa matriz para cinco níveis de probabilidade e/ou consequências, como segue:

		IMPACTO				
		Irrelevante	Baixo	Média	Crítico	Extremo
Probabilidade	Quase certo	Amarelo	Amarelo	Vermelho	Vermelho	Vermelho
	Provável	Amarelo	Amarelo	Amarelo	Vermelho	Vermelho
	Possível	Azul	Amarelo	Amarelo	Amarelo	Vermelho
	Pouco provável	Azul	Azul	Amarelo	Amarelo	Amarelo
	Raro	Azul	Azul	Azul	Amarelo	Amarelo

Há de mencionar outros modelos de avaliação de risco, utilizando-se análises semi-quantitativas com atribuições número de probabilidades, conforme exposição de TCU-SEGESEX (2017)⁶¹.

Mapa de riscos

Uma de avaliação de risco pode ser feita através da construção de um mapa de riscos, ou em uma matriz de risco (Bundesrechnunghof, 2017) também baseada na metodologia da FERMA. Para facilitar a visualização desse mapa, deve-se atribuir a escala de 1 a 3 para as probabilidades sendo: 1 para baixa; 2 para média e 3 para alta. Da mesma forma deve-se atribuir notas de 1 a 3 para o impacto (prejuízo, degradação de imagem, paralisação de um serviço essencial, etc..) caso o risco venha a se realizar. Resultante da combinação do impacto x probabilidade, tem se a gradação do risco (também de 1 a 3). Uma tabela de graduação do risco segue abaixo. Um modelo mapa de riscos resultante pode ser elaborado conforme

⁶¹ Páginas 25-30.

modelo a seguir (sugere-se a leitura de exemplo do Tribunal de Contas de Portugal preenchido no ANEXO I):

Probabilidade	Impacto	Gradação do risco
1	1	1
1	2	1
1	3	2
2	1	1
2	2	2
2	3	3
3	1	2
3	2	3
3	3	3

MAPA DE RISCOS					
Atividade	Descrição do Risco	PR	IM	GR	Medidas de prevenção
		1	1	1	
		2	2	2	
		3	3	3	

PR - Probabilidade do risco

IM - Impacto; 1 - Baixo; 2 - Médio; 3 – Baixo

GR - Grau do Risco; 1 -Fraco; 2 - Moderado; 3 - Elevado

SUGESTÃO DE ITEM DE AUDITORIA

Um controle interno com maior grau de maturidade ocorre quando a entidade tem ciência da necessidade de mapeamento de riscos (RECHNUNGSHOF, 2016). Para avaliação dos processos de identificação e análise de riscos, a equipe de auditoria deve verificar se a envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação ampla dos riscos, envolvendo as pessoas das áreas relacionadas onde o risco pode acontecer, havendo as seguintes perguntas como guia (TCU-SEGESEX, página 76):

Política de gestão de riscos	Sim	Não	N.A	Descrição / OBS
A entidade tem ciência da prática de gestão de riscos ⁶² ?				
Há na entidade um processo de identificação, análise de riscos, documentação e correspondente tratamento de riscos? Há atribuição de responsabilidades claras para mitigação e respostas a riscos?				
A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização? Há algum plano de gerenciamento de riscos?				
São envolvidas pessoas com conhecimento adequado, bem como os gestores das respectivas áreas para identificação e tratamento de riscos?				
São utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco?				
O processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e risco de corrupção, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos?				
O processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto?				
Os riscos identificados são analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos?				
Todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento ou mapeamento, bem como são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas?				
Os riscos identificados são analisados em termos de probabilidade de ocorrência e de impactos nos				

⁶² Rechnungshof (2016), página 113.

objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos?				
---	--	--	--	--

Caso não haja qualquer atividade de identificação dos riscos, deve-se recomendar à entidade que promova alguma política de identificação de riscos. Pode-se sugerir as metodologias disponíveis como ISO 31000 (2009) ou FERMA (2003). Sugere-se que a equipe de auditoria tenha familiaridade com esses modelos para ter uma referência robusta de como uma boa metodologia deve ser aplicada.

Cabe a observação que, apesar da avaliação de risco ser uma prática quase que essencial à construção de um controle interno que funcione eficientemente, é papel do órgão ou entidade pública fazer a avaliação dos riscos por sua conta, não devendo a equipe de auditoria assumir essa avaliação por completo, cabendo ao controle externo avaliar qual é o grau de maturidade e orientação ao risco que o órgão auditado tem, mas possivelmente realizar recomendações⁶³ caso encontre oportunidades de melhorias de controles.

4.2.1. Tratamento dos riscos

As medidas preventivas do risco são de natureza diversa, destinando-se a

- Evitar o risco, eliminando a sua causa, ou descontinuando as atividades que geram os riscos;
- Prevenir ou reduzir o risco, procurando minimizar a probabilidade de ocorrência do risco ou do seu impacto negativo, possivelmente através de criações de controles e treinamentos com funcionários;
- Aceitar o risco e os seus efeitos, quando sua probabilidade e/ou impacto é baixo;

⁶³ O TCU já construiu um modelo próprio de avaliação de Maturidade. Vide TCU (2018): Gestão de Riscos – Avaliação de Maturidade, páginas 52 a 59.

- Transferir o risco para terceiros quando possível (por exemplo, contratado seguros).

A análise de riscos só se completa quando as ações que a gestão adota para respondê-los são também avaliadas, chegando-se ao nível chamado de risco residual. O risco residual é aquele que remanesce depois de considerado o efeito das respostas adotadas pela gestão para reduzir a probabilidade e ou o impacto dos riscos, incluindo controles internos e outras ações.

Conforme descrito anteriormente, as formas de resposta a riscos podem variar entre reduzir, evitar, transferir ou aceitar o risco, incluindo o estabelecimento de atividades de controle para assegurar que as respostas definidas pela administração sejam efetivamente aplicadas.

A avaliação das respostas a riscos e atividades de controle correspondentes – ou simplesmente controles – é parte integrante da análise de riscos. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco. Um bom plano de riscos deve conter explicitamente a quem foi delgado para gerenciar os controles.

Caso seja elaborado um mapa de riscos como exemplo do Anexo I, tais atividades devem ser descritas no campo “medidas de prevenção”. As atividades de controle também são geralmente referidas simplesmente como controles internos, que serão tratadas na seção seguinte.

Estudo de caso em Portugal – Planos de gerenciamento de riscos e Planos de prevenção da corrupção e infrações conexas:

O Conselho de Prevenção da Corrupção (CPC), entidade independente que funciona junto do Tribunal de Contas, aprovou a Recomendação nº 1/2009 do CPC, publicada no DR, II Serie, nº 140 de 22 de julho, através da qual todos os organismos públicos são obrigados a elaborar Planos de Prevenção da Corrupção e Infrações Conexas, bem como relatórios anuais sobre a execução dos mesmos. Tais planos são orientados por matrizes de riscos.

Vários exemplos de planos de gerenciamento de riscos e de podem ser encontrados publicados on-line, podendo servir como sugestões modelo para implementação de planos de risco para os órgãos da administração pública na PMSP⁶⁴, mas devendo observar as adaptações legais e da realidade da PMSP ou da especificidade do serviço.

4.3. Atividades de Controle

As atividades de controle são as políticas e procedimentos estabelecidos para mitigar os riscos e alcançar os objetivos da entidade. Idealmente, os controles internos devem ser desenhados após uma avaliação de riscos com ferramentas estruturadas, isto é, desenhados para mitigar as causas dos riscos, de forma a restar apenas o chamado risco residual.

As atividades de controle ocorrem em toda as unidades de uma organização, em todos os níveis e todas as funções. Eles incluem uma gama de controles investigativos e preventivos. A ISSAI 9100 lista os seguintes exemplos como atividade de controles:

- (1) procedimentos de autorização e aprovação;
- (2) segregação de funções (autorização, processamento, registro, revisão);
- (3) controles sobre acesso a recursos e registros;
- (4) verificações;
- (5) reconciliações;
- (6) revisões do desempenho operacional;
- (7) revisões de operações, processos e atividades;
- (8) supervisão (atribuição, revisão e aprovação, orientação e treinamento).

⁶⁴ Exemplos: Plano de Integridade e Transparência do Instituto de Informática da Segurança Social de Portugal: http://www.seg-social.pt/documents/10152/15732360/Plano_Integridade_Transparencia_2018.pdf/cda30d13-3e1b-4b39-a9fa-4ac5b703e1e3
Banco de Portugal: https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/plano_de_gestao_de_riscos_de_corrupcao_e_infracoes_conexas_-_relatorio_de_execucao_-_2017.pdf

Algumas dessas práticas de controle voltadas para especificamente para prevenção da corrupção já foram descritas no capítulo 0.

Para ser eficaz, as atividades de controle precisam:

- ser apropriadas (isto é, o controle certo no lugar certo e proporcional ao risco envolvido, mas levando-se em consideração o custo do controle em termos de consumo de trabalho e tempo);
- funcionar consistentemente de forma permanente. Isto é, ser cumprido com zelo por todos os funcionários envolvidos e não negligenciado quando a(s) pessoa(s) encarregada(s) está ausente ou há sobrecarga de trabalho;
- ter um custo benefício positivo (isto é, o custo de implementação e execução em termos de consumo de tempo do controle deve ser não exceda os benefícios derivados);

As atividades de controle incluem uma variedade de políticas e procedimentos como os seguintes exemplos:

1. Autorização e procedimentos de aprovação

A autorização e a execução de transações e eventos são feitas apenas por pessoas que atuam dentro do escopo de sua autoridade. A autorização é o principal meio de assegurar que apenas transações e eventos válidos sejam iniciados como pretendido pela administração. Os procedimentos de autorização, que devem ser documentados e comunicados claramente aos coordenadores/supervisores e funcionários, devem incluir as condições e os termos específicos sob os quais as autorizações devem ser feitas. A conformidade com os termos de uma autorização significa que os funcionários agem de acordo com diretivas e dentro das limitações estabelecidas pela administração ou pela legislação.

2. Segregação de funções (autorização, processamento, gravação, revisão)

Para reduzir o risco de erros, desperdícios ou atos ilícitos e o risco de não detectar tais problemas, nenhum indivíduo ou equipe deve controlar todos os

principais estágios de uma transação ou evento. Em vez disso, os deveres e responsabilidades devem ser atribuídos sistematicamente a um número de indivíduos para garantir que existam verificações e balanços eficazes. As principais funções incluem autorizar e registrar transações, processar e revisar ou auditar, conforme já descrito no item 3.4.

3. Controles sobre acesso a recursos e registros

O acesso a recursos e registros deve ser limitado a indivíduos autorizados que são responsáveis pela custódia e / ou uso dos recursos. A responsabilidade pela custódia é evidenciada pela existência de recibos, estoques ou outros registros que atribuem a custódia e registram a transferência da custódia.

Deve ser dada atenção especial sobre controles sobre TI, no tocante de permissões sobre inserções de registros, alterações de dados e correspondentes exclusões (vide página 31).

4. Verificações

Transações e eventos significativos são verificados antes e depois do processamento. Por exemplo, quando bens são entregues, o número de bens fornecidos deve ser verificado com o número de mercadorias encomendadas/licitadas. Em seguida, o número de mercadorias faturadas deve ser verificado com o número de mercadorias efetivamente recebidas.

Nos casos em que envolvem banco de dados com inserções e modificações de informações, principalmente nos casos em que envolva algum tipo de autorização como pagamentos de benefícios ou concessão de permissões ou restrições, deve-se haver verificações de procedimentos através de corpo de prova de algumas de algumas das operações. Um sistema em que há pessoas realizando tais verificações de forma rotativa é adequado. Verificações com corpo de prova, ou teste substantivo, podem ser executadas por amostragem por um possível departamento de auditoria interna.

5. Reconciliações

Os registros são reconciliados com os documentos apropriados regularmente, especialmente em operações contábeis. Como exemplo, os registros contábeis relativos a contas bancárias devem reconciliados com os extratos bancários correspondentes.

6. Revisões de desempenho operacional

O desempenho operacional é revisado em comparação a um conjunto de padrões base, avaliando a eficácia e eficiência. Se as avaliações de desempenho determinar que as realizações reais não atendem aos objetivos estabelecidos padrões, os processos e atividades estabelecidos para alcançar os objetivos devem ser revisados para determinar se melhorias são necessárias.

7. Revisões de operações, processos e atividades

Operações, processos e atividades devem ser revisados periodicamente para assegurar que estejam em conformidade (*compliance*) com os regulamentos, políticas, procedimentos ou outros requisitos vigentes. Esse tipo de revisão das operações reais de uma organização deve ser claramente distinguido do monitoramento do controle interno.

8. Supervisão (atribuição, revisão e aprovação, orientação e treinamento)

Uma supervisão adequada ajuda a atingir os objetivos de controle interno alcançados. Deve se atentar que a função de supervisão não é suficiente no sentido de gerenciar as pessoas, mas deve revisar e aprovar os trabalhos de sua equipe, comunicando claramente os deveres e responsabilidades atribuídos a cada membro da equipe. O trabalho de revisão deve ser sistematicamente o trabalho de cada um na medida do necessário.

A delegação de trabalho de um supervisor não deve diminuir sua responsabilidade e deveres. Os supervisores devem, assim, prover a orientação e o treinamento necessários à sua equipe a fim de se evitar possíveis erros ou mesmo detectar má conduta.

A lista acima de 1 a 8 não é exaustiva, mas enumera as atividades mais comuns de controle preventivo e investigativo. As atividades de controle 1 a 3 são preventivas, 4 a 6 são mais investigativas; e 7 a 8 são preventivas e investigativas. As entidades públicas devem alcançar um equilíbrio adequado entre as atividades de controle preventivo e investigativo, geralmente uma mistura de controles.

4.4. Informação e comunicação

A informação e a comunicação são essenciais para realizar todos os objetivos de controle interno. Informações pertinentes devem ser incluídas e comunicadas em de uma forma que permita que os funcionários cumpram suas responsabilidades sobre os controles internos e outras responsabilidades (ISSAI 9100).

A comunicação interna eficaz é um elemento central para garantir que as regras e diretrizes de integridade sejam aplicadas de maneira oportuna e adequada, porque é necessário disseminar a mensagem da alta administração sobre a relevância do gerenciamento de riscos e do comprometimento da instituição com práticas anticorrupção. Assim, as instituições públicas devem de criar mecanismos que facilitem o fluxo vertical, horizontal e transversal de informação dentro da entidade, de modo a promover uma comunicação dinâmica, simples e rápida entre as diferentes linhas de autoridade⁶⁵.

Os sistemas de informação devem produzir relatórios que contêm informações de gestão à alta gerência, financeiras e não financeiras e relacionadas à adesão à legislação (*compliance*) que permitem executar e controlar as atividades da entidade. Eles lidam não apenas com dados gerados internamente, mas também com eventos externos, atividades e condições necessárias para permitir a tomada de decisões e relatórios.

Um bom sistema de comunicação permite que os servidores recebam da alta administração uma mensagem clara de que as responsabilidades de combate à

⁶⁵ ISSAI 5700, página 48, linhas 5 a 10.

corrupção, controle interno e a prioridade da integridade devem ser levadas a sério⁶⁶.

Os métodos de comunicação dentro das instituições incluem manuais, normas internas, diretrizes, portarias, procedimentos, relatórios, memorandos, relatórios estatísticos, notificações, quadros de avisos, sites, intranet, mensagens e vídeos gravados, e-mail e discursos, entre outros.

A comunicação sobre questões de integridade deve incluir que os funcionários saibam que, no caso de que se percebam possíveis falhas sobre um controle existente, possam comunicar às médias gerências, ou mesmo a alta administração, as causas subjacentes que o levaram a ser capaz de corrigir as fraquezas estruturais dos controles⁶⁷.

Esses meios de comunicação devem garantir a qualidade das informações em termos de integridade, confiabilidade, integridade, precisão e pertinência; a divulgação de informações pouco confiáveis ou equivocadas afeta a imagem da instituição e aumenta a possibilidade de materialização da corrupção⁶⁸. Assim, as instituições precisam desenvolver, administrar e testar seus sistemas de informação e traçar um plano de melhoria contínua para garantir a eficácia e a confiabilidade das informações que transmite, incluindo às informações ao público externo (cidadãos).

A operação dos sistemas de informação e comunicação deve basear-se em um plano cujas metas e objetivos estejam relacionados ao plano estratégico institucional, garantindo a existência de mecanismos para identificar as necessidades futuras de informação.

Além disso, como parte do processo de gestão da informação, a instituição deve controlar, analisar, avaliar e melhorar sua infraestrutura tecnológica, a fim de aumentar sua capacidade de resposta a seus usuários.

⁶⁶ ISSAI 5700, página 46, linhas 24 a 26.

⁶⁷ ISSAI 5700, página 48. Linhas 15 a 18.

⁶⁸ ISSAI 5700, página 47, linhas 11 a 16.

Idealmente, a instituição pode estabelecer mecanismos adequados para que os funcionários comuniquem informações de integridade pertinentes e relevantes a níveis hierárquicos superiores, sem depender de seu supervisor direto. Por sua vez, o dirigente chefe e a alta administração devem mostrar uma verdadeira vontade de ouvir (ISSAI 5700⁶⁹).

Para ajudar a garantir a qualidade das informações internas e relatórios, realizar as atividades de controle interno e tornar o monitoramento mais eficaz e eficiente, o sistema de controle interno e todas as atividades e eventos significativos devem ser documentados de forma completa e clara (por exemplo, com mapas de processos, fluxos de trabalho e manuais de procedimentos). A documentação do sistema de controle interno deve incluir a identificação das estruturas, políticas da organização, suas categorias operacionais e objetivos relacionados e os procedimentos de controle como reação à mitigação ao risco. Uma organização deve ter provas escritas dos componentes do processo de controle interno, incluindo seus objetivos e atividades de controle⁷⁰. Por isso, entende-se importante como boa prática que as instituições façam um plano de gerenciamento, um plano de integridade, ou ambos integrados.

Comunicação Externa

Segundo as recomendações da ISSAI 5700⁷¹, a fim de mitigar a possível corrupção de partes externas, é importante que as entidades estabeleçam comunicação efetiva com todas as entidades que possam ter impacto na integridade de suas atividades, programas, projetos, operações e outras atividades institucionais.

Portanto, as instituições podem implementar canais formais de comunicação com outras entidades públicas, fornecedores, contratados, consultores, cidadãos e outros grupos de interesse que possam contribuir para a qualidade e o desenho das funções, produtos e serviços oferecidos pela instituição.

⁶⁹ Página 48, linhas 26 a 29.

⁷⁰ ISSAI 9100, página 38.

⁷¹ Página 49.

Da mesma forma, é importante que a instituição garanta que todas as partes externas com as quais se comunica sejam informadas das regras éticas que regem as ações da entidade e transmitam a mensagem de que ações impróprias, como a apresentação de faturas imprecisas ou a tentativa de suborno, entre outros, será detectado e sancionado.

4.5. Atividade de monitoramento

O monitoramento do controle interno visa assegurar que os controles estejam operando conforme o esperado e que sejam modificados adequadamente para mudanças nas condições. O monitoramento também deve avaliar se, no cumprimento da missão da entidade, os objetivos gerais estabelecidos na definição de controle interno estão sendo alcançados. Isso é realizado por meio de atividades de monitoramento contínuas, avaliações pontuais ou uma combinação de ambos, a fim de ajudar a garantir que o controle interno continue a ser aplicado em todos os níveis e em toda a entidade. O monitoramento das atividades de controle interno deve ser claramente distinguido de revisar as operações de uma organização, que é uma atividade de controle interno (ISSAI 9100⁷², 2016).

As atividades de monitoramento incluem:

a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e nas probabilidades de risco, que podem requerer revisão dos tratamentos correntemente adotados e suas prioridades, e levar à identificação de riscos emergentes;

b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;

c) analisar eventos (incluindo os “quase incidentes de eventos”), mudanças, tendências, sucessos e fracassos e aprender com eles;

d) garantir que os controles sejam eficazes e eficientes no desenho e na operação (TCU-SEGESEX, 2017).

⁷² Página 41

e) Detectar controles que não estejam sendo uma resposta adequada aos riscos.

5. Auditoria – Resumo de procedimentos de avaliação do controle interno sob ótica da prevenção da corrupção

O presente capítulo condensa as questões a ser levantadas como possibilidade de roteiro de auditoria. As questões aqui descritas já foram de maneira geral expostas ao longo de todos os capítulos. Trata-se apenas de uma compilação, mas não dispensa a leitura dos respectivos itens para o entendimento da avaliação, a fim de se realizar as recomendações à unidade auditada de forma convincente.

O principal papel do controle externo é verificar qual é o grau de maturidade dos controles internos de organização⁷³ e propor recomendações, orientado a unidade auditada a práticas para um controle interno mais maduro, direcionado à gestão de riscos e à prevenção à corrupção. A figura à página seguinte ilustra os possíveis graus de maturidade:

⁷³ O termo grau de maturidade é utilizado comumente neste tipo de avaliação pelo controle externo de vários países: Vide Rechnunsghof (2016), página 25-26 (Reifegradmodelle); e TCU (2018).



Fonte: Rechnungshof (2016, página 30)

Um bom guia inicial para execução de auditoria a controles interno é dado pelo “Roteiro de Auditoria de Gestão de Riscos” (TCU-SEGESEX, 2017), a qual passe-se a citá-lo nesse momento diretamente em seu conteúdo. Contudo, há uma abordagem distinta no presente, pois diversos aspectos do papel da prevenção da corrupção em conjunto com o gerenciamento de riscos serão combinados em relação as possibilidades de avaliação e recomendações sobre a formação do controle interno.

Levantamento inicial de dados

A etapa inicial para este tipo de auditoria é buscar o entendimento à organização. Para tal, deve-se levantar informações das diversas fontes: legislação, mapas de processos, entrevistas com gestores, mas buscando-se obter um entendimento abrangente da organização e do seu ambiente, a fim de conhecer a entidade se organiza e funciona para otimizar o seu desempenho, assim como os fatores relevantes do ambiente no qual ela busca atingir. O objetivo principal dessa etapa é identificar o direcionamento estratégico da organização (missão, visão, valores fundamentais); os objetivos-chaves, estratégicos e de atividades.

A fase do entendimento da entidade tem o objetivo de: a) identificar quem deve ser entrevistado e o que deve ser questionado; b) priorizar as áreas que devem ter seus processos de gerenciamento de riscos examinados; c) definir a informação requerida ou a evidência que será buscada e a fonte de informação. d) determinar o instrumento de coleta de dados ou procedimento de auditoria mais adequado às circunstâncias (exemplo: entrevista ou questionário); e) programar a agenda com as partes envolvidas.

Este estudo preliminar é essencial para planejar a auditoria, dado que se trata de um tipo de auditoria operacional, e por isso, deve ser planejada. A razão se fundamento em dois aspectos: auditorias operacionais costumam-se ter maior duração de execução que comparadas às auditorias de legalidade; auditorias operacionais necessitam maior compreensão das atividades da organização como um todo, não se restringindo à análise de um só instrumento, como um só contrato.

A equipe pode iniciar obtendo um entendimento preliminar mediante inspeção de relatórios de gestão da organização, de levantamentos anteriormente realizados, de informações sobre a estrutura, as competências e operações disponibilizadas em páginas da Internet, de informações orçamentárias e financeiras publicadas ou obtidas no SOF.

A partir disso, pode-se planejar os procedimentos adicionais para aprofundar o entendimento da entidade. A razão de um bom planejamento deve ser considerada, visto otimizar a elaboração de uma agenda de entrevistas e um

cronograma para a aplicação dos demais procedimentos necessários para a conclusão dessa fase de obtenção de entendimento (TCU-SEGEX, 2017).

Neste quesito, são relevantes as seguintes informações para auxílio da familiarização com a entidade:

a) natureza jurídica e competências legais, quais são derivados os objetivos-chaves da organização;

b) missão e visão declaradas, em contraste com as competências legais anteriormente citadas;

c) estruturas organizacional, de governança e operacional;

d) fontes de receitas e execução orçamentária e financeira (aplicações de recursos definidos em programas, ações e projetos orçamentários constantes do Plano Plurianual (PPA) e da Lei Orçamentária Anual (LOA), e seus respectivos objetivos;

e) Plano ou mapa estratégico em vigor se houver, com a descrição das perspectivas e a enumeração das ações estratégicas dentro de cada área foco de atuação e ou perspectiva;

g) Planos e Programas de metas.

Um planejamento da execução da auditoria é importante, considerando que essas informações vão orientar a execução da auditoria e otimizar tempo de levantamento. O planejamento da auditoria deve conter as informações-chaves e a indicação dos temas e fatores mais importantes que, no julgamento profissional do dirigente e ou do supervisor da auditoria, são significativos para direcionar os esforços da equipe de trabalho, bem como onde e quem deverá ser entrevistado, ou quais informações devem ser levantadas.

Um plano de auditoria pode ser modificado ao longo do tempo, em razão do entendimento mais profundo da entidade, visto que a equipe vai adquirindo ao trabalhar melhor as informações para elaborar o planejamento. Neste caso, a

supervisão da auditoria deve ser notificada para atualizar a estratégia. Alguns elementos em um plano de auditoria devem ser considerados como:

- ✓ Determinar a duração das atividades de planejamento
- ✓ Aplicação dos procedimentos de coleta e análise de dados
- ✓ Tempo para de avaliação das evidências
- ✓ Elaboração de um relatório preliminar e final.

Embora não seja uma atividade rotineira do TCMSP, usualmente, em auditorias operacionais são incluídos comentários de gestores, enviando-se um relatório preliminar à unidade auditada, e posteriormente, o Relatório final já com os comentários da área auditada⁷⁴. Tal prática é comum ao TCU para auditorias operacionais. Contudo, recomenda-se levantar se tal prática será adotada ao TCMSP para este tipo de auditoria.

A partir deste plano inicial, seguem-se os pontos de verificação:

5.1. Avaliação do ambiente de controle, código de conduta e sistema de gerenciamento de riscos

Para lidar com riscos e aumentar a chance de alcançar objetivos, as organizações devem adotar abordagens de sistemas gestão de riscos. Em qualquer situação, é importante que a organização se apoie em modelos reconhecidos como os apresentados no capítulo 4, ou mesmo em outros

⁷⁴ ISSAI 300, pág 9: Os auditores devem comunicar às entidades auditadas os principais aspectos da auditoria, incluindo o objetivo, as questões e o objeto da auditoria. A comunicação geralmente será feita oficialmente, por meio escrito e, durante a auditoria, de forma regular. Os auditores devem se comunicar com as entidades auditadas durante todo o processo de auditoria, por meio de interações construtivas à medida que diferentes achados, argumentos e perspectivas são avaliados. As entidades auditadas devem ter a oportunidade de comentar os achados de auditoria, as conclusões e as recomendações antes que a EFS emita seu relatório de auditoria. Quaisquer discordâncias devem ser analisadas e os erros materiais corrigidos. A análise dos comentários deve ser registrada em papéis de trabalho de modo que as alterações no relatório preliminar de auditoria, ou as razões para não fazer alterações, fiquem documentadas.

existentes. Caso não haja um processo efetivo de gestão de riscos, a equipe de auditoria pode realizar recomendações visando implementá-lo⁷⁵.

Sobre a avaliação inicial do ambiente de controle, pode-se analisar as capacidades existentes na organização em termos de liderança, políticas, estratégias e de preparo das pessoas, incluindo aspectos relacionados à cultura da organização para que a gestão de riscos tenha as condições necessárias para prosperar e fornecer segurança razoável do cumprimento dos objetivos da entidade.

Os seguintes aspectos podem ser levados em consideração que visa analisar a cultura dentro de uma organização:

Aspetos de governança	Sim	Não	N.A	Descrição / OBS
A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos fornecendo normas, orientações e supervisionando a inclusão desses aspectos-chaves nos programas de apoio ao desenvolvimento de gestores?				
Há o reforço do comprometimento das lideranças com a cultura de gestão baseada em riscos?				
Estão instituídas políticas, programas e medidas definindo padrões de comportamento desejáveis, além dos códigos de ética e de conduta como: canais de comunicação para cima e de denúncia, ouvidoria, e avaliação da aderência à integridade e aos valores éticos?				
A alta administração está completa e diretamente envolvida em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade?				
Todo o pessoal na organização, inclusive prestadores de serviços e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de se levar a sério				

⁷⁵ Um guia para orientação inicial de implementação de programas de gerenciamento de risco pode ser encontrado no capítulo 6 do documento do TCU intitulado “Referencial básico de Gestão de Riscos”.

suas responsabilidades de gerenciamento riscos, bem como é orientado e sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes?				
Há meios de comunicação de amplo conhecimento dos funcionários que no caso de que se perceba possíveis falhas sobre um controle existente, possam comunicar às médias gerências, ou mesmo a alta administração, as causas subjacentes que o levaram a ser capaz de corrigir as fraquezas estruturais dos controles?				

Fonte: (TCU-SEGECEX, 2017 pág 67).

O código de ética e seu tratamento neste sentido possui alta relevância (item 3.1). A respeito do Código de Ética, recomenda-se à equipe de auditoria analisar como é dado o tratamento este Código de fato nas secretárias, autarquias e empresas públicas da PMSP tendo a planilha abaixo como guia exemplificativo⁷⁶, mas com a seguinte pergunta como norte principal: Qual é a relevância do Código de Ética na instituição?

Avaliação da aplicação do código de Conduta	Sim	Não	N.A	Descrição / OBS
A gestão é pro ativa no sentido de encorajar e apoiar procedimentos éticos e o cumprimento da legislação e do código de conduta em vigor?				
Há treinamentos/sensibilização periódicos a servidores sobre o código de conduta (anual, bianual, etc.) ou sobre valores éticos e de integridade?				
Há divulgação do código de ética na intranet? É mencionado com alguma frequência?				
Existe evidências sobre a valorização do código de ética?				
Há treinamento a novos servidores ingressantes a respeito do código?				
Ele é mencionado nos documentos internos?				

⁷⁶ Planilha elaborada a partir de perguntas mencionadas na ISSAI 5700, bem como nas planilhas de avaliação ao risco do Tribunal de Contas de Portugal de uso interno (não disponível ao público).

Os servidores/funccionários encontram-se de uma forma geral cientes das suas responsabilidades, dos limites de sua autoridade e das práticas da atividade do órgão/entidade como um todo?				
É dada importância ao código pela alta gerência/administração? A alta administração e os responsáveis pela governança reconhecem importância da cultura, integridade e valores éticos, e da consciência de riscos?				

Em referência da última pergunta da tabela acima, a fim de evidenciar a relevância do código de ética em um determinado órgão, sugere-se realizar a aplicação de um questionário a gestores e/ou funcionários para avaliar o nível de conhecimento deste código na prática.

Vale lembrar, contudo que o código de conduta não deve ser apenas uma mera regra normativa formal. É necessária conscientização e sensibilização dentro da instituição junto aos funcionários através de treinamentos (INTOSAI, 2016⁷⁷). A intenção dessa disseminação é melhorar ou alterar a cultura dentro de uma organização pública estabelecendo padrões de comportamentos esperados, e não somente prever punições em caso de infrações ao próprio código. Tal aspecto é o elo comportamental do sistema de prevenção da corrupção.

Além da disseminação do código de ética, uma unidade ou comitê específico pode ser estabelecido para assegurar que o código de ética seja utilizado adequadamente nos casos de infração, compondo o sistema de integridade da organização, e para impor eventuais punições à violação do código de ética, havendo como exemplos, unidades de correção, corregedoria ou Comitê de Ética⁷⁸.

Um outro ponto de verificação é analisar se a entidade possui um programa ou plano de integridade (Vide capítulo 4.1). Idealmente a entidade pode construir um

⁷⁷ Every public institution should disseminate the code of ethics as an integrated part of corruption prevention. ISSAI 5700, pág 29, linha 10 e 11.

⁷⁸ A ISSAI 5700, pág 29, linhas 25-27, recomenda no caso de um comitê que seja composto por representantes da alta gerência, divisão jurídica, divisão de auditor interno e uma parte independente.

plano/programa nesse sentido, contudo não existe obrigação legal de fazê-lo⁷⁹. Vale atentar que a construção de um plano de integridade pode ser sugerida⁸⁰ como boa prática à entidade, podendo-se recomendar o Manual para implementação de programas de integridade (CGU, 2007) como guia, devendo-se observar as devidas adaptações aos Regulamentos e Leis da PMSP.

Da mesma maneira, é desejável um plano de gerenciamento de riscos utilizando-se as metodologias reconhecidas como COSO (versão 2004, conhecida como COSO II, ou versões mais recentes) ou ISSO 3100 (2009), revelando-se um grau de maturidade maior com relação à modelagem do controle interno. Deve-se destacar que um plano de gerenciamento de riscos⁸¹ pode englobar um plano de integridade, ou seja, a entidade pode construí-los de forma conjunta e englobada, visto que existem vários pontos de tangência entre os dois. Um possível guia inicial de orientação que se pode recomendar à entidade é o documento denominado “10 passos para a boa gestão de riscos” (TCU, 2018 “c”).

Neste aspecto, a administração federal pode ser guia como referência de recomendação, considerando que a Instrução normativa conjunta do Ministério do

⁷⁹ Há de se mencionar que âmbito federal está em vigor o Decreto federal nº 9.023, de alcance à administração federal, e que determina a criação de programas de integridade, destacando-se:

Art. 19. Os órgãos e as entidades da administração direta, autárquica e fundacional instituirão programa de integridade, com o objetivo de promover a adoção de medidas e ações institucionais destinadas à prevenção, à detecção, à punição e à remediação de fraudes e atos de corrupção, estruturado nos seguintes eixos:

I - comprometimento e apoio da alta administração;

II - existência de unidade responsável pela implementação no órgão ou na entidade;

III - análise, avaliação e gestão dos riscos associados ao tema da integridade; e

IV - monitoramento contínuo dos atributos do programa de integridade.

Art. 20. O Ministério da Transparência e Controladoria-Geral da União, no prazo de cento e oitenta dias, contado da data de entrada em vigor deste Decreto, estabelecerá os procedimentos necessários à estruturação, à execução e ao monitoramento dos programas de integridade dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

⁸⁰ Deve-se notar que a adoção de um Plano de Integridade é discricionário à administração visto que não há obrigação legal e fazê-lo.

⁸¹ Documentos como “10 passos para a boa gestão de riscos” do TCU (<https://portal.tcu.gov.br/biblioteca-digital/10-passos-para-a-boa-gestao-de-riscos.htm>) e “Referencial básico de gestão de riscos” podem ser utilizados como referenciais (<https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>).

Planejamento/CGU Nº 1/2016 obrigação de implantação de sistema de controles com foco no gerenciamento de riscos⁸².

Avaliação e tratamento de riscos (Item 4.2)

A ciência da entidade sobre a prática de gerenciamento de riscos é essencial para um controle interno robusto. Para avaliação dos processos de identificação e análise de riscos, a equipe de auditoria deve verificar se a envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação consistente dos riscos, havendo as seguintes perguntas como guia (TCU-SEGESEX, 2017⁸³):

Política de gestão de riscos	Sim	Nã o	N. A	Descriçã o / OBS
A entidade tem ciência da prática de gestão de riscos ⁸⁴ ?				
Há na entidade um processo de identificação, análise de riscos, documentação e correspondente tratamento de riscos? Há atribuição de responsabilidades claras para mitigação e respostas a riscos?				
A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização? Há algum plano de gerenciamento de riscos?				
São envolvidas pessoas com conhecimento adequado, bem como os gestores das respectivas áreas para identificação e tratamento de riscos?				

⁸² O Art. 3º dessa Instrução estabelece que “os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público. Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo federal. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas. Assim, tendo em vista os objetivos estabelecidos pelos órgãos e entidades da administração pública, e os riscos decorrentes de eventos internos ou externos que possam obstaculizar o alcance desses objetivos, devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto sobre os objetivos organizacionais.”

⁸³ Página 76.

⁸⁴ Rechnungshof (2016), página 113.

São utilizadas técnicas e ferramentas adequadas aos objetivos e tipos de risco?				
O processo de identificação de riscos considera explicitamente a possibilidade de fraudes, burla de controles e risco de corrupção, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos?				
O processo de identificação de riscos produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto?				
Os riscos identificados são analisados em termos de probabilidade de ocorrência e de impacto nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos?				
Todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento ou mapeamento, bem como são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas?				
Os riscos identificados são analisados em termos de probabilidade de ocorrência e de impactos nos objetivos, como base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos?				

Caso não haja qualquer atividade de identificação dos riscos, deve-se recomendar à entidade que promova alguma política de identificação de riscos. Pode-se sugerir as metodologias disponíveis como ISO 31000 (2009) ou FERMA (2003). Sugere-se que a equipe de auditoria tenha familiaridade com esses modelos para ter uma referência robusta de como uma boa metodologia deve ser

aplicada, bem como de documentos exemplificativos de planos de gestão de risco na prática⁸⁵.

Sugere-se adicionalmente como um possível paradigma o Plano de Gestão de Riscos de Gestão⁸⁶ do Tribunal de Contas de Portugal, uma vez que este pode ser utilizado como exemplo de possibilidade de referência de gerenciamento de riscos por possuir um mapa de riscos em seus anexos do referido plano, bem como neste documento encontra-se a explicação da metodologia que foi aplicada.

Apoio ao controle interno (item 4.1.3)

Verificar se unidade auditada possui em sua declaração de missão, ou documentos recentes relacionados a metas e estratégias, podendo-se prever a criação de unidade de auditoria interna, unidade de revisão ou unidade de controle interno, ou caso existente, se efetivamente haja um suporte da alta administração e importância. Uma auditoria interna ao órgão, e diretamente vinculada à alta direção, poderia vir fortalecer o controle interno neste sentido⁸⁷. Os seguintes pontos podem ser verificados:

Os seguintes pontos podem ser verificados:

Aspetos relacionados com auditoria interna ou área específica de controle interno	Sim	Não	N.A	Descrição / OBS
A entidade dispõe de Gabinete de Auditoria Interna, unidade de controle interno, unidade de revisão ou unidade de controle de qualidade?				
A unidade acima está diretamente ligada ao órgão do dirigente máximo?				
No caso de existirem relatórios efetuados pelos órgãos de controle interno ou auditoria				

⁸⁵ Exemplos: <http://www.planejamento.gov.br/assuntos/patrimonio-da-uniao/programa-de-modernizacao/linha-do-tempo/arquivos-e-publicacoes/plano-de-gestao-de-riscos.pdf/view>
<https://www.policiajudiciaria.pt/wp-content/uploads/2012/01/p25419-1.pdf>

⁸⁶ Disponível em https://www.tcontas.pt/pt/plano_risco/despacho_34_2012_gp.pdf. Vide especialmente Anexos II e III, páginas 17 a 34 do referido documento.

⁸⁷ Neste sentido, a ISSAI 9100 (página 19) reflete que “Se a alta administração acredita que o controle interno é importante, os outros membros da organização perceberão isso e responderão respeitando conscientemente os controles estabelecidos. Por exemplo, a criação de uma unidade de auditoria interna como parte do sistema de controle interno é um sinal forte da administração de que o controle interno é importante.”

interna, existem reuniões e as situações detectadas são acompanhadas?				
A nível do controle interno, os pontos fracos detectados são corrigidos?				
Foram efetuadas ações de controle à entidade, nos últimos três anos?				
A administração, auditoria interna ou unidade de controle interno identificou algum tipo de risco de fraude ou suspeita de alguma fraude em curso?				

Observação sobre auditoria interna na PMSP:

Ressalta-se que a auditoria interna foi atribuída a Controladoria Geral do Município de São Paulo – CGM, conforme Artigo 118 e Artigo 119 da Lei 15.764. Considerando o papel da GCM, há que ser estudado se não há objeção legal de criação dentro de um órgão um gabinete de auditoria interna, uma vez que o Art. 113 da referida Lei prevê dentro da GCM a Coordenadoria de Auditoria Interna para “exercer as atividades de órgão central do Sistema de Auditorias do Poder Executivo Municipal”. Por outro lado, não há objeção na Lei, a princípio, para criação de um departamento interno ao órgão para auditoria interna descentralizada.

Neste sentido, a administração federal se encontra mais avançada em razão do Decreto federal nº 9.203/2017 bem como pela Instrução a Instrução Normativa Conjunta IN-MP/CGU nº 01/2016. Tais normativos poderia ser mencionado como sugestão de boa prática, observando-se, contudo, a reserva de discricionariedade do executivo. Recomenda-se à leitura dos estudos de caso no item 4.1.3 (página 46).

5.2. Avaliação do controle interno com orientação de boas práticas de prevenção da corrupção

Os seguintes pontos foram abordados ao longo do capítulo 3, sendo que apenas seguem-se exatamente as mesmas sugestões de possibilidade de abordagem, mas de maneira compilada.

Treinamentos (item 3.2.1)

As seguintes questões orientam a respeito de treinamentos:

- ✓ É realizado treinamentos do código de ética, ou mesmo sobre um programa ou plano de integridade na instituição?
- ✓ Com que frequência?
- ✓ Há alguma política de reciclagem ou educação continuada, de forma que mantenha um alto nível de conhecimento, atualização e produtividade da equipe da entidade?

Caso não haja treinamentos específicos, pode-se orientar à Origem criar um programa de treinamento voltado ao código de ética e valorização da integridade.

As seguintes práticas são orientadas à prevenção da corrupção, recomendando-se a equipe de auditoria orientar a entidade em relação à possibilidade de adoção destas, mas respeitando-se os limites de discricionariedade.

Rotação de funções (Item 3.2.2)

A avaliação da prática de rotação de funcionários pode ser orientada às seguintes perguntas. Vale atentar que embora tal medida seja discricionária, pode ser recomendada como boa prática:

Rotação de funções	Sim	Não	N.A	Descrição / OBS
A entidade tem alguma política em relação à rotação de trabalho?				
Se existir, como é implementada? Com qual frequência? A política de rotação é baseada em análise de risco?				
A política está sendo implementada? Se não, por quê?				
Quem toma decisões em relação à rotação de tarefas?				
Quem é elegível para a rotação de trabalho?				

Uma política de rotação existente é revisada? Com que frequência?				
Caso não exista política de rotação de funcionários: há áreas que a equipe de auditoria identifica e recomenda possibilidade de rotação?				

Fonte: ISSAI 5700, pág 34/35.

Atenta-se que para adotar uma política de rotatividade de trabalhos para reduzir o risco de corrupção dentro da organização, ideal é que a instituição faça uma avaliação completa do risco em cada uma das áreas que compõem aquela instituição, vezes que há áreas mais vulneráveis à corrupção e outras menos. Só então um sistema de controles internos relacionados à rotação de tarefas pode ser projetado para lidar com esses riscos específicos.

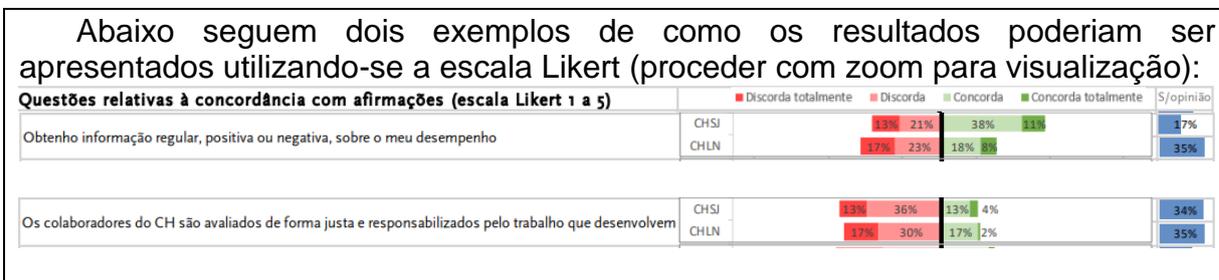
Política de promoção baseada em mérito (item 3.2.3)

Uma avaliação sobre se a organização segue um modelo de promoção baseado em mérito pode ser feita através de elaboração de questionários on-line junto a funcionários, questionando sobre a política da organização. Abaixo, segue um possível modelo:

Avaliação sobre ambiente e envolvimento de trabalho - Escala Likert de 1 a 5 -1 - Discordo Totalmente, 2 – Discordo, 3 - Nem Concordo nem Discordo, 4 – Concordo, 5 - Concordo Totalmente	Discorda totalmente/ Discorda	Concorda totalmente / Concorda	Sem opinião
Os funcionários do órgão são avaliados de forma justa e responsabilizados pelo trabalho que desenvolvem			
O órgão consegue atrair e reter os melhores profissionais			
Vejo o órgão como o local certo para desenvolver uma carreira de médio/longo prazo			
Estou satisfeito em ser funcionário do órgão			
As promoções para chefia são baseadas em mérito			
Os critérios para promoções são justos			
A minha remuneração é a adequada às minhas funções e responsabilidades			
Obtenho informação regular, positiva ou negativa, sobre o meu desempenho			

OBS – Utilizar escala Likert de 1 a 5 -1 - Discordo Totalmente, 2 – Discordo, 3 – Nem Concordo nem Discordo, 4 – Concordo, 5 - Concordo Totalmente.

Fontes: Planilha de Avaliação do Risco Global e Avaliação do Sistema de Controlo Interno Global do Tribunal de Contas de Portugal ⁸⁸;e Relatório de Auditoria às práticas de gestão no Centro Hospitalar Lisboa Norte, EPE, e no Centro Hospitalar de São João EPE⁸⁹.



Estrutura de gestão e integração organizacional (item 3.2.4)

Para uma análise da estrutura de gestão pode-se aplicar, como sugestão, o seguinte questionário on-line junto aos funcionários. Para tal, utiliza-se um questionário de graduação de notas sobre afirmações de um a cinco para cada questionamento (escala Likert). Posteriormente, nas questões onde há discordância com das afirmações, em etapa seguinte a equipe de auditoria poderia proceder a uma investigação mais a fundo para se extrair as causas de problemas, utilizando-se questionários de perguntas abertas aos funcionários ou gestores de nível intermediário, abrindo-se a possibilidade de a auditoria realizar recomendações aos gestores:

Avaliação sobre ambiente e envolvimento de trabalho	Discorda totalmente / Discorda	Concorda totalmente / Concorda	Sem opinião
A estratégia do órgão que trabalho, as suas políticas e os seus objetivos são comunicados com clareza aos funcionários			
A forma como os serviços e níveis hierárquicos do órgão estão organizados é adequada e contribui para o seu bom funcionamento			
Existe abertura da gestão de topo a propostas de mudança para melhorar o funcionamento do órgão			

⁸⁸ Planilhas coletas em âmbito de pesquisa. Sem publicação externa.

⁸⁹ https://www.tcontas.pt/pt/actos/rel_auditoria/2018/2s/rel012-2018-2s.pdf

É-me dado conhecimento adequado das mudanças ocorridas e em curso no órgão			
A comunicação entre os Serviços/ Áreas/ Direções é aberta e produtiva			
Existe boa comunicação e cooperação entre diferentes áreas			
Reconheço capacidade de liderança nos meus superiores na estrutura de gestão			
Reconheço competência e dedicação nos meus pares da estrutura de gestão			
O órgão/instituição tem os meios físicos e humanos adequados ao exercício da sua atividade, para poder corresponder aos objetivos definidos			
O Serviço/ Área/ Direção em que trabalho tem os meios físicos e humanos adequados ao exercício da sua atividade, para poder corresponder aos objetivos definidos			
Conheço os objetivos anuais definidos para o órgão em termos de atividade / produção			
Conheço os objetivos do Serviço/ Área/ Direção em que trabalho			
Participo na definição dos objetivos do Serviço/ Área/ Direção em que trabalho			
O meu papel no órgão, as minhas tarefas e as minhas responsabilidades estão claramente definidas e são do meu conhecimento			
Por vezes recebo ou tenho acesso a informação contraditória sobre o mesmo assunto (por exemplo, produção mensal, indicadores de qualidade, recursos humanos, consumos, etc)			
Tenho a autonomia adequada ao exercício das minhas funções			
Existe uma boa colaboração entre os dirigentes/ gestores/ administradores da área clínica e os da área de gestão			
Participo na tomada de decisões importantes que dizem respeito ao órgão como um todo			
Participo na tomada de decisões importantes que afetam ou dizem diretamente respeito ao Serviço/ Área/Direção em que trabalho			

O órgão tem-me proporcionado formação profissional adequada às minhas funções e responsabilidades			
A formação disponibilizada pelo órgão corresponde às necessidades dos funcionários do Serviço/ Área/ Direção em que trabalho			
Estou satisfeito em pertencer ao Serviço/ Área/ Direção em que trabalho			
O órgão é visto pelos cidadãos como a referência de qualidade no Serviço que presta			
O órgão presta um serviço de qualidade aos usuários na minha opinião dentro de suas possibilidades e limitações de recursos, independente de como os cidadãos percebam o serviço			
O órgão encontra-se num processo de melhoria contínua			

OBS – Utilizar escala Likert de 1 a 5 -1 - Discordo Totalmente, 2 – Discordo, 3 – Nem Concordo nem Discordo, 4 – Concordo, 5 - Concordo Totalmente.

Fontes: Planilha de Avaliação do Risco Global e Avaliação do Sistema de Controlo Interno Global do Tribunal de Contas de Portugal ⁹⁰;e Relatório de Auditoria às práticas de gestão no Centro Hospitalar Lisboa Norte, EPE, e no Centro Hospitalar de São João EPE⁹¹.

Princípio dos múltiplos olhos ou conferência cruzada (item 3.3)

Analisar se princípio da conferência (quatro olhos) é utilizado nas áreas vulneráveis ao risco. Caso não seja utilizado, sugerir à área auditada o uso dessa prática combinando com um devido mapeamento de riscos.

Deve-se atentar que em licitações, em âmbito de Análise de Editais ou acompanhamentos de Editais, pode-se observar as regras específicas da Lei 8.666/93 em que já está presente o princípio dos quatro olhos como uma obrigação legal a partir da formação de comissão de licitação (vide página 24).

Segregação de funções (item 3.4)

Inicialmente, deve-se verificar se a instituição tem uma política clara com relação à segregação de funções. Pode-se avaliar se sistema de controle interno

⁹⁰ Planilhas coletas em âmbito de pesquisa. Sem publicação externa.

⁹¹ https://www.tcontas.pt/pt/actos/rel_auditoria/2018/2s/rel012-2018-2s.pdf

prevê a segregação entre as funções de autorização, execução, atesto/aprovação, registro e revisão ou fiscalização, de modo que nenhuma pessoa possa ter completa autoridade sobre uma parcela significativa de qualquer atividade administrativa.

Quanto a segregação de funções obrigatória do Artigo 9º da Lei 8.666/93, pode-se verificar uma amostra aleatória de alguns processos administrativos de contratação, examinado especificamente este requisito do Art. 9º, mas sem realizar uma análise formal a cada, pois demandaria tempo em excesso.

Dependendo do tempo disponível para consecução da auditoria, a equipe pode buscar tarefas em que há riscos de manipulação por serem exercidas por mesma pessoa, através da análise de cada uma das atividades e serviços que a entidade audita realiza. Para isso, pode-se elaborar um mapa de processos para clarificar cada etapa e estágio das atividades de uma entidade, pois um mapa de processos (fluxo de trabalho), contendo os respectivos responsáveis em cada etapa do fluxo facilitar esclarecer se cada se está ocorrendo sobreposição indevida de funções.

Em outro ponto, deve-se atentar para política dos sistemas (softwares) e o nível de permissão dos usuários. Sugere-se analisar a política de senhas e permissão de autorização de uso na entidade e quem efetivamente as detêm, onde apenas as pessoas devidas devem ter acesso e permissão onde haja possibilidade de alteração, exclusão ou inclusão de registros.

Um estudo aprofundado das políticas de registro e permissão de dados visando detectar pontos de fragilidade que podem ser burlados pode ser realizado. Pode ser apropriado fazer um conjunto de testes em verificação dos registros a fim de se detectar eventuais pontos de fragilidade. Para tal, a equipe de auditoria necessita aprofundar-se dos meandros de como é estabelecido a política de segurança. Um corpo de prova de testes no local pode ser verificado. Contudo, o órgão auditado poderia, como boa prática, manter uma rotina de verificação permanente por alguém que seja responsável em fazer verificações de rotina com corpo de prova.

Supervisão adequada (item 3.5)

Além do princípio dos quatro olhos, uma supervisão adequada quantos às chefias com relação aos seus subordinados é essencial. Por vezes, as chefias são sobrecarregadas em muitos afazeres, e podem a ter pouco tempo disponível para supervisão. As seguintes perguntas orientam possíveis avaliações nestes aspectos, podendo ser levantadas por entrevistas:

- ✓ Há evidências que as chefias efetivamente conferem os trabalhos de seus subordinados?
- ✓ Como são estabelecidas as rotinas de conferências (caso existente)? Quais aspectos são de fato conferidos? Com que frequência e como as conferências ocorrem? Em cada uma das transações/tarefas concluídas?
- ✓ A relação supervisores/funcionários é adequada, de forma que possa haver tempo suficiente para supervisionar os trabalhos de seus subordinados?

Questões de avaliação geral sobre controles internos (item 3.6)

As seguintes questões⁹² supletivamente podem ser utilizadas pela equipe de auditoria para avaliação do controle interno. Deve-se observar que a equipe de auditoria há de avaliar quais questões serão respondidas, pois algumas necessitam de certo tempo de avaliação ou mesmo uso de questionários específicos para tal, e assim, as respostas dependerão do tempo de auditoria:

Aspetos relacionados com a Gestão e atividade da entidade	Sim	Não	N.A	Descrição / OBS
Existem funcionários cuja sarda teria um impacto negativo material sobre a entidade ou sobre as suas operações?				
São elaboradas periodicamente informações para apoio às decisões da gestão?				
Existem alterações frequentes e significativas nos administradores, gerentes e diretores, nos sistemas contabilísticos ou na natureza das				

⁹² Fonte : Planilhas elaboradas e utilizadas internamente pelo Tribunal de Contas de Portugal denominadas "Avaliação do sistema de contolo interno" e "Avaliação do risco global".

transações que tenham elevado o risco de ocorrerem erros ou omissões?				
Estão os serviços adequadamente dotados de pessoal em número e conhecimentos, de forma a desempenhar adequadamente as suas funções?				
Há frequentes alterações na(s) atividade(s) da entidade?				
Verificam-se com frequência mudanças da administração, incluindo a saída dos principais administradores?				
Existe uma estrutura hierárquica e uma adequada subdivisão de funções definida para a entidade?				
A entidade está inserida em um setor/Secretaria onde existe um forte peso ao nível das decisões políticas ou outras tomadas?				
A entidade está dependente de um reduzido n.º de fornecedores/empresas?				

As seguintes questões são relacionadas aos sistemas de Tecnologia de Informação – TI:

Aspetos relacionados com os sistemas de informação – TI	Sim	Não	N.A	Descrição / OBS
Foram introduzidos novos sistemas de informação com significância para o trabalho de auditoria ou os existentes sofreram modificações?				
Há atividades que existem oportunidades de automação?				
Quais os sistemas de informação de que a entidade dispõe? Existe articulação entre os vários sistemas de informação?				
O tipo de software utilizado apresenta-se adequado face às necessidades da entidade e providencia outputs de forma prática com informação relevante, em um formato adequado e para cada área significativa da entidade?				
Encontram-se previstas adequadas políticas e procedimentos de segurança por forma a evitar acessos não autorizados a equipamentos informáticos, software ou outras informações armazenadas nos sistemas de informação?				
Existe evidência de ter existido alguma ruptura ou falha nos sistemas de informação durante o período em análise?				

6. Referência bibliográfica

ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO 31000: **Gestão de Riscos: Princípios e diretrizes**. Rio de Janeiro, 2009.

BUNDESRECHNUNGSHOF (2017) - Tribunal de Contas federal da Alemanha. Modell eines Risikomanagements für die Bundesverwaltung. Bonn, Alemanha. Disponível no [link](#).

CGU (2017) – Controladoria Geral da União. **Manual para implementação de programas de integridade**. Brasília. Disponível em http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manual_profip.pdf

COSO ERM (2013) -Committee of Sponsoring Organizations of The Treadway Commission. **Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura**. Tradução: PriceWaterhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2007. <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>

FERMA (2003) - FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS. **Normas de Gestão de Risco**. Bruxelas, Bélgica. Disponível em http://www.ifc-camboriu.edu.br/~nildo/si/Normas_GR.pdf

INTOSAI (2016) – International Organization of Superior Audit Institutions. **ISSAI 5700 – Guideline for the Audit of Corruption Prevention**. Bonn, Alemanha. Disponível para download em inglês, alemão, francês e árabe em: http://www.issai.org/en_us/site-issai/issai-framework/4-auditing-guidelines.htm..

INTOSAI (2004) – International Organization of Superior Audit Institutions. **INTOSAI GOV 9100 - Guidelines for Internal Control Standards for the Public Sector**. Viena, Áustria. Disponível para download (fazer busca dentro da página) em inglês, alemão, francês e árabe:

http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm.

MAIA (2015), Maia, Antonio João Marques. **Corrupção, Fatores Organizacionais: Explicativos da Corrupção**. Lisboa.

ONU (2004) – Organização das Nações Unidas. **Convenção das Nações Unidas Contra Corrupção**. Vienna, Áustria. Disponível (português) em:

https://www.unodc.org/documents/lpo-brazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf .

Original (inglês) em:

http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

RECHNUNGSHOF (2016) – Tribunal de Contas da Áustria. **Leitfaden zur Überprüfung von Internen Kontrollsystemen**. Viena. Disponível em:

https://www.rechnungshof.gv.at/fileadmin/downloads/_jahre/2016/beratung/verwaltungsreform/Positionen_2016_03.pdf

TCP-Tribunal de Contas de Portugal (2012). **Plano de Prevenção de Riscos de Gestão (incluindo os riscos de corrupção e infrações conexas) da Direcção-Geral do Tribunal de Contas**. Lisboa, Portugal. Disponível em https://www.tcontas.pt/pt/plano_risco/despacho_34_2012_gp.pdf

TCU-SEGECEX (2017). **Roteiro de Auditoria de Gestão de Riscos**. Portaria SEGECEX nº 9 de 18.95.2017. Brasília. Disponível em <http://portal.utfpr.edu.br/transparencia/auditoria/legislacao-e-normas/portaria-09-2017-segecex>

TCU (2018). **Gestão de Riscos: Avaliação de Maturidade**. Brasília. <https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm>

TCU (2018, “b”). **Referencial básico de Gestão de Riscos**. Brasília. <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>

TCU (2018, “c”). **10 passos para a boa gestão de riscos**. Brasília. Disponível em <https://portal.tcu.gov.br/biblioteca-digital/10-passos-para-a-boa-gestao-de-riscos.htm>.

7. ANEXO I - Exemplo de Mapa de Riscos

Exemplo de um mapa de riscos preenchido a partir do Plano de prevenção de riscos do Tribunal de Contas de Portugal

ANEXO III - QUADRO 1 - Plano de Prevenção de Riscos de Gestão incluindo os riscos de corrupção e infrações conexas comum aos Departamentos e Serviços da DGTC – Sede e Secções Regionais					
Atividade/Perfil funcional	Identificação dos Riscos	PO	GC	GR	Medidas de Prevenção
Exercício ético e profissional das funções	Risco de quebra dos deveres funcionais e valores, tais como a independência, integridade, responsabilidade, transparência, objetividade, imparcialidade e confidencialidade (RT01)	1	3	2	Acompanhamento e supervisão pelos dirigentes do rigoroso cumprimento dos princípios e normas éticas inerentes às funções Observância de orientações e mecanismos que garantam a prevenção e o cumprimento dos princípios e valores éticos Observância de medidas conducentes a prevenir a quebra de sigilo, designadamente quanto aos mecanismos de acesso e acompanhamento restrito dos processos, nas suas diferentes fases Declaração ética sobre conflito de interesses e impedimentos Preferência da colegialidade na realização das acções, com especial relevância nas de controlo Acompanhamento e supervisão dos técnicos e equipas de trabalho pelos dirigentes Rotatividade adequada do pessoal
Controlo de qualidade	Risco de falha do controlo de qualidade dos procedimentos e produtos (RT02)	2	2	2	Supervisão e revisão dos procedimentos adoptados e dos produtos elaborados Adopção e difusão das melhores práticas e conhecimentos Segregação de funções
Competências técnicas	Risco de inadequação do perfil técnico e comportamental ao exercício das funções (RT03)	1	3	2	Partilha de conhecimentos, experiências e informação técnica Adequação das necessidades formativas ao perfil exigido Motivação individual e dos grupos de trabalho Mecanismos de aferição externa dos comportamentos no exercício das funções
Atendimento e relacionamento com terceiros	Risco de prestação de informação inadequada (RT04)	2	2	2	Definição de níveis de responsabilidade

Escala de Risco:
 Probabilidade da Ocorrência (PO) e Gravidade da Consequência (GC): 1 – Baixo; 2 – Médio; 3 – Alto
 Graduação do Risco (GR): 1 – Fraco; 2 – Moderado; 3 – Elevado

8. ANEXO II – Lista exemplificativa de possíveis riscos do Tribunal de Contas Federal da Alemanha

O documento do Tribunal de Contas Federal da Alemanha intitulado “*Modell eines Risikomanagements für die Bundesverwaltung*” descreve algumas possibilidades de risco em seu conteúdo, agrupados por categorias. Cabe sempre ressaltar que estes riscos devem ser levados em conta a realidade alemã, vez que teremos riscos distintos dado a realidade administrativa-legal brasileira. Os riscos são agrupados por tipos:

1. Finanças
2. Funcionamento geral e capacidade de agir
3. Estratégia
4. Capacidade operativa
5. Eficiência da administração
6. Mecanismos de controle
7. Pessoal
8. Adesão às normas legais
9. Integridade e reputação

1 - Riscos Associados à administração financeira e orçamento

O ponto de partida para este grupo de risco é o orçamento. Um foco principal está nos recursos monetários que uma entidade precisa para executar suas tarefas.

Financiamento insuficiente (fase de preparação do orçamento)

O projeto de orçamento pode ser incompleto e não reflete as necessidades reais de recursos do órgão. Razões podem, por exemplo avaliação de necessidades incompletas, erros de julgamento, falta de consciência de risco ou simplesmente erros de cálculo.

Gestão Financeira Inadequada	A gestão de fundos viola os regulamentos relevantes, por ex. por desperdício ou má orientação de fundos. Como consequência, mesmo que o orçamento seja calculado corretamente, a dotação não cobre as necessidades de recursos durante o período orçamentário. Dependendo da extensão da violação legal, os riscos de reputação também podem surgir.
Contabilidade incorreta	A entidade pode não conseguir comprovar devidamente a utilização de recursos financeiros disponibilizados para o efeito se contrapondo com as devidas notas de comprovação da despesa. Os riscos de reputação também podem ser percebidos aqui.
Recursos insuficientes como resultado de erros operacionais	A qualidade das decisões depende de como as autoridades preparam as informações relevantes com antecedência. Nesse contexto, é particularmente importante apresentar possibilidades alternativas de ação e suas consequências. As deficiências na fase de planejamento influenciam diretamente a qualidade das decisões durante a implementação. Decisões errôneas operacionais representam um risco para o desempenho direto das atividades e podem contribuir para a má orientação dos recursos.
Alocação inadequada de recursos como resultado de decisões fora da entidade	A estrutura sob a qual a entidade executa suas atividades pode mudar como resultado de decisões além de seu controle. Isso pode tornar obsoleta a base de planejamento do trabalho operacional. Em determinadas circunstâncias, os recursos necessários para concluir a tarefa sob as condições alteradas são insuficientes.

2 – Riscos gerais de funcionamento

Evento externo prejudicial: danos provocados pela natureza, fogo, inundação, etc.	Aborda os riscos sob a forma "clássicas" que podem incluir ferimentos materiais ou pessoais.
Evento externo prejudicial: ação de sabotagem (traição para casos de segurança nacional, fraude, etc.), parada por greves, etc.	O risco surge de uma ação não conforme por indivíduos ou organizações em benefício próprio ou especificamente em detrimento da autoridade e / ou do público em geral.

Falha ou interrupção de TI

A ação administrativa no século XXI depende quase inteiramente do funcionamento da TI. Interrupções técnicas de TI ou sua manipulação deliberada, portanto, representam um alto risco para a atribuição de tarefas às autoridades.

3 - Estratégia

A estratégia dá uma ideia para onde a organização deve ir. Mostra como uma agência ou unidades organizacionais individuais planejam atingir suas metas de longo prazo.

O planejamento estratégico se concentra em aspectos relevantes para a prestação de serviços a longo prazo, cumprimento de tarefas e realização de metas. Fornece o enquadramento para as atividades operacionais da Entidade.

Déficits nos processos decisórios estratégicos

A estratégia define o caminho que uma autoridade deseja seguir para atingir seus objetivos de longo prazo. Déficits nos processos de tomada de decisões estratégicas podem resultar em objetivos incompletos ou inadequados. A má orientação de recursos ou o comprometimento da implementação da estratégia podem ser o resultado.

Má implementação da estratégia escolhida

Uma organização deve derivar seus objetivos operacionais da estratégia. Atingir as metas dará uma contribuição significativa para o alcance da estratégia. Os objetivos são, portanto, o elo real entre planejamento e controle estratégico e operacional. Quando objetivos imprecisos ou inadequados são formulados, existe o risco de que os recursos sejam mal direcionados e / ou a estratégia não seja realizada conforme o planejado.

4 – Risco Operativo de execução de tarefas

Riscos nos procedimentos administrativos	<p>A execução dos serviços pode ser inadequado ou insuficiente. Isso também pode gerar riscos à adesão legal e eficiência da ação administrativa do órgão.</p> <p>As causas podem ser que de outros riscos pré-existentes estão acontecendo, por ex. Estruturas organizacionais inadequadas, recursos insuficientes, pessoal insuficientemente qualificado ou corrupção. Procedimentos administrativos incompletos ou incorretamente descritos aumentam o potencial de risco.</p>
Risco de projeto	<p>Uma característica essencial de um projeto é o tempo necessário, com um início e um fim definidos da tarefa. Um projeto geralmente é único, novo ou complexo, o que o diferencia do trabalho administrativo "normal".</p> <p>Uma abordagem insuficientemente estruturada para o trabalho do projeto compromete o sucesso do projeto, por exemplo, se uma definição de projeto vinculante ou regras claras do projeto estiverem faltando. Um risco de projeto também pode acumular se o foco é exclusivamente nos resultados, mas compromissos, custos, recursos e qualidade como fatores de sucesso são negligenciados. O mesmo se aplica aos déficits no planejamento e controle de projetos.</p>

5 – Eficiência Administrativa

Fase de planejamento: Avaliação econômica inexistente ou inadequada	<p>Estudos de eficiência devem apontar a necessidade de medidas financeiramente eficazes logo na fase de planejamento e sistematicamente esclarecer se</p> <ol style="list-style-type: none"> 1) a meta estabelecida pode ser alcançada com a medida planejada, 2) se os recursos necessários são possíveis em relação aos resultados esperados e 3) o uso de recursos é o mais baixo possível. <p>Sem essas investigações ex ante, as autoridades públicas não podem reconhecer os riscos econômicos. Estudos econômicos já devem incluir declarações sobre os objetivos da ação, bem como os critérios e procedimentos para monitorar o sucesso na fase de planejamento (veja abaixo).</p>
--	---

<p>Fase de Implementação: Acompanhamento insuficiente ou inexistente da execução</p>	<p>No caso de ações que se estendam por mais de dois anos, e em outros casos apropriados, as verificações de desempenho que as acompanham devem ser realizadas de acordo com os cronogramas individualmente ou em momentos em que há realizações parciais de uma atividade. As ações permanentes destinam-se a ser usadas pelas autoridades públicas para fornecer análises de desempenho nos momentos em que esperam resultados definitivos ou realizações parciais. Com os resultados das análises de desempenho, as autoridades podem decidir se continuam, corrigem ou encerram uma ação</p>
<p>Depois da ação: Avaliação final insuficiente ou inexistente do sucesso</p>	<p>I. Controle de realização de metas O controle de metas determina o grau de realização do objetivo no momento de sua verificação final. Isso é feito com base em uma comparação de destino real. Para este propósito, os objetivos (sub) originalmente planejados são comparados com a assimilação real atingida. O estado real da medida implementada resulta de uma representação atual das quantidades de concreto, tempos, prazos, condições de estrutura, etc. Em uma etapa subsequente, ela é comparada com a sua realização final.</p> <p>Ao mesmo tempo, o controle de metas de metas constitui o ponto de partida para considerações sobre se as metas definidas ainda são válidas. Se as metas definidas na fase de planejamento da análise de rentabilidade tiverem mudado, isso deve ser levado em conta em todas as decisões futuras para as quais o controle de sucesso deve formar a base.</p> <p>Se o controle da realização do alvo falhar, a autoridade diminuirá sua chance, se necessário, de terminar a ação atualmente antieconômica ou de impedir uma ação não eficiente no futuro por meio de efeitos de aprendizagem.</p>

	<p>II Controle de impacto Por meio de avaliação de impacto, é determinado se a ação foi adequada para a realização dos objetivos. Assim, a conexão causal entre a ação e a realização do objetivo é avaliada. Todos os efeitos pretendidos e não intencionais devem ser determinados de forma adequada. Isso também inclui os riscos que se concretizaram, independentemente de terem sido levados em consideração na fase de planejamento. Se resultar da avaliação de impacto que a ação alternativa adotada foi inadequada para alcançar o objetivo principal.</p>
	<p>III. controle de eficácia O controle de eficácia permite que as autoridades determinem: 1) se a implementação da ação foi econômica em termos de consumo de recursos (economia de execução) 2) se a ação era globalmente eficiente em termos de objetivos globais (efetividade) No caso da economia de execução, é examinado se a ação poderia ser implementada com o consumo de recursos previsto na fase de planejamento. Ao examinar a efetividade, as autoridades devem fazer um esforço razoável para determinar se a ação é eficiente em geral. Para fazer isso, eles devem considerar todos os efeitos monetários e não monetários positivos e negativos da medida e defini-los em relação uns aos outros.</p>

6 – Mecanismos de controle

A administração é, em última instância, responsável pelo trabalho adequado e eficiente de sua autoridade. Portanto, tem um interesse próprio para garantir isso com controles apropriados. Se a estrutura e / ou conteúdo desses controles não forem adequados para neutralizar adequadamente os riscos existentes, a atividade da entidade poderá ser prejudicada. Os déficits de controle se tornam um risco. Eles são muitas vezes a causa de maiores riscos em outras etapas.

7 – Pessoal

Os riscos relacionados ao pessoal de uma Instituição podem surgir do gerenciamento de recursos humanos, por exemplo, procedimentos de recrutamento, suporte de pessoal ou hierarquia vertical acentuada de trabalho. Além disso, deve ser considerado os riscos inerentes a indivíduos individuais, como exemplos, Idade, saúde ou satisfação no trabalho.

Existem correlações entre os vários riscos de pessoal, bem como entre estas e outras áreas de risco.

<p>Cultura da liderança</p>	<p>Entende-se a cultura de liderança predominantemente como um aspecto no nível da psicologia. Trata-se de conciliar objetivos estratégicos e operacionais, autoimagem e cultura interna, recursos, etc., dentro de uma organização, promovendo assim o sucesso da organização. Com relação à equipe gerencial, suas habilidades de liderança também são abordadas. Por exemplo, se as demandas dos funcionários e realidade diferem claramente, se as metas não são consistentes com a visão ou conflitantes entre si, ou se o pessoal da administração perde as habilidades de liderança necessárias para lidar corretamente com sua equipe, há riscos em boa conclusão das tarefas. Dano de reputação, alta rotatividade de pessoal ou lealdade decrescente são alguns dos possíveis riscos consequentes.</p>
<p>Ambiente de trabalho</p>	<p>O termo "ambiente de trabalho" deve ser considerado no cotidiano das autoridades com os funcionários. O foco é particularmente em aspectos como interação e comunicação. O clima de trabalho afeta a satisfação profissional, bem como no desempenho e motivação dos funcionários.</p>
<p>Igualdade, participação, discriminação.</p>	<p>Os requisitos legais em matéria de igualdade, participação e antidiscriminação devem ser observados. Violações podem levar a maiores riscos para o ambiente de trabalho, recrutamento, reputação e assim por diante. Os riscos do processo também podem crescer. Violações a estas regras podem ser uma indicação de fraqueza na cultura de liderança.</p>
<p>Vagas não preenchidas</p>	<p>A execução do serviço é prejudicada, porque o poder público tem vagas e postos suficientes, mas estes não são ocupados de forma significativa.</p>

Ocupação difícil de vagas, falta de atratividade, falta de mercado e / ou fatores negativos de localização	Este risco é devido à dificuldade de preencher vagas. Portanto, precede outros riscos decorrentes das consequências de cargos vagos. Os fatores que influenciam este risco são fora do controle da autoridade (localização geográfica, concorrência com outros setores, mão-de-obra qualificada não existente, etc.).
Alta rotatividade	A alta rotatividade na força de trabalho representa riscos para a conclusão da tarefa, por exemplo, os automatismos do processo são prejudicados ou o conhecimento especializado e a experiência podem ser perdidos. Pode ser o resultado de outros riscos já realizados, por ex. de um mau ambiente de trabalho, condições de trabalho desfavoráveis ou falta de atratividade salarial.
Déficit qualitativo	Se os funcionários de uma entidade não tiverem as qualificações profissionais exigidas para as tarefas que lhes são confiadas, isso terá um impacto negativo na atribuição de tarefas, pelo menos a médio prazo. Por exemplo, uma alta rotatividade de pessoal ou dificuldade no recrutamento de pessoal pode aumentar o risco de deficiências de qualidade entre os funcionários.

8 - Regularidade da execução das atividades

Uma execução imprópria, isto é, se as disposições legais não são observadas, pode-se desencadear riscos consecutivos. Lidar com riscos de observação às normas legais regularidade da atividade é, portanto, também preventivo e tem um caráter de sinalização.

Tais riscos geralmente são chamados de "riscos de sanduíche". Eles são precedidos por riscos que já aconteceram, e os riscos consequentes se seguem destes.

Base legal dos procedimentos administrativos	Os procedimentos administrativos precisam ser modulados de forma que suportem a conclusão adequada das tarefas. Deve-se minimizar o risco de ação imprópria. Em nenhuma circunstância devem fornecer "atalhos" que favoreçam violações legais.
---	--

Conformidade com os regulamentos legais ou requisitos regulamentares	O cumprimento das disposições legais ou dos requisitos regulamentares deve ser uma questão óbvia para uma autoridade - e na grande maioria dos casos isso será. No entanto, a administração das autoridades deve sempre considerar a ocorrência de violações das regras e sua capacidade de se armar adequadamente.
---	---

9 – Integridade e reputação

Os riscos para a integridade e reputação de uma entidade são predominantemente riscos consequentes. A maioria deles é precedida por falhas ou eventos danosos, cujas causas devem ser tomadas em outros lugares da avaliação de risco. Danos à integridade e reputação podem, no entanto, desenvolver uma tendência de auto reforço, que se dissocia das causas reais. Portanto, eles também devem ser tratados como um risco separado.

Ações legais / irregulares durante a execução de tarefas	A administração é vinculada por lei. Sua tarefa deve, portanto, ser legalmente compatível. Condutas ilegais ou irregulares acumulam-se às expectativas da população, bem como dos empregados. Pode prejudicar seriamente a confiança na integridade de uma autoridade, especialmente se as violações não forem "acidentais".
Interesse de conflitos de dirigentes	Mesmo a aparência de que a ação regulatória não é direcionada à finalidade pública, mas possivelmente aos interesses dos particulares de indivíduos na autoridade, pode comprometer a integridade e a reputação.
Comportamento de má-fé ou comportamento corrupto de funcionários	Independentemente ou além do dano material, os riscos para a integridade e a reputação de um órgão público se desenvolvem a partir de casos de fraude e corrupção. As deficiências frequentemente vão muito além do caso individual relevante, porque são contrárias a uma expectativa central das tarefas desempenhadas pela autoridade: o estado de direito e a lei. Para piorar a situação, a percepção pública muitas vezes não diferencia mais as falhas dos funcionários e das autoridades.

<p>Desinformação direcionada</p>	<p>Notícias falsas direcionadas e deliberadamente divulgadas ("notícias falsas", "embuste") são um fenômeno que tem sido percebido cada vez mais no passado recente. Muitas vezes, eles são lançados via mídia eletrônica e, portanto, se espalham muito rapidamente. Ao contrário dos outros riscos reputacionais, eles não são baseados em um comportamento (errado) da autoridade</p>
<p>Falta de proximidade com os cidadãos e / ou orientação para o serviço, comunicação inadequada</p>	<p>Os riscos também podem surgir de ações não transparentes, burocracia excessiva, infraestrutura inadequada para entrar em contato com as autoridades devidas. A longo prazo, uma entidade corre o risco de arriscar seus benefícios a sociedade- e, portanto, sua própria existência. Pode também perder os defensores necessários, por exemplo em questões orçamentárias.</p>