

TRIBUNAL DE CONTAS DA UNIÃO

REFERENCIAL DE COMBATE A FRAUDE E CORRUPÇÃO

Aplicável a Órgãos e Entidades da Administração Pública



República Federativa do Brasil

Tribunal de Contas da União

MINISTROS

Raimundo Carreiro (Presidente)
José Múcio Monteiro (Vice-Presidente)
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz
Ana Arraes
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Paulo Soares Bugarin (Procurador-Geral)
Lucas Rocha Furtado (Subprocurador-Geral)
Cristina Machado da Costa e Silva (Subprocuradora-Geral)
Marinus Eduardo De Vries Marsico (Procurador)
Júlio Marcelo de Oliveira (Procurador)
Sérgio Ricardo Costa Caribé (Procurador)
Rodrigo Medeiros de Lima (Procurador)

TRIBUNAL DE CONTAS DA UNIÃO

REFERENCIAL DE COMBATE A FRAUDE E CORRUPÇÃO

Aplicável a Órgãos e Entidades da Administração Pública

Brasília, 2017

© Copyright 2017, Tribunal de Contas da União.
Impresso no Brasil / Printed in Brazil

<www.tcu.gov.br>

Permite-se a reprodução desta publicação,
em parte ou no todo, sem alteração do conteúdo,
desde que citada a fonte e sem fins comerciais.

Brasil. Tribunal de Contas da União.

Referencial de combate a fraude e corrupção : aplicável a órgãos e entidades da Administração Pública / Tribunal de Contas da União. – Brasília : TCU, Coordenação-Geral de Controle Externo dos Serviços Essenciais ao Estado e das Regiões Sul e Centro-Oeste (Coestado), Secretaria de Métodos e Suporte ao Controle Externo (Semec), 2017.
132 p.

1. Corrupção - Brasil. 2. Crime contra a administração pública. 3. Abuso de poder. 4. Fraude. 5. Administração pública. I. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

APRESENTAÇÃO

O Brasil enfrenta uma série de desafios para combater a fraude e corrupção nas organizações públicas. O Tribunal de Contas da União (TCU) está atento a essa conjuntura em sua missão de "aprimorar a Administração Pública em benefício da sociedade por meio do controle externo". Isso se dá principalmente com a realização de fiscalizações.

Ciente de suas responsabilidades, e com o objetivo de cooperar para o contínuo e sistemático combate a corrupção, a Corte de Contas apresenta este referencial, como forma de aumentar a efetividade de suas ações em relação a esse desvio de conduta humana que devasta a gestão governamental e consome os resultados e os benefícios que deveriam ser dirigidos à sociedade.

As atuações dos tribunais de contas e das controladorias, no âmbito administrativo, e dos ministérios públicos e das polícias judiciárias, na esfera criminal, dão grandes resultados no combate a fraude e corrupção. Contudo, a moderna teoria de Linhas de Defesas aponta o administrador público como o principal agente nesse combate. Os gestores de uma organização, em conjunto com os servidores, empregados e terceirizados, compõem a linha de frente na defesa do patrimônio público, especialmente porque vivem o dia a dia das operações da organização. Logo, estão na melhor posição para perceber e identificar desvios e aplicar as correções necessárias.

Como contribuição nesse processo, a publicação traz sugestões que, se implantadas na organização, ajudam a preservar o interesse e o patrimônio público. Tais propostas são baseadas tanto no ordenamento jurídico nacional como em boas práticas adotadas internacionalmente.

As ações ora prescritas aplicam-se às organizações dos poderes Executivo, Legislativo e Judiciário, nas esferas federais, estaduais e municipais. Assim, qualquer instituição com alguma atuação pública pode se beneficiar das soluções descritas neste referencial.

Este trabalho se junta a outros três, quais sejam, Referencial Básico de Governança, Referencial para Avaliação de Governança em Políticas Públicas e Referencial para Avaliação da Governança do Centro de Governo, que integram o esforço de aperfeiçoar a Administração Pública em benefício da sociedade.

Referidas publicações são mostras do presente e do futuro do que já começamos concretamente a fazer, além de outras iniciativas de combate a fraude e corrupção, como a construção dos painéis de informações que possibilitam, no âmbito interno, o acompanhamento da gestão do Tribunal e, no externo, a verificação das políticas públicas; o desenvolvimento do e-TCE; e a execução de auditorias preditivas e contínuas, sempre a procura de novas formas de realizar os trabalhos, na busca por melhores resultados.

Aroldo Cedraz de Oliveira
Presidente do Tribunal de Contas da União

SUMÁRIO

1.INTRODUÇÃO ____ 7

1.1. Objetivo do referencial ____ 7
1.2. Público-alvo do referencial ____ 10
1.3. Conceitos fundamentais ____ 10
1.4. Gestão de risco ____ 18
1.5. Avaliação do custo-benefício no combate a fraude e corrupção ____ 23
1.6. Dos mecanismos de combate a fraude e corrupção ____ 26

2.PREVENÇÃO ____ 27

P1 – Gestão da ética e integridade ____ 29
P2 – Controles preventivos ____ 38
P3 – Transparência e ***accountability*** ____ 51

3.DETECÇÃO ____ 55

D1 – Controles detectivos ____ 56
D2 – Canal de denúncias ____ 59
D3 – Auditoria interna ____ 63

4.INVESTIGAÇÃO ____ 68

I1 – Pré-investigação ____ 70
I2 – Execução da investigação ____ 74
I3 – Pós-investigação ____ 80

5.CORREÇÃO ____ 81

C1 – Ilícitos éticos ____ 82
C2 – Ilícitos administrativos ____ 83
C3 – Ilícitos civis ____ 89
C4 – Ilícitos penais ____ 90

6. MONITORAMENTO ____ 93

M1 – Monitoramento contínuo ____ 93
M2 – Monitoramento geral ____ 94

7.REFERÊNCIAS BIBLIOGRÁFICAS _____ **97**

8.ANEXOS _____ **102**

Anexo 1 – Relação entre Coso e gestão de risco de fraude _____ 102
Anexo 2 – Exemplo de matriz para avaliação do recebimento de presentes _____ 103
Anexo 3 – Exemplo de questionamentos quanto ao plano de combate a fraude e corrupção _____ 106
Anexo 4 – Exemplo de matriz de avaliação da política anticorrupção _____ 108
Anexo 5 – Exemplo de plano de combate a fraude e corrupção _____ 110
Anexo 6 – Exemplo de matriz de responsabilidade _____ 112
Anexo 7 – Exemplo de fluxograma para tratamento de fraudes e corrupções _____ 114
Anexo 8 – Exemplo de avaliação de risco de fraude e corrupção _____ 115
Anexo 9 – Exemplo de análise de risco de corrupção _____ 116
Anexo 10 – Processo de avaliação de risco de fraude pela norma AS 8001-2008: Fraud and corruption control _____ 118
Anexo 11 – Exemplo de matriz para avaliação de treinamento anticorrupção _____ 125
Anexo 12 – Quesitos para avaliação do comprometimento da organização no combate a fraude e corrupção _____ 128
Anexo 13 – Exemplos de indicadores de fraude ***(red flags)*** _____ 130

1. INTRODUÇÃO

1.1. Objetivo do referencial

No ano VI a.C, o estadista ateniense Sólon da Grécia, estava disposto a perdoar todas as dívidas das pessoas com entes públicos e privados. O nobre propósito era evitar que elas se tornassem escravas caso não honrassem a dívida, como costume da época. No entanto, antes de aprovar a lei, contou a amigos, que, se aproveitando da informação privilegiada, pegaram grandes empréstimos e compraram terras. Após a lei perdoando as dívidas, seus amigos enriqueceram.

O relato acima mostra que a corrupção é uma antiga prática que existe desde os primórdios das sociedades. Relatos de abuso do poder para obtenção de vantagens indevidas sempre existiram ao longo da história, e no Brasil não foi diferente. No noticiário recente brasileiro avolumam-se investigações de fraudes cometidas contra o patrimônio público. Os esquemas desbaratados mostram que a administração pública está sob o ataque em diversas frentes de quadrilhas especializadas. Não por acaso, a investigação chamada de "Operação Lava Jato" inaugurou um novo patamar para os desvios, que passou de milhões para a casa de bilhões de reais.

Essa realidade mostra que praticamente qualquer organização, como órgão, autarquia, empresa pública, sociedades de economia mista, parcerias público-privadas, fundações, organizações sociais, fundos de pensão etc. está sob risco de fraude e corrupção, bastando para tal a existência de recursos públicos disponíveis para atrair a cobiça dessas máfias. Por vezes, nem isso é necessário. O poder regulatório ou decisório de um órgão ou entidade sobre questões que afetem o mercado ou o patrimônio de particulares atraem igualmente esse risco.

Ao mesmo tempo que isso ocorre, gestores dos mais variados órgãos e entidades e das três esferas e dos três poderes lutam para melhorar a administração pública, em especial os serviços públicos. A sociedade cobra, e com razão, padrões cada vez mais altos de serviços, elevando os desafios da atividade para os gestores. No entanto, haverá um momento em que nem mais recursos, nem mais servidores serão suficientes para fazer frente e atenuar as consequências dos desvios.

Assim, é preciso reconhecer a fraude e corrupção como grandes obstáculos ao progresso social do país. Nesse sentido, torna-se necessário um salto de qualidade na governança e gestão pública por meio da redução dos níveis de fraude e corrupção

para patamares de países desenvolvidos. Esse referencial visa justamente contribuir para o alcance desse objetivo.

Entretanto, a mensuração do nível de corrupção de um país é dificultada pela sua própria natureza oculta. Apenas se pode aferir efetivamente os casos que são descobertos, e a partir deles tentar se inferir o montante não descoberto. Em vista dessa dificuldade, outra forma indireta de se mensurar a corrupção é avaliando a percepção de corrupção que entidades têm de um país.

A organização não governamental Transparência Internacional[1] adota esse método e publica anualmente o Índice de Percepção de Corrupção de 175 países, com base em estudos de instituições independentes especializadas em governança e análise de ambiente de negócios. Em 2015, o Brasil obteve a posição 76ª no ranking. Isso dá uma medida do tanto que ainda se pode ganhar na gestão pública com o combate a corrupção.

E essa é uma cruzada mundial. A Organização das Nações Unidas estabeleceu o Plano de Objetivos de Desenvolvimento Sustentável para 2030[2]. O objetivo 16.5 dispõe que "reduzir substancialmente a corrupção e o suborno em todas as suas formas" é uma meta global[3].

No Brasil, o combate a fraude e corrupção se dá pela atuação de diversos órgãos, cada um dentro de sua esfera e escopo de atuação. O Tribunal de Contas da União integra essa rede como um ator importante, porque sempre atuou para combater a fraude e corrupção via controle externo. Além do papel fiscalizador e sancionador, o TCU reconhece que é importante contribuir com os gestores com orientação e assim prevenir os desvios. Por esse motivo, o TCU elaborou esse referencial.

O propósito desse referencial é compilar o conhecimento prático que vem sendo aplicado por organizações públicas e privadas, dentro e fora do Brasil, no combate a fraude e corrupção e dissemina-lo aos gestores públicos de todas as esferas de governo. A experiência mostra que não há medida única ou desassociada da governança e da gestão capaz de resolver esse problema por conta própria. O combate

1 http://www.transparency.org

2 https://nacoesunidas.org/pos2015/agenda2030/

3 (FURTADO, 2015, p. 382). "Diversos fenômenos verificados no cenário internacional ao longo das duas últimas décadas do século XX levaram a Comunidade Internacional a repensar as posturas até então adotadas para enfrentar a corrupção, tema até então tratado como de interesse interno de cada país e incapaz de ser enfrentado no plano internacional ou multilateral. Ao longo dos últimos anos, verificou-se verdadeira inversão na postura da Comunidade Internacional, que passou a tratar a corrupção como um dos temas mais relevantes em suas áreas de atuação."

à fraude e corrupção se faz no dia a dia, em diversas frentes e por todos os membros da organização.[45]

Para elaboração do presente referencial, foram consultados diversos documentos correlatos, normas e padrões, dentre os quais:

- A Framework for Managing Fraud Risks in Federal Programs (GAO, 2015);
- AS 8001-2008 Fraud and Corruption Control (STANDARDS AUSTRALIA, 2008);
- Fraud Control in Australian Government Entities (ANAO, 2011);
- Fraud Examiners Manual (ACFE, 2015);
- Guia de avaliação de risco de corrupção (UNGC, 2013);
- Guia de integridade pública: Orientações para a administração pública federal: direta, autárquica e fundacional (BRASIL, 2015a);
- Managing the Business Risk of Fraud: a Pratical Guide (IIA, 2008);
- Manual de direito disciplinar para empresas estatais (BRASIL, 2015c);
- Manual de processo administrativo disciplinar (BRASIL, 2015b);
- NBR ISO 31000: Gestão de riscos – princípios e diretrizes (ABNT, 2009);
- Referencial básico de governança aplicável a órgãos e entidades da administração pública (BRASIL, 2014);
- Tackling External Fraud (NAO, 2008);
- The Three Lines of Defense in Effective Risk Management and Controls (IIA, 2015).

Em vista disso, parte do conteúdo desse referencial é orientativo, não tendo, portanto, caráter normativo ou vinculante, e partes são baseadas em normativos legais. Portanto, as partes orientativas descritas neste documento não criam direitos ou garantias, nem substituem as leis específicas, decretos, resoluções, portarias ou instruções normativas ou qualquer outro normativo aplicável à organização.

4 Em linha com a proposta deste referencial, está em elaboração a norma ISO 37001:2016 – *Sistemas de gestão antissuborno – requisitos com diretrizes para uso.* Essa norma internacional trará boas práticas para organizações de todos os portes e setores para fazer esse enfrentamento, e os seus principais aspectos foram considerados neste referencial.

5 Neste referencial o termo "organização" refere-se a qualquer órgão, autarquia, fundação, empresa pública ou de economia mista, conselhos profissionais, organizações sociais e outras entidades de natureza pública dos três poderes e das esferas federal, estadual e municipal.

1.2. Público-alvo do referencial

Este referencial foi elaborado para uso de servidores[6] de entidades e órgãos públicos de qualquer hierarquia na organização, desde recém-empossados até da alta administração, uma vez que o combate a fraude e corrupção é dever de todos que se ocupam da administração pública. Além dos servidores em geral, cabe à auditoria interna um papel importante nesse enfrentamento, de modo que várias práticas apresentadas são exclusivas da auditoria interna ou contam com a sua participação.

Em termos de natureza jurídica da organização, o referencial foi concebido para ajudar qualquer organização pública, seja da administração direta ou indireta, empresas públicas e de economia mista, conselhos profissionais, organizações sociais e de qualquer poder ou esfera, federal, estadual e municipal. Mas isso não significa que todas as práticas recomendadas devam ser adotadas por todas as organizações.

Dependendo das características da organização, como porte, atividade exercida e natureza jurídica, algumas práticas se aplicam integral ou parcialmente e outras podem não se aplicar. Cabe aos gestores a discricionariedade de decidir a melhor forma de preparar a sua organização para combater a fraude e corrupção.

1.3. Conceitos fundamentais

Neste referencial os termos "fraude" e "corrupção" são mencionados exaustivamente. No entanto, não existe um consenso internacional sobre a definição desses termos. A própria Convenção das Nações Unidas contra a Corrupção (UN, 2004) não apresenta uma definição para o termo "corrupção". O resultado é que cada país ou entidade internacional define-os conforme o seu contexto jurídico. Mas para uniformização do entendimento, alguns conceitos básicos de fraude e corrupção são apresentados conforme são adotados pelo referencial.

1.3.1. Fraude

Pela norma ISA 240 da Iaasb[7], fraude é um "ato intencional praticado por um ou mais indivíduos entre gestores, responsáveis pela governança, empregados ou terceiros, envolvendo o uso de falsidade para obter uma vantagem injusta ou ilegal".

6 Neste referencial o termo "servidor" refere-se a todo aquele que preste serviço de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, desde que ligado a qualquer órgão ou entidade da administração pública federal, estadual ou municipal.

7 International Auditing and Assurance Standards Board é um órgão normalizador independente, definindo padrões internacionais para a auditoria, controle da qualidade, avaliação e serviços relacionados, facilitando a convergência das normas nacionais e internacionais.

Outra definição internacional vem da obra *Managingthe Business Risk of Fraud: A Practical Guide*[8]: fraude é qualquer ato ou omissão intencional concebido para enganar os outros, resultando na vítima sofrendo perdas e/ou o autor obtendo um ganho.

Nas Normas Brasileiras de Contabilidade[9] o termo fraude refere-se a ato intencional de omissão ou manipulação de transações, adulteração de documentos, registros e demonstrações contábeis. A fraude pode ser caracterizada por manipulação, falsificação ou alteração de registros ou documentos, de modo a modificar os registros de ativos, passivos e resultados; apropriação indébita de ativos; supressão ou omissão de transações nos registros contábeis; registro de transações sem comprovação; e aplicação de práticas contábeis indevidas.

A intenção é um elemento importante para diferenciar a fraude do erro. O erro, ainda que possua potencial de grande prejuízo, não é objeto deste referencial. A fraude também pode ocorrer pela omissão. Quanto ao benefício, em geral, implica em ganhos para o agente ou para terceiros, mas não necessariamente o benefício existirá. A fraude pode ocorrer pela lesão intencional, ainda que o agente não se beneficie dela. Ou até sem lesão, desde que o agente esteja se beneficiando. Existindo ganho, este pode ser direto, o mais comum, ou indireto, por recebimento de vantagem ainda que sem valoração financeira.

1.3.2. Corrupção

Na legislação penal brasileira, em sentido estrito, a corrupção se apresenta de duas formas: corrupção ativa e corrupção passiva, que respectivamente e suscintamente significam oferecer ou solicitar alguma vantagem indevida. Mas no cotidiano a corrupção é um termo guarda-chuva que abriga diversas outras condutas. O diagrama[10] abaixo, de autoria do Ministério Público Federal, relaciona as condutas que caracterizam o comportamento corrupto pelo ordenamento nacional e incluem tanto infrações penais quanto civis e administrativas.

8 Editado em conjunto pelo Institute of Internal Auditors, The American Institute of Certified Public Accountants e Association of Certified Fraud Examiners.

9 NBC T 11 - IT - 03 - fraude e erro.

10 http://combateacorrupcao.mpf.mp.br/tipos-de-corrupcao



FIGURA 1: Condutas que fazem parte do gênero "corrupção"

Todas essas condutas apresentam as suas especificidades, mas podem ser agrupadas pela definição de "corrupção" adotada pela Transparência Internacional: "corrupção é o abuso do poder confiado para ganhos privados".

Abuso de poder envolve a prática de atos ilícitos ou ilegítimos de forma deliberada ou intencional e se caracteriza pela quebra de confiança por parte do agente que comete o ato. Pode envolver agentes públicos ou privados. O ganho privado, ainda

que seja, geralmente, de ordem econômica, pode ser de qualquer natureza, inclusive a fuga a uma obrigação; pode ser repassada direta ou indiretamente ao beneficiário; e pode ser destinada ao agente que comete o abuso de poder ou a um terceiro.

A Transparência Internacional ainda classifica a corrupção como grande, pequena e política, dependendo da quantidade de dinheiro desviado e do setor em que ela ocorre.

A grande corrupção consiste em atos cometidos no alto nível de governo que distorcem as políticas ou o funcionamento central do Estado, permitindo que os líderes se beneficiem à custa do bem público, que envolvem somas expressivas de recursos, visando o enriquecimento pessoal ou financiamento político e tem a participação da classe política, altos funcionários públicos e elite empresarial.

A pequena corrupção envolve pequenos valores e ocorre de forma isolada, refere-se ao abuso diário do poder confiado a servidores de nível baixo e médio em suas interações com os cidadãos comuns, que, muitas vezes, estão tentando acessar bens ou serviços básicos em hospitais, escolas, departamentos de polícia e outras organizações.

A corrupção política é uma manipulação de políticas, instituições e regras de procedimento na alocação de recursos e financiamentos pelos decisores políticos, que abusam de sua posição para sustentar o seu poder, status e riqueza.

Outro conceito relevante é o de corrupção sistêmica, que se concretiza quando a corrupção é criada ou estimulada pelo próprio sistema, em razão de suas ineficiências, falta de rigor, excesso de informalidade (ou de burocracia). Nessas situações, o pagamento de suborno é prática corrente, tanto para se obter serviços regulares como para burlar as normas aplicáveis. As instituições políticas e econômicas estão contaminadas pela corrupção e existe alto nível de tolerância, tanto por parte dos agentes políticos como por parte da população quanto às práticas corruptas. Nesse contexto, as instituições são fracas ou inexistentes, o judiciário não é independente, não há supervisão legislativa, a sociedade civil e a mídia não são atuantes.

Em face das diversas definições, neste referencial os termos "fraude" e "corrupção" serão usados em conjunto, como um binômio, para expressar tanto o abuso de poder[11] quanto o falseamento ou ocultação da verdade, com vistas a enganar terceiros, sendo ambos para obter vantagem indevida para si ou para terceiros.

11 O abuso de poder pode se dar tanto por ação quanto por omissão, porque ambos são capazes de afrontar a lei.

1.3.3. Teoria do triângulo da fraude

A fraude nas organizações foi objeto de estudo de Donald R. Cressey (1953), que teorizou um modelo que ficou conhecido como "Triângulo da fraude". Por esse modelo, para uma fraude ocorrer, é necessária a ocorrência de três fatores: pressão, oportunidade e racionalização.



FIGURA 2: Triângulo da fraude

A primeira aresta do triângulo da fraude é a *pressão*, mas em algumas representações do triângulo, essa aresta é também chamada de *incentivo* ou *motivação*. A pressão é o que motiva o crime em primeiro lugar. Essa pressão pode ter várias origens, mas em geral se trata de algum problema financeiro do indivíduo, que por não conseguir resolver por meios legítimos, passa a considerar cometer uma ilegalidade para resolver o seu problema. A pressão pode ter origem pessoal ou profissional. Exemplos de *pressão* podem ser incapacidade de honrar as suas dívidas pessoais, vício no jogo ou em drogas, problemas de saúde, metas de produtividade no trabalho, desejo por padrão de vida superior.

A segunda aresta, *oportunidade*, refere-se à fraqueza do sistema, na qual o servidor tem o poder e habilidade para explorar uma situação que faz a fraude possível. A *oportunidade* define o método com que a fraude será cometida. O indivíduo deve vislumbrar uma forma de usar e abusar de sua posição de confiança para resolver o seu problema financeiro com uma percepção de baixo risco de ser pego. A *oportunidade* é criada por controles ineficazes e falhas na governança e, quanto maior for a percepção de oportunidade, maior a probabilidade de a fraude ocorrer. Outros fatores relacionados com a percepção de oportunidade são: a assunção de que a organização não está

ciente; os servidores não serem verificados periodicamente quanto ao cumprimento das políticas; a crença de que ninguém se importa e que ninguém vai considerar a transgressão grave. Mesmo que a *pressão* seja extrema, a fraude não vai ocorrer se a *oportunidade* não estiver presente.

A terceira aresta é a *racionalização*, que significa que o indivíduo antes de transgredir formula algum tipo de racionalização moralmente aceitável antes de se envolver em comportamentos antiéticos. A racionalização refere-se à justificação de que o comportamento antiético é algo diferente de atividade criminosa. Os transgressores se veem como pessoas comuns e honestas que são pegas em más circunstâncias. As racionalizações comuns são "eu estava apenas pegando emprestado o dinheiro", "eu merecia esse dinheiro", "eu tinha que desviar o dinheiro para ajudar minha família", "eu não sou pago o que mereço", "minha organização é desonesta com outros e merece ser trapaceada".

- Pela teoria do triângulo da fraude é necessária a ocorrência de três fatores: pressão, oportunidade e racionalização.

A partir do triângulo da fraude, outra teoria introduziu o "diamante da fraude". Nesse modelo, a nova aresta é a *capacidade*. Isso significa que para a fraude ocorrer, além dos fatores do triângulo da fraude, o transgressor precisa ter as habilidades pessoais e técnicas para cometer a fraude. Assim, a *pressão* é a causa-raiz da fraude, que leva o indivíduo a *racionalizar* e buscar uma *oportunidade*, e quando esse cenário está montado, bastaria a *capacidade* do indivíduo para a fraude ocorrer.

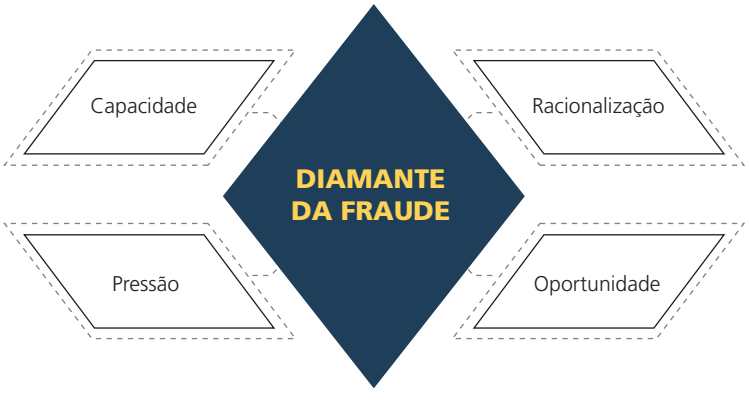


FIGURA 3: Diamante da fraude

1.3.4. Três linhas de defesa

Em uma organização moderna é comum que vários setores sejam responsáveis, de alguma forma, por tratar dos riscos da organização. Auditores internos, controladores financeiros e de qualidade, segurança patrimonial e de TI são exemplos de atividades que lidam com a gestão de riscos.

A questão é como coordenar todos esses atores para que fiquem claros os seus papéis, evitando a duplicação de esforços ou, pior ainda, deixando lacunas nos controles. O modelo de três linhas de defesa se propõe a designar as responsabilidades em forma de coordenação entre os envolvidos. O modelo pode ser visto abaixo:

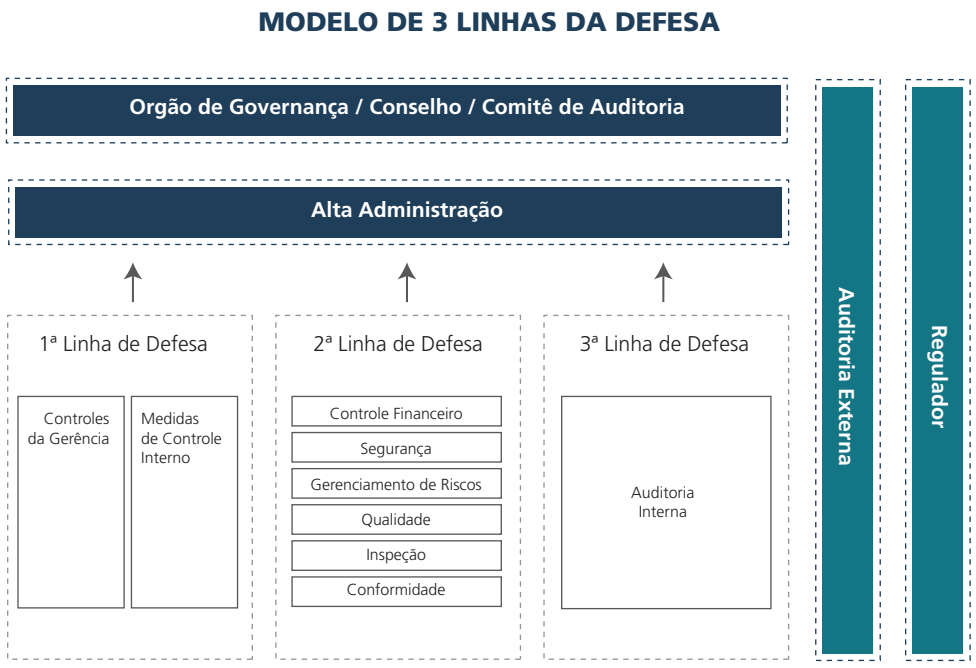


FIGURA 4: Declaração de Posicionamento do IIA: as três linhas de defesa do gerenciamento eficaz de riscos e controles, 2013

A primeira linha de defesa é composta pelos controles operacionais e internos dos gestores. Os gestores detêm os riscos do negócio e os gerenciam. Eles são responsáveis por implementar medidas corretivas nos processos e nos controles deficientes. É responsabilidade deles manter um controle interno efetivo. Os gestores devem identificar, avaliar e controlar os riscos, contribuindo para melhorar as políticas internas e assegurando que as atividades desenvolvidas estejam compatíveis com os objetivos da organização.

Os gestores são a primeira linha de defesa por estarem mais próximos na execução das atividades cotidianas da organização. É por isso que os gestores têm a capacidade de identificar primeiro os problemas na execução das atividades e de responder a esses problemas. Como decorrência disso, são os responsáveis por definir e implementar os controles necessários.

Na segunda linha de defesa está incluída a unidade de gestão de riscos, ou o exercício dessa função. Essa unidade ou função serve para monitorar e contribuir para a implementação de práticas de gestão de risco pelos gestores. Assistem os gestores na definição da tolerância ao risco e na forma como as informações de risco e controles são divulgadas internamente na organização.

Além da gestão de riscos, pode-se incluir também nessa linha de defesa as atividades de *compliance*, que significa monitorar os riscos de desconformidade com leis e regulamentos, a controladoria, que monitora os riscos financeiros, e a função antifraude e anticorrupção, que monitora o risco de fraude e corrupção.

As atividades da segunda linha de defesa possuem alguma independência da primeira linha de defesa. No entanto, como na segunda linha de defesa se trata também de atividades de gestores por natureza, no caso, gestores de risco, eles podem intervir diretamente na definição e implementação dos controles. Isso compromete a capacidade deles em oferecer uma análise totalmente independente à alta administração e aos órgãos de governança.

A terceira linha de defesa é composta pela auditoria interna da organização. Cabe à auditoria interna fornecer à alta administração[12] e órgãos de governança a avaliação objetiva e independente quanto à eficácia dos controles internos, da gestão de risco e da governança. O escopo dessa avaliação tipicamente inclui: eficiência e eficácia das operações, salvaguarda dos ativos, confiabilidade da comunicação interna, conformidade de leis, regulamentos e contratos. O estabelecimento da auditoria interna deve ser um compromisso com a governança em qualquer organização. A auditoria interna deve seguir os padrões para a atividade e reportar-se funcionalmente à mais alta instância interna de governança e, administrativamente, à alta administração.

As atividades e estruturas descritas nas três linhas de defesa dizem respeito à própria estrutura da organização e reportam-se a alta administração e/ou a conselhos e comitê de auditoria, por exemplo. Externamente à organização existem os órgãos de controle externo, os ministérios públicos, as polícias judiciárias e, eventualmente, dependendo da atividade, uma entidade reguladora. Essas instâncias podem ser consideradas outras linhas de defesa, mas que estão fora da governança e gestão da organização.

12 Neste referencial o termo "alta administração" refere-se à autoridade máxima e dirigentes superiores da organização.

Todas as linhas de defesa devem existir de alguma forma em todas as organizações, independentemente do tamanho ou complexidade. A gestão de riscos normalmente é mais forte quando existem três linhas de defesa separadas e claramente identificadas. No entanto, em casos excepcionais, especialmente em pequenas organizações, a primeira e segunda linhas de defesa podem ser combinadas.

- Os gestores são a primeira linha de defesa por estarem mais próximos na execução das atividades cotidianas da organização. É por isso que os gestores têm a capacidade de identificar primeiro os problemas na execução das atividades e de responder a esses problemas.

1.4. Gestão de risco

O risco da ocorrência de uma fraude e corrupção deve ser considerado pela organização em suas atividades. A forma como isso é realizado assume comumente o nome de gestão de risco de fraude e corrupção. A gestão de risco de fraude e corrupção é crucial para identificar, analisar e tratar incidentes com potenciais lesivos à organização, seja impedindo ou minimizando seus impactos.

A gestão de risco de fraude e corrupção deve estar integrada à atividade de gestão de riscos da organização, que é uma atividade mais ampla pois inclui uma visão sistêmica dos riscos mais relevantes a que a organização está submetida.

Os riscos de fraude e corrupção podem ter interseções a outros riscos da organização, de modo que a sua efetiva abordagem precisa considerar a existência de riscos de diferentes naturezas.

Inversamente, controles existentes para um tipo de risco podem estar mitigando riscos de outras naturezas.



FIGURA 5: Relação entre vários riscos da organização (ANAO, 2011)

Os riscos que ameaçam uma organização são de diferentes naturezas. Os riscos operacionais são eventos que podem comprometer as atividades rotineiras da organização; os riscos legais decorrem de alterações legislativas e normativas que afetam as atividades da organização; os riscos de tecnologia da informação são ameaças que exploram vulnerabilidades dos ativos informacionais da organização; os riscos patrimoniais provocam perdas nos ativos tangíveis e intangíveis da organização; e os riscos de fraude e corrupção são condutas praticadas contra o patrimônio ou os interesses da organização.

Um ativo intangível muito valioso para qualquer organização pública ou privada é a sua reputação. O valor da reputação, por ser de difícil apreciação, acaba sendo negligenciado pelos gestores.

Gestão de riscos é a identificação, avaliação e priorização de riscos seguida de uma aplicação coordenada e econômica de recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos ou maximizar o aproveitamento de oportunidades. O objetivo da gestão de riscos é promover meios para que as incertezas não desviem os esforços da organização de seus objetivos.

Todas as atividades de uma organização envolvem riscos decorrentes da natureza das atividades, de novas realidades, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração pública, bem como da necessidade de mais transparência e prestação de contas e de cumprir variados requisitos legais e regulatórios.

Por isso, as organizações precisam gerenciar riscos, identificando-os, analisando-os e, em seguida, avaliando se devem ser modificados por algum critério de modo a criar as condições para o alcance dos objetivos e de seus propósitos.

A gestão de riscos corretamente implementada e aplicada de forma sistemática, estruturada e oportuna gera benefícios que impactam diretamente os cidadãos e outras partes interessadas da organização. Assim, viabiliza o adequado suporte às decisões de alocação e uso dos recursos públicos, bem como aumenta a eficácia no atingimento de objetivos, ao criar e proteger valor público mediante a otimização de desempenho e resultados entregues.

Para a implementação de uma gestão de riscos, a organização pode adotar padrões internacionais criados para estruturar essa atividade. Citam-se os mais comuns: o Coso II [13]e a NBR ISO 31000[14,15]. É nesses padrões que a gestão de risco de fraude e corrupção pode estar integrada[16].

No âmbito do executivo federal existe a Instrução Normativa Conjunta MP/CGU nº 01/2016, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de risco e governança no âmbito do Poder Executivo Federal. A parte de gestão de risco dessa IN é baseada no Coso II.

1.4.1. NBR ISO 31000

A NBR ISO 31000 fornece princípios e diretrizes para gerenciar qualquer tipo de risco em toda ou em parte de qualquer tipo de organização. Trata-se de uma norma geral, independentemente de indústria, setor ou área e não concorre com outras normas sobre gestão de riscos em áreas específicas.

Seus objetivos são servir como um 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.

---

13 Trata-se de modelo de gestão (COSO, 2013) de riscos predominante no cenário corporativo internacional, especialmente na América do Norte, desenvolvido pela PricewaterhouseCoopers LLP sob encomenda do Coso (Committe of Sponsoring Organizations of the Treadway Commission) com o propósito de fornecer uma estratégia de fácil utilização pelas organizações para avaliar e melhorar o gerenciamento de riscos.

14 A NBR ISO 31000 fornece princípios e diretrizes para gerenciar qualquer tipo de risco na totalidade ou em parte de qualquer tipo de organização. Trata-se de uma norma geral, independentemente de indústria, setor ou área, e não concorre com outras normas sobre gestão de riscos em áreas específicas.

15 Os modelos citados foram concebidos pensando no setor privado, mas o uso desses modelos pode ser estendido ao setor público com as adaptações necessárias. A exemplo do *Standards for Internal Controls in the Federal Government* editado pelo Government Accountability Office e conhecido por *Green Book*. O *Green Book* é uma adaptação do Coso para o ambiente público americano.

16 Ver no Anexo 1 – Relação entre Coso e a gestão de risco de fraude.

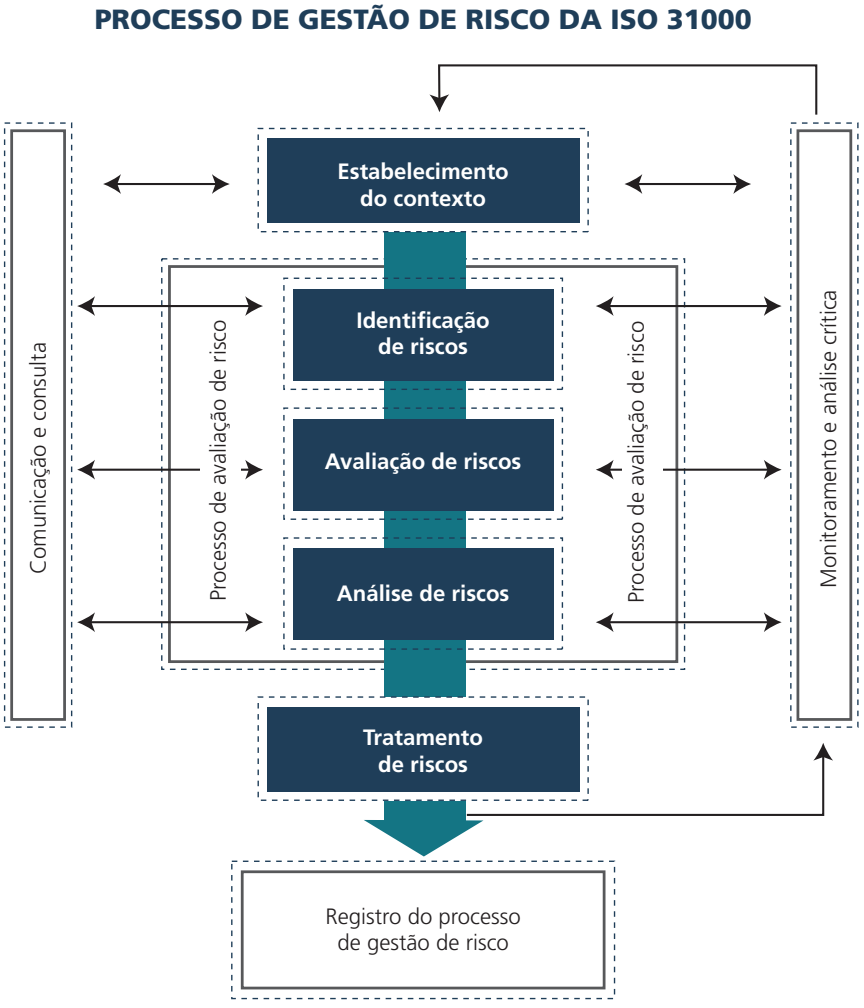


FIGURA 6: Processo de gestão de risco pela NBR ISO 31000

Nesse sentido, a NBR ISO 31000 pode ser aplicada no contexto de fraude e corrupção. Um processo robusto de avaliação de risco de fraude e corrupção envolve comunicação e consulta a servidores-chave em todos os níveis dentro de uma organização durante todas as fases do processo de gestão de riscos. Essa comunicação deve abordar questões relacionadas com o risco em si, as suas causas, o seu impacto e as medidas tomadas para tratá-lo.

Essa abordagem assegura que os responsáveis pela implementação do processo de gestão de riscos e as partes interessadas compreendam a base de tomada de decisão e as razões pelas quais ações específicas são necessárias.

Estabelecer o contexto é fundamental e envolve articular os objetivos da organização e os parâmetros externos e internos a serem levados em conta na gestão de riscos. Essa etapa também define os critérios de escopo e de risco para o resto do processo.

Identificar os riscos de fraude e corrupção exige que as organizações considerem os riscos, internos e externos, incluindo a cultura organizacional, e quando relevante para as suas operações, o potencial de fraude e corrupção internacional. As organizações também podem considerar riscos de fraude e corrupção que podem surgir no futuro. Por exemplo, riscos de fraudes decorrentes de uma mudança em um sistema de TI ou outras mudanças significativas nos processos organizacionais.

É também importante que os riscos de fraude e corrupção sejam levados em consideração na concepção de um novo sistema ou programa. Identificar os riscos de fraude e corrupção a nível de sistema e de programa ajuda as organizações a avaliar o risco global da organização e a refletir esses riscos em seus objetivos de planejamento estratégico.

Como fraude e corrupção implicam desonestidade, a identificação desses riscos exige uma atitude cética para fazer questionamentos: como um fraudador ou corrupto pode explorar as fraquezas do nosso sistema de controle? Como um fraudador ou corrupto poderia substituir ou contornar os controles? O que poderia um fraudador ou corrupto fazer para esconder a fraude?

Documentar e atribuir responsabilidade pelos riscos e controles é importante. A área de negócios responsável pela gestão de risco de uma fraude e corrupção em especial deve ser identificada, e o prazo para a implementação de qualquer medida corretiva deve ser documentado em planos de gestão de riscos.

Uma organização também deve monitorar e revisar seus controles de fraude e corrupção regularmente. As mudanças na eficácia ou pertinência desses controles podem ter impacto sobre a avaliação de risco de fraude e corrupção da organização tanto para aumentar quanto diminuir esse risco. Espera-se que a auditoria interna da organização avalie periodicamente se a estrutura de controle de fraude e corrupção está adequada e funciona de forma econômica e eficaz.

- Toda organização está sujeita aos riscos de fraude e corrupção
- A gestão de risco é essencial para o controle da fraude e corrupção
- A gestão de risco de fraude e corrupção é aplicação dos princípios e técnicas da gestão de risco na avaliação dos riscos de fraude e corrupção

1.5. Avaliação do custo-benefício no combate a fraude e corrupção

As práticas indicadas neste referencial requerem da organização esforços tanto de recursos humanos quanto financeiros, o que significa que combater a fraude e corrupção consome recursos que poderiam estar sendo empregados em outras atividades da organização.

Com isso em vista, a organização deve buscar, permanentemente, que os benefícios de um plano de gestão de risco de fraude e corrupção e os controles implantados dele decorrentes suplantem os seus custos[17]. A burocracia que cria controles desnecessários ou com relação custo-benefício desvantajosa deve ser evitada a todo modo. É sempre possível ter controles para combater a fraude e corrupção, mas esses controles devem permitir que as organizações entreguem seus resultados aos cidadãos honestos no menor tempo e custo possíveis (GAO, 2015).

Nessa equação os controles preventivos, em geral, apresentam melhor relação custo-benefício e por isso devem ser a primeira opção a ser avaliada, pois evitam, por exemplo, que a organização pague algo indevido e, posteriormente, tenha que implementar medidas corretivas e punitivas custosas. No entanto, como dito no parágrafo anterior, o combate a fraude e corrupção é instrumento para consecução dos objetivos da organização e não para dificultar o seu alcance.

Por outro lado, existem certos riscos de fraude e corrupção que, por sua natureza, podem levar a organização a decidir não implantar controles preventivos específicos, em razão da relação custo-benefício desvantajosa. Nesses casos, deve-se considerar a implementação de controles detectivos. Isso não significa que a organização tenha tolerância à fraude e corrupção, apenas que em determinados casos muito excepcionais não vai tentar impedi-las, mas se a fraude ou corrupção for posteriormente detectada, tolerância zero deverá ser aplicada.

Essa medida só ocorrerá quando o controle preventivo se mostrar claramente desfavorável, provocando embaraço à execução da política pública ou onerando sobremaneira a sua execução. No entanto, a regra geral de que a prevenção é o controle de melhor custo-benefício continua válida. O ideal é que haja tanto controles preventivos quanto detectivos em vigor, se o custo-benefício dos controles permitirem ambos.

Organizações pequenas podem não ter os recursos para implementar alguns controles. Para essas organizações, uma estratégia para se obter uma melhor relação

17 O art. 14 do Decreto-Lei 200/1967 dispõe: "O trabalho administrativo será racionalizado mediante simplificação de processos e supressão de controles que se evidenciarem como puramente formais ou cujo custo seja evidentemente superior ao risco."

custo-benefício na aplicação de controles para combater a fraude e corrupção seria investir em um controle preventivo e detectivo para suas áreas de alto risco inerente e onde os esforços tenham os maiores impactos. A organização deve focar seus recursos nas medidas antifraude e anticorrupção mais efetivas.

A avaliação e escolha do controle deve ser feita caso a caso, dependendo dos recursos disponíveis, custo potencial e nível de risco – em algumas instâncias pode ser mais prático ter apenas um controle detectivo e nenhum controle preventivo para um risco de fraude ou corrupção e vice-versa.

A organização deve também considerar nas suas avaliações de custo-benefício da implementação de controles antifraude e anticorrupção que controles automáticos tendem a ser mais confiáveis e eficientes que controles manuais, pois não são suscetíveis a erros humanos e possíveis retrabalhos. Além disso, controles que são direcionados para riscos específicos podem ser mais custosos do que controles gerais, como a exigência de que novos servidores assinem o compromisso com a política antifraude e anticorrupção da organização. Porém, por outro lado, controles focados em riscos específicos podem diminuir o custo da identificação das etapas em que a fraude e corrupção ocorrem, porque são capazes de identificar mais rápido o momento em que a fraude e corrupção ocorreu. Cabe, portanto, à organização somente aplicar os controles após avaliação de diversas opções e da relação custo-benefício.

Para avaliação da relação custo-benefício é interessante também que a organização envide esforços para estimar as perdas por fraude e corrupção que ocorrem em seus programas, contratos, repasses etc., tanto em termos financeiros como não financeiros.

Identificar perdas financeiras e não financeiras resultantes da real ou possível ocorrência de fraude e corrupção é a primeira medida para a definição da implantação de medidas antifraude e anticorrupção. Estimativas de potenciais economias decorrentes da implementação de controles ajudam na definição da prioridade que a organização dará ao combate a fraude e corrupção frente aos demais dispêndios organizacionais.

Ainda que não seja possível calcular precisamente essas perdas, alguma estimativa é melhor que nenhuma e é essencial para avaliar o custo-benefício dos controles. Afinal, como julgar se um controle é oneroso sem fazer uma estimativa das perdas na ausência desse controle?

Tais estimativas, então, estabelecem uma base para que os desempenhos dos controles possam ser avaliados. Se realizadas com frequência, as estimativas de perdas ajudam a organização a avaliar a eficiência e eficácia dos controles e se o risco de fraude e corrupção se reduziu.

Essas estimativas podem ser realizadas por modelos estatísticos e técnicas de amostragem. A precisão obtida dependerá de quanto se quer investir nessas estima-

tivas, porque uma avaliação superficial é fácil de se executar, mas à medida que se demanda mais precisão, mais oneroso se torna esse processo.

As medidas antifraude e anticorrupção não devem ser aplicadas uniforme e indistintamente em todas as organizações. Cada organização deve avaliar quais medidas são apropriadas para os seus riscos e benefícios esperados, considerando o seu tamanho, a sua natureza e a sua complexidade específica.

Grandes organizações possuem estruturas e pessoal que facilitam a implementação de controles antifraude e anticorrupção. Além disso, o tipo e a materialidade da fraude e corrupção que atingem grandes organizações podem ser diferentes daquelas sofridas por pequenas organizações, fazendo com que nestas a relação custo-benefício seja desvantajosa para a implementação de alguns controles.

Pequenas organizações podem implementar medidas preventivas básicas, como, por exemplo, evitar a concentração de autorizações relevantes em um único servidor, embora, para essa mesma organização, possa também ser difícil possuir servidores suficientes para o estabelecimento da ideal segregação de funções. Dessa forma, medidas compensatórias devem ser empregadas, tais como autorizações relevantes serem submetidas à alta administração da organização ou a um conselho de administração ou equivalente.

Para reduzir os custos de identificação de controles, uma ação importante a ser adotada por pequenas organizações é identificar as boas práticas mais efetivas de combate a fraude e corrupção implementadas por outras organizações, inclusive grandes, e avaliar como podem ser adaptadas às suas necessidades.

- Toda organização é suscetível à ocorrência de fraude e corrupção e deve avaliar a abrangência e a profundidade da implementação de controles considerando os seus riscos, o seu tamanho, a sua natureza e a sua complexidade.
- O benefício decorrente da implementação de controles antifraude e anticorrupção deve ser maior que o seu custo.
- Para se obter uma melhor relação custo-benefício na aplicação de controles, a organização deve focar nas áreas de maior risco e onde os esforços tenham os maiores impactos.
- É sempre possível ter controles para combater a fraude e corrupção, mas esses controles devem permitir que as organizações entreguem seus resultados aos cidadãos honestos no menor tempo e custo possíveis.

1.6. Dos mecanismos de combate a fraude e corrupção

Nos capítulos seguintes estão estruturados os cinco mecanismos de combate a fraude e corrupção: prevenção, detecção, investigação, correção e monitoramento. A cada mecanismo foi associado um conjunto de componentes que contribuem direta ou indiretamente para o alcance do seu objetivo. Por sua vez, vinculado a cada componente, foi associado um conjunto de práticas. As práticas são o detalhamento das atividades no seu nível mais operacional.

No entanto, essa estrutura não é estanque. Várias práticas apresentam vínculos e reflexos em outros componentes e mecanismos. A divisão proposta é meramente conceitual para facilitar a compreensão.



FIGURA 7: Estrutura de Mecanismos e Componentes

2. PREVENÇÃO

O primeiro mecanismo desse referencial trata da prevenção. A mais eficiente e proativa atitude para preservar os recursos públicos é prevenir que sejam desviados dos seus propósitos. Ainda que os componentes da prevenção (gestão da ética, controles preventivos, transparência e *accountability*[18]) não impeçam totalmente a ocorrência de fraude e corrupção, eles fazem parte das primeiras atividades de defesa para diminuir o risco de fraude e corrupção numa organização. Em geral, devido ao melhor custo-benefício, medidas preventivas devem ser adotadas para evitar o risco de fraude e corrupção, reduzindo as chances do seu cometimento.

Uma vez que o recurso toma um destino fraudulento, tentar mitigar o dano provocado por um desvio é uma atividade pouco eficiente[19]. O histórico de recuperação administrativa desses ativos é desfavorável para qualquer esfera de governo e de poder. Os meios de recuperação são lentos e custosos, obrigando a organização a alocar recursos humanos, e, portanto, mais recursos financeiros, para recuperar o recurso desviado e sem garantia de êxito.

Entretanto, a maior perda não está no recurso desviado nem no seu custo de recuperação, porque mesmo se ao fim de um procedimento administrativo ou judicial for possível recuperar um recurso desviado, o dano provocado pela perda de oportunidade é irrecuperável. Na medida em que um recurso é alocado a atender a uma política pública, um serviço público, uma obra ou algum outro benefício à sociedade e por conta do desvio deixa de se atingir esse objetivo inicial, a posterior recuperação desse recurso não vai restabelecer o benefício social que deixou de ser proporcionado, gerando uma perda de oportunidade.

18 Accountability refere-se à obrigação que têm as pessoas ou entidades às quais se tenham confiado recursos, incluídas as empresas e organizações públicas, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas e de informar a quem lhes delegou essas responsabilidades (BRASIL, 2011). Espera-se que os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis (IBGC, 2015). Conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam a sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações (BRASIL, 2016).

19 Esse modelo reativo é chamado pelo Government Accountability Office de *pay-and-chase,* ou seja, primeiro se faz o gasto e depois de verificada a fraude se persegue o ressarcimento do dano. O objetivo da prevenção é reduzir o *chase* até o limite em que o esforço e o custo da prevenção se equipara ao potencial de perda.

O risco de fraude e corrupção deve ser considerado já nas etapas iniciais de elaboração de políticas, programas, atividades ou processos públicos, para que medidas preventivas sejam concebidas desde a origem.

Portanto, a prevenção não é só mais eficiente na preservação do recurso público, mas também confere efetividade ao benefício social que se pretenda alcançar com esses recursos. Com isso em mente, o mecanismo da prevenção é composto por três componentes: gestão da ética, controles preventivos, transparência e *accountability*.

Por meio de um ambiente ético, reduz-se a disposição para desvios de condutas e formação de conluios e aumenta-se a propensão para denúncias. Por meio de controles, reduz-se o risco de que vulnerabilidades sejam exploradas por fraudadores e corruptos. Por meio da transparência e *accountability*, aumenta-se a capacidade de observação dos atos e fatos na gestão pública pelas partes interessadas (*stakeholders*[20]) da organização e aferição dos resultados obtidos.

- A prevenção evita a ocorrência de fraude e corrupção e, usualmente, é mais barata que medidas corretivas.
- A mais eficiente e proativa atitude para preservar os recursos públicos é prevenir que sejam desviados dos seus propósitos.
- O risco de fraude e corrupção deve ser considerado já nas etapas iniciais de elaboração de políticas, programas, atividades ou processos públicos, para que medidas preventivas sejam concebidas desde a origem.

Mecanismo – Prevenção
Componente P1 – Gestão da ética e integridade
Prática P1.1 – Promover a cultura da ética e da integridade na organização
Prática P1.2 – Estabelecer comportamento ético e íntegro da alta administração
Prática P1.3 – Estabelecer, divulgar e esclarecer o código de ética e de conduta
Prática P1.4 – Promover comissão de ética
Prática P1.5 – Estabelecer situações de conflito de patrimônio e de sua alteração significativa

20 *Stakeholders* são pessoas, grupos ou instituições com interesse em bens, serviços ou benefícios públicos, podendo ser afetados positiva ou negativamente, ou mesmo envolvidos no processo de prestação de serviços públicos. Em resumo, são aqueles cuja atuação e opinião deve ser levada em conta na formulação de estratégias, na *accountability* e na transparência. No setor público, abrangem: agentes políticos, servidores públicos, usuários de serviços, fornecedores, mídia e cidadãos em geral, cada qual com interesse legítimo na organização pública, mas não necessariamente com direitos de propriedade (IFAC, 2001).

Mecanismo – Prevenção
Prática P1.6 – Instituir política de prevenção de conflito de interesse
Prática P1.7 – Regular o recebimento de presentes e participação em eventos
Prática P1.8 – Registrar e publicar audiências
Prática P1.9 – Adotar termo de compromisso com os padrões éticos e de integridade
Componente P2 – Controles preventivos
Prática P2.1 – Estabelecer sistema de governança com poderes de decisão balanceados e funções críticas segregadas
Prática P2.2 – Estabelecer política e plano de combate a fraude e corrupção da organização
Prática P2.3 – Estabelecer política e práticas de gestão de recursos humanos para prevenir fraude e corrupção
Prática P2.4 – Estabelecer política e práticas de gestão de relacionamento com entidades e pessoas que recebam recursos financeiros ou que dependam do poder de compra e de regulação da organização
Prática P2.5 – Gerenciar riscos e instituir mecanismos de controle interno para o combate a fraude e corrupção
Prática P2.6 – Implantar função antifraude e anticorrupção na organização
Prática P2.7 – Promover programa de capacitação sobre combate a fraude e corrupção
Prática P2.8 – Comunicar a política e gestão de risco de fraude e corrupção e os resultados das correções aos casos detectados
Componente P3 – Transparência e *accountability*
Prática P3.1 – Promover a cultura da transparência e divulgação proativa das informações, utilizando-se especialmente dos meios de tecnologia da informação
Prática P3.2 – Promover a cultura da prestação de contas e responsabilização pela governança e gestão

P1 – Gestão da ética e integridade

Se a prevenção é o mecanismo mais eficaz no combate a fraude e corrupção, a gestão da ética e integridade é o seu componente imprescindível[21]. A gestão da ética e integridade é a fundação para a gestão das demais atividades da organização. Se omissa ou falha, manchará a gestão, e qualquer atividade pode levantar dúvidas quanto à legitimidade, probidade e motivação dos seus atos. Sem essa confiança de que a gestão está sendo feita pelos motivos certos, servidores e partes interessadas

21 Os inúmeros escândalos relacionadas a fraude e corrupção, a falta de profissionalismo, o baixo desempenho e a pouca entrega das organizações públicas justificam a necessidade de se abordar o tema "ética e integridade" de forma mais direta (EUROSAI, 2014).

podem se questionar se vale a pena manter os seus valores e passar a assumir comportamento reprovável, levando a organização a uma espiral decadente.

A gestão da ética se faz tanto com controles sutis (*soft controls*) quanto controles duros (*hard controls)* (IIA, 2015). Os controle sutis podem ser considerados medidas que influenciam a motivação – lealdade, integridade, tom da alta administração, inspiração e valores dos servidores. O comportamento resultante dessas medidas é a cultura organizacional. Já os controles duros podem ser definidos como medidas que induzem uma mudança direta e visível no comportamento dos servidores por meio de normas, estruturas, controles, tarefas, responsabilidades e autorizações.

Enquanto os controles duros são tangíveis, objetivos e fáceis de testar, os controles sutis são intangíveis, subjetivos e difíceis de testar. Devido a essa característica, as auditorias internas têm dificuldade de avaliar os controles sutis, preferindo atuar nos controles duros, o que abre espaço para condutas antiéticas, ainda que em conformidade com os normativos.

As práticas do componente "gestão da ética e integridade" baseiam-se principalmente no exemplo da alta administração, no estabelecimento de códigos, estrutura, comunicação, treinamento, sanções e monitoramento. Prestigiar a integridade dos servidores e promover o comportamento ético da alta administração são medidas abstratas, ao passo que estabelecer um código e comissão de ética são medidas concretas. As práticas desse componente previnem as fraudes, levando os envolvidos com a organização a nem considerarem a hipótese de as cometer.

- As pessoas possuem ambições que, por vezes, são contidas por limites éticos e de integridade. Compete às organizações promover e reforçar esses limites para que ambições sustentadas por fraude e corrupção não se materializem.
- Se a prevenção é o mecanismo mais eficaz no combate a fraude e corrupção, a gestão da ética e integridade é o seu componente imprescindível

Prática P1.1 – Promover a cultura da ética e da integridade na organização

A organização deve permanentemente promover a cultura da ética e da integridade a partir, especialmente, do exemplo de conduta íntegra da alta administração e por meio do estabelecimento de código de ética e de conduta, da sua divulgação e comunicação, da sua internalização mediante programas e eventos de treinamento e

conscientização com a participação de todos os integrantes da organização, beneficiários de programas, usuários de serviços públicos e fornecedores.

O sucesso de uma organização depende da sua cultura ética e da integridade de seus servidores. A alta administração deve entender e assumir que é o principal vetor de promoção da cultura ética e da integridade da organização por meio de suas ações e decisões.

A ética organizacional decorre dos valores e princípios da organização. Os valores organizacionais são, usualmente, expressos por intermédio de suas principais crenças, que ficam subjacentes às suas escolhas, como a defesa do interesse público, a imparcialidade, a transparência e o *accountability*, devendo ser normatizados por intermédio de códigos de ética. Os princípios decorrem, por sua vez, da transformação dos valores éticos em normas ou códigos de conduta, com o propósito de, por exemplo, evitar conflito de interesse, recebimento de presentes, clientelismo, nepotismo e outras formas de favoritismo.

A integridade refere-se aos valores e princípios pessoais que regem o comportamento de cada servidor. A integridade decorre da virtude e da incorruptibilidade, portanto da ausência de fraude e corrupção. Um servidor íntegro não se corrompe por situações momentâneas, infringindo as normas e as leis, os valores e os princípios éticos. Por outro lado, um servidor não íntegro poderá seguir as normas e as leis, os valores éticos, somente para evitar problemas, e não em razão do seu caráter. Em virtude disso, é relevante que as organizações visem não somente a promoção da cultura ética, mas também da integridade de seus servidores, que redundará na integridade organizacional como um todo.

Há uma relação dinâmica entre ética e integridade, em que uma fortalece e reforça a outra. A integridade pessoal é o alicerce para a ética, enquanto atividades organizacionais éticas encorajam a integridade pessoal. Pessoas que se esforçaram para um alto padrão de integridade gostarão de transferir seus princípios para a vida profissional. As palavras e atitudes de servidores que possuem alto nível de integridade vão estar alinhadas com os valores e princípios de uma organização ética e íntegra.

Os padrões éticos e de integridade, uma vez implantados, devem servir de critério para seleção, avaliação e promoção de pessoal. Com isso, a organização estabelece a mensagem de que o comportamento íntegro é valorizado e reconhecido, estimulando que mais servidores participem desse movimento.

Integridade significa mais do que simplesmente observar as normas, os códigos e as leis decorrentes dos valores e princípios. As normas e leis proporcionam um limite mínimo, um ponto de partida para a moralidade. É preciso mais do que isso.

Uma política de integridade requer uma combinação de repressão e prevenção. Se por um lado a organização adota medidas quando um servidor age inapropriadamente (repressão), por outro deve fazer tudo para que não haja desvios que possam induzir seus servidores a agirem dessa forma (prevenção). A prioridade deve ser na prevenção, não só pela efetividade, mas porque no cômputo geral o custo do investimento é usualmente menor do que o custo de reparação de danos causados por comportamento inapropriado.

É desafiador para as organizações estabelecer e obedecer os seus próprios padrões éticos e de integridade. Situações antiéticas surgem a todo instante e em todos os níveis hierárquicos, sondando por espaço em meio a conduta íntegra. É requerida muita disciplina para, permanentemente, portar-se conforme os padrões éticos e de integridade estabelecidos. O comportamento ético e íntegro é o garantidor de que a organização não se desvie de seus propósitos públicos. Decorre disso a importância da promoção contínua da cultura ética e da integridade.

Toda essa promoção da cultura ética e de integridade deve ser permanentemente monitorada, com o intuito de avaliar a sua efetividade e adotar medidas corretivas quando necessário.

- Uma organização íntegra se faz pelo comportamento íntegro diário de todos os seus servidores, alta administração e membros de conselhos.
- Todos numa organização são responsáveis por manter um ambiente ético, íntegro e de não tolerância a fraude e corrupção.
- O comportamento ético e íntegro é o garantidor de que a organização não se desvie de seus propósitos públicos.

Prática P1.2 – Estabelecer comportamento ético e íntegro da alta administração

A atitude estabelecida pela alta administração se reflete em todos os aspectos das ações da organização. Se a alta administração acredita que os controles internos são importantes, os demais membros e servidores dentro da organização perceberão e responderão conscientemente, observando os controles estabelecidos.

Assim, o compromisso, o envolvimento e o suporte da alta administração em estabelecer um comportamento ético fomentam uma atitude positiva e de apoio para aplicação de controles para prevenir e mitigar ameaças de fraude e corrupção nas organizações.

Para ajudar a assegurar que postura da liderança (*tone at the top*[22]) incentive a cultura ética, todos os membros da alta administração devem focar nos seguintes itens: i) ser um modelo a ser seguido, enquanto líder, pessoa e cidadão; ii) deixar claro aos servidores da organização que qualquer tipo de comportamento não ético, especialmente relacionado à fraude e corrupção, não será tolerado; iii) estar preparado para adotar ações corretivas firmes, incluindo aplicação de medidas disciplinares; e iv) demonstrar que adota medidas efetivas sempre que os casos de má conduta são descobertos ou relatados.

Portanto, não basta a alta administração dar o exemplo, ela deve também ter um observável alto nível de compromisso com o controle da fraude e corrupção, tanto os praticados pela organização quanto os contra a organização. O alto nível de consciência do risco de fraude e corrupção deve estar presente em todos os níveis mais altos da gestão, da alta administração e de membros de conselhos. Se esse alto nível de consciência não for evidente, essas instâncias administrativas devem receber treinamento que reforce os cuidados e atitudes apropriadas que devem ter perantes os riscos e controles de fraude e corrupção.

- Os gestores e servidores possuem a responsabilidade por promover e manter a cultura da ética e da integridade na organização. A alta administração deve sempre incentivar e monitorar essa promoção e, em todos os momentos, demonstrar de forma inequívoca e contundente o compromisso com a ética e a integridade e a não tolerância à fraude e corrupção.
- Lidere com ética e combata os desvios: é essencial que as organizações públicas estabeleçam mecanismos para encorajar e reforçar o comportamento ético de suas lideranças e servidores. Mais do que isso, demonstre estar sempre agindo de acordo com o interesse da sociedade, de modo que a população confie que os recursos públicos estão sendo geridos no seu exclusivo interesse.

22 Pela Association of Certified Fraud Examiners, *tone at the top* refere-se ao ambiente ético que é criado no local de trabalho pela liderança da organização. Seja qual for a postura da alta administração, esta terá um efeito sobre os trabalhadores da empresa. Se o tom definido pelos gerentes defende a ética e integridade, os funcionários estarão mais inclinados a defender os mesmos valores. No entanto, se a alta administração parece despreocupada com a ética e se concentra exclusivamente nos resultados, os empregados serão mais propensos a cometer uma fraude, porque eles sentem que a conduta ética não é um foco ou prioridade dentro da organização. Funcionários prestam muita atenção para o comportamento e as ações de seus chefes e eles seguem a sua liderança. Em suma, os funcionários vão fazer o que eles testemunham os seus chefes fazerem.

Prática P1.3 – Estabelecer, divulgar e esclarecer o código de ética e de conduta

Consiste no estabelecimento de código de ética que disponha sobre os valores e princípios que devem nortear as escolhas dos servidores e de código de conduta detalhando o comportamento esperado, as condutas vedadas e as punições possíveis. Esses códigos devem ser elaborados pela organização levando-se em conta a sua complexidade e seus riscos associados.

Tanto a alta administração quanto os servidores devem estar submetidos a algum tipo de mandamento ético e íntegro, ainda que por meio de códigos específicos. Nos casos em que já houver um código de ética normatizado por instância hierárquica superior, a organização pode complementar elaborando código de conduta detalhando o comportamento à sua realidade.

Entretanto, não basta a existência desses códigos, eles devem ser conhecidos por todos os servidores da organização, permanentes ou temporários, efetivos ou contratados. Os servidores devem ser esclarecidos de seus teores e sobre como, na prática, eles se aplicam em suas atividades diárias. Cópias eletrônicas e impressas devem estar disponíveis a todos. Um canal deve estar disponível aos servidores para esclarecer dúvidas quanto à interpretação dos códigos, que serão respondidas pela comissão de ética.

Treinamentos regulares sobre o conteúdo dos códigos devem ser realizados para servidores, alta administração, membros de conselhos, beneficiários de programas, usuários de serviços públicos, fornecedores e demais partes interessadas, e focar, especialmente, os servidores que ingressam na organização e aqueles que são indicados para a gestão, alta administração e conselhos da organização.

Testemunham-se, atualmente, graves problemas na área pessoal, profissional e política em que qualquer servidor, de qualquer nível, age sem limites éticos e de integridade. Quando a reputação das organizações é maculada, acarreta grande perda para a organização, para os bons servidores e para os cidadãos honestos. Organizações de todos os tipos estão agora realizando ações proativas para prevenir desvios éticos e de integridade, reforçando controles, comunicando e oferecendo treinamento sobre ética e integridade. O objetivo é mitigar os riscos reputacionais para a organização.

Os servidores, membros da alta administração e de conselhos, após serem apresentados ao código de ética e de conduta e conscientizados de sua importância, devem firmar um termo de que entendem e prometem comportar-se de acordo com os padrões éticos e de integridade esperados. O plano de capacitação deve prever reciclagem periódica nos assuntos éticos e de integridade, no qual se culminaria com a ratificação do compromisso inicial.

No caso de admissão ao cargo ou emprego, essa capacitação deve ser incluída no curso de formação para garantir que, antes de iniciar a sua atividade laboral, o servidor tenha sido conscientizado da existência e da importância desses códigos.

Além dos servidores, a alta administração e membros de conselhos devem ser chamados a conhecer os códigos de ética e de conduta da organização, momento em que devem ratificar o compromisso de obedecê-los.

Prática P1.4 – Promover comissão de ética

Para que o código de ética e o código de conduta sejam divulgados, interpretados e aplicados, cada organização deve constituir formalmente uma comissão de ética. À comissão de ética cabe atuar como instância consultiva dos servidores. Além disso, a comissão de ética é responsável por analisar e decidir sobre condutas que possam ter infringido o código de ética e o de conduta, além de definir as sanções cabíveis e supervisionar as ações de promoção da ética e da integridade da organização. Para a sua maior independência, a comissão deve estar vinculada ao órgão de direção ou à autoridade máxima da organização. Critérios devem ser estabelecidos para a indicação dos integrantes, que devem possuir conhecimento e reputação compatíveis com o cargo.

Recomenda-se o estabelecimento de mandatos para os membros da comissão de ética. Isso tende a conferir-lhes maior independência no desempenho de suas funções, na medida em que fica afastada a possibilidade de remoção extemporânea por parte da direção da organização.

A existência da comissão de ética, a sua função e as suas decisões sobre ato ou fato submetido à sua apreciação devem ser plenamente divulgadas na organização, exceto quando houver previsão legal de sigilo.

Uma vez constituída a comissão de ética, a organização deve garantir os recursos humanos, materiais e financeiros para que a comissão cumpra com efetividade as suas atribuições. A atividade de membro na comissão deve ter preferência sobre outras que o servidor designado porventura acumule para assegurar o seu pleno funcionamento.

- Crie uma comissão de ética e garanta o seu pleno funcionamento.

Prática P1.5 – Estabelecer situações de conflito de patrimônio e de sua alteração significativa

Dependendo da atividade regulatória e fiscalizatória da organização e dependendo da posição do cargo e hierarquia do servidor, em especial da alta administração,

o patrimônio pessoal deste profissional pode, real ou potencialmente, ser afetado pelas atividades da organização.

Nesse caso, esse servidor afetado deve informar à comissão de ética sobre esse patrimônio que possa suscitar conflito com as atividades da organização e indicar o modo pelo qual irá evitar o conflito. Isso previne que ganhos patrimoniais, ainda que involuntários, afetem a credibilidade do servidor no desempenho de suas funções.

Outra medida que pode ser adotada, dependendo também da organização e da hierarquia do servidor, é a notificação compulsória de alteração significativa no patrimônio de um servidor. Essa medida previne que uma modificação substancial do padrão de vida possa suscitar desconfiança na probidade do servidor. Na ocorrência de um fato gerador de variação significativa de patrimônio, independente da origem do fato, o servidor deve comunicar à comissão de ética essa variação, acompanhada de justificativas. A comissão ou os códigos de ética e de conduta devem estabelecer critérios para caracterizar essa variação significativa. Toda informação patrimonial deverá ser tratada com sigilo pela organização. Essas medidas complementam as exigências de declaração de bens e renda já previstas em lei[23].

Prática P1.6 – Instituir política de prevenção de conflito de interesse

Conflito de interesse é um conjunto de circunstâncias que cria riscos de que o julgamento ou ações relativas ao interesse primário do servidor venham a ser indevidamente influenciadas por um interesse secundário. Interesse primário refere-se aos principais objetivos de sua atividade enquanto agente público, notadamente o interesse público, e o interesse secundário significa, em geral, ganhos financeiros, mas também podem assumir a natureza de interesses pessoais, científicos, educacionais, assistenciais, religiosos, sociais etc[24].

Os interesses secundários não são considerados irregularidades em si, mas passam a ser questionáveis quando podem ter influência sobre o interesse primário. Ou seja, o conflito pode existir mesmo que o servidor não esteja sendo influenciado pelo interesse secundário. O conflito existe se as circunstâncias levam a crer (baseado

23 A Lei 8.429/1992 dispõe que todo servidor apresente declaração de bens em sua posse e atualize-a anualmente junto ao serviço de pessoal competente. Na esfera federal, a Lei 8.730/1993 dispõe que, além dos bens, o servidor declare as suas fontes de renda.

24 A Lei 12.813/2013 define conflito de interesse como "a situação gerada pelo confronto entre interesses públicos e privados, que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública". Para o Institute of Internal Auditors, conflito de interesse é "qualquer relacionamento que não seja ou não pareça ser o de melhor interesse para a organização. O conflito de interesse prejudicaria a habilidade do indivíduo para desempenhar objetivamente os seus deveres e responsabilidades".

em experiências passadas e evidências objetivas) que há o risco de decisões serem indevidamente influenciadas por interesses secundários.

Assim, a existência de um conflito de interesse é independente da ocorrência de alguma fraude ou corrupção. Portanto, é importante identificar conflitos de interesse e voluntariamente tomar medidas para que sejam desfeitos antes da ocorrência de alguma fraude ou corrupção.

As situações reais que caracterizam o conflito de interesse dependem de cada caso, tanto do interesse primário do servidor na organização quanto dos possíveis interesses secundários. Cabe à organização mapear a sua estrutura e identificar os cargos, setores e atividades que possam estar mais suscetíveis a desenvolver conflito de interesse.

Uma vez identificados esses pontos, as circunstâncias que caracterizem o conflito de interesse podem estar dispostas nos códigos de ética e de conduta, bem como as ações que o servidor deve tomar para evitá-las.

Prática P1.7 – Regular o recebimento de presentes e participação em eventos

Deve ser vedado que servidores recebam presentes oferecidos por pessoa, empresa ou entidade que tenha interesse em decisão que possa ser tomada pela organização. Como presente, entende-se qualquer benefício direto ou indireto, tais como ingresso para eventos, hospedagem, empréstimo de veículo ou moradia, concessão de transporte de qualquer natureza, *upgrades* em passagens, pagamento de refeições e descontos em geral não extensivos a qualquer um[25].

No entanto, podem não se caracterizar como presente, brindes promocionais do ofertante e sem valor comercial distribuídos em caráter geral na organização. O código de ética pode estabelecer um preço-limite para o valor desses brindes e frequência de distribuição admitida para melhor delimitação da vedação.

A participação em seminário, congresso e outros eventos pode ser uma fonte de conflito de interesse, pois dependendo das condições pode estar mascarando um recebimento de presente. Para evitar essa situação, deve-se observar condições que se aplicam tanto no caso de participação por interesse institucional quanto pessoal.

Se a participação for de interesse institucional, deve ser preferencialmente custeada pela própria organização. No entanto, se o promotor do evento não puder se beneficiar de decisão do servidor e não estiver sob jurisdição regulatória da organização, é aceitável a sua contribuição. Quando a participação for por interesse pessoal,

25 Ver no Anexo 2 – Exemplo de matriz para avaliação do recebimento de presentes.

esta pode ser custeada pelo promotor do evento, desde que o servidor torne pública as condições aplicáveis à sua participação, a sua eventual remuneração, e que o promotor do evento não possa se beneficiar de decisão do servidor.

Prática P1.8 – Registrar e publicar audiências

O servidor ocupante de cargo, a partir de uma determinada hierarquia, e a alta administração, quando mantiver contato por meio de audiência com particulares, pessoa física ou jurídica, devem realizar registro contendo o tema tratado, o dia, a hora e os participantes. Para essas audiências, faz-se necessário estar acompanhado de pelo menos um outro servidor. O registro deve ser efetuado ainda que a audiência seja realizada fora do local de trabalho.

A agenda de audiências concedidas e acompanhada dessas informações deve ser divulgada, permanentemente, no sítio da organização da internet, exceto se a matéria tratada estiver sob sigilo legal. Essa medida serve para dar garantia ao servidor e transparência no trato das questões públicas.

Prática P1.9 – Adotar termo de compromisso com os padrões éticos e de integridade

Uma boa prática é utilizar termos de compromisso, em que servidores, alta administração e membros de conselhos podem confirmar por escrito, anualmente, que cumpriram os doze meses anteriores com os padrões éticos e de integridade da organização e com a política antifraude e anticorrupção da organização e que vão continuar cumprindo nos próximos doze meses. O propósito dessa medida é criar um efeito moral no subscritor do termo para induzi-lo a seguir os normativos.

P2 – Controles preventivos

Uma vez estabelecido um ambiente positivo de cultura organizacional por meio das práticas do componente anterior, a prevenção ainda requer o ceticismo de que nem todos, incluindo a alta administração, membros dos conselhos, servidores e partes interessadas, se comportarão conforme esperado apenas pela influência de seus valores morais e éticos. Havendo oportunidade, existirão pessoas dispostas a atentar contra a organização. Mesmo que esse contingente seja pequeno perante o todo, pelo desejo de obter ganhos ilícitos eles podem provocar grandes perdas à organização.

Para a organização se proteger desse grupo de pessoas, a prevenção se faz por meio de controles. Esses controles geram uma expectativa nos potenciais fraudadores e corruptos de que poderão ser pegos e com isso podem preferir não correr esse

risco. Os controles preventivos funcionam dissuadindo o cometimento da fraude e da corrupção.

Existe forte ligação entre a incidência de fraude e corrupção e fracos controles preventivos. Em muitos casos em que a fraude e corrupção são detectadas, é possível que tenha havido falha nos controles preventivos que deixaram o incidente ocorrer. É essencial que a organização reavalie seus controles preventivos direcionados para a fraude e corrupção ocorrida e decida se algum aperfeiçoamento é necessário. Em caso positivo, o aperfeiçoamento deve ser implementado assim que for possível, desde que a relação custo-benefício seja vantajosa.

A organização deve sempre considerar que está permanentemente sujeita à ocorrência de fraude e corrupção e ciente de que nem toda fraude e corrupção pode ser prevenida e, nesses casos, deve avaliar se é mais vantajoso implementar controles detectivos do que preventivos.

- Existe forte ligação entre a incidência de fraude e corrupção e fracos controles preventivos. Em muitos casos em que a fraude e corrupção são detectadas, é possível que tenha havido falha nos controles preventivos que deixaram o incidente ocorrer.



FIGURA 8: Visão dos controles preventivos

Prática P2.1 – Estabelecer sistema de governança com poderes de decisão balanceados e funções críticas segregadas

A organização deve identificar as funções que tomam decisões críticas e segregá-las, de modo que a competência de decisão não esteja concentrada em uma única instância. Essa concentração é maléfica, na medida em que permite cometimento de fraude e corrupção e sua ocultação. A ideia da segregação de funções é que nenhum servidor possa estar numa posição capaz de executar todas as etapas necessárias para cometer uma fraude e corrupção e ocultá-la.

Além da segregação, a organização deve considerar implantar uma política de rotação de pessoal. Dependendo da criticidade da função, um prazo pode ser estabelecido para uma pessoa ocupar uma posição. A longa permanência de uma pessoa na mesma função pode encorajá-la a cometer fraude e corrupção, haja vista que conhecerá os controles existentes e a frequência e a profundidade das auditorias.

A organização deve avaliar caso a caso tanto as funções que requeiram segregação quanto rotação. O excesso de segregação pode burocratizar a tomada de decisão, retardando-a além do esperado. E o excesso de rotação pode prejudicar a continuidade das operações pela perda de memória organizacional.

Prática P2.2 – Estabelecer política e plano de combate a fraude e corrupção da organização

Quando a gestão de risco organizacional identificar alto risco de fraude e corrupção, a organização deve elaborar e documentar uma política e um plano de combate a fraude e corrupção[26].

A política de combate a fraude e corrupção é um documento emitido pela alta administração que contém o tom da organização no combate a fraude e corrupção e onde fica consignado o que se espera dos membros dos conselhos, da alta administração, gestores, demais servidores e partes interessadas na atividade, assim como as consequências de se praticá-las. Inclui, também, uma definição de fraude e corrupção no contexto da organização, garantias de sigilo e de não retaliação ao denunciante, além de diretrizes de como denúncias devem ser apuradas[27].

Para programas de grande porte e que perpassam por várias organizações, ainda que cada organização tenha a sua política antifraude e anticorrupção, cabe avaliar se uma política específica para o programa se justifica. Nesse caso, a organização

26 Ver no Anexo 3 – Exemplo de questionamentos quanto ao plano de combate a fraude e corrupção.

27 Ver no Anexo 4 – Exemplo de matriz de avaliação da política anticorrupção.

coordenadora pode emitir uma política exclusiva para o programa e que unifique os entendimentos entre todas as organizações afetadas.

A política deverá ser desdobrada em um plano de prevenção de nível operacional que contenha as estratégias e ações da organização no combate a fraude e corrupção[28]. Detalha quem é responsável e por quais atividades de controle ou gestão de risco de fraude e corrupção[29], estabelece o que será feito e um cronograma de implantação das atividades e por quais áreas. Também deverá explicar o propósito e as razões pelas quais as medidas serão adotadas e estabelecer as relações colaborativas com órgãos de fiscalização, controle, investigação e judiciais. É importante enfatizar que essa documentação deve definir e estabelecer os papéis e responsabilidades da alta administração, gestores e demais servidores e partes interessadas, interna e externamente, à organização[30].

Ademais, inclui documentar cuidadosamente todos os procedimentos de testes realizados para garantir o adequado funcionamento dos controles preventivos e detectivos, da investigação e da correção dos problemas identificados, bem como os resultados de desempenho obtidos a partir do monitoramento realizado.

A figura abaixo representa essa política. No centro, temos o interesse da organização em iniciar o combate a fraude e corrupção, expressa pela vontade genuína da alta administração em se comprometer com isso. Essa iniciativa movimenta as cinco engrenagens dos mecanismos, que movimentam as dos componentes, que impulsionam as das práticas.

28 Ver no Anexo 5 – Exemplo de plano de combate a fraude e corrupção.

29 Ver no Anexo 6 – Exemplo de matriz de responsabilidade.

30 Ver no Anexo 7 – Exemplo de fluxograma para tratamento de fraudes.

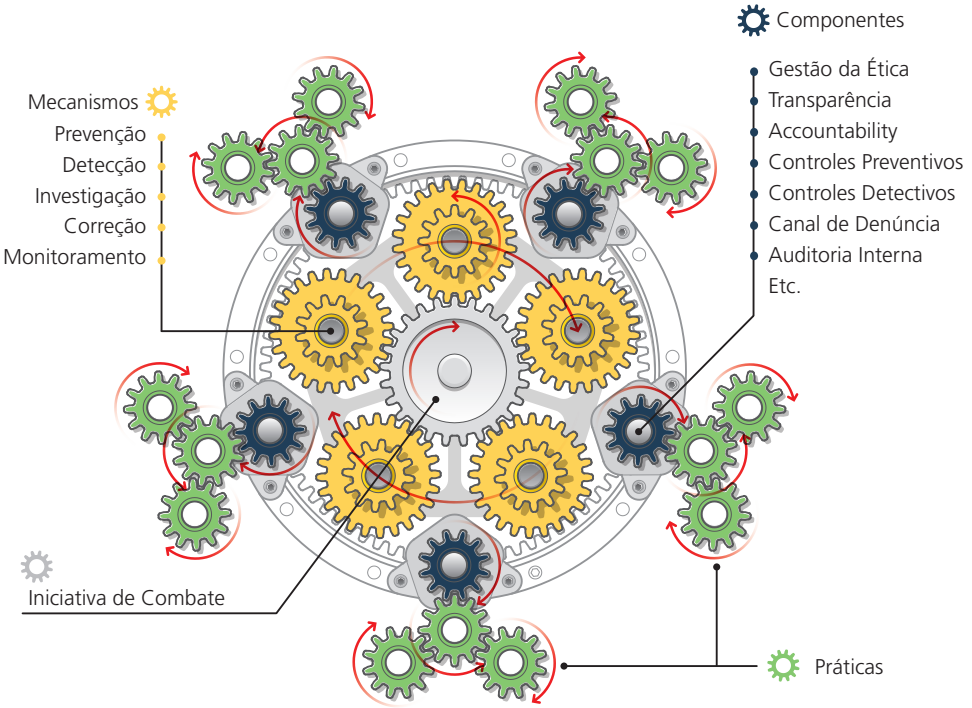


FIGURA 9: Relação de mecanismos, componentes e práticas

Prática P2.3 – Estabelecer política e práticas de gestão de recursos humanos para prevenir fraude e corrupção

Políticas e práticas de recursos humanos são incentivos positivos para a prevenção de fraude e corrupção nas organizações. Assim, o fortalecimento do gerenciamento de recursos humanos baseia-se em princípios de eficiência, eficácia e transparência e em critérios objetivos, como o mérito, a equidade e a aptidão.

Procedimentos adequados de recrutamento, contratação e capacitação de servidores, especialmente de cargos considerados vulneráveis à fraude e corrupção e fomento de uma remuneração adequada, são mecanismos importantes para prevenir a fraude e corrupção.

Além da análise formal dos documentos previstos em edital, a organização deve avaliar a fidedignidade deles e analisar os antecedentes profissionais pessoais de candidatos a servidores, com o seu consentimento. Servidores que cometeram fraude e corrupção em uma nova organização possivelmente tiveram também conduta desonesta em empregos anteriores. Essa avaliação deve ser realizada antes da contratação, antes do término do período probatório e nos casos de promoção para posições que

envolvam alto risco de fraude e corrupção, assim entendido para posições com alto poder de compra e de regulação.

Os servidores devem assinar uma declaração de se comprometer a informar à organização a ocorrência de processos criminais ou financeiros contra a sua pessoa. Essa declaração deve fazer parte do compromisso do servidor com o código de ética e de conduta previsto na prática "Adotar termo de compromisso com os padrões éticos e de integridade".

É uma boa prática estabelecer processos de seleção para cargos de direção e funções com critérios transparentes e divulgação dos resultados para que os servidores e partes interessadas exerçam indiretamente um controle das nomeações. Para cargos de livre nomeação, deve-se incluir uma análise de antecedentes por meio de certidões emitidas por órgãos administrativos e judiciais.

O nepotismo deve ser vedado nas suas diversas formas[31] [32]. A organização deve estar atenta para identificar essas situações. É uma boa prática submeter o nomeado ou contratado a termo de declaração de que a sua contratação não incorre nesta prática.

No desligamento do servidor da organização, medidas devem ser tomadas para garantir a segurança organizacional. Por exemplo, revogação de senhas de sistemas e e-mail corporativos e recolhimento de crachá, documentos, certificados digitais, uniformes e aparelhos eletrônicos.

A organização deve assegurar que a sua área de recursos humanos ou correspondente possua documentação relativa aos procedimentos administrativos e disciplinares que devam ser adotados em casos de fraude e corrupção.

Prática P2.4 – Estabelecer política e práticas de gestão de relacionamento com entidades e pessoas que recebam recursos financeiros ou que dependam do poder de compra e de regulação da organização

No relacionamento dos servidores com terceiros, pode surgir o risco de fraude e corrupção, especialmente quando há recursos financeiros envolvidos ou quando a organização regula alguma atividade. Caso prático são as licitações e contratos, em que empresas perseguem o objetivo de conquistar contratos, e seus prepostos

31 No âmbito federal, o Decreto 7.203/2010 dispõe sobre a vedação do nepotismo.

32 Súmula Vinculante 13 do STF: A nomeação de cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, da autoridade nomeante ou de servidor da mesma pessoa jurídica investido em cargo de direção, chefia ou assessoramento, para o exercício de cargo em comissão ou de confiança ou, ainda, de função gratificada na administração pública direta e indireta em qualquer dos poderes da União, dos Estados, do Distrito Federal e dos Municípios, compreendido o ajuste mediante designações recíprocas, viola a Constituição Federal.

mantêm contato com representantes de comissões de licitação. O mesmo se aplica ao relacionamento com representantes de entidades sem fins lucrativos que buscam celebrar convênios e outras formas de transferência financeira, ou no relacionamento entre organização reguladora e regulada, e fiscalizadora e fiscalizada.

O acesso e o relacionamento entre os servidores da organização e esses terceiros devem estar disciplinados internamente com padrões claros de conduta e imparcialidade na seleção, para que conflitos de interesse não surjam e levantem suspeitas de favorecimentos.

O risco de fraude e corrupção é reduzido se a organização conhece bem os terceiros com quem ela está lidando, especialmente nas compras mais significantes, em que o risco de recebimento de propina e comissões secretas é alto. A organização deve proceder a verificações complementares por intermédio de consulta a informações públicas da organização contratada e da sua alta administração, verificações telefônicas, notícias veiculadas na mídia, entre outros.

A organização também deve estabelecer procedimentos específicos para prevenir a ocorrência de fraude e corrupção no relacionamento com terceiros, tais como a rotação de pessoal e a divulgação de canais de denúncia, incentivando terceiros a registrarem indicações de condutas fraudulentas ou corruptas envolvendo a organização ou pessoa relacionada a ela.

Prática P2.5 – Gerenciar riscos e instituir mecanismos de controle interno para o combate a fraude e corrupção

As organizações devem adotar um processo de gerenciamento periódico e sistemático de riscos organizacionais que contemple a identificação, análise e avaliação dos seus principais riscos[33].

A frequência com que a organização deve conduzir essa avaliação de risco depende de fatores como o tamanho da entidade, sua natureza, complexidade, riscos gerais do setor em que a organização atua, a diversidade de processos e atribuições, a distribuição geográfica, o nível de controle pelo qual a organização é monitorada por órgãos reguladores e de fiscalização e o nível e a frequência de mudanças operacionais e tecnológicas. Usualmente, essa avaliação é realizada de dois em dois anos[34].

O objetivo final dessa avaliação é o estabelecimento de controles internos que mitiguem os principais riscos. Porém, o estabelecimento de controles internos genéricos não necessariamente resolve todos os riscos de fraude e corrupção. O risco

33 Ver no Anexo 8 – Exemplo de avaliação de risco de fraude.

34 Ver no Anexo 9 – Exemplo de análise de risco.

de fraude e corrupção, apesar de ser mais um tipo de risco para a organização, requer controles específicos para mitigá-los. Isso significa que a alta administração, com apoio de unidades especializadas (por exemplo comitê de ética, comitê de riscos, comitê de conformidade etc.), deve gerenciar a probabilidade de ocorrência de fraude e corrupção, que atente contra a boa e regular gestão dos bens e recursos públicos.

A figura abaixo apresenta um exemplo de aplicação de medidas de prevenção conforme a classificação de severidade dos riscos na organização:

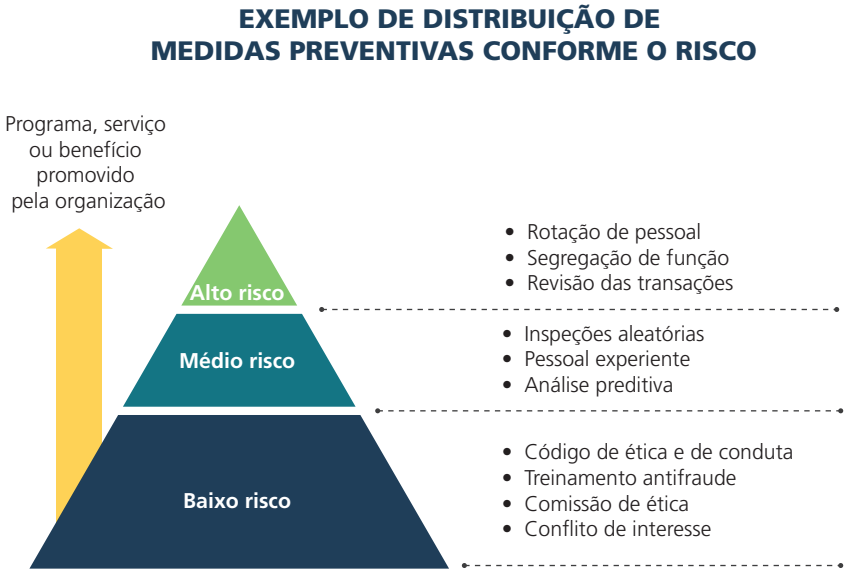


FIGURA 10: Exemplo de aplicação de controles conforme o risco (ANAO, 2011)

Para serem eficientes e eficazes, os controles internos devem submeter todos na organização, do servidor à alta administração. Isso não significa que todos devam ser submetidos, necessariamente, aos mesmos controles internos. Os controles podem e devem ser particularizados, conforme o risco oferecido pelo agente.

Nesse sentido, a gestão do risco de fraude e corrupção deve ser executada dentro do âmbito da gestão de risco organizacional, haja vista a interseção entre os diferentes riscos existentes (Figura 5). Todavia, mesmo que a avaliação de risco de fraude e corrupção possa estar alinhada a outras iniciativas de avaliação de risco, será benéfico para muitas organizações manter a avaliação de risco de fraude e corrupção como uma atividade autônoma, considerando os objetivos específicos e o foco dessa avaliação.

A gestão de risco de fraude e corrupção é composta, usualmente, de cinco elementos: estabelecer o ambiente de controle; identificar o risco inerente de fraude e corrupção; avaliar e classificar os riscos por intermédio da probabilidade e do impacto do risco inerente de fraude e corrupção; atuar nos riscos inerentes e residuais remanescentes de fraude e corrupção com maior probabilidade e impacto por meio do estabelecimento de controles mitigatórios apropriados, e monitorar, avaliar e comunicar a implementação dos controles[35].

Estabelecer ambiente de controle significa identificar os aspectos cultural, legal, regulatório, político, governança, estruturas, estratégias, processos, normas, relações com partes interessadas, entre outros, especialmente no que tange aos aspectos de fraude e corrupção, com vistas a uma melhor avaliação dos riscos inerentes de fraude e corrupção na organização.

Identificar o risco inerente de fraude e corrupção significa mapear as fraudes que potencialmente podem ocorrer na ausência de controles internos. Neste conjunto inclui-se todo tipo de esquema fraudulento e de corrupção, envolvendo incentivos, pressões e oportunidades. Deve ser dada atenção aos incentivos institucionais, pois mesmo sendo criados com a boa intenção de fomentar alguma prática, o erro na dosimetria pode provocar comportamentos indesejáveis.

Nesse processo de identificação de riscos, é importante considerar o potencial de que o servidor fraudador ou corrupto venha a burlar os controles. Em geral, os servidores conhecem os controles existentes e caso queiram cometer um ato fraudulento ou de corrupção usará seu conhecimento da organização para esconder seus atos.

A identificação dos riscos requer informações de diversas fontes. É importante que o gestor crie uma equipe para a identificação de riscos que inclua indivíduos de diversas áreas de conhecimento, por exemplo o pessoal das áreas de compras, de finanças, de recursos humanos, da contabilidade, do setor jurídico, relacionamento com o público, consultores. É importante ouvir, também, os demais gestores de riscos para que a gestão do risco de fraude e corrupção esteja em harmonia com a gestão de riscos em geral da organização. Auditores internos com experiência em combater fraude e corrupção podem contribuir com essa identificação repassando as suas experiências e os resultados de avaliações anteriores.

Historicamente, as funções de auditoria interna contemplavam avaliações de risco de fraude e corrupção. Entretanto, é cada vez mais aceito que a avaliação de risco de fraude e corrupção deva ser uma função da gestão e que a função de auditoria

35 Para outro exemplo, ver o Anexo 10 – Processo de avaliação de risco de fraude pela norma AS 8001-2008: Fraud and corruption control.

interna deva continuar suficientemente independente para ser capaz de desempenhar objetivamente seu papel de avaliar controles internos.

Identificados os riscos inerentes, avalia-se a probabilidade de sua ocorrência e seu impacto na organização. Esse julgamento é feito com base na experiência dos gestores e no histórico de ocorrências. Isso resultará numa relação ordenada do risco inerente mais grave ao menos ofensivo.

Depois que os riscos relevantes de fraude e corrupção foram identificados e avaliados, os controles internos existentes devem ser confrontados com esses riscos. Os riscos de fraude e corrupção que ainda permanecerem mesmo com adoção dos controles integram o conjunto de riscos residuais de fraude e corrupção. A organização tem que avaliar o potencial desses riscos residuais e decidir sobre os controles preventivos e detectivos que deseja lançar mão para mitigá-los ou se aceitará a permanência do risco residual, ou seja, aquele que ainda permanece mesmo com a implantação dos controles.

Após definidos os controles, compete à atividade de gestão de risco monitorar, avaliar e comunicar regularmente se esses controles estão sendo efetivamente implementados pelo gestor, retroalimentando o processo de gestão de risco como um todo. A atividade de gestão de risco enquadra-se na segunda linha de defesa, enquanto a da implementação dos controles pelo gestor trata-se da primeira linha de defesa. São instâncias separadas que possibilitam uma melhor segregação de funções.

As deficiências relatadas devem ser consideradas no âmbito da gestão de risco de fraude e corrupção, a fim de se verificar se os relatos estão compatíveis com os riscos assumidos e a necessidade de alguma alteração nessa gestão. O propósito desse monitoramento é assegurar que a gestão de riscos de fraude e corrupção esteja apropriada para as operações da organização e permita alcançar os objetivos para os quais foi estabelecida.

Uma vez descoberta uma fraude e corrupção, é necessário avaliar se os controles falharam ou se decorria de um cenário não previsto. Os controles devem ser reforçados ou criados, conforme o caso, considerando sempre a relação custo-benefício da sua implementação.

Uma característica fundamental para o sucesso de uma de gestão de risco de fraude e corrupção e de sua avaliação é a adesão da alta administração, de gestores seniores e de outros encarregados pela governança, como o conselho de governança, o conselho de auditoria, o conselho de ética, um comitê de gestão de risco, entre outros. Sem esse apoio de alto nível, a gestão de risco e a sua avaliação podem perder o ímpeto, evitar ou inadequadamente lidar com determinados problemas ou ter a sua qualidade afetada por outros gestores que escolheram não participar da gestão de risco.

A responsabilidade geral pela avaliação de risco de fraude e corrupção deve ser assumida pelos encarregados pela governança, como os conselhos citados ou por um comitê designado com essa finalidade. Para organizações que não possuem um conselho de administração ou governança ou um comitê encarregado, a responsabilidade geral pode ser atribuída à alta administração.

A alta administração deve ser responsável por realizar a avaliação de risco, informando periodicamente aos órgãos encarregados pela governança sobre o estado e os resultados desta avaliação e a implementação de qualquer plano de ação de mitigação de risco resultante.

Além dos membros da alta administração e de gestores seniores, podem estar envolvidos servidores da área de *compliance*, jurídica, de atendimento ao público, de aquisições, de contabilidade, de finanças, de recursos humanos e da auditoria interna. Também, pode ser valioso envolver servidores de diferentes níveis de experiência e hierarquia na organização, como da administração sênior e da equipe júnior. O pessoal sênior geralmente sabe como as funções devem operar, e o pessoal de nível mais inferior conhece as operações na prática.

Prática P2.6 – Implantar função antifraude e anticorrupção na organização

Em organizações que apresentam alto risco de fraude e corrupção, é importante a criação de uma função antifraude e anticorrupção. Essa função deve ser composta por um indivíduo ou uma equipe, em tempo parcial ou total, dependendo do tamanho, natureza, complexidade e tipos de riscos da organização. Este profissional deverá ser responsável por administrar as informações sobre a ocorrência de fraude e corrupção, supervisionar, monitorar e avaliar a implementação dos controles de fraude e corrupção e realizar investigações, com pessoal próprio, cedido de outras unidades ou contratado externamente.

Essa função pode auxiliar na identificação e avaliação dos riscos e controles de fraude e corrupção, mas não é responsável por sua gestão e implementação. É importante que essa pessoa ou equipe não esteja vinculada à auditoria interna para que mantenha a sua independência ao avaliar a função antifraude e anticorrupção da organização.

Essa função deve ter como atribuições receber qualquer relato ou denúncia de fraude e corrupção, tanto interna como externamente à organização; desenvolver um sistema de registro, resposta e monitoramento dos relatos ou denúncias de fraude e corrupção; servir como repositório do conhecimento do risco de fraude e corrupção; prover a capacitação de qualquer atividade relacionada ao combate a fraude e cor-

rupção; elaborar, implementar e executar um plano regular de avaliação do risco de fraude e corrupção na organização, abarcando experiências e práticas anteriores.

É desejável que o pessoal designado para essa função tenha a capacidade de entender e traduzir as melhores práticas de controle de fraude e corrupção em uma linguagem amigável de forma que possa ministrar ou coordenar capacitações acerca dessa temática. É recomendável que o profissional esteja atualizado com as boas práticas adotadas nesse campo e que possua formação adequada; participe de relevantes seminários, conferências e workshops sobre o tema; que mantenha documentos e matérias de referência; e estabeleça relacionamento com os servidores responsáveis pela gestão de riscos e implementação de controles de fraude e corrupção e auditoria interna.

Recomenda-se a organização de um repositório de conhecimento, que consiste em um sistema de gestão de incidentes de fraude e corrupção. O objetivo desse sistema é centralizar todas as informações relativas à fraude e corrupção para que diversas partes interessadas, tais como os gestores de negócio e de risco, a alta administração e a auditoria interna possam avaliar o histórico de fraude e corrupção e as suas tendências e tomem medidas cabíveis em suas áreas de competência.

São informações importantes para esse sistema: data da denúncia, data do incidente, como o incidente foi reportado, natureza do incidente e setor afetado, valor da perda potencial ou efetiva, ação tomada e resultados obtidos. Nesse sistema, além de constar as denúncias recebidas pelo canal de denúncias, deve ser registrado também qualquer outro incidente de fraude e corrupção que a organização tenha identificado ou tomado conhecimento por outros meios.

Tanto a função antifraude e anticorrupção quanto a auditoria interna promovem avaliações da gestão de riscos e controles de fraude e corrupção na organização, porém a função antifraude e anticorrupção faz parte da segunda linha de defesa e reporta-se ao gestor, e a auditoria interna faz parte da terceira linha de defesa, reportando-se à alta administração e aos órgãos responsáveis pela governança, como conselhos de administração e de auditoria.

Em alguns casos essa atividade é atribuída à auditoria interna, mas a sua exclusão dessa atividade visa contribuir para a manutenção da sua independência durante a avaliação dos controles internos.

Prática P2.7 – Promover programa de capacitação sobre combate a fraude e corrupção

Consiste em criar iniciativas para conscientizar gestores, auditores internos, servidores, terceirizados e contratados sobre a importância de se implementar ações

propositivas de combate a fraude e corrupção na organização por meio de programas de capacitação[36].

Servidores, gestores e auditores internos ao assumirem o cargo e depois, periodicamente, devem ser submetidos a capacitação que os conscientize sobre os diversos aspectos relacionados à fraude e corrupção. Partes interessadas que tenham impacto na gestão, como fornecedores, devem ser incluídos nessas capacitações.

As ações de capacitação podem ser organizadas de várias formas, como cursos presenciais ou a distância, workshops, divulgação de conteúdo antifraude e anticorrupção em periódico da organização, e-mail corporativo, vídeos etc.

É importante, também, divulgar informações sobre a política de gerenciamento do risco de fraude e corrupção e discutir consequências resultantes da prática de fraude e corrupção, tais como sanções, ações disciplinares e outras formas de correção e punição. Como resultado, a capacitação ajuda a criar uma cultura de integridade, ética e conformidade com leis e regulamentos dentro da organização.

- A capacitação ajuda a criar uma cultura de integridade, ética e conformidade com leis e regulamentos dentro da organização.

Prática P2.8 – Comunicar a política e gestão de risco de fraude e corrupção e os resultados das correções aos casos detectados

Refere-se ao dever da administração de comunicar interna e externamente informações de qualidade necessárias à consecução dos objetivos da organização. A administração deve fornecer comunicações específicas e dirigidas que abordam expectativas de comportamento e responsabilidades das pessoas que atuam na organização. Uma comunicação apropriada é necessária, não somente dentro da organização, como também fora dela.

Essa comunicação deve transmitir a importância da política e gestão de riscos de fraude e corrupção para o alcance dos objetivos da organização, a linguagem comum de riscos e a responsabilidade de cada um na gestão de riscos.

A organização deve manter os servidores e partes interessadas conscientes do que é considerado fraude e corrupção, alertando-os do que devem fazer caso identifiquem alguma atividade suspeita. Manter um sentimento de que a probabilidade de ser pego é alta produz uma efetiva dissuasão de intenções fraudulentas e corruptas.

36 Ver no Anexo 11 – Exemplo de matriz para avaliação de treinamento anticorrupção.

Além disso, divulgar amplamente os resultados de casos de fraude e corrupção detectados e punidos exemplarmente tem um efeito dissuasivo que auxilia na sua prevenção. A expectativa de que a organização irá detectar, investigar e punir a fraude e corrupção ajuda a deter potenciais fraudadores e corruptos em razão das prováveis sanções que podem ser impostas, como demissão, multa, confisco de bens, responsabilização civil e penal, entre outras.

Essa comunicação deve ser realizada regularmente e pode ser operacionalizada por intermédio de relatórios de gestão e financeiro anuais; de páginas internas e externas da internet; de e-mails institucionais, de campanhas e *press release* em mídias locais e nacionais. Algumas informações são importantes e devem ser comunicadas, por exemplo: que a organização possui controles para prevenir e detectar fraudes e corrupção; que há alta probabilidade de fraudadores e corruptos serem identificados e punidos; os casos de correção e punição; a existência de canal de denúncias; e o custo da fraude e corrupção para os cidadãos honestos.

O objetivo principal da comunicação é fazer com que servidores, beneficiários de programas, usuários de serviços públicos, fornecedores e outras partes interessadas conheçam o compromisso da organização em combater a fraude e a corrupção e em obter de todos o apoio efetivo a esse combate. Uma estratégia adequada de comunicação tem um grande poder para mudar a atitude do público em geral frente à fraude e à corrupção.

As comunicações devem ser avaliadas especialmente no tocante à sua efetividade e ao alcance dos objetivos. Deve-se buscar uma relação custo-benefício adequada. Não obstante, é difícil de se estabelecer uma ligação direta entre a comunicação e a diminuição da fraude e corrupção, devido a outros fatores que possam influenciar essa diminuição.

P3 – Transparência e *accountability*

Se a organização se esforça para ter um ambiente correto e ético e atua para que a fraude e corrupção não ocorram, não há motivos para que ela não demonstre isso à sociedade. Permitir que terceiros observem as decisões da alta administração e acompanhem os resultados da gestão contribuirá para que a própria organização reveja os seus processos antifraude e anticorrupção, identificando os aspectos que precisam ser melhorados. Mas isso só é possível se a organização instrumentalizar a sociedade com dados e fatos, promovendo a transparência e o *accountability*.

Prática P3.1 – Promover a cultura da transparência e divulgação proativa das informações, utilizando-se especialmente dos meios de tecnologia da informação

A transparência é um dos mecanismos mais eficientes e essenciais para o combate a fraude e corrupção. Para tanto, a organização deve conscientizar seus servidores, a alta administração, os membros de conselhos e as partes interessadas da natureza pública das informações.

Toda informação produzida ou custodiada pela organização é precipuamente pública, e isso precisa ser bem compreendido por todos. Sendo assim, não cabe avaliação de conveniência quanto à publicidade da informação. Se houver informação com alguma restrição de acesso, isso deve ser tratado como uma exceção, que só ocorrerá após uma classificação que a torne sigilosa por tempo determinado.

O objetivo de se buscar a transparência é instrumentalizar o controle social. Isso faz com que qualquer pessoa em qualquer lugar possa ser um fiscal da gestão pública. Os ambientes transparentes dificultam que os desvios prosperem, pois elevam a probabilidade de que as ocorrências de fraudes e corrupções sejam identificadas.

Para a melhor efetividade da transparência, as informações devem estar prontamente disponíveis ao público, independentemente de requerimento de interessados. A organização deve rotineiramente publicar as suas informações, à medida que as produza e receba. Dessa forma, estarão atualizadas e, a qualquer momento, poderão ser consultadas sem a necessidade de uma provocação exterior à organização.

A internet deve ser o principal meio de divulgação das informações. Os sítios em que estiverem disponíveis as informações devem, também, oferecer a informação no formato de dados abertos, o que significa permitir que as informações não sejam só pesquisáveis, mas também exportáveis em arquivos. Com esse tipo de formato, amplia-se o controle social, pois se permite que pesquisadores, imprensa, sociedade civil organizada e qualquer interessado controlem a gestão a partir das informações brutas, desenvolvendo novos relatórios, aplicações e sistemas de controle social. Por exemplo, já existem muitos exemplos de sítios e aplicativos para *smartphones* voltados ao acompanhamento do orçamento público, das doações eleitorais, da atuação político-partidária etc.

Mesmo que as informações estejam disponíveis na internet, a organização deve manter serviço de informação ao cidadão para orientar sobre como obter a informação desejada. Esse serviço envolve receber requerimentos de acesso e acompanhar a sua tramitação. O serviço deve estar disponível por múltiplos canais, como telefone, formulário na internet e atendimento presencial.

Além disso, as informações devem estar também disponíveis em formatos compatíveis com as necessidades especiais das pessoas com deficiência. Isso implica

que sítios da internet devem atender a padrões de acessibilidade para acesso amplo, independente da limitação pessoal.

Além das informações gerais, a organização deve disponibilizar informações que favoreçam o combate a fraude e corrupção. A identificação dessas informações pode ser feita em parceria com entidades de combate a fraude e corrupção, como órgãos de controle, de fiscalização, de investigação e judiciais, e com a sociedade em geral, especialmente por intermédio de pesquisas.

- Os ambientes transparentes dificultam que os desvios prosperem, pois elevam a probabilidade de que as ocorrências de fraudes e corrupções sejam identificadas.

Prática P3.2 – Promover a cultura da prestação de contas e responsabilização pela governança e gestão

A prestação de contas da organização e a responsabilização pela governança e gestão, que compõem o conceito de *accountability*, requerem que a alta administração voluntariamente divulgue os resultados alcançados pela organização, tanto nas atividades-meio quanto nas atividades finalísticas da organização.

Em relação às atividades-meio, deve-se divulgar, por exemplo:

- a gestão patrimonial dos principais bens móveis, a exemplo de veículos e equipamentos, informando a sua natureza, quantidades e destinação, e dos bens imóveis, a destinação e o estado de uso;
- os procedimentos licitatórios e contratos firmados, não apenas em relações, mas com cópia dos principais documentos que integrem esses procedimentos;
- os dados da execução orçamentária, detalhados e atualizados, em especial das despesas, repasses e transferências de recursos;
- política de recursos humanos, benefícios oferecidos e, a depender da natureza da organização, a remuneração individualizada de seus servidores, inclusive o recebimento de diárias e a identificação das viagens.

Mais importantes ainda são os resultados obtidos nas atividades finalísticas. São essas que justificam o propósito da organização. Os principais objetivos e indicadores devem ser tornados públicos, bem como as respectivas metas definidas, prazos e os resultados alcançados. O objetivo é permitir que o controle social acompanhe o desempenho das atividades da organização e, assim, saber se a sua função está sendo cumprida adequadamente. Os resultados de trabalhos realizados por auditoria interna

e externa devem estar disponíveis, além das prestações de contas anuais, seu parecer e julgamento.

Conhecendo-se como os insumos da organização (orçamento, pessoal, patrimônio) são geridos e os resultados finalísticos alcançados, pode-se aferir a efetividade da organização. Se a efetividade for baixa, especialmente se houver outras organizações similares para comparação, é o caso de se avaliar se há má gestão ou indícios de fraude e corrupção.

- Os principais objetivos e indicadores devem ser tornados públicos, bem como as respectivas metas definidas, prazos e os resultados alcançados.

3. DETECÇÃO

A prevenção da fraude e corrupção, que foi apresentada no primeiro mecanismo, está relacionada com a sua detecção, mas não são a mesma coisa. A prevenção, como mostrado, inclui políticas, processos, capacitação e comunicação para evitar que a fraude e corrupção ocorram, enquanto a detecção foca atividades e técnicas para identificar tempestivamente quando uma fraude ou corrupção ocorreu ou está ocorrendo. A detecção consiste na obtenção de informações suficientes que garantam uma investigação. Essas informações podem resultar de controles estabelecidos, de auditorias realizadas e de fontes internas e externas à organização.

Um forte fator de dissuasão da fraude e corrupção é a consciência em todos de que mecanismos detectivos estão em vigor, o que acaba tendo o efeito de prevenção. Entretanto, enquanto na prevenção as medidas são aparentes, na detecção as medidas são, por natureza, ocultas, o que significa que, em sua maioria, são executadas sem que servidores e partes interessadas saibam que estão sendo operacionalizadas no dia a dia da organização.

O objetivo primário da detecção é evidenciar a fraude e corrupção que está ocorrendo ou já ocorreu. A detecção tem a função de identificar as fraudes e corrupções, caso as medidas preventivas falhem. Há que se considerar que, mesmo com as práticas de prevenção implantadas, alguns agentes podem decidir pelo cometimento de fraude e corrupção, seja porque avaliam que os riscos são baixos, seja porque os benefícios são vultosos, ou seja, a relação risco-benefício da fraude e da corrupção é, ainda, favorável na sua avaliação.

No combate a determinados esquemas de fraude e corrupção, os mecanismos de detecção se tornam mais atraentes, pois apresentam custo-benefício melhor do que os mecanismos de prevenção[37]. No entanto, toda organização deve considerar tanto a prevenção quanto a detecção da fraude, pois, combinados, esses mecanismos aumentam a efetividade da estratégia de combate.

Esse mecanismo é composto pelos controles detectivos, pelo canal de denúncia e pela auditoria interna.

37 Em programas executados com múltiplos beneficiários e em ampla distribuição territorial, a fraude pode ocorrer de forma pulverizada e de pequeno valor, o que tornaria o custo-benefício dos controles preventivos desfavoráveis. Nesse caso, a detecção da fraude é mais viável do que a prevenção, especialmente se baseada em tratamento de dados.

- Um forte fator de dissuasão da fraude e corrupção é a consciência em todos de que mecanismos detectivos estão em vigor, o que acaba tendo o efeito de prevenção. Entretanto, enquanto na prevenção as medidas são aparentes, na detecção as medidas são, por natureza, ocultas.

Mecanismo – Detecção
Componente D1 – Controles detectivos
Prática D1.1 – Controles reativos de detecção
Prática D1.2 – Controles proativos de detecção
Prática D1.3 – Documentar as técnicas de detecção de fraude e corrupção
Componente D2 – Canal de denúncias
Prática D2.1 – Estabelecer canal de denúncias
Prática D2.2 – Garantir o sigilo das denúncias e o seu gerenciamento
Prática D2.3 – Análise e admissibilidade das denúncias
Componente D3 – Auditoria interna
Prática D3.1 – Avaliar a política, o plano, a gestão de risco de fraude e corrupção e os controles internos da organização
Prática D3.2 – Avaliar a cultura e gestão da ética e da integridade
Prática D3.3 – Planejar e realizar auditorias e investigações de fraude e corrupção
Prática D3.4 – Estabelecer uma sistemática de divulgação de relatórios que tratam de fraude e corrupção

D1 – Controles detectivos

Assim como o gestor da atividade é o principal agente na prevenção por meio de controles internos, ele também é o principal responsável pelos controles internos detectivos. O propósito desses controles é verificar os registros em busca de fraude e corrupção que já ocorreram ou estão ocorrendo.

A detecção dessas fraudes e corrupções não só aciona os mecanismos de investigação e de correção a fim de identificar e punir o responsável e recuperar o montante desviado, mas pode também impedir a sequência de novas fraudes e corrupções, possuindo, portanto, efeitos preventivos.

Prática D1.1 – Controles reativos de detecção

A implementação sistemática de indicadores de possível fraude e corrupção (*red flags*) melhora a eficiência e eficácia das ações de detecção. Os indicadores são

circunstâncias que são incomuns nas atividades da organização e em razão disso precisam ser investigadas.

Como as organizações se valem de tecnologia da informação para executar seus processos, muitos indicadores podem ser automatizados, de forma que pode ser implementada uma supervisão contínua e sobre todas as transações.

O uso de indicadores inclui três etapas:

- identificar indicadores;
- implementar indicadores;
- avaliar transações detectadas.

A identificação de indicadores consiste em mapear as circunstâncias que são incomuns na organização, o que requer experiência na atividade. Isso deve ser feito pelo gestor da atividade, mas com apoio do gestor de risco e da função antifraude e anticorrupção, quando esta existir.

Na segunda etapa, implementa-se o indicador, preferencialmente nos sistemas informatizados da organização. Um sistema de supervisão com os indicadores implementados permite acompanhar em tempo real as transações que são realizadas nos sistemas da organização. Se algum indicador importante não for viável nesse processo de automação, deve-se avaliar o custo-benefício de um controle manual.

Na terceira etapa, o sistema de supervisão, ao detectar que algum evento atende aos critérios do indicador, adota as decisões pré-definidas pelo gestor. As decisões podem ser de duas ordens. A primeira é impedir o prosseguimento da transação, encaminhando-a para análise humana. Caberá ao gestor verificar se a transação realmente é indício de uma fraude e corrupção ou apenas um falso positivo[38]. No primeiro caso precisa-se apurar, e, no segundo, libera-se a transação.

O fato de paralisar a transação requer que a medida de avaliação seja rápida, o que nem sempre é viável quando há grande volume de detecções. Então, a segunda opção de decisão que o sistema de supervisão pode tomar é permitir que a transação se conclua, encaminhando a ocorrência ao gestor para que avalie se cabe alguma apuração. Nesse caso, o gestor pode avaliar em lote todas as transações detectadas.

Uma transação pode acionar mais de um indicador, o que reforçaria os indícios sobre ela. Então, o sistema pode utilizar isso para ponderar e gerar uma métrica de criticidade para classificar as transações em níveis de riscos.

38 Falso positivo nesse caso é uma transação que o sistema de supervisão detectou por atender aos critérios do indicador e que, portanto, apresentam indício de fraude, mas que ao se verificar, observa-se que há justificativas para a sua ocorrência sem vinculação à atividade fraudulenta.

A vantagem de um acompanhamento contínuo é a tempestividade para impedir que uma possível fraude e corrupção prossiga livremente.

São exemplos de indicadores: aprovação de processos ou fases em tempo rápido; pagamentos realizados por pessoa, em valores e dias e horários não usuais; contratação com dispensa com valor logo abaixo do limite; licitação com preço pouco abaixo do orçamento etc[39].

Prática D1.2 – Controles proativos de detecção

Além dos indicadores implantados na prática anterior, que são reativos, uma vez implantados, automaticamente detectam as ocorrências com base nos indicadores mapeados. Existem também os controles proativos, que requerem que os gestores os promovam periodicamente. Para tanto, a organização pode usar técnicas de análise de dados e outras ferramentas tecnológicas para detectar atividades fraudulentas. Esse conjunto de técnicas são chamadas de *data mining*[40], *data matching*[41] e *data analytics*.[42]

Por meio da análise de dados, após a limpeza e modelagem dos dados brutos é possível identificar anomalias e tendências em grandes bases transacionais. A diferença dessa técnica para um acompanhamento contínuo baseado em indicadores é que nesta o gestor precisa conhecer e implementar os indicadores, ao passo que, com o uso de técnicas de análise de dados, a própria técnica aponta o que seriam os indicadores, ou seja, identifica o comportamento anômalo e suspeito.

Esse comportamento nem sempre é intuitivo para o gestor, o que o impede de identificá-lo por meio de sua experiência. Em alguns casos pode até ser contraintuitivo. Nessa situação, apenas a análise de dados pode revelar essa realidade.

Relações ocultas entre pessoas, entidades e eventos podem ser identificadas com análise de dados, e as relações suspeitas podem ser encaminhadas para apuração específica. Para apresentação dos resultados, as técnicas de visualização de dados

---

39 Ver mais exemplos no Anexo 13 – Exemplos de red flags.

40 *Data mining* é o processo de selecionar, explorar e modelar grandes quantidades de dados para revelar padrões, tendências e relações que podem ajudar a identificar casos de fraude e corrupção. http://www2.sas.com/proceedings/sugi22/DATAWARE/PAPER128.PDF

41 *Data matching* descreve os esforços para comparar dois conjuntos de dados coletados. Isso pode ser feito de muitas maneiras diferentes, mas o processo é muitas vezes baseado em algoritmos programados, onde computadores executam análises sequenciais de cada item individual de um conjunto de dados, comparando-a com cada item de um outro conjunto de dados. https://www.techopedia.com/definition/28041/data-matching

42 *Data analytics* é um processo de inspeção, limpeza, transformação e modelagem de dados com o objetivo de descobrir informações úteis, sugerindo conclusões, e apoiar a tomada de decisões. A análise dos dados tem várias facetas e abordagens, que engloba diversas técnicas sob uma variedade de nomes, em diferentes negócios, ciência e domínios das ciências sociais. https://en.wikipedia.org/wiki/Data_analysis

devem ser consideradas, pois comunicam com mais efetividade para qualquer perfil de audiência.

As anomalias apontadas por esse tipo de análise não necessariamente indicam a ocorrência de fraude e corrupção, mas eventos singulares que merecem avaliação individualizada para a exclusão da possibilidade de fraude e corrupção e, no caso da não exclusão, uma investigação.

Prática D1.3 – Documentar as técnicas de detecção de fraude e corrupção

A organização deve documentar as técnicas desenvolvidas e implementadas na detecção de fraude e corrupção e o desempenho delas deve ser testado e registrado, a fim de melhorá-las e eliminar os controles ineficientes.

A documentação envolve, mas não se limita, a planejar o processo de detecção de fraude e corrupção, os controles específicos, os papéis e responsabilidades pela implementação, pelo monitoramento, pela apuração, pela comunicação e pelos recursos tecnológicos requeridos.

Ao divulgar que implementa controles detectivos com o objetivo de dissuasão, portanto como medida preventiva, os aspectos técnicos desses controles devem ser resguardados do público e mesmo no âmbito da organização. A alta administração deve definir os perfis de acesso a essa informação. Essa medida tem o propósito de evitar que os controles possam ser burlados e que os fraudadores e corruptos escapem da detecção.

D2 – Canal de denúncias

A denúncia é um dos principais mecanismos pelo qual a fraude e a corrupção é identificada. As organizações nunca eliminarão o risco de fraude e corrupção por completo. Por mais que se esforcem em detectar fraude e corrupção com base em controles e informações internas, há limites práticos para isso.

Controles baseados em amostragem deixam margem para que a fraude e corrupção ocorram por longos períodos até serem detectados. A fraude e corrupção que ocorrem abaixo dos limiares dos controles, em geral por gestores que sabem dos valores desses limiares, se tornam também invisíveis. Fraude e corrupção cometidas mediante conluio de servidores, alta administração, beneficiários de programas, usuários de serviços públicos e fornecedores desafiam todos os controles possíveis.

Esses são exemplos que justificam a adoção de canais denúncias. Os olhos e ouvidos dos cidadãos e das partes interessadas estão em todos os lugares, e a organização deve estar preparada para se aproveitar desse controle difuso e gratuito.

Prática D2.1 – Estabelecer canal de denúncias

Significa que a organização implementa e opera um canal por onde denúncias de fraude e corrupção contra a organização possam ser reportadas. O propósito do canal é contribuir com informações à função antifraude e anticorrupção, ao gestor, à auditoria interna e à corregedoria para identificar e cessar as fraudes e as corrupções. Além disso, o canal serve de mecanismo de dissuasão de potenciais fraudadores e corruptos. As pesquisas indicam que uma das medidas mais efetivas para detecção de fraude e corrupção são as denúncias recebidas[43].

O canal deve estar disponível para qualquer cidadão fazer uma denúncia, e a organização deve permanentemente divulgá-lo, especialmente a servidores e partes interessadas, tais como beneficiários de programas, usuários de serviços públicos e fornecedores. O canal deve oferecer várias opções de denúncia, além de formulários eletrônicos na internet, por e-mail, telefone, carta e presencialmente. O formulário eletrônico deve ser estruturado de forma que induza o denunciante a reportar o máximo de informações relevantes que conheça, permitindo à organização tratar as informações recebidas de forma adequada. No caso de denúncias por telefone e presenciais, o atendente deve estar capacitado para conduzir a entrevista com o denunciante.

O canal de denúncia deve ser avaliado e monitorado, por exemplo, identificando o número e tipos de denúncias e o que aconteceu com as denúncias recebidas.

- As pesquisas indicam que uma das medidas mais efetivas para detecção de fraude e corrupção são as denúncias recebidas.

Prática D2.2 – Gerenciar as denúncias recebidas

A organização deve tomar medidas para assegurar que os denunciantes[44] se sintam confortáveis em denunciar, proporcionando a eles a oportunidade do anonimato, se preferirem. A facilidade em denunciar é ponto-chave na eficiência e eficácia do canal de denúncias.

No caso do recebimento de uma denúncia anônima, a organização deve, preliminarmente e em caráter sigiloso, antes de instaurar um processo formal, adotar medidas informais tendentes a apurar a verossimilhança dos fatos denunciados. Após essa apuração preliminar e sumária, caso a organização se convença de que há uma

43 Relatórios Occupational Fraud and Abuse Survey da ACFE e KPMG Fraud Survey

44 Na literatura estrangeira o denunciante é chamado de *whistleblower*, ou seja, aquele que toca o apito para chamar atenção para a fraude.

razoável probabilidade de serem verdade os fatos denunciados, deve então instaurar, de ofício, um processo formal de investigação, totalmente desvinculado da denúncia[45] [46].

No momento da denúncia, caso identificada, deve estar claro para o denunciante que eventualmente a sua identificação pode se tornar pública ao final da investigação[47].

As denúncias devem ser tratadas sigilosamente até decisão definitiva sobre a matéria[48]. No caso de denúncias por servidores, a organização deve estabelecer políticas que proíbam retaliação a servidores que denunciem de boa-fé[49]. O canal deve estar preparado para recepcionar inclusive denúncias contra a alta administração. Nesse caso, elas devem ser reportadas a uma instância superior, a exemplo de conselhos de administração ou órgãos colegiados[50].

Um único sistema de gerenciamento deve ser usado para registar as denúncias e seu acompanhamento, para que facilite a resolução pelo gestor, os testes dos auditores internos e a supervisão das instâncias superiores. Esse sistema pode ser o mesmo ou integrado ao sistema de gestão de incidentes de fraude e corrupção mantido pela função antifraude e anticorrupção, quando esta existir.

Condutas antiéticas também podem ser reportadas pelo canal, pois podem resultar ou estar encobrindo fraude e corrupção. A organização deve normatizar que as denúncias sejam, tempestivamente, encaminhadas para o setor apropriado para a sua apuração, seja a área de pessoal, segurança patrimonial, comissão de ética, departamento jurídico, almoxarifado, função antifraude e anticorrupção etc.

A organização deve estabelecer e divulgar os procedimentos a serem adotados interna e externamente sobre as denúncias recebidas, inclusive prevendo o encaminhamento para corregedoria e órgãos de controle, de fiscalização, de investigação e judiciais.

---

45 O Supremo Tribunal Federal firmou jurisprudência de que "nada impede a deflagração da persecução penal pela chamada 'denúncia anônima', desde que esta seja seguida de diligências realizadas para averiguar os fatos nela noticiados" (HC 99.490, relator: Ministro Joaquim Barbosa, DJe 31/1/2011).

46 "Não há ilegalidade na instauração de processo administrativo com fundamento em denúncia anônima, por conta do poder-dever de autotutela imposto à Administração e, por via de conseqüência, ao administrador público" (MS 2006/0249998-2; relator: Ministro Paulo Gallotti; 3ª Seção; DJe 5/9/2008).

47 Resolução SF nº 16/2006.

48 A Lei de Acesso à Informação, Lei 12.527/2011, dispõe no art. 23, inciso VIII que são passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção e repressão de infrações.

49 Lei 8.443/1992, art. 55 § 2º. O denunciante não se sujeitará a qualquer sanção administrativa, cível ou penal, em decorrência da denúncia, salvo em caso de comprovada má-fé.

50 Lei 8.112/1990, art. 126-A. Nenhum servidor poderá ser responsabilizado civil, penal ou administrativamente por dar ciência à autoridade superior ou, quando houver suspeita de envolvimento desta, a outra autoridade competente para apuração de informação concernente à prática de crimes ou improbidade de que tenha conhecimento, ainda que em decorrência do exercício de cargo, emprego ou função pública.

Prática D2.3 – Análise e admissibilidade das denúncias

Cada denúncia deve ser avaliada por uma pessoa preparada para isso. Nem todas as denúncias precisam ser investigadas. A denúncia deve trazer elementos que justifiquem movimentar a estrutura organizacional. A investigação interna demanda mobilização de pessoal para integrar equipe de investigação, espaço físico para os trabalhos, paralisação de pessoal para entrevistas, e para justificar isso precisa-se ter um conjunto pertinente de indícios. A denúncia bem realizada traz, usualmente, elementos sobre sete quesitos:

- O quê: o que está sendo fraudado e corrompido?
- Quem: quem é ou são os fraudadores e corruptos?
- Por que: por qual motivo se está realizando a fraude e corrupção, qual o seu propósito?
- Como: qual a forma de atuação dos fraudadores e corruptos, como eles executam a fraude?
- Quanto: quanto em valor ou bens está sendo desviado?
- Quando: em qual data, por qual período de tempo ou desde quando vem sendo realizada a fraude e corrupção?
- Onde: unidade da organização ou sistema de informática onde foi realizada a fraude e corrupção?

Nesse sentido, é importante disponibilizar um formulário eletrônico estruturado ou com orientações, de forma a induzir o denunciante a reportar o máximo de informações relevantes. Se o formulário for apenas um campo livre para inserção de texto, o denunciante fica à deriva para narrar o que quiser, o que não é interessante, pois o denunciante, em geral, não tem experiência do que precisa ser relatado. É provável que ele dê mais ênfase em sua indignação com a fraude e corrupção do que trazer elementos fáticos para uma avaliação.

Naturalmente, pode ser que mesmo induzido o denunciante desconheça algum quesito. Isso não é um problema, pois a partir dos outros quesitos a função antifraude e anticorrupção, corregedoria ou quem fará a admissibilidade, pode identificar internamente as outras respostas. Mas por garantia, caso o contato com o denunciante esteja disponível, vale a pena questioná-lo sobre alguma informação que falte ou não esteja clara.

A análise da denúncia deve concluir por sua admissão quando há verossimilhança. Isso significa que os elementos trazidos fazem sentido e estão de acordo com a realidade já conhecida pela organização, ou seja, é plausível de estar ocorrendo o que foi denunciado. Apesar disso, o avaliador não deve se fechar a denúncias improváveis,

visto que o fraudador ou o corrupto pode executar a fraude e corrupção pouco prováveis justamente para evitar ser detectado.

D3 – Auditoria interna

A responsabilidade primária pela identificação de fraude e corrupção numa organização reside nos responsáveis pela gestão. A auditoria interna auxilia a organização no tocante à avaliação da eficácia e adequação da política e do plano de combate a fraude e corrupção, da gestão de risco de fraude e corrupção, dos respectivos controles internos e da gestão da ética e da integridade organizacional, por meio de aconselhamento e de propostas de aperfeiçoamento, sendo a sua função primordial avaliar se os controles internos implementados pelo gestor são adequados para mitigar os riscos de fraude e corrupção identificados. Pode, também, auxiliar o gestor a identificar e avaliar os riscos enfrentados por sua organização[51].

Assim, a importância que uma organização atribui às atividades de auditoria interna é uma indicação do compromisso da alta administração com uma política e um plano de combate a fraude, com uma gestão de riscos, com a ética, com a integridade e com controles internos de fraude e corrupção eficientes e eficazes.

Eventualmente, a auditoria interna pode identificar fraude e corrupção no curso de uma auditoria ou contribuir com seu conhecimento técnico para subsidiar a investigação de fraude e corrupção. Em organizações com alto risco de fraude e corrupção, a auditoria interna tem sido demandada a detectar indícios ou investigar a ocorrência de fraude e corrupção.

Investigações, usualmente, utilizam como base as falhas de controle e os indícios de fraude e corrupção identificados nas avaliações. Auditorias internas com papel complementar de investigação devem possuir suficientes competências sobre esquemas de fraude e corrupção, técnicas de investigação, medidas corretivas e punitivas, e cooperação e parceria com órgãos de controle, de fiscalização, de investigação e judiciais.

---

51 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 os 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 os seus objetivos. (IN MP/CGU 01/2016)

Grandes organizações usualmente possuem unidades antifraude e anticorrupção com atribuição de investigação. Nesse caso podem ser formadas parcerias entre essa unidade e a auditoria interna com o objetivo de melhor investigar os eventuais casos.

Na condução de auditorias a responsabilidade do auditor interno no tocante à detecção de fraude e corrupção é ter suficiente conhecimento sobre: os esquemas de fraude e corrupção para ser capaz de identificar indícios dessas ocorrências; a existência de controles fracos que podem permitir a ocorrência de fraude e corrupção; testes adicionais direcionados para a identificação de outros indicadores de fraude e corrupção; avaliação de indicadores de fraude e corrupção que podem ter ocorrido e decidir se alguma ação adicional é necessária e se uma investigação deveria ser recomendada; notificação de autoridades apropriadas da organização, se existir suficiente indício para recomendar uma investigação.

As avaliações realizadas pela auditoria interna acerca da adequação e suficiência dos controles internos de fraude e corrupção são fundamentais para a identificação de indícios e até mesmo de evidências de fraude e corrupção e servem de base para investigações internas ou externas.

A organização deve proporcionar aos auditores internos oportunidade de capacitação na teoria e na prática de combate a fraude e corrupção para poderem desempenhar o papel esperado deles.

Prática D3.1 – Avaliar a política, o plano, a gestão de risco de fraude e corrupção e os controles internos da organização

Deve-se realizar revisão periódica da implementação da política e do plano de gestão de risco de fraude e corrupção da organização por meio da aplicação de procedimentos de auditoria que permitam testar e aferir adequabilidade e a conformidade dos controles internos estabelecidos para prevenir e detectar potencial fraude e corrupção.[52]

A responsabilidade por gerir o risco de fraude e corrupção é do gestor, em conjunto com a unidade de gestão de risco e a função antifraude e anticorrupção, quando existentes. No entanto, a auditoria interna pode dar recomendações quanto aos riscos identificados, sua probabilidade e impacto e quanto à adequação dos con-

52 Ver exemplo no Anexo 12 – Quesitos para avaliação do comprometimento da organização no combate a fraude e corrupção.

troles internos. Implica que os auditores internos tenham suficiente conhecimento sobre o negócio para avaliar o risco de fraude e corrupção[53].

Considerando a gestão de risco no plano de auditoria, a auditoria interna pode ajudar a detectar fraude e corrupção, mesmo em avaliações de adequação de controles. Um bom ponto de partida é o uso de indicadores de fraude (*red flags*[54]) adequados para o escopo da auditoria.

Conforme comentado na prática P2.6 – Implantar função antifraude e anticorrupção na organização, tanto a função antifraude e anticorrupção quanto a auditoria interna promovem avaliações acerca da implementação de controles de fraude e corrupção na organização, porém a função antifraude e corrupção faz parte da segunda linha de defesa e reporta-se à alta administração, e a auditoria interna faz parte da terceira linha de defesa, reportando-se tanto à alta administração quanto aos órgãos responsáveis pela governança, como conselhos de administração e de auditoria, permitindo, nesse último caso, maior independência para as suas avaliações.

- A auditoria interna faz parte da terceira linha de defesa, reportando-se tanto à alta administração quanto aos órgãos responsáveis pela governança, como conselhos de administração e de auditoria, permitindo, nesse último caso, maior independência para as suas avaliações.

Prática D3.2 – Avaliar a cultura e gestão da ética e da integridade

A auditoria interna deve, periodicamente, avaliar se a cultura e a gestão da ética e da integridade na organização estão sendo monitoradas pelo gestor, especialmente nos aspectos:

- da atualização dos códigos de ética e de conduta;
- da comunicação e divulgação regular e eficiente dos valores e princípios;

53 Os auditores internos devem possuir conhecimento suficiente para avaliar o risco de fraude e a maneira com o qual é gerenciado pela organização, porém, não se espera que possuam a especialização de uma pessoa cuja principal responsabilidade seja detectar e investigar fraudes. Norma 1210.A2 do Institute of Internal Auditors.
A atividade de auditoria interna deve avaliar o potencial de ocorrência de fraude e como a organização gerencia o risco de fraude. Norma 2120.A2 do Institute of Internal Auditors.
Os auditores internos devem considerar a probabilidade de erros significativos, fraudes, não conformidades e outras exposições ao desenvolver os objetivos do trabalho. Norma 2210.A2 do Institute of Internal Auditors.

54 Red flags é um conjunto de circunstâncias que são incomuns por natureza ou destoam da atividade normal. É um sinal de que algo está fora do normal e pode precisar ser investigado. Mas não indicam culpa ou inocência, apenas fornecem possíveis sinais de alerta de fraude (ISSAI 5530).

- do envolvimento dos servidores, alta administração, membros dos conselhos, beneficiários de programas, usuários de serviços públicos e fornecedores e do compromisso deles em seguir os preceitos estabelecidos;
- da atuação da comissão de ética em receber manifestações e adotar providências;
- da apuração e sanção dos desvios éticos e de integridade.

- *No contexto de crises financeiras, há interesse crescente na inovação, na qualidade da gestão, na necessidade de estimular a performance organizacional, na eficiência e na boa governança. A procura por* ***ligações causais entre ética e resultado organizacional*** *está também influenciando o debate acadêmico e profissional.* ***Se uma inequívoca conexão causal pode ser estabelecida entre resultado organizacional e ética e integridade, então isso vai ter significante e positiva implicação na justificativa de se auditar ética.*** *Prof. Christoph Demmke*

Prática D3.3 – Planejar e realizar auditorias e investigações de fraude e corrupção

O planejamento de auditorias consiste em elaborar um plano anual de atividades para a auditoria interna. Nesse plano, deve-se incluir auditorias para avaliação de controles e da execução das atividades da organização, delimitando o objetivo e o escopo, definindo a estratégia metodológica a ser adotada e estimando os recursos, os custos e o prazo necessários à sua realização.

A realização de auditorias para avaliação de controles de fraude e corrupção requer que os auditores internos identifiquem e avaliem o risco de fraude e corrupção e reúnam evidências suficientes e adequadas para respaldar os achados e as conclusões da auditoria.

As auditorias devem ser realizadas para avaliar se os controles do gestor para mitigar riscos de fraude e corrupção são adequados e suficientes. O propósito da auditoria não é identificar casos de fraude e corrupção, mas o auditor deve estar preparado caso isso ocorra. Quando confirmado um indício de fraude ou corrupção, os auditores devem tomar medidas para garantir que os achados de auditoria sejam adequadamente respondidos de acordo com as suas competências e circunstâncias específicas.

Um entendimento da área e das atividades e operações auditadas propicia ao auditor identificar potenciais áreas de alto risco suscetíveis a fraude e corrupção e

elaborar procedimentos de auditoria compatíveis para esses riscos. Algumas das áreas mais comuns de alto risco são: aquisições, receitas, patrimônio, pessoal e transferências.

As investigações são planejadas e realizadas para apurar algum indício específico de fraude e corrupção. Podem ter origem no canal de denúncia, detectado por meio de análise de dados, demanda externa, provocada por uma auditoria ou outra origem. O propósito da investigação é confirmar os indícios, ou não, identificando responsabilidades e apurando o prejuízo.

As normas internas da organização devem definir a responsabilidade pelas investigações. A auditoria interna pode conduzir ou participar da investigação se esses normativos permitirem, mas é preferível que a função antifraude e anticorrupção realize as investigações (IIA, 2009).

Após a conclusão das auditorias e investigações, com o objetivo de verificar as providências adotadas e aferir seus efeitos, faz-se necessário acompanhar e monitorar o cumprimento das recomendações da auditoria, das ações de reparação de perdas e/ou punitivas propostas, bem como dos resultados delas advindos.

Prática D3.4 – Estabelecer uma sistemática de divulgação de relatórios que tratam de fraude e corrupção

Deve-se definir uma sistemática formal para divulgação de relatórios que tratam de assuntos sensíveis, como a fraude e corrupção, com o objetivo de que as informações apuradas sejam adequadamente ajustadas e orientadas para os destinatários apropriados, como a polícia judiciária, o ministério público, os tribunais de contas e as controladorias gerais. Deve-se adotar as devidas cautelas na elaboração e encaminhamento desses relatórios a fim de se preservar a integridade das evidências obtidas, garantir a confidencialidade dos dados e evitar expor os auditores, investigadores e investigados a uma situação de fragilidade.

4. INVESTIGAÇÃO

A investigação tratada nesse mecanismo não é a mesma realizada pela polícia judiciária (polícia civil e polícia federal) ou pelo ministério público. Aqui se refere à atividade administrativa promovida pela própria organização com o objetivo de buscar informações relevantes para esclarecer um incidente específico de fraude e corrupção. Nos normativos legais e na prática das organizações, a investigação é comumente chamada de "investigação preliminar"[55], "sindicância investigativa"[56] ou simplesmente "apuração", mas para fins deste referencial será chamada apenas de "investigação".

A investigação refere-se a procedimento preliminar sumário, instaurado com o objetivo de investigar irregularidades cometidas no emprego, cargo ou função ocupada e destinado a elucidar possível cometimento de infração disciplinar, cuja apuração seja de interesse superior ou segundo decisão de autoridade da organização.

Por se tratar de procedimento de cunho meramente investigativo, que não podem dar ensejo à aplicação de penalidades disciplinares e que são realizados a título de convencimento primário da organização acerca da ocorrência ou não de determinada irregularidade funcional e de sua autoria, as investigações possuem as características de serem sigilosas, meramente investigativas, não punitivas e prescindem a observância do contraditório e da ampla defesa. Pode-se considerar três tipos de investigação:

Sindicância investigativa, ou chamada de preparatória ou inquisitorial[57]: trata-se de um procedimento preliminar sumário, instaurado com o fim de investigar irregularidade disciplinar que serve de alicerce ao processo administrativo disciplinar. Não há prescrição de um rito próprio e preestabelecido em todos os detalhes para a sua instauração, podendo adotar, extensivamente, no que for cabível, rito e prazos da sindicância acusatória. Pode ser instaurada por qualquer autoridade administrativa.

55 Pelo inciso I do art. 4º da Portaria CGU 335/2006 – "investigação preliminar: procedimento sigiloso, instaurado pelo Órgão Central e pelas unidades setoriais, com objetivo de coletar elementos para verificar o cabimento da instauração de sindicância ou processo administrativo disciplinar".

56 Não confundir com a sindicância prevista na Lei 8.112/1990, que por ser medida punitiva prevê ampla defesa. Será tratada no mecanismo de correção.

57 Manual de processo administrativo disciplinar – CGU. Não se encontra elencado expressamente na Lei 8112/90, cuja existência formal está prevista, além do disposto na doutrina e jurisprudência, no inciso II do art. 4º da Portaria CGU 335/2006.

Sindicância patrimonial[58]**:** desempenha papel de destaque na apuração das infrações administrativas potencialmente causadoras de enriquecimento ilícito do agente público, na medida em que, mediante análise da evolução patrimonial do agente, poderão ser extraídos suficientes indícios de incompatibilidade patrimonial capazes de instruir a deflagração do processo administrativo disciplinar e na propositura da ação de improbidade administrativa.

Com vistas à colheita dessas informações, a comissão investigante poderá se valer de diversas fontes de consulta, como cartórios de registros imobiliários, cartórios de registros de títulos e documentos, departamentos de trânsito, juntas comerciais, capitania de portos, entre outros, inclusive de outros entes da federação.

Poderá, também, solicitar o afastamento dos sigilos fiscal e bancário do servidor investigado. Caberá à comissão solicitar à procuradoria integrante da Advocacia-Geral da União competente o ajuizamento de processo de afastamento de sigilo bancário e fiscal perante o órgão judiciário, devendo, para esse fim, demonstrar a necessidade e a relevância da obtenção dessas informações para a completa elucidação dos fatos sob apuração no bojo da sindicância patrimonial.

Sindicância celetista: trata-se de um procedimento de apuração preliminar, aplicável para empregados de empresas estatais regidos pelo regime celetista, destinado a elucidar possível cometimento de infração disciplinar (BRASIL, 2015c).

Essa sindicância meramente investigativa constitui-se em relevante instrumento informativo, capaz, inclusive, de apresentar à autoridade competente indícios de materialidade e autoria da possível infração disciplinar.

Portanto, é aconselhável que, antes de aplicar a penalidade, a empresa faça uma sindicância, tomando por escrito as informações dos empregados envolvidos e das testemunhas.

Ressalte-se que a obrigatoriedade de praticar tal procedimento está condicionada à expressa previsão em normativo da empresa ou acordo/convenção coletiva de trabalho.

É o regimento interno da empresa que deve estabelecer quem é competente para dar início a esse procedimento disciplinar. Não havendo previsão expressa, os dirigentes da empresa, ou seja, aqueles que exercem o poder empregatício, contratando e demitindo funcionários, têm competência para instaurar sindicância em face de seus subordinados.

---

58 Manual de processo administrativo disciplinar – CGU. Tipificada no inciso VII do art. 9º da Lei de improbidade administrativa (Lei 8.429/92), possuindo previsão normativa no Decreto 5.483/2005, inciso IV do art. 132 e art. 143 da Lei 8112/90 e na Portaria CGU nº 335/2006.

Em resumo, o propósito primário da investigação é coletar informações para subsidiar qualquer ação subsequente, seja na esfera administrativa, civil e penal. Entretanto, outros efeitos decorrem da realização de investigações, tais como cessar a fraude e corrupção em andamento ou dissuadir a sua prática e reforçar controles internos. O mecanismo "investigação" é composto de três componentes: pré-investigação, execução da investigação e pós-investigação.

Mecanismo – Investigação
Componente I1 – Pré-investigação
Prática I1.1 – Desenvolver plano de resposta à fraude e corrupção
Prática I1.2 – Realizar avaliação inicial do incidente
Prática I1.3 – Estabelecer equipe de investigação
Prática I1.4 – Estabelecer parcerias com outras organizações
Componente I2 – Execução da investigação
Prática I2.1 – Desenvolver plano de investigação
Prática I2.2 – Estabelecer a confidencialidade da investigação
Prática I2.3 – Investigar e responder os atos de fraude e corrupção
Prática I2.4 – Realizar entrevistas eficazes
Prática I2.5 – Examinar documentos
Componente I3 – Pós-investigação
Prática I3.1 – Revisar controles internos após a ocorrência de uma fraude e corrupção

I1 – Pré-investigação

A organização deve considerar que, inevitavelmente, poderá ser vítima de fraude e corrupção a qualquer momento. Por isso não se deve esperar que uma fraude e corrupção ou indício delas ocorra para estruturar uma resposta a ela. Essa estrutura deve estar pronta, requerendo apenas seu acionamento quando necessário. Tentar estruturar respostas em tempo de crise, com pressões políticas, da mídia e da sociedade, abre espaço para atropelos e futuras impugnações por erros cometidos.

A principal medida é ter o plano de resposta à fraude e corrupção elaborado. A partir dele, estrutura-se qualquer investigação a partir da necessidade de apuração de ocorrências em potencial.

Prática I1.1 – Desenvolver plano de resposta à fraude e corrupção

Consiste em estabelecer e manter um plano de resposta para quando uma possível fraude e corrupção for detectada. A existência desse plano é importante para assegurar que a organização responda a suspeita de uma fraude e corrupção eficientemente, o que significa de forma apropriada e tempestiva. O plano inclui as ações que a organização tomará quando a suspeita surgir. Como cada fraude e corrupção pode ser diferente, no plano não deve constar como a investigação específica deve ser conduzida, mas como ajudar a organização a gerenciar a sua resposta, minimizar os riscos e maximizar o potencial de sucesso.

O plano permite que a gestão responda à fraude e corrupção denunciada ou detectada de forma consistente e compreensiva. A existência do plano também contribui com a prevenção, pois passa a mensagem de que a gestão leva a sério o combate a ocorrência de fraude ou corrupção. O plano deve guiar as ações necessárias quando a potencial fraude ou corrupção é reportada ou identificada. O plano deve ser o mais simples possível para que seja facilmente entendido e gerido em situações de pressão e urgência. O plano de resposta deve contemplar:

- protocolo de denúncia: uma vez que uma fraude e corrupção é reportada no canal de denúncias, deve haver um procedimento que notifique as partes interessadas e, dependendo da natureza e severidade das alegações, dispare ações que escalem a notificação para as instâncias apropriadas;
- instalação de equipe de resposta: em geral, os incidentes devem ser examinados pelo gestor da atividade, mas fatores de risco podem fazer que uma equipe de resposta independente da atividade em que ocorreu a suspeita de fraude e corrupção seja necessária e uma investigação instaurada. Esses fatores podem ser a credibilidade da alegação, tipo de incidente, sua severidade e potencial negativo, a probabilidade de judicialização e histórico de eventos similares. A equipe deve ser composta por pessoas com competência para examinar a natureza da fraude e corrupção;
- resposta tempestiva: o tempo é crítico para a resposta ao incidente. O gestor e a equipe de reposta devem estar preparados para lidar com inúmeras questões em pouco tempo e sob condições adversas. A equipe de reposta deve responder as seguintes questões: É necessária uma investigação? Requer apoio da auditoria interna, da função

antifraude e anticorrupção ou da corregedoria? A polícia e/ou órgãos reguladores precisam ser imediatamente envolvidos? É necessário aconselhamento jurídico? Há necessidade de apoio de especialistas externos? Qual estrutura física de apoio é necessária? Qual estratégia adequada de comunicação com a mídia?;

- endereçar problemas imediatos: emitir ordem aos servidores para sustar qualquer destruição de documentos físicos e eletrônicos para a sua preservação. Por documento entende-se contratos, faturas, correspondência, relatórios, apresentações, e-mails, mensagens de telefone, ofícios, registros médicos etc. Para documentos eletrônicos, a área de TI deve ser contatada para providenciar essa sustação;
- identificação de quem deve ser informado: dependendo do incidente, vários setores podem ter interesse na fraude e corrupção e devem ser informados. Por exemplo, o setor jurídico, o setor de recursos humanos, a corregedoria, a auditoria interna, função antifraude e anticorrupção, o setor de segurança patrimonial, o setor responsável pela gestão de risco etc. Entretanto, a informação do incidente deve ser compartilhada apenas com as partes afetadas.

Prática I1.2 – Realizar avaliação inicial do incidente

A avaliação inicial conduzida pelo gestor e a equipe de resposta deve considerar se, a partir das informações iniciais disponíveis, deve-se ou não iniciar uma investigação. A avaliação deve ser rápida, e a organização deve ter em vista um prazo que julgue compatível.

Para essa avaliação deve ser conhecido o contexto (a maneira e a data que se conheceu a suspeição, as áreas suspeitas, a fonte da informação) e a natureza da denúncia (é verossímil?; quem é o sujeito da denúncia e qual a sua relação com a organização?; quando ocorreu a conduta alegada e como?; quão grave é a denúncia?; qual a hierarquia dos servidores envolvidos, é possível a denúncia ser maior do que o esperado?; pode ter impacto para os clientes dos serviços prestados?; quem detém informação para suportar ou refutar a denúncia?; há terceiros se beneficiando do denunciado?).

Pode-se entrar em contato com o denunciante, se seus dados estiverem disponíveis, para extrair mais informações, por exemplo: como ficou sabendo da ocorrência, se há outras testemunhas, a sua motivação etc. A partir da entrevista pode-se avaliar a credibilidade da denúncia.

A decisão por investigar ou não deve ser formalizada pela equipe de resposta contendo a motivação da decisão.

Prática I1.3 – Estabelecer equipe de investigação

Uma vez definida necessidade da investigação, uma equipe deve ser montada, conforme as competências necessárias para a compreensão dos indícios, inclusive com especialistas externos, se for necessário. Para o sucesso da investigação, as características dos membros devem ser favoráveis ao trabalho em equipe. Deve-se considerar, também, o tamanho da equipe, se há conflito de interesse entre membros internos e externos e a necessidade de independência dos membros. Os membros devem firmar termo de confidencialidade para assegurar o sigilo da investigação e respaldar contrapressões por informação de algum superior imediato de membro da equipe ou de superiores em geral que não fazem parte da equipe. À equipe de investigação devem ser delegados os poderes para examinar, requerer e copiar documentos físicos e eletrônicos e acessar instalações da organização que estejam no âmbito da investigação.

Um líder deve ser escolhido para a equipe. Esse líder deve ter experiência em investigação, ser independente da atividade afetada, ter autoridade suficiente para recrutar novos recursos, acesso à alta administração e preferencialmente hierarquia superior aos investigados.

Para a seleção dos integrantes da equipe de investigação, a organização deve manter um grupo de servidores previamente capacitados na condução de investigação para que estejam disponíveis para integrá-las se necessário. Esse grupo de servidores geralmente é oriundo da função antifraude e anticorrupção, nos casos da sua existência, da auditoria interna ou da corregedoria.

Prática I1.4 – Estabelecer parcerias com outras organizações

A organização deve procurar estabelecer parcerias com outras organizações com o objetivo de obter subsídios para garantir que a investigação da fraude e corrupção seja realizada com as melhores condições possíveis.

O estabelecimento de parcerias colaborativas favorece a implementação mais efetiva de estratégias de prevenção, detecção, investigação e correção de fraude e corrupção.

A parceria deve envolver órgãos congêneres, tribunais de contas, ministério público, polícia judiciária, associações empresariais, entidades de combate a fraude e corrupção, fornecedores e prestadores de serviço, entre outros, com os quais pode-se compartilhar informações sobre riscos e esquemas de fraude e corrupção, boas práticas ou lições aprendidas relacionadas ao tema.

Fraudadores e corruptos podem estar agindo em várias organizações simultaneamente, por isso a parceria com outras organizações permite ganho de escala, a identificação de riscos comuns, troca de experiências e informações e maior possibilidade de obtenção de evidências.

I2 – Execução da investigação

A execução da investigação é ir a campo para verificar a ocorrência da fraude e corrupção, a sua extensão, identificar responsáveis, determinar prejuízos e coletar evidências por meio de técnicas investigativas.

Prática I2.1 – Desenvolver plano de investigação

A equipe de investigação deve, em conjunto, elaborar um plano de investigação. Cada caso deve ter um plano específico, mas em linhas gerais o plano deve conter:

- revisão das informações existentes sobre o caso para nivelamento de conhecimento entre os membros;
- definição dos objetivos da investigação: apesar de os objetivos em geral serem determinar se houve a fraude ou corrupção e quem a realizou, a investigação pode incluir outros objetivos, como prevenir outras perdas, assegurar evidências para ações disciplinares, administrativas, civis e penais, recuperar perdas, promover a cultura antifraude e anticorrupção pelo exemplo;
- definição de quem da organização, em geral da alta administração, deve ser mantido informado da evolução da investigação pela equipe;
- definição do escopo da investigação: com base nos objetivos definidos, determinar o nível de profundidade e abrangência da investigação, determinar se o limite é por assunto, por departamento ou territorial por exemplo, determinar se há restrições (tempo, recurso, legal ou operacional), determinar os níveis hierárquicos a serem investigados, determinar se o fato é isolado ou difuso;
- Determinar o cronograma da investigação com início e fim das atividades, os papéis de cada membro nas atividades e os produtos esperados. Além do tempo, o cronograma pode levar em consideração a área funcional e a atividade dos membros no sequenciamento das atividades. Esse cronograma deve ser ajustado ao longo da investigação sempre que fatos novos assim requererem.

Prática I2.2 – Estabelecer a confidencialidade da investigação

A investigação de fraude e corrupção deve ser orientada pelo sigilo. Se isso for negligenciado e detalhes se tornarem públicos, a investigação pode ser comprometida. Além disso, se detalhes da investigação são vazados, os servidores ficarão relutantes em realizar futuras denúncias, e suspeitas que se provarem infundadas também

podem prejudicar a imagem de pessoas investigadas. Além disso, se o denunciante for revelado poderá sofrer retaliação.

O gestor dos servidores que serão investigados deve ser avisado que suspeitos e testemunhas podem ficar ausentes de seus postos durante a investigação prestando informações. A quantidade de informação a ser compartilhada com o gestor dependerá das circunstâncias. Não se deve alertar todos os servidores da organização de que uma investigação será realizada, nem os seus propósitos.

O principal objetivo é evitar que o suspeito fique sabendo da investigação. Se isso acontecer, vários eventos adversos podem ocorrer e prejudicar o andamento da investigação. Por exemplo, o fraudador ou corrupto pode destruir ou alterar provas. Para evitar isso é bom tomar medidas, como conhecer a pessoa investigada e a que tipo de informações ela tem acesso, investigar fora do horário do expediente, agir rápido e discretamente no horário do expediente, reforçar as consequências de um vazamento e tomar declaração de confidencialidade dos entrevistados.

Para as reuniões da equipe e guarda de documentos eletrônicos e físicos coletados pela investigação, deve ser providenciada uma sala com acesso restrito apenas à equipe. Os documentos eletrônicos devem ser criptografados, e os físicos, tarjados de confidencial. Não se deve comentar sobre a investigação em público.

Prática I2.3 – Investigar e responder os atos de fraude e corrupção

Requer que os incidentes selecionados após avaliação inicial sejam investigados em tempo hábil, os responsáveis, punidos e as perdas, recuperadas. É importante a organização assegurar que as mesmas regras serão aplicadas a todos os níveis, incluindo a alta administração.

Os responsáveis pela investigação de fraude e corrupção devem assegurar que exista uma base suficiente e consistente para propor as ações corretivas:

- ação disciplinar – pode resultar na rescisão, demissão, suspensão, advertência ou aviso, bem como recomendação de medidas de gestão de pessoal ou de gerência administrativa;
- ação administrativa – a organização pode decidir por prosseguir a sua própria ação contra os autores para recuperar as perdas sofridas, por meio, por exemplo, da instauração de tomada de contas especial. Sanções podem ser aplicadas, tais como a multa, inabilitação para cargo público, declaração de inidoneidade para licitar ou contratar com a administração pública, declaração de inabilitação para assumir cargo público.
- ação judicial – a organização pode remeter o caso para a aplicação da lei. É desejável que um membro da alta administração, tal como

o consultor jurídico, autorize o encaminhamento do processo para a instância judicial.

- Releva destacar que na execução das ações corretivas deve-se considerar não só o valor do custo financeiro de recuperação, como também o valor de dissuasão e de percepção da integridade e da reputação da organização.

Prática I2.4 – Realizar entrevistas eficazes

Durante a investigação provavelmente será necessário ouvir pessoas para esclarecer os fatos. O investigador deve estar preparado para conduzir entrevistas tanto com suspeitos quanto com testemunhas. As entrevistas devem ser sequenciadas a partir das pessoas mais externas aos fatos, em geral testemunhas, até o principal suspeito, e das mais cooperativas às mais relutantes. A execução de uma entrevista envolve cinco etapas[59].

- Planejamento e preparação

O planejamento envolve pensar todas as etapas da entrevista para garantir que o entrevistador permaneça no controle da entrevista na direção certa e no tempo disponível. O entrevistador deve compreender o objetivo da entrevista e as circunstâncias prévias do incidente investigado. O bom entrevistador deve ter forte habilidade interpessoal e empatia e deve evitar ostentar autoridade.

No planejamento, além da definição do propósito da entrevista, o local da entrevista deve ser escolhido e preparado. O espaço físico da entrevista envolve o local, a disposição dos assentos e questões logísticas, como infraestrutura para apresentações, se necessário.

O bom entrevistador deve adotar postura investigativa, conduzindo a entrevista com objetividade, evitando fazer perguntas de maneira acusatória e induzindo o entrevistado a fornecer a informação voluntariamente.

- Engajamento e explicação

A fase de abertura é crucial para o sucesso de uma entrevista. Se o entrevistador puder envolver o entrevistado em conversa amistosa e descontraída, isso pode criar um clima favorável para que toda a entrevista transcorra relaxada. Cortesia, cordialidade e

59 Baseado no modelo *PEACE – Preparation and Planning, Engage and Explain, Account, Clarify and Challenge, Closure and Evaluation.*

compreensão devem ser empregados pelo entrevistador e podem fazer toda a diferença no resultado da entrevista. Entrevistadores de sucesso investem algum tempo para descobrir o que motiva os entrevistados e com isso extrair mais informações.

Nessa fase deve-se aproveitar para explicar algumas formalidades da entrevista, como possível gravação e outros procedimentos, a fim de desmistificar o processo e dar segurança ao entrevistado de que ele não será enganado. O entrevistado pode ser solicitado para comentar sobre questões que ainda não foram explicadas ou repetir com as suas próprias palavras alguma explicação já dada. O entrevistador pode repetir as palavras do entrevistado e verificar se o entrevistado entendeu corretamente.

Em qualquer fase da entrevista, a fim de garantir a equidade, o entrevistado pode ser encorajado a fazer perguntas ao entrevistador, caso haja algo que não entenda. O entrevistador pode usar a fase de engajamento como treinamento para a fase seguinte da entrevista, estabelecendo o controle e deixando o entrevistado pronto. O entrevistado será incentivado a responder uma pergunta simples, e o entrevistador aproveita para avaliar a capacidade de comunicação do entrevistado.

Uma vez que essa fase de engajamento passe, a testemunha será solicitada a dar a sua versão dos fatos. O entrevistador fará as perguntas para esclarecer a versão ou interromper quando alguma informação adicional é necessária.

- Relato

Nessa fase, o entrevistador obtém o relato completo dos eventos do entrevistado. As três etapas principais são: obtenção do relato do entrevistado sobre os eventos; expandindo e esclarecendo o relato; contestando o relato do entrevistado com outras informações (se necessário).

Boa capacidade de questionamento e audição é necessária para induzir um relato preciso e confiável. Durante o processo de relato, um entrevistado pode mudar de cooperativo para não cooperativo, por isso é importante para o entrevistador estar totalmente alerta durante a entrevista. O entrevistador deve ser capaz de detectar alterações na linguagem e no comportamento do entrevistado. Recomenda-se que os entrevistadores façam todas as perguntas relevantes, mesmo que a resposta seja "sem comentários" para que não haja lacunas na entrevista.

Depois que o entrevistado começar a dar o seu relato, o entrevistador pode usar técnicas de questionamento, resumindo o que foi dito, repetindo perguntas, variando as perguntas sobre as mesmas circunstâncias, variando as respostas anteriores do entrevistado para sugerir que ele já disse algo ou encorajar formas diferentes de se recordar dos mesmos fatos.

Ao final dessa fase, o entrevistador pode precisar esclarecer ou contestar o relato do entrevistado. Isso pode ser preciso, porque algo que o entrevistado disse não ficou claro para o entrevistador ou porque as informações são contraditórias com outras informações já conhecidas. Essa etapa pode envolver a contestação tanto de inconsistências no próprio relato, como incluir contestações pré-planejadas a partir de informações retidas, a fim de testar o que o entrevistado possa dizer na ausência de conhecimento de certos pontos-chave.

- Encerramento

A fase de encerramento deve garantir que o entrevistado compreenda o que aconteceu durante a entrevista, que as informações que ele deu são suficientes em todos os aspectos relevantes e que quaisquer áreas cinzentas tenham sido suficientemente esclarecidas.

O entrevistador deve confirmar que todos os aspectos do relato foram cobertos, permitindo que o entrevistado dê qualquer informação adicional que ele achar que pode ser relevante.

- Avaliação

Nessa última fase, o entrevistador deve rever as suas notas para ver se as metas e objetivos da entrevista foram alcançados. Além disso, o entrevistador também irá rever a investigação à luz das informações obtidas durante a entrevista e pode refletir sobre a eficácia da entrevista.

Prática I2.5 – Examinar documentos

Consiste em analisar documentos em busca de evidências da fraude e corrupção. Os investigadores devem estar atentos a falsificações, mesmo que não sejam peritos. Se algum documento for suspeito de ser falso, um perito documental deve ser providenciado.

É importante evitar manusear o documento original para preservá-lo, para isso devem ser utilizadas cópias. Os originais não devem ser dobrados, grampeados, presos por clips, nem riscados, para não criar indentações. Os investigadores devem saber os vários tipos de perícias possíveis para acioná-las se preciso, tais como: identificar assinaturas falsas; identificar o autor de assinaturas e manuscritos; alteração e supressão de documentos; detectar montagem de documentos; comparar tintas e papéis; identificar copiadora ou a impressora de origem, para acionar a perícia quando for relevante a verificação.

Outras falsificações dispensam perícia para serem identificadas. Por exemplo: os mesmos erros de grafia ou de cálculos, padrões idênticos de formatação e letra cursiva similares em documentos de fontes supostamente diferentes indiciam processos forjados.

É importante que haja o adequado registro e documentação das provas e evidências coletadas na investigação, de forma a assegurar a sua disponibilidade, confiabilidade e confidencialidade, uma vez que tais informações podem se tornar a base de futuros processos administrativos e judiciais. A transferência de custódia de documentos deve ser registrada para se manter rastreabilidade sobre quem os possuiu e para qual motivo.

Documentos eletrônicos também podem ser examinados. Se for assinado digitalmente, deve-se verificar a validade da certificação digital do emissor. Para documentos gerados pela internet, como certidões negativas, sua validade pode ser verificada no sítio da entidade emissora.

Documentos eletrônicos de qualquer natureza podem ser comparados com documentos que constam em outras fontes para verificar se são os mesmos ou se houve alguma alteração. Isso pode ser feito comparando-se o código *hash*[60] dos dois arquivos.

Para a realização de inspeção em meios eletrônicos em busca de evidências, há a necessidade de pessoal capacitado para identificar, recuperar, coletar, processar e preservar os dados digitais. Um perito digital pode recuperar, por exemplo:

- arquivos apagados;
- arquivos temporários salvos;
- lista de arquivos de impressos;
- sítios visitados;
- comunicação por meio de mensageiros digitais;
- documentos criados, modificados ou acessados;
- dados copiados, corrompidos ou movidos;
- data e hora de arquivos que foram criados, acessados, modificados, instalados, apagados ou baixados.

Um perito utilizará ferramentas que preservarão a fonte das evidências para que qualquer contestação de adulteração das evidências feita pelo suspeito em sua defesa não prospere tanto no processo administrativo quanto civil ou judicial.

---

60 A função *hash* quando aplicada sobre um arquivo gera um código único para cada tipo de arquivo. Se dois arquivos forem idênticos, apresentarão o mesmo código *hash*.

I3 – Pós-investigação

A execução da investigação se encerra com a elaboração do relatório de investigação. O relatório tratará das questões específicas da fraude e corrupção, mas pode trazer recomendações gerais para melhorar os controles internos. O resultado de toda investigação deve ser considerado como insumo nos processos da organização.

Prática I3.1 – Revisar controles internos após a ocorrência de uma fraude e corrupção

Consiste em fazer a revisão das políticas, estratégias, planos, gestão e controles de risco de fraude e corrupção na organização, com base nas provas reunidas e conclusões de eventual auditoria sobre o assunto. Deve-se considerar todos os registros de perdas identificados devido à fraude e corrupção, tais como entrevistas com investigados, depoimentos de testemunhas, evidências físicas, dados computacionais, bem como provas adicionais de terceiros, tais como serviços de perícia em geral.

Tais informações ampliam e melhoram a capacidade organizacional para prevenir e detectar novas ocorrências de fraude e corrupção.

5. CORREÇÃO

Se, mesmo com as práticas de prevenção e detecção implantadas, a fraude e corrupção ocorreram na organização, é imprescindível que medidas corretivas sejam tomadas. Essas medidas, além de promoverem a mitigação do dano e a devida sanção aos responsáveis no caso concreto, emitem, para servidores, beneficiários de programas, usuários de serviços públicos e fornecedores ou qualquer outra parte interessada da organização, a mensagem de que ela não se omite perante a fraude e corrupção.

Cada tipo de fraude e corrupção requer um procedimento apropriado. Por vezes, o mesmo ato fraudulento ou corrupto requer mais de um procedimento, haja vista que a aplicação da sanção disciplinar e a mitigação dos danos requerem procedimentos distintos e, inicialmente, independentes. Os procedimentos são, em geral, conduzidos pela corregedoria ou outro órgão com essa competência, conforme a natureza da organização.

O mecanismo de correção está estruturado em quatro componentes, sendo cada um localizado em uma esfera de correção. A sequência dos componentes é dada pelo potencial de gravidade do ilícito, consequentemente da gravidade da sanção. As práticas trazem os principais procedimentos existentes no ordenamento nacional, mas não são exaustivas, pois alguns procedimentos são específicos para algumas organizações e por isso não estão listados. Da mesma forma, nem todos os procedimentos mencionados servem para todas as organizações, pois a natureza jurídica da organização determina quais são os procedimentos aplicáveis.

O termo "correção" desse mecanismo significa corrigir o problema, mas não necessariamente aplicando medidas correcionais, aquelas que resultam em punição, pois algumas práticas listadas não têm essa característica.

As práticas aqui descritas não têm a pretensão de exaurir o assunto de cada procedimento, que naturalmente além de serem derivadas de algum diploma legal são afetadas pelas respectivas jurisprudência e doutrina.

A organização pode desejar evitar a atenção adversa da mídia ao divulgar os resultados das medidas correcionais, entretanto a transparência de informações em relação aos resultados dessas medidas contra a fraude e corrupção têm os seguintes benefícios:

- abordar questões éticas, que podem ser usadas como parte de um programa de sensibilização contra a fraude e corrupção;
- agir como um elemento dissuasor para os outros;

- demonstrar que medidas disciplinares são tomadas contra os responsáveis por fraudes e corrupção;
- demonstrar o compromisso da organização em ter uma cultura ética e de integridade e antifraude e anticorrupção.

Mecanismo – Correção
Componente C1 – Ilícitos éticos
Prática C1.1 – Procedimento ético preliminar
Prática C1.2 – Processo de apuração ética e de integridade
Componente C2 – Ilícitos administrativos
Prática C2.1 – Sindicância
Prática C2.2 – Processo administrativo disciplinar (PAD)
Prática C2.3 – Termo circunstanciado administrativo (TCA)
Prática C2.4 – Tomada de contas especial (TCE)
Prática C2.5 – Processo administrativo de responsabilização (PAR)
Componente C3 – Ilícitos civis
Prática C3.1 – Ação civil de improbidade administrativa
Prática C3.2 – Ação civil de improbidade empresarial
Componente C4 – Ilícitos penais
Prática C4.1 – Responsabilização penal

C1 – Ilícitos éticos

Os ilícitos éticos são a forma mais leve de infração que o servidor ou a parte interessada podem cometer. Por consequente, a sanção é branda, em geral, resumindo-se em aplicação de censura nos assentamentos. No entanto, a importância de se apurar e aplicar a sanção está na mensagem que se passa para todos na organização e fora dela. Além disso, grandes esquemas fraudulentos podem ter início a partir de pequenos desvios éticos que foram reiteradamente negligenciados. Assim, mais fácil do que apagar um grande incêndio é eliminar os focos de faíscas.

Prática C1.1 – Procedimento ético preliminar

Uma vez recebida pela comissão de ética alguma notícia, representação ou denúncia de transgressão ética, cabe, preliminarmente, a instauração de um proce-

dimento para averiguação dos fatos. O objetivo desse procedimento é confirmar a existência da transgressão e identificar a sua suposta autoria.

O procedimento inicia-se com a verificação de admissibilidade da demanda, que deve conter a conduta antiética cometida e elementos de prova ou indicação de onde podem ser encontrados. A existência de indicação de autoria é recomendada, mas não decisiva. Se admitida a demanda, prosseguirá a investigação com a coleta documental e, se conveniente, a oitiva do investigado. Com base no relatório produzido, a comissão decidirá se arquiva o processo, propõe um acordo de conduta com o investigado ou converte num processo de apuração ética.

Se decidido por um acordo de conduta e a proposta for aceita pelo investigado, fica o processo sobrestado por período definido em código de ética. Findo esse período, e se cumprido o acordo, o processo é arquivado. Se descumprido, é convertido em processo de apuração ética.

Prática C1.2 – Processo de apuração ética e de integridade

Instaurado o processo de apuração ética e de integridade, a comissão notificará o investigado para em prazo determinado, apresentar a sua defesa prévia por escrito, indicando os documentos e as testemunhas que suportem a sua defesa. Se o investigado se abstiver de apresentar defesa, um servidor deverá ser nomeado para defendê-lo.

Analisada a defesa prévia, o relatório deve ser elaborado, e o investigado, notificado para apresentar alegações finais em prazo determinado. Em seguida, a comissão deverá proferir a sua decisão, que pode ser pela censura, recomendação ou acordo de conduta.

Se houver indícios de que atos cometidos possuem repercussão na esfera administrativa, civil e penal, a comissão de ética deve encaminhar cópia do processo à autoridade competente para apuração, tais como departamento de recursos humanos, o setor jurídico ou o ministério público, sem prejuízo da adoção das medidas de sua competência.

C2 – Ilícitos administrativos

Engloba todas as infrações cometidas contra a lei que disciplina o cargo ou emprego e os regulamentos internos da organização. Tanto os procedimentos de apuração e responsabilização quanto as medidas punitivas são da alçada da própria organização, o que faz desses procedimentos um importante instrumento de correção da fraude e corrupção cometida.

Prática C2.1 – Sindicância

A sindicância punitiva ou acusatória: refere-se a um procedimento preliminar sumário, instaurado para apurar irregularidades de menor gravidade no serviço público, com caráter eminentemente punitivo, e que deve respeitar o contraditório, a oportunidade de defesa e o devido processo legal (BRASIL, 2006).

Em linhas gerais, quando a infração disciplinar apurada for punível com advertência ou suspensão por até 30 dias, pode ser utilizada a sindicância acusatória. Por outro lado, se a punição aplicável for suspensão por mais de 30 dias, a demissão, a cassação de aposentadoria, a disponibilidade ou a destituição de cargo em comissão impõe-se à instauração do processo administrativo disciplinar.

Assim sendo, a instauração da sindicância acusatória deve cingir-se às situações em que se tem preliminar convicção de que os fatos não são demasiadamente graves ao ponto de ensejar as penalidades para as quais a lei exige o processo administrativo disciplinar. Na dúvida, em sendo verificada eventual gravidade para os fatos, é recomendável a instauração de um plano do processo administrativo disciplinar.

Cabe destacar que se sujeitam a esse procedimento servidores públicos estáveis ou em estágio probatório em cargo efetivo, bem como ocupantes de cargo em comissão e de função comissionada. Não se sujeitam, notadamente, os agentes políticos, militares, particulares em colaboração com o poder público, temporários, terceirizados, celetistas, estagiários e consultores de programas internacionais.

Prática C2.2 – Processo administrativo disciplinar (PAD)

Trata-se de um instrumento legal para apurar, administrativamente, responsabilidade de servidor por infração praticada no exercício de suas atribuições, ou que tenha relação com as atribuições do cargo em que se encontre investido.

Uma vez comprovada a infração disciplinar pela própria organização, por meio de processo administrativo disciplinar, será possível a aplicação das seguintes sanções: i) advertência; ii) suspensão; iii) demissão; iv) cassação de aposentadoria ou disponibilidade; v) destituição de cargo em comissão; ou vi) destituição de função comissionada.

Conforme a Lei nº 8.112/90, o processo administrativo disciplinar pode ser submetido a rito ordinário ou sumário[61].

O processo administrativo disciplinar sob o rito ordinário se desenvolve nas seguintes fases: i) instauração, com a publicação do ato que constituir a comissão; ii) inquérito administrativo, que compreende instrução, defesa e relatório; e iii) julgamento.

---

61 Processo administrativo disciplinar sob o rito sumário comporta também a espécie sindicância acusatória (art. 145, II, da Lei nº 8.112/1990), comentado neste referencial, que trata do procedimento sobre sindicância.

Será conduzido por comissão composta de três servidores estáveis designados pela autoridade competente, que indicará, dentre eles, o seu presidente, que deverá ser ocupante de cargo efetivo superior ou de mesmo nível, ou ter nível de escolaridade igual ou superior ao do indiciado.

O prazo para a conclusão do processo disciplinar ordinário não excederá sessenta dias, contados da data de publicação do ato que constituir a comissão, admitida a sua prorrogação por igual prazo, quando as circunstâncias o exigirem.

O processo administrativo disciplinar sumário, por sua vez, é aplicável apenas quando da apuração dos seguintes ilícitos administrativos: acumulação ilegal de cargos, abandono de cargo e inassiduidade habitual.

Em linhas gerais, o rito sumário possui as seguintes especificidades: os prazos são reduzidos em relação ao rito ordinário, e a portaria de instauração deve explicitar a materialidade do possível ilícito. As provas a serem produzidas no processo sumário são, em tese, meramente documentais, pois para se verificar a ilicitude nesses casos não há necessidade de outras medidas probatórias.

O prazo para a conclusão do processo administrativo disciplinar submetido ao rito sumário não excederá trinta dias, contados da data de publicação do ato que constituir a comissão, admitida a sua prorrogação por até quinze dias, quando as circunstâncias exigirem.

A intenção do legislador ao estabelecer o processo sumário foi agilizar a averiguação das respectivas transgressões, que por envolverem apenas prova documental se processam mais rápido.

As penalidades disciplinares serão aplicadas: i) pelo presidente da República, pelos presidentes das Casas do Poder Legislativo e dos tribunais federais e pelo procurador-geral da República, quando se tratar de demissão e cassação de aposentadoria ou disponibilidade de servidor vinculado ao respectivo poder, órgão ou entidade; ii) pelas autoridades administrativas de hierarquia imediatamente inferior quando se tratar de suspensão superior a trinta dias; iii) pelo chefe da repartição e outras autoridades na forma dos respectivos regimentos ou regulamentos, nos casos de advertência ou de suspensão de até trinta dias; iv) pela autoridade que houver feito a nomeação, quando se tratar de destituição de cargo em comissão.

Em relação às empresas estatais, que podem ser empresas públicas ou de economia mista, não há na legislação trabalhista uma exigência para que se instaure um prévio processo administrativo disciplinar para a aplicação de penalidade aos empregados públicos. No entanto, não podem os respectivos gestores aplicar penalidades na ausência de provas da conduta infracional e com inobservância dos princípios do contraditório e ampla defesa, sob pena de sua invalidação, inclusive pela Justiça do Trabalho.

Nesse sentido, uma vez prevista em regulamento interno a necessidade de realização de prévio processo para a aplicação de pena disciplinar, a estatal não poderá dispensá-lo e aplicar sanção a um empregado, alegando que a legislação trabalhista não prevê essa garantia. Terá ela que realizar o procedimento previsto em seus regulamentos, sempre que verificar a necessidade de exercício do poder disciplinar.

As empresas estatais adotam uma espécie de procedimento disciplinar dividido em duas fases bem distintas: a primeira, de aspecto inquisitorial, na qual são produzidas as provas necessárias para a convicção da comissão responsável; e a segunda, em regra, formalizada por meio de instrumento no qual restará firmada a conclusão preliminar da comissão acerca da materialidade e autoria do fato sob apuração, ou seja, se ocorreu a irregularidade e quais os empregados envolvidos. Apenas na segunda fase do processo é estabelecido o contraditório, pois apenas nesse segundo momento a comissão tem condições de formalizar uma peça de acusação em desfavor dos envolvidos, facultando-lhes solicitar a produção de novas provas ou mesmo contestar aquelas levantadas previamente.

São três espécies de penas passíveis de serem impostas pela administração ao faltoso, aplicadas pela maioria das empresas estatais nos procedimentos disciplinares: i) advertência (verbal ou escrita); ii) suspensão; e iii) dispensa com justa causa.

Prática C2.3 – Termo circunstanciado administrativo (TCA)

Trata-se de instrumento que visa a apuração, mediante rito sumário, de casos de extravio ou dano a bem público, que implique prejuízo de pequeno valor que não justifique a instauração de procedimento de apuração conduzido por comissão. O TCA[62] só será utilizado quando o extravio ou o dano não for intencional, ou seja, não tiverem origem dolosa (BRASIL, 2015c).

Como parâmetro para classificar o prejuízo de pequeno valor, aplica-se o limite estabelecido para as hipóteses de dispensa de licitação, conforme o art. 24, II da Lei nº 8.666/93. Esse limite considera o valor necessário para repor o bem extraviado ou reparar o bem danificado. O TCA se aplica tanto para bens patrimoniados quanto bens sob guarda da organização.

O TCA deve ser autuado na forma de processo, não sendo necessária a publicação de ato de instauração e de designação de condutor, atribuição que recai sobre o chefe do setor responsável pela gerência de bens e materiais da unidade.

62 Instrução Normativa nº 4, de 17/2/2009. Decreto nº 5.483/2005. Acesso ao sítio da CGU: http://www.cgu.gov.br/sobre/perguntas-frequentes/atividade-disciplinar/procedimentos-disciplinares, em 26/4/2016.

O responsável deverá lavrar o TCA, descrevendo o fato, identificando o servidor envolvido, propiciando-lhe manifestação no processo em cinco dias. Ao final, o responsável deverá apresentar parecer conclusivo, com proposta de julgamento para o titular da unidade de lotação do servidor à época do fato, que poderá acatar ou não a proposta.

Entretanto, se, ao final do TCA, ficar demonstrado o dolo do servidor, ou se por ação culposa o servidor não quiser ressarcir o erário, a organização deve proceder ao Processo Administrativo Disciplinar.

Prática C2.4 – Tomada de contas especial (TCE)

Diante de fatos como a negativa de prestar contas de recursos transferidos a convênios, contratos de repasse, termo de colaboração e termo de fomento; o desvio de recursos financeiros ou bens públicos; ou de algum ato ilegal, ilegítimo e antieconômico que provoque dano financeiro, a organização deve tomar medidas administrativas imediatas para caracterização ou eliminação do dano, observados os princípios norteadores dos processos administrativos. Esgotadas as medidas administrativas sem a eliminação do dano, a organização deve, imediatamente, instaurar uma tomada de contas especial.

Tomada de contas especial (TCE) é um processo administrativo, com rito próprio, instaurado para apurar responsabilidade por ocorrência de dano à administração pública federal, com apuração de fatos, quantificação do dano, identificação dos responsáveis e obter o respectivo ressarcimento. Os responsáveis podem ser tanto pessoas físicas quanto jurídicas.

É importante o gestor competente instaurar a tomada de contas especial, pois a sua omissão implica na sua responsabilização solidária aos responsáveis pelo dano. E no curso de suas atividades, se a auditoria interna tomar ciência de algum desses danos, deve, formalmente, alertar a alta administração. Na omissão do gestor, o Tribunal de Contas (TC) respectivo pode determinar a sua instauração.

A tomada de contas especial deve ser encaminhada ao TC para julgamento e só não será enviada se o dano for ressarcido pelos responsáveis ou não for comprovada a ocorrência do dano.

Mas nem todo dano pode demandar uma tomada de contas especial. Pelos custos envolvidos na realização desse processo, apenas deve ser instaurado o processo para os danos que potencialmente ultrapassem o valor estabelecido pelo TC respectivo e se houver transcorrido menos de dez anos entre a data provável de ocorrência do dano e a primeira notificação dos responsáveis pela autoridade administrativa competente.

É muito importante a quantificação do dano para a imputação do débito aos responsáveis. Quando não for possível a verificação exata do real valor, deve-se esti-

mar, por métodos confiáveis, o valor mais justo possível. Sobre esse valor incidirá a atualização monetária e juros moratórios.

No caso de recurso federal, o processo da TCE deve ser encaminhado ao TCU com todas as peças necessárias em até 180 dias do término do exercício financeiro em que foi instaurada.

Prática C2.5 – Processo administrativo de responsabilização (PAR)

Se contra a organização foi praticado um ato lesivo por pessoa jurídica, cabe a instauração de um processo administrativo de responsabilização. A pessoa jurídica pode ser sociedade empresária ou simples, personificada ou não, e fundações, associações de pessoas ou entidades.

Por esse processo, a pessoa jurídica responde objetivamente por sua conduta, o que dispensa a prova de culpa para que seja responsabilizada pelo dano. Os atos lesivos que a Lei 12.846/2013 alude são, em geral, atos de corrupção contra a organização.

O processo deve ser instaurado pela autoridade máxima da organização ou, em caso de órgão da administração direta, do seu Ministro de Estado. Entretanto, antes da instauração, pode ser providenciada uma investigação preliminar. Essa investigação tem objetivo de apurar indícios de autoria e materialidade para subsidiar, por meio de relatório, a decisão da autoridade máxima pela instauração do PAR. Portanto, essa investigação será sigilosa, sem contraditório e terá caráter não punitivo.

Uma vez instaurado o PAR, uma comissão será designada para avaliar os fatos e circunstâncias conhecidas e intimará a pessoa jurídica para apresentar defesa. A comissão pode propor cautelarmente à autoridade máxima que suspenda os efeitos de ato ou processo objeto da investigação.

A responsabilização da pessoa jurídica é independente da responsabilização individual dos seus dirigentes, que responderão como pessoa física no processo devido.

Se a conduta da pessoa jurídica incluir infrações administrativas das normas de licitação e contrato, que também sejam condutas lesivas pela Lei 12.846/2013, o PAR também pode apurar essas infrações.

As sanções que podem ser aplicadas são a multa proporcional ao faturamento bruto, excluídos tributos, e a publicação extraordinária da condenação em veículo impresso, no sítio eletrônico e no estabelecimento da condenada. Além dessas sanções, são cabíveis as previstas na Lei 8.666/1993 quando constatadas as infrações previstas nessa lei. Essas sanções são declaração de inidoneidade para licitar ou contratar com a administração pública, suspensão, multa e advertência.

A instauração do PAR não afeta nem é prejudicada por outros procedimentos instaurados para ressarcimento integral do dano, como a TCE.

Se o relatório final do PAR verificar a ocorrência de eventuais ilícitos em outras esferas, deve ser encaminhado para o ministério público e para o órgão de representação judicial da organização.

C3 – Ilícitos civis

No caso de contratos administrativos de bens e serviços, na ocorrência de danos ao erário, existe a possibilidade de retenção de créditos a pagar e execução da garantia contratual para satisfazer o ressarcimento integral. No entanto, quando o dano exceder essas provisões ou não houver relação financeira com o responsável pelo dano, será necessária a via judicial para atingir esse objetivo, pois só essa via tem os meios coercitivos para se executar uma dívida.

Prática C3.1 – Ação civil de improbidade administrativa

Se servidores ou terceiros, pessoas físicas ou jurídicas, praticarem atos de improbidade contra a organização, caberá a ela promover medidas nos âmbitos administrativo e civil. Por improbidade entende-se todo o rol de condutas enquadradas na Lei nº 8.429/1992. No âmbito administrativo, a organização deve adotar os procedimentos disciplinares contra os servidores responsáveis pelos atos ímprobos. No âmbito civil, a organização deve ajuizar ação contra os servidores e terceiros, beneficiários diretos e indiretos do ato.

É importante observar que para as condutas ímprobas não cabe a responsabilidade objetiva. Além disso, exige-se a presença de dolo para os casos dos arts. 9º e 11 da Lei nº 8.429/1992, enquanto para o art. 10 basta a culpa.

A organização deve buscar o ressarcimento integral dos prejuízos sofridos ou que resultaram em enriquecimento ilícito para servidores ou terceiros. O prejuízo pode ter origem dolosa ou culposa, por ação ou omissão, de servidor ou terceiro.

Caso haja a participação de terceiro no ato de improbidade, é necessário identificar o servidor envolvido, pois não cabe ação exclusivamente contra o terceiro sem a presença de servidor no polo passivo da demanda.

Em caso de forte indício de responsabilidade, a organização pode requerer medida cautelar, na qual pedirá em juízo, por meio de sua procuradoria ou representando o Ministério Público, o sequestro dos bens do servidor ou terceiro para garantir economicamente o ressarcimento integral. Essa medida pode ser pedida sem que seja ouvida a parte adversa se houver risco de alienação, oneração ou dilapidação patrimonial de bens do acionado, dificultando ou impossibilitando o eventual ressarcimento futuro. A decretação de indisponibilidade de bens pode recair sobre aqueles

adquiridos anteriormente ao suposto ato e deve levar também em consideração o valor de possível multa civil como sanção autônoma.

As sanções que podem ser aplicadas são de ressarcimento integral do dano, perda dos bens acrescidos ilicitamente ao patrimônio, perda da função pública, suspensão dos direitos políticos, pagamento de multa e proibição de contratar com o poder público ou receber benefícios ou incentivos fiscais ou creditórios.

O ressarcimento não se limita ao prejuízo material, mas inclui multa e danos morais à organização ou a terceiros. No prazo de 30 dias da medida cautelar, a organização deve propor a ação principal com documentos ou justificação que contenham indícios suficientes da existência do ato de improbidade.

Se já estiverem prescritas as sanções decorrentes de atos de improbidade administrativa, ainda assim cabe o prosseguimento da demanda quanto ao pleito de ressarcimento dos danos ao erário, que é imprescritível (art. 37, parágrafo 5º da CF).

A responsabilização na esfera judicial não será possível se houver acordo de leniência previsto na Lei 12.846/2013, firmado entre a pessoa jurídica e a organização, com a participação da advocacia pública e do Ministério Público.

Prática C3.2 – Ação civil de improbidade empresarial

Além das sanções que a pessoa jurídica pode sofrer pelo processo administrativo de responsabilização, ela fica passível de ação civil para perdimento de bens, direitos ou valores que representem vantagem ou proveito, direta e indiretamente, obtidos da infração, suspensão ou interdição parcial de suas atividades, dissolução compulsória da pessoa jurídica e proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas e de instituições financeiras públicas ou controladas pelo poder público.

Essas sanções podem ser aplicadas de forma isolada ou cumulativa. Pode ser requerida indisponibilidade de bens, direitos ou valores para garantia do pagamento da multa ou da reparação integral do dano causado.

Assim como no item anterior, a responsabilização na esfera judicial não será possível se houver acordo de leniência firmado entre a pessoa jurídica e a organização, com a participação da Advocacia Pública e do Ministério Público.

C4 – Ilícitos penais

A infração ética, administrativa ou civil, pode ter repercussão também na esfera penal. Assim, independentemente de haver medidas nessas esferas, a autoridade

administrativa que tem conhecimento de indícios de crime ou contravenção também é obrigada a representar o Ministério Público[63].

Contudo, isso não impede qualquer procedimento realizado nessas esferas. Pelo contrário, a infração deve ser tratada em todas as esferas afetadas, pois cada uma apresenta um conjunto sancionador diferente.

Prática C4.1 – Responsabilização penal

O servidor público federal responde administrativamente, civil e penalmente pelo exercício irregular de suas atribuições. Essas responsabilidades possuem características próprias, sofrendo diferentes gradações conforme situações que podem se apresentar como condutas irregulares ou ilícitas no exercício das atividades funcionais, possibilitando a aplicação de diferentes penalidades, que variam de instância para instância.

Dessa forma, o cometimento de conduta irregular pode ensejar a responsabilização penal (criminal), que abrange crimes e contravenções imputadas ao servidor, nessa qualidade, sujeitando-o a responder a processo criminal e a suportar os efeitos legais da condenação.

Ademais, as sanções administrativas, civis e penais poderão se cumular, sendo independentes entre si[64]. Todavia, mesmo se confirmando, em princípio, a independência dessas instâncias, há situações em que, uma vez decididas no juízo criminal, repercutem necessariamente nas instâncias civil e administrativa.

Além disso, a absolvição penal que negue a existência do fato (infração) ou negue a autoria do servidor (não foi o servidor o autor do fato) implica o afastamento da responsabilidade administrativa e civil. Porém, a absolvição penal por insuficiência de provas não afasta a responsabilidade administrativa do servidor. Portanto, na hipótese de insuficiência de provas, mantém-se a punição administrativa.

As sanções variam de acordo com o grau de lesividade aos princípios e interesses administrativos, e os principais crimes funcionais contra a administração pública estão tipificados no Código Penal[65], sendo processados mediante ação penal pública incondicionada, proposta pelo Ministério Público perante o Poder Judiciário.

---

63 Art. 154 da Lei nº 8.112/1990: Os autos da sindicância integrarão o processo disciplinar, como peça informativa da instrução. Parágrafo único. Na hipótese de o relatório da sindicância concluir que a infração está capitulada como ilícito penal, a autoridade competente encaminhará cópia dos autos ao Ministério Público, independentemente da imediata instauração do processo disciplinar.
Art. 171 da Lei nº 8.112/1990: Quando a infração estiver capitulada como crime, o processo disciplinar será remetido ao Ministério Público para instauração da ação penal, ficando trasladado na repartição.

64 Art. 125 da Lei nº 8.112/1990: As sanções civis, penais e administrativas poderão cumular-se, sendo independentes entre si.

65 Crimes funcionais tipificados nos arts. 312 a 326, bem como nos arts. 359-A ao 359-H do Código Penal.

As sanções cabíveis, conforme o caso, podem ser de privação de liberdade, restrição de direitos ou multa[66].

Dentre os principais crimes praticados por servidores públicos contra a administração pública previstos na legislação, destacam-se:

- peculato: consiste em apropriar-se o funcionário de dinheiro, valor ou outro bem móvel, público ou particular, de que tem a posse em razão do cargo;
- concussão: ocorre quando o funcionário exige vantagem indevida, em razão do cargo;
- corrupção passiva: consiste na solicitação ou recebimento de vantagem indevida para a prática ou omissão de ato inerente à função;
- prevaricação: configura-se quando o funcionário retarda ou deixa de praticar, indevidamente, ato de ofício, para satisfazer interesse ou sentimento pessoal;
- advocacia administrativa: consiste em patrocinar interesse privado perante a administração pública, valendo-se da qualidade de funcionário;
- violação de sigilo funcional: ocorre quando o funcionário revela fato de que tem ciência em razão do cargo e que deva permanecer em segredo.

Cabe destacar que existem outras transgressões não relacionadas no Código Penal, mas que se configuram como crime. Nesse sentido, cita-se como exemplo a Lei de Abuso de Autoridade[67], que disciplina o delito de abuso de autoridade (ou abuso de poder). Merece mencionar, também, a Lei das Licitações e Contratos Administrativos, tendo em vista a tipificação de determinadas condutas consideradas criminosas[68].

Os prazos de prescrição previstos na lei penal aplicam-se às infrações disciplinares qualificadas como crime na Lei 8.112/1990. Assim, se o servidor cometer infração administrativa que configure também infração penal, não será punido administrativamente se ocorrer prescrição penal. O emprego irregular de recursos públicos, por exemplo, pela citada lei[69], é punível com demissão, cujo prazo prescricional é de 5 anos. No entanto, aplica-se o prazo de prescrição da lei penal, que é menor[70].

66 Art. 32, incisos I, II e III do Código Penal.

67 Lei nº 4898/1965.

68 Criminalização de condutas que atentam contra o princípio da Licitação Pública (arts. 89 a 98 da Lei nº 8.666/1993).

69 Art. 132, VIII, com art. 142, I da Lei nº 8.112/1990.

70 Prazo prescricional na forma do art. 109 do Código Penal.

6. MONITORAMENTO

M1 – Monitoramento contínuo

Ao longo da execução das práticas, os gestores responsáveis podem observar que ajustes devem ser realizados nas práticas e nos controles internos. Se o gestor detiver competência para reajustá-los, deve fazê-lo de imediato; se não, deve encaminhar o problema para quem tem essa competência. O importante é que, quando identificada, uma falha na prática ou controle interno que possa ser explorada por um fraudador ou corrupto seja rapidamente sanada. Isso só é possível se a atividade de monitoramento for contínua.

Para esse monitoramento, cada gestor responsável por implementar qualquer prática ou controle deve manter um painel de indicadores para subsidiar a sua decisão e da alta administração quanto à efetividade dessa medida.

Por exemplo, a gestão da ética e da integridade pode ser continuamente monitorada para verificar se:

- os códigos de ética e de conduta permanecem atualizados;
- a comunicação e divulgação dos valores e princípios têm sido regulares e utilizado os meios mais eficientes;
- os servidores, alta administração, membros dos conselhos, beneficiários de programas, usuários de serviços públicos e fornecedores têm recebido capacitação tempestiva e regular;
- a comissão de ética tem recebido manifestações e adotado providências;
- os casos de desvios éticos e de integridade têm sido apurados, e as sanções previstas, aplicadas.

Quanto aos controles preventivos e detectivos implementados, esses indicadores podem ser, mas não se limitando a:

- quantidade de servidores e partes interessadas capacitadas em conscientização antifraude e anticorrupção;
- quantidade de servidores que firmaram termo de compromisso;
- quantidade de áreas submetidas a gestão de risco;
- quantidade de riscos identificados e sua gravidade;
- quantidade de riscos mitigados;

- quantidade de risco residuais;
- quantidade de informações e dados disponíveis e taxa de acesso;
- quantidade de solicitação de acesso à informação e taxa de atendimento;
- comunicações realizadas;
- quantidade de notícias negativas na mídia;
- quantidade de medidas disciplinares instauradas;
- quantidade de esquemas fraudulentos e corruptos conhecidos e cometidos contra a organização;
- quantidade e natureza das denúncias recebidas pelo canal de denúncias;
- quantidade e natureza de fraude e corrupção apuradas, confirmadas e sanadas;
- recorrência da fraude e corrupção;
- a tempestividade na implementação de controles;
- quantidade de auditoria em fraude e corrupção realizadas pela auditoria interna;
- quantidade de investigações de fraude e corrupção;
- estimativa das perdas incorridas com a fraude e corrupção e a época em que foi cometida;
- *benchmarking*[71] com os dados de fraude e corrupção em organizações congêneres.

As deficiências relatadas devem ser consideradas no âmbito da gestão de risco de fraude e corrupção a fim de se verificar a necessidade de alguma alteração. O propósito desse monitoramento é assegurar que as práticas e controles internos estejam apropriados para as operações da organização e alcancem os objetivos para os quais foram estabelecidos.

M2 – Monitoramento geral

Implantar um plano abrangente de combate a fraude e corrupção exige atuação em diversas frentes na organização. Deve-se, efetivamente, envolver todas as atividades da organização, de forma que seja difícil a um observador externo discer-

71 *Benchmarking* consiste no processo de busca das melhores práticas numa determinada indústria e que conduzem ao desempenho superior. É visto como um processo positivo e através do qual uma empresa examina como outra realiza uma função específica, a fim de melhorar a forma como realiza a mesma função ou uma semelhante.

nir o que é a cultura e a gestão da organização das atividades de combate a fraude e corrupção implantadas.

Mas a organização, naturalmente, muda com o tempo. O ambiente externo, os objetivos da organização, a tecnologia disponível, o corpo de servidores, os fornecedores, vários fatores mudam ao longo da existência da organização. Assim como também mudam as fraudes e as corrupções realizadas contra a organização.

Isso significa que todo o arcabouço de práticas descritas neste referencial e implantadas na organização deve ser monitorado periodicamente. O monitoramento geral inclui a reavaliação de cada prática quanto à sua eficiência e eficácia e pode resultar no seu reforço, no seu abrandamento ou eliminação.

O monitoramento geral não se confunde com o monitoramento contínuo. É por meio do monitoramento contínuo que os gestores podem identificar e resolver precocemente incidentes. O monitoramento geral é uma reavaliação geral e periódica e deve considerar os resultados alcançados como um todo nas atividades-fim da organização para considerar como critério na avaliação do desempenho da política e plano de combate a fraude e corrupção vigentes.

Todas as práticas devem ser questionadas quanto à sua eficiência e eficácia. Dependendo de sua natureza e das mudanças ocorridas na conjuntura da organização, uma prática pode não ser mais pertinente, devendo ser eliminada. Uma prática que não cumpre o seu papel gera apenas esforço da organização, sem contrapartida alguma. Vale aqui a mesma análise de custo-benefício feita para os controles.

No entanto, requer atenção na avaliação da eficiência e eficácia da prática averiguar se houve por parte da organização o devido apoio para que a prática pudesse ter atingido os seus objetivos. Se a prática apenas constou como existente e nunca recebeu implementação ou fora de forma deficiente, não é possível, nesse caso, atestar a prática de ineficaz.

Se a prática foi parcialmente eficaz, e considerando que ela recebeu os meios necessários da organização para o seu exercício, é necessário avaliar o que mudou na conjuntura interna e externa da organização para reajustá-la ao novo cenário.

Pode não ter havido mudança alguma na conjuntura, do que se conclui que a eficácia parcial da prática decorre de algum desacerto na sua implantação original. Nesse caso, deve-se revisar a sua concepção, corrigindo as falhas e reforçando as fraquezas.

Como última possibilidade, caso a prática venha cumprindo o seu papel, cabe avaliar se seria possível manter a sua eficácia com algum relaxamento. Pode ser que a prática esteja superdimensionada, considerando as necessidades, provocando burocracia desnecessária. Se for este o caso, então algum alívio não prejudicaria a sua eficácia,

mas demandaria menos esforço da organização. Não significa que se deva descuidar dela, mas tentar elevar a eficiência utilizando menos recursos.

As alterações promovidas por essa reavaliação podem demandar capacitação de pessoal para atender às mudanças praticadas. Essa necessidade deve ser considerada para efetivação das práticas alteradas.

A periodicidade do monitoramento geral deve ser decidida pela organização, considerando a velocidade das mudanças que observa na sua conjuntura e a constatação de casos de fraude e corrupção que identifica. Outro requisito importante é que quem avalia o monitoramento geral precisa ter competência organizacional para determinar ou implantar as mudanças que forem necessárias, sob pena do monitoramento geral se tornar no seu propósito, que é readequar a organização para o combate da fraude e corrupção.

- Todas as práticas devem ser questionadas quanto à sua eficiência e eficácia. Dependendo de sua natureza e das mudanças ocorridas na conjuntura da organização, uma prática pode não ser mais pertinente, devendo ser eliminada. Uma prática que não cumpre o seu papel gera apenas esforço da organização, sem contrapartida alguma.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. *NBR ISO 31000*: Gestão de riscos – Princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

ACFE – ASSOCIATION FOR CERTIFIED FRAUD EXAMINERS. *Fraud Examiners Manual.* Austin, 2015. Disponível em: <http://www.acfe.com/products.aspx?id=4294986149>. Acesso em: 8 nov. 2016.

ANAO – AUSTRALIAN NATIONAL AUDIT OFFICE. Fraud Control in Australian Government Entities. Camberra, 2011. Disponível em: <https://www.anao.gov.au/work/better-practice-guide/fraud-control-australian-government-entities>. Acesso em: 8 nov. 2016.

BRASIL. Casa Civil. Decreto nº 5.483, de 30 de junho de 2005. Regulamenta, no âmbito do Poder Executivo Federal, o art. 13 da Lei no 8.429, de 2 de junho de 1992, institui a sindicância patrimonial e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5483.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Decreto nº 7.203, de 4 de junho de 2010. Dispõe sobre a vedação do nepotismo no âmbito da administração pública federal. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7203.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Exposição de motivos nº 37, de 18 de agosto de 2000. Código de conduta da Alta Administração Federal. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/codigos/codi_conduta/cod_conduta.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 8.429, de 2 de junho de 1992a. Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de

mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8429.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 8.443, de 16 de julho de 1992b. Dispões sobre Lei Orgânica do Tribunal de Contas da União e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8443.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 8.666, de 21 de junho de 1993a. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da administração pública e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8666cons.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 8.730, de 10 de novembro de 1993b. Estabelece a obrigatoriedade da declaração de bens e rendas para o exercício de cargos, empregos e funções nos Poderes Executivo, Legislativo e Judiciário, e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8730.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 12.813, de 16 de maio de 2013a. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo Federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei nº 9.986, de 18 de julho de 2000, e das Medidas Provisórias nº 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2013/Lei/L12813.htm>. Acesso em: 8 nov. 2016.

_____. Casa Civil. Lei nº 12.846, de 1º de agosto de 2013b. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Subchefia para Assuntos Jurídicos*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>. Acesso em: 8 nov. 2016.

_____. Controladoria-Geral da União. Portaria nº 335, de 30 de maio de 2006. Regulamenta o Sistema de Correição do Poder Executivo Federal, de que trata o Decreto nº 5.480, de 30 de junho de 2005. *Diário Oficial da União*. Disponível em: <http://www.cgu.gov.br/sobre/legislacao/arquivos/portarias/portaria_cgu_335_2006.pdf>. Acesso em: 8 nov. 2016.

_____. Controladoria-Geral da União e Ministério do Planejamento. Instrução Normativa Conjunta nº 1, de 11 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Disponível em: <http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.pdf>. Acesso em: 8 nov. 2016.

_____. *Normas de auditoria do Tribunal de Contas da União*. Brasília, DF: Tribunal de Contas da União, 2011.

_____. *Dez passos para a boa governança*. Brasília, DF: Tribunal de Contas da União, 2014a.

_____. *Guia de integridade pública*: orientações para a administração pública federal: direta, autárquica e fundacional. Brasília, DF: Controladoria-Geral da União, 2015a. Disponível em: <http://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/guia-de-integridade-publica.pdf>. Acesso em: 8 nov. 2016.

_____. *Manual de processo administrativo disciplinar*. Brasília, DF: Controladoria-Geral da União, 2015b.

_____. *Manual de direito disciplinar para empresas estatais*. Brasília, DF: Controladoria-Geral da União, 2015c.

_____. *Referencial b*ásico de *governança aplicável a órgãos e entidades da administração pública*. 2. ed. Brasília, DF: Tribunal de Contas da União, 2014b.

CRESSEY, Donald R. *Other People's Money*. Montclair: Patterson Smith, 1953.

COSO – COMMITTEE OF SPONSORING ORGANIZATIONS OF TREADWAY COMMISSION. *Internal Control*: Integrated Framework: Executive Summary. Durham, 2013.

EUROSAI – European Organisation of Supreme Audit Institutions. *Auditing Ethics in the Public Sector*. Espanha, 2014. Disponível em: <http://www.eurosai.org/handle404?exporturi=/export/sites/eurosai/.content/documents/working-groups/audit-ethics/RelDoc/TFAE_paper-Auditing-Ethics-in-Public-Sector.pdf>. Acesso em: 10 set. 2016.

FURTADO, Lucas Rocha. *As raízes da corrupção no Brasil*. Belo Horizonte: Fórum, 2015.

GAO – U.S. GOVERNMENT ACCOUNTABILITY OFFICE. *A Framework for Managing Fraud Risks in Federal Programs*. Washington, 2015. Disponível em: <http://gao.gov/products/GAO-15-593SP>. Acesso em: 15 abr. 2016.

IBGC – Instituto Brasileiro de Governança Corporativa. *Código das melhores práticas de governança corporativa*. Disponível em: <http://www.ibgc.org.br/userfiles/2014/files/CMPGPT.pdf>. Acesso em: 8 de nov. 2016.

IFAC – International Federation of Accountants. *Governance in the Public Sector*: a Governing Body Perspective. Disponível em: <http://www1.worldbank.org/publicsector/pe/April2003Seminar/Course%20Readings/08.%20Internal%20Control%20and%20Audit/Study_13_Governance.pdf>. Acesso em: 8 nov. 2016.

IIA – THE INSTITUTE OF INTERNAL AUDITORS. *Internal Auditing and Fraud*. 2009. Disponível em:<https://na.theiia.org/standards-guidance/Member%20Documents/Fraud_PG_FINAL__12-09-2009_.pdf>. Acesso em: 8 nov. 2016.

IIA – THE INSTITUTE OF INTERNAL AUDITORS. *Managing the Business Risk of Fraud*: a Pratical Guide. 2008. Disponível em: <https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf>. Acesso em: 8 nov. 2016.

_____. *Soft Controls*: What Are the Starting Points for the Internal Auditor? 2015. Disponível em: <https://www.iia.nl/SiteFiles/Publicaties/IIA_Bro%20A4%20Soft%20Controls%20Engels%2002.pdf>. Acesso em: 8 nov. 2016.

_____. *The Three Lines of Defense in Effective Risk Management and Controls*. 2013. Disponível em: <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>. Acesso em: 8 nov. 2016.

NAO – NATIONAL AUDIT OFFICE. *Tackling external fraud*. London, 2008. Disponível em: <https://www.nao.org.uk/wp-content/uploads/2013/02/Tackling_External_Fraud.pdf>. Acesso em: 8 nov. 2016.

PLUTARCO. *The Parallel Lives*: The Life of Solon. Harvard: Loeb Classical Library Edition, 1914. v. 1.

STANDARDS AUSTRALIA. AS 8001-2008: *Fraud and Corruption Control.* Sydney, 2008. Disponível em: <https://www.saiglobal.com/PDFTemp/Previews/OSH/AS/AS8000/8000/8001-2008.pdf>. Acesso em: 8 nov. 2016.

UNGC – UNITED NATIONS GLOBAL COMPACT OFFICE. *Guia de avaliação de risco de corrupção*. 2013. Disponível em: <https://nacoesunidas.org/rede-brasileira-do-pacto-global-lanca-guia-em-portugues-para-empresas-avaliarem-risco-de-corrupcao>. Acesso em: 10 maio 2016.

UN – United Nations. *United Nations Convention Against Corruption*. Disponível em: <https://www.unodc.org/unodc/en/treaties/CAC/>. Acesso em: 8 nov. 2016.

8. ANEXOS

Anexo 1 – Relação entre Coso e gestão de risco de fraude

Extraído de *Managing the Business Risk of Fraud: a Pratical Guide*, do IIA (2008).

Componente Coso	Gestão de risco de fraude
Ambiente de controle	• Estabelecer *tone at the top* adequado e cultura organizacional; • Documentar as estratégias de controle de fraude, código de ética e conduta, seleção de pessoal e normas de promoção; • Estabelecer, reforçar ou avaliar as funções da auditoria interna; • Desenvolvimento de currículo e promover treinamento; • Desenvolver uma política e metodologia para investigar o potencial de ocorrências de fraudes; • Investigação de denúnicas e suspeitas de fraudes; • Promover controles para prevenir, impedir e detectar a fraude; • Implementação e manutenção de um canal de denúncias.
Avaliação de risco de fraude	• Estabelecer processo de avaliação de risco de fraude que considere fatores de risco de fraude • e esquemas fraudulentos; • Envolver o pessoal adequado no processo de avaliação de risco de fraude; • Avaliações de risco de fraude em bases regulares.
Atividades de controle antifraude	• Definir e documentar controles mitigatórios e relacionado com os riscos de fraudes identificados; • Modificação de controles existentes, concepção e implementação de controles preventivos e detectivos e implementação de tecnologias de apoio.
Informação e comunicação	• Promover a importância do programa de gestão de risco de fraude e a posição da organização sobre o risco de fraude, tanto interna como externamente, através de programas de comunicação corporativa. • Conceber e fornecer treinamento de sensibilização para a fraude.
Atividade de monitoramento	• Fornecimento de avaliação periódica dos controles antifraude; • Usar avaliações independentes do programa de gestão de risco de fraude, auditoria interna ou de outras fontes; • Implementação de tecnologia para auxiliar no monitoramento e detecção contínua de atividades.

Anexo 2 – Exemplo de matriz para avaliação do recebimento de presentes

Extraído do *Guia de avaliação de risco de corrupção* da agência United Nations Global Compact Office (2013).

B. Matriz de pontuação do processo de rastreamento de presentes, hospitalidade e entretenimento

#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
1	A empresa rastreia presentes recebidos por seus funcionários?	3	3	Todos, independente do valor- 3, Alguns (por exemplo, acima do valor limite)- 2, Não- 1
2	A empresa rastreia entretenimento/ hospitalidade fornecida para os seus funcionários?	1	2	Todos, independente do valor- 3, Alguns (por exemplo, acima do valor limite)- 2, Não- 1
3	A empresa rastreia presentes fornecidos por seus funcionários para terceiros?	1	3	Todos, independente do valor ou beneficiário- 3, Alguns (por exemplo, acima do valor limite ou fornecido para certo tipo de beneficiário, por exemplo, funcionários de governo)- 2, Não- 1
4	A empresa rastreia entretenimento/ hospitalidade fornecida por seus funcionários para terceiros?	2	2	Todos, independente do valor ou beneficiário- 3, Alguns (por exemplo, acima do valor limite ou fornecido para certo tipo de beneficiário, por exemplo, funcionários de governo)- 2, Não- 1
5	Presentes, hospitalidade e entretenimento exigem aprovação antecipada?	2	2	Todos, independente do valor ou beneficiário- 3, Alguns (por exemplo, acima do valor limite ou fornecido para certo tipo de beneficiário, por exemplo, funcionários de governo)- 2, Não- 1

B. Matriz de pontuação do processo de rastreamento de presentes, hospitalidade e entretenimento				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
6	Se a resposta for SIM para a p5, essa solicitação de aprovação exige análise e aprovação por conformidade ou função legal? (Ou seja, quem analisa e aprova as solicitações do funcionário para presentes, hospitalidade e entretenimento?)	2.5	2	Sim, para todas as solicitações; 1-2 assinaturas de aprovação incluindo compliance ou jurídico exigidos- 3 Sim, para solicitações acima de um certo limite ou para tipos específicos de beneficiário; 1-2 assinaturas de aprovação necessárias, incluindo uma de compliance; outras solicitações precisam de uma assinatura de aprovação (ou seja, de um supervisor)- 2.5 Sim, para solicitações acima de um certo limite ou para tipos específicos de beneficiário; no mínimo duas assinaturas de aprovação necessárias, incluindo uma de compliance; para outras solicitações, nenhuma aprovação necessária- 2 1.5 Apenas acima de um certo limite ou para certos tipo de beneficiário, com uma assinatura de aprovação (por exemplo, supervisor de algum beneficiário)- 1.5 Não-1
7	Na ausência de aprovação formal antecipada para presentes, hospitalidade e entretenimento fornecidos para terceiros, o processo de rastreamento exige divulgação "retroativa"?	3	2	Todos, independente de valor -3, Alguns (por exemplo, acima de um valor limite)- 2, Não- 1
8	Na ausência de aprovação formal antecipada (ou quando a aprovação não foi solicitada), o processo de rastreamento exige divulgação "retroativa" para presentes e entretenimento recebidos de terceiros pelos funcionários?	3	2	Todos, independente do valor- 3, Alguns (por exemplo, acima do valor limite)- 2, Não- 1

B. Matriz de pontuação do processo de rastreamento de presentes, hospitalidade e entretenimento				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
9	O processo ou ferramenta exige ou permite a verificação de terceiros de acordo com a base de dados de "parte politicamente exposta" (PEP)?	3	1	Sim, exigido para todos os presentes, hospitalidade e entretenimento acima de certos limites (ou outros critérios), discricionários para outros- 2.5 Sim, discricionário apesar do critério- 2 Não- 1.
10	Para todos os presentes e entretenimentos fornecidos para terceiros, o processo exige ser pago com os fundos da empresa (por exemplo, cartão de crédito da empresa, ou seja, nenhuma despesa pessoal é permitida para negócios relativos a presentes, hospitalidade e entretenimento para clientes, fornecedores, parceiros de negócios, provedores de serviços e outras partes correlatas).	2	1	Sim- 3 Alguns, mas nem todos, ou algumas vezes mas não sempre- 2, Não- 1
11	O processo de rastreamento é automatizado e fácil de usar.	3	1	Sim- 3, Mais ou menos - 2, No- 1
12	O processo de rastreamento e os requisitos correlatos foram claramente comunicados a todos os funcionários relevantes.	3	2	Sim- 3, Mais ou menos - 2, No- 1
13	O processo de rastreamento permite rastreamento cumulativo por beneficiário e provedor de presente e entretenimento, além de sua empresa.	3	2	Sim- 3, Mais ou menos (por exemplo, presente oferecido mas não recebido, apenas presentes e não entretenimento, algumas unidades de negócios, mas não outras, etc.)- 2, Não- 1

B. Matriz de pontuação do processo de rastreamento de presentes, hospitalidade e entretenimento				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
14	O processo de rastreamento cobre toda a empresa?		2	Sim- 3, A maior parte da empresa - 2, Uma parte menor da empresa- 1
15	Há consequências disciplinares por não seguir o processo estabelecido?	1	2	Sim-3, Talvez- 2, Não- 1
16	O processo de rastreamento e as ferramentas associadas são avaliados periodicamente por eficiência?	1	2	Sim, periodicamente e com escopo/profundidade adequado- 3 Simcom pouca frequência e/ ou escopo limitado- 2 Não- 1
	PONTUAÇÃO PONDERADA TOTAL (escala de 1 a 3)			2.35

Anexo 3 – Exemplo de questionamentos quanto ao plano de combate a fraude e corrupção

A alta administração e alta gerência têm que constantemente fazer os questionamentos abaixo:

- Quem
  - » Quem analisa e avalia o plano de combate a fraudes?
  - » Quem não fez o treinamento de conscientização antifraude?
  - » Quem analisa os riscos de fraude em minha organização/programa?

- O quê
  - » Quais são os indutores de risco de fraude no nível da organização e de programas?
  - » Qual é o meu papel no controle da fraude?
  - » O que é uma resposta apropriada aos riscos de fraude na minha organização/programa?

- Quando
  - » Quando eu me envolvo nas estratégias de prevenção e detecção de fraude?
  - » Quando denunciamos fraudes na organização?
  - » Quando vamos analisar as atividades de fraudes?

- Onde
  - » Onde posso encontrar a política de antifraude da minha organização?
  - » Onde está a orientação sobre como denunciar fraudes na minha organização/programa?
  - » Onde posso consultar questões de fraudes graves e complexas?

- Por quê
  - » Por que a nossa organização/programa corre o risco de fraude?
  - » Por que a governança é tão importante para um controle eficaz da fraude?
  - » Por que os nossos riscos de fraude não foram revisados quando a nossa estrutura organizacional mudou?

- Como
  - » Como faço para garantir que os riscos de fraude estão contemplados na concepção do programa?
  - » Como eu sei que nossas estratégias de antifraude estão funcionando em minha organização/programa?
  - » Como a minha organização decide se uma suspeita de fraude será investigada?

Anexo 4 – Exemplo de matriz de avaliação da política anticorrupção

Extraído do *Guia de avaliação de risco de corrupção* da agência United Nations Global Compact Office (2013).

C. Matriz de pontuação da política anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante:1)	Guia de critérios de pontuação
1	A empresa tem uma política anticorrupção?	3	3	Sim, uma política única global ou uma combinação de políticas local e global- 3, Sim, políticas locais apenas onde necessário - 2, Sim, políticas locais apenas em alguns, mas não em todos os locais expostos-1.5, Não (se não, responda "não" para todas as perguntas abaixo)- 1
2	Qual é o formato da política?	3	2	Incluída no código de conduta mais um documento autônomo (mais detalhado- 3, Apenas incluída no código de conduta- 1
3	O conteúdo da política é adequada e suficientemente abrangente (ou seja, a política aborda todas as questões/tópicos pertinentes com detalhe suficiente)?	2	3	Sim- 3, Mais ou menos - 2, Não- 1 Observação: se a política só está disponível como um capítulo do código de conduta, veja se o conteúdo é suficientemente abrangente para comunicar as expectativas de comportamento.
4	A linguagem da política é clara, legível e consistente> É fácil de entender para o funcionário médio?	2	2	Sim- 3, Mais ou menos - 2, Não- 1
5	A política é bem organizada e estruturada?	2	2	Sim- 3, Mais ou menos - 2, Não- 1

C. Matriz de pontuação da política anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante:1)	Guia de critérios de pontuação
6	Qual é a posição da política sobre pagamentos de facilitação?	2	3	Não permitido, exceto nas situações de perigo de vida- 3, Geralmente não permitido, exceto quando houver permissão prévia, por escrito- 2.5, Geralmente permitido, em circunstâncias definidas, sem necessidade de permissão prévia, por escrito- 1.5 Permitido- 1 Indefinido - 1 Varia dependendo do local- 1.
7	Se houver versões da política local diferentes, elas são consistentes com a política corporativa, e/ou entre si em termos de padrões, conteúdo e apresentação?	2.5	1	Geralmente, sim- 3, Mais ou menos, mas algumas são mais restritivas que o padrão geral da empresa- 2.5, Mais ou menos, mas algumas são mais lenientes do que o padrão geral da empresa- 1.5, Não- 1 N/A já que temos uma única política global- 3
8	A política está disponível nas línguas onde a empresa opera?	3	3	Sim, em todos ou na maioria dos países onde a empresa opera, inclusive nos principais locais de risco- 3, Em alguns, mas não em todos os principais locais de risco- 2, Não- 1
9	A política é facilmente acessível na intranet da empresa por segmentos de funcionários relevantes?	3	2	Sim- 3, Mais ou menos- 2 Não- 1
10	A política tem sido bem comunicada para grupos de funcionários relevantes?	3	3	Sim- 3, Mais ou menos- 2 Não- 1

C. Matriz de pontuação da política anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante:1)	Guia de critérios de pontuação
11	Há um processo de confirmação da política que envolve funcionários relevante periodicamente (por exemplo, anualmente, ou a cada 2 ou 3 anos)?	3	2	Sim, todos os funcionários relevantes- 3, Alguns, mas não todos os funcionários relevantes- 2,Não- 1
12	A política é analisada e atualizada periodicamente (por exemplo, a cada 2 ou 3 anos)?	2	1	Sim- 3 Algumas, mas não todas, ou algumas vezes, mas não sempre - 2 Não-1
PONTUAÇÃO PONDERADA TOTAL (escala de 1 a 3)				2.25

Anexo 5 – Exemplo de plano de combate a fraude e corrupção

1. Súmario executivo
    a. Definição de fraude
    b. Compromisso com o combate a fraude e corrupção
    c. Código de conduta
    d. Relação do plano com outras políticas da organização
    e. Papéis e responsabilidades

2. Estratégia de combate a fraude
    a. Estabelecimento de função antifraude
    b. Responsabilidade pelos controles antifraude
    c. Responsabilidade de gestão de risco de fraude
    d. Conscientização contra fraude
    e. Prevenção da fraude

f. Detecção da fraude
g. Reportando a fraude
h. Investigação da fraude

3. Gestão de risco de fraude
    a. Programa de gestão de risco de fraude
    b. Revisão das estratégias e controles antifraude
    c. Avaliação da gestão de risco
    d. Implementação das propostas de ações

4. Procedimentos de notificação de fraude
    a. Implementação de canal de denúncia
    b. Análise das denúncias
    c. Sigilo dos denunciantes

5. Seleção de pessoal
    a. Verificação de antecedentes
    b. Capacitação antifraude

6. Conflito de interesse
    a. Normatização de situações de conflito
    b. Campanha de conscientização
    c. Análise das condutas identificadas ou comunicadas

7. Procedimento de investigação
    a. Plano de resposta à fraude
    b. Análise preliminar de notificação de fraude
    c. Estabelecimento de equipe de investigação

8. Estratégia da auditoria interna
    a. Plano de auditoria interna
    b. Revisão dos controles internos antifraude
    c. Detecção e apuração de fraudes

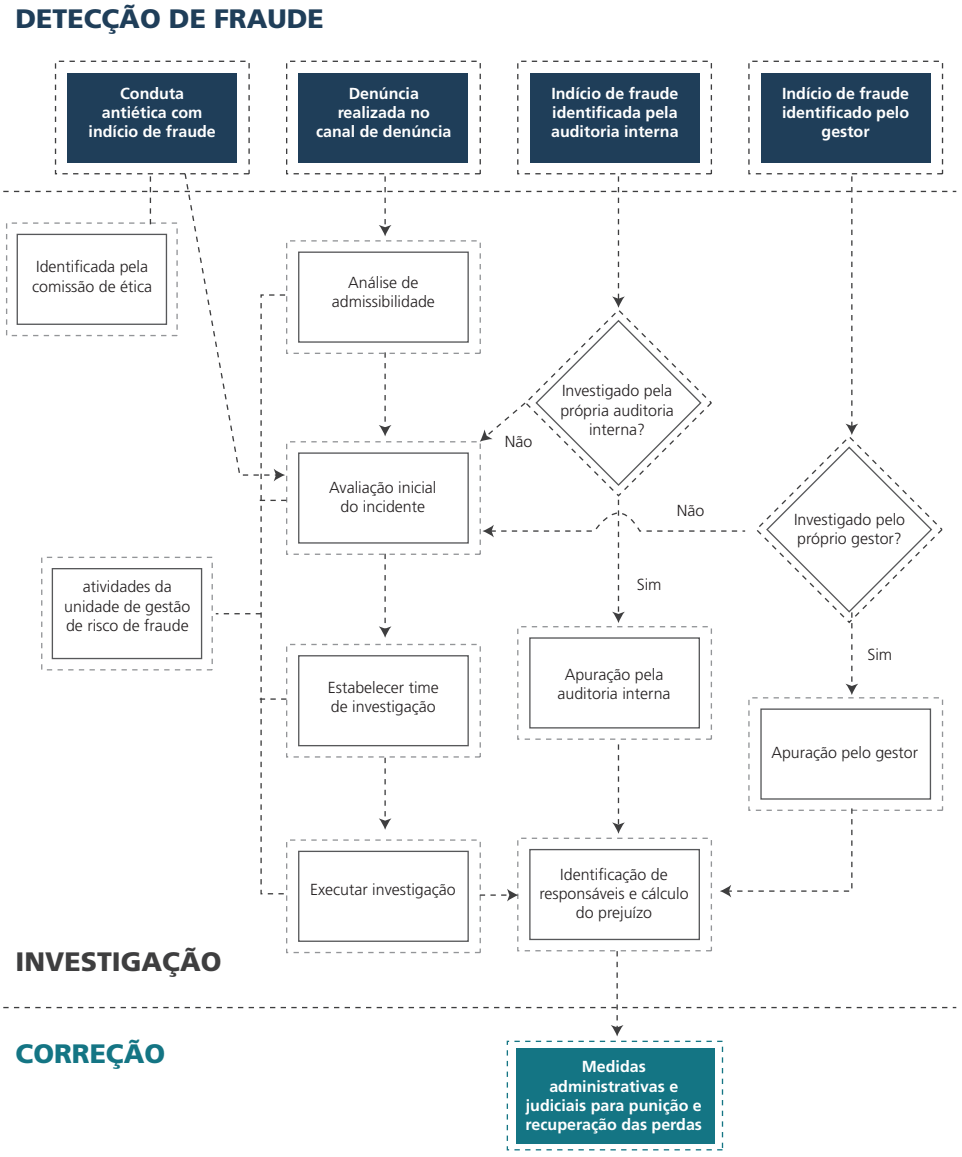
Anexo 6 – Exemplo de matriz de responsabilidade

Exemplo adaptado do Institute of Internals Auditors (2008).

Exemplo de Matriz de responsabilidade de plano de prevenção e combate a fraude e corrupção					
Ação Requerida	Unidade Antifraude	Auditoria interna	Alta administração	Comissão de ética	Setor financeiro
1. Controles preventivos	S	S	P		S
2. Notificação de incidente	P	S	S		S
3. Investigação de fraudes	P	S			
4. Recuperação de desvios					
5. Recomendações para prevenir fraudes	C	P	S		S
6. revisão de controles internos		P			
7. Publicidade e notas à impressa	S	S	S		
8. Controles preventivos	S	S	S	S	
9. Ações legais	S	S			
10. Ações corretivas	S	S	S		
11. Monitorar recuperação de desvios	S	S	S		P
12. Controles Detectivos	C	S	S		
13. Treinamento antifraude	P	S		C	
14. Análise de risco de vulnerabilidades	S	S			
15. Questões de ética	S	S	S	P	
16. Canal de denúncias	P	S		S	
17. Plano de respostas à fraude	P	S	S		
P - responsável primário S - responsável secundário C - responsabilidade compartilhada					

Exemplo de Matriz de responsabilidade de plano de prevenção e combate a fraude e corrupção					
Ação Requerida	Alta Gerência	Unidade de gestão de risco	Assessoria de comunicação	Jurídico	Recursos Humanos
1. Controles preventivos	C	S	S	S	S
2. Notificação de incidente	S	S	S	S	S
3. Investigação de fraudes	S				S
4. Recuperação de desvios	P			C	
5. Recomendações para prevenir fraudes	S	S	S	S	S
6. revisão de controles internos					
7. Publicidade e notas à impressa			P		
8. Controles preventivos	P	S			
9. Ações legais				P	
10. Ações corretivas	P	S			
11. Monitorar recuperação de desvios					
12. Controles Detectivos	P				
13. Treinamento antifraude					S
14. Análise de risco de vulnerabilidades	C	P			
15. Questões de ética					S
16. Canal de denúncias	S				
17. Plano de respostas à fraude					
P - responsável primário S - responsável secundário C - responsabilidade compartilhada					

Anexo 7 – Exemplo de fluxograma para tratamento de fraudes e corrupções



Anexo 8 – Exemplo de avaliação de risco de fraude e corrupção

Adaptado da proposta do Institute of Internal Auditors para uma avaliação de risco de fraude (2008).

Partindo-se do item "a", monta-se uma tabela na qual todos os demais itens são respondidos para cada risco de fraude identificado.

a. **Riscos de fraudes identificados**: deve incluir uma lista completa dos potenciais riscos e esquemas de fraudes que a organização possa sofrer. Essa lista será diferente para diferentes organizações e deve ser elaborada a partir de pesquisas setoriais, entrevistas com servidores e partes interessadas e histórico do canal de denúncia.
b. **Probabilidade de ocorrência**: para elaborar um programa de gestão de risco de fraude eficiente, é importante avaliar a probabilidade de cada um dos riscos de fraudes identificados para que a organização estabeleça controles antifraude adequados aos riscos que são mais prováveis. Para efeitos da avaliação, é adequado avaliar a probabilidade de riscos como remoto, razoavelmente possível e provável.
c. **Significância para a organização**: fatores quantitativos e qualitativos devem ser considerados para a avaliação da significância de risco de fraude para uma organização. Por exemplo, certos riscos de fraude podem representar apenas um irrelevante risco financeiro para a organização, mas pode indiretamente impactar consideravelmente a sua reputação e, portanto, seria considerado um risco mais significativo. Para efeitos de avaliação, deve ser suficiente avaliar a significância dos riscos como imaterial, significativo e material.
d. **Pessoas ou áreas sujeitas ao risco**: com os riscos de fraude identificados e avaliados, é importante avaliar quais as pessoas ou áreas, dentro e fora da organização, que estão sujeitas a esses riscos. Esse conhecimento vai ajudar a organização na sua resposta ao risco de fraude, incluindo o estabelecimento apropriado de segregação de funções, rotação de pessoal, hierarquia de aprovação e auditoria contínuas.
e. **Controles internos antifraude vigentes**: mapeamento dos controles pré-existentes aos riscos de fraude relevantes identificados. Note-se que isso ocorre depois que os riscos de fraudes são identificados e avaliados quanto à probabilidade e significância. Progredindo nessa ordem, esse modelo pretende que a organização avalie os riscos de

fraudes identificados inerentes ao negócio, ou seja, sem a consideração dos controles internos.

f. **Avaliação da efetividade dos controles internos**: a organização deve ter um processo para avaliar se os controles identificados estão funcionando de forma eficaz e mitigando os riscos de fraudes conforme previsto.
g. **Riscos residuais**: após o exame da estrutura de controle interno, a conclusão pode ser que certos riscos de fraude não estão sendo mitigados adequadamente por vários fatores, incluindo certos controles previstos não estarem implementados ou os controles operarem deficientemente. Esses riscos residuais devem ser avaliados pela organização no desenvolvimento da resposta ao risco de fraude.
h. **Resposta ao risco de fraude**: riscos residuais devem ser avaliados pela organização, e uma resposta ao risco de fraude deve ser proposta para endereçar cada risco residual. A resposta ao risco de fraude pode ser uma combinação de implementação de controles, auditoria contínua ou deixar atividade.

Anexo 9 – Exemplo de análise de risco de corrupção

Extraído do *Guia de avaliação de risco de corrupção* da agência United Nations Global Compact Office (2013).

Local/ região: país A **Unidade de negócio: negócio XYZ**			
Fator de risco de corrupção	Clima de negócios local		
Risco de corrupção	Suborno de funcionário público para garantir, reter ou influenciar uma decisão de negócios imprópria.		
Esquema de corrupção	a) Pagamentos potenciais impróprios para funcionários de alfândega para facilitar processos relativos a importação de produtos ou para liberar a importação de produtos ilegais.	b) Pagamentos potenciais impróprios para autoridades fiscais para garantir a redução ou eliminação de passivos fiscais.	c) Pagamentos potenciais impróprios para funcionários de governo para garantir uma parcela desejada de propriedade ou termos de arrendamento favoráveis.

Local/ região: país A **Unidade de negócio: negócio XYZ**			
Probabilidade	Média	Média	Média
Impacto Potencial	Alto	Alto	Alto
Risco Inerente	Alto	Alto	Alto
Controle anticorrupção	• Procedimentos e política global anticorrupção, incluindo conteúdo específico sobre pagamentos para alfândega • Treinamento anticorrupção para funcionários, desenhado especificamente para regiões selecionadas e funções essenciais • Linha direta de delação global • Auditorias anticorrupção anuais sobre pagamentos para funcionários da alfândega em regiões/ países selecionados	• Procedimentos e política global anticorrupção, incluindo conteúdo específico sobre pagamentos para autoridades fiscais • Treinamento anticorrupção para funcionários, desenhado especificamente para regiões selecionadas e funções essenciais • Linha direta de delação global • Auditorias anticorrupção anuais sobre pagamentos para autoridades fiscais	• Procedimentos e política global anticorrupção, incluindo conteúdo específico sobre pagamentos para funcionários de governo por arrendamentos de propriedade • Treinamento anticorrupção para funcionários, desenhado especificamente para regiões selecionadas e funções essenciais • Linha direta de delação global • Auditorias anticorrupção anuais sobre interações/ transações com funcionários de governo para garantir arrendamentos de propriedade
Classificação do controle de mitigação	Eficiente	Eficiente	Eficiente
Risco Residual	Baixo	Baixo	Baixo

Anexo 10 – Processo de avaliação de risco de fraude pela norma AS 8001-2008: Fraud and corruption control

Traduzido da norma AS 8001-2008: Fraud and corruption control (STANDARDS AUSTRALIA, 2008)

3.6.3 Processo de avaliação de fraude e risco de corrupção

3.6.3.1 *Metodologias de avaliação de fraude e risco de corrupção*

As entidades que exercem uma avaliação de fraude e risco de corrupção têm tradicionalmente usado uma das três metodologias alternativas seguintes:

(A) Avaliação independente dos processos e procedimentos, incluindo uma série de entrevistas individuais com o pessoal relevantes e revisão da documentação de controle interno.

(B) Um levantamento de fraude e risco de corrupção pela emissão e análise de um questionário adaptado para a entidade ou as unidades de negócios ou funções operacionais da entidade sendo avaliada.

(C) Uma oficina consultiva envolvendo o máximo de contribuições do pessoal da unidade de negócios que está sendo avaliada, em que uma "equipe de avaliação de risco" formada para cada unidade de negócios identifique e avalie os riscos relevantes para o negócio-unidade.

Essas abordagens sugeridas são coerentes com as orientações estabelecidas no HB 436:2004, que propõe as seguintes quatro metodologias alternativas para a identificação de risco organizacional:

(1) brainstorming em equipe.

(2) técnicas estruturadas, tais como gráficos de fluxo, revisão do projeto do sistema, análise de sistemas, Hazard e estudos de operabilidade (Hazop) e modelação operacionais.

(3) Para situações menos claramente definidas, tais como a identificação de riscos estratégicos,processos com estrutura mais geral como "what if" e análise de cenários podem ser usadas.

(4) Quando os recursos são limitados, uma abordagem mais flexível pode ter de ser utilizada por exemplo, concentrando-se em um menor número de elementos-chave ou usando uma abordagem-checklist.

A escolha da abordagem mais adequada (ou uma combinação de abordagens) dependerá de uma série de fatores, incluindo orçamento, disponibilidade de tempo dos participantes, urgência, restrições geográficas e estruturais.

Em relação a cada risco identificado, a AS/NZS 4360: 2004 requer que o processo de avaliação inclua: (i) avaliação preliminar dos riscos que foram identificados, a fim de considerar que riscos devem ser objeto de análise mais detalhada; (ii) a avaliação de processos, dispositivos existentes ou práticas (controles internos) que agem para minimizar os riscos; (iii) uma avaliação das consequências para a entidade, se tivesse ocorrido o risco; (iv) uma avaliação da probabilidade de ocorrência do evento no contexto das estratégias e controles existentes; e (v) uma estimativa do nível de risco através da combinação das consequências e probabilidades.

O objetivo final do processo de avaliação de riscos será uma compreensão dos riscos de fraude e corrupção que sofre a organização como uma base para desenvolver e implementar itens de ação que visam uma maior mitigação dos riscos.

A saída a partir de uma consideração desses parâmetros poderia ser um gráfico no formato mostrado na Apêndice B, em que cada risco é representado graficamente de acordo com a sua probabilidade relativa de ocorrência e consequência para a entidade, se tivesse ocorrido a fraude ou corrupção. Enquanto alguma forma de representação gráfica dos riscos identificados é considerada vantajosa, outros formatos além do mostrado no Apêndice B poderiam ser usados e seriam igualmente válidos.

3.6.3.2 *Etapas do processo de avaliação de risco*

Detalhes de cada um dos passos do processo de avaliação do risco, tal como estabelecido na figura, tendo em conta a aplicação particular do processo para a avaliação de risco de fraude e corrupção, como seguem:

(A) *Estabelecer o contexto*

Para uma avaliação de risco ser eficaz, ela precisa ser conduzida com uma completa consideração do contexto dentro do qual uma entidade opera. Isso envolverá obter da entidade uma compreensão de:

- contexto externo que defina a relação entre a entidade e o seu ambiente externo, incluindo a consideração da natureza das ameaças que enfrentam o entidade, motrizes da fraude e corrupção dentro da indústria e amplo ambiente no qual a entidade opera, e requisitos jurisdicional e regulamentar;
- contexto interno que proporcione uma compreensão da entidade, incluindo consideração da natureza do negócio, a sua cultura, as principais partes interessadas, incidentes de fraude e corrupção e tendências históricas, principais impulsionadores de negócios, os seus sistemas de informação e o funcionamento do seu ambiente de controle;

- contexto de gerenciamento de risco, que envolve a determinação do escopo, limites e parâmetros das atividades de gestão de riscos de fraude e corrupção a serem empreendidas;
- critérios de risco, pelo qual cada risco será avaliado para determinar se o risco pode ser tolerado ou irá necessitar de tratamento; e
- abordagem e estrutura para o resto da gestão de risco de fraude e corrupção a realizar processo.
- documentar o estabelecimento do contexto é uma boa prática empresarial que deve ser seguida sempre quando possível.

(B) *Identificar os riscos*

O objetivo da identificação de riscos é desenvolver uma lista de riscos de fraude e corrupção e suas fontes que poderiam ter um impacto potencial sobre a realização dos objetivos da entidade. Uma lista abrangente de riscos deve ser criada, independentemente de eles estarem sob o controle da entidade ou não. Tal lista é comumente referida como um registro de riscos, que deve ser documentado com detalhes suficientes para facilitar a posterior análise e futuras avaliações de fraude e corrupção.

Um número de abordagens pode facilitar grandemente uma melhor compreensão das fontes de riscos, incluindo:

- o mapeamento dos processos de negócios em consulta com os proprietários e "operadores" desses processos;
- definir um modus operandi plausível de potenciais incidentes de fraude e corrupção; e
- examinar os resultados de investigações anteriores de fraude e corrupção de dentro dos estudos de caso de entidade e de outras entidades.

(C) *Analisar os riscos*

A análise de risco é um mecanismo pelo qual uma melhor compreensão desses riscos é conseguida, em última análise, para facilitar a análise melhorada das opções de tratamento. A análise do risco envolve uma análise das consequências desses riscos e suas respectivas probabilidades em função da eficácia da gama de controles presentes.

Uma análise preliminar do risco pode ser realizada como um dispositivo de rastreio para eliminar o "baixo risco" e permitir que a atenção e os recursos se concentrem em riscos de nível superior para análise mais detalhada e profunda, que será geralmente iniciada com uma análise da eficácia dos controlos existentes na gestão

desses riscos identificados. A avaliação deve concluir, em relação a cada controle, se é ou possa vir a tornar-se:

- eficaz;
- parcialmente eficazes; ou
- ineficaz,
- na redução do risco de fraude ou corrupção relacionadas a eles.

Controles que devem ser considerados incluem qualquer um que pode afetar tanto a consequência ou a probabilidade do risco de fraude ou corrupção, tais como:

- requisitos e normas regulamentares;
- quadros de cultura e comportamento ético;
- políticas e práticas de governança;
- práticas de recrutamento, incluindo triagem prévia e em emprego;
- procedimentos operacionais-padrão;
- práticas de reconciliação, de garantia e de auditoria;
- práticas de segurança lógica e física, sistemas e infraestrutura;
- processos de relatórios de incidentes e investigação; e
- monitoramento e relatórios de gestão.

A avaliação de cada controle interno considerado não deve representar-se em termos de sua capacidade de mitigar o risco do negócio em geral. Pelo contrário, é uma avaliação do impacto percebido que o controle sobre a fraude específica ou risco de corrupção sob consideração.

Na realização da análise dos riscos, mede-se a consequência comumente com base no nível de perda financeira que poderia potencialmente ocorrer, o que pode ser classificado tanto para as perdas de um único incidente ou perdas acumuladas ao longo de um determinado tempo. No entanto, riscos de fraude e corrupção também podem dar origem a uma série de consequências não financeiras que também devem ser consideradas, incluindo regulatória, jurídica, segurança, desempenho dos negócios, confiança das partes interessadas, reputação, bem-estar pessoal e impactos morais. Por exemplo, um incidente de fraude ou corrupção poderia ter consequência financeira menor imediata, mas a longo prazo, uma significativa erosão do valor da marca.

A probabilidade de um evento de fraude ou corrupção é medida tendo em consideração a consequência de o risco ocorrer. O contexto determinará em grande parte a escala de probabilidade que deve ser usada. Por exemplo, uma tabela pode basear-se no

risco ao longo da vida da entidade, pela duração da presença da entidade em mercados ou locais específicos, ou sobre outros períodos de tempo definidos ou atividade.

Há uma série de outros fatores (geralmente específica para certos tipos de fraude e risco de corrupção) que pode ter um efeito sobre a probabilidade ou consequência que devem ser considerados, incluindo os seguintes:

Consequência para a entidade, se tivesse ocorrido o risco:

(1) O potencial valor de perda que seria sofrido pela entidade: a consequência de um incidente de fraude ou corrupção do tipo contemplado será tipicamente um impacto financeiro na entidade. A consequência financeira diretamente associada a fraude ou corrupção do tipo contemplado, se ocorreu, deve ser considerada em relação a todos os outros riscos enfrentados pela entidade (ou seja, não apenas limita-se ao impacto financeiro provável que surgir na relação de outros riscos de fraude ou de corrupção).

(2) O impacto financeiro e não financeiro na entidade ao investigar e lidar com as típicas violações do risco contemplados: o valor potencial de perda deve também considerar as "consequências legais" que fluem de um incidente detectado de fraude ou corrupção incluindo a responsabilidade dos administradores, a responsabilidade por ações dos funcionários e as perdas de terceiros. Outros impactos financeiros incluem as perdas decorrentes de interrupção do negócio, diminuição no preço das ações e distração da gestão.

(3) O impacto sobre a reputação da entidade com partes interessadas, governo, acionistas e sua reputação do negócio em geral: as consequências de tal incidente também incluem consequências não financeiras ou reputacionais que devem ser levadas em conta na avaliação do impacto sobre a entidade.

Probabilidade de ocorrência do risco:

(4) O volume de transações associadas com a função específica do negócio: quanto maior for o número de transações associadas com uma função de negócio, maior o risco relativo de fraude ou corrupção associado a essa função de negócios.

(5) Na medida em que a tecnologia está envolvida em as transações associadas com a fraude ou risco de corrupção: transações que são fortemente dependentes de tecnologia estão em maior risco de fraude do que aquelas que envolvem o processamento manual, porque o escrutínio humano detalhado das operações é muitas vezes insuficiente ou a um nível muito mais elevado do que as operações processadas manualmente.

(6) A natureza do benefício potencial para perpetradores: ativos atraentes, como dinheiro ou itens que podem ser facilmente convertidos em dinheiro, são mais propensos a ser desviados do que os ativos menos atraentes e seriam indicativo de uma disposição maior ao risco de fraude do que os ativos que são menos desejáveis.

(7) A incidência anterior do risco dentro da entidade: indiscutivelmente, quanto maior o número de casos do tipo dentro da entidade, maior a probabilidade de sua ocorrência.

(8) A incidência anterior do risco dentro da indústria em que a entidade opera dentro da economia em geral: quanto maior o número de incidentes do tipo dentro da indústria em que a entidade opera (ou na economia geral), maior a chance de que tal incidente ocorra dentro do próprio funcionamento da entidade.

(9) O estado atual de cultura de integridade da entidade (geralmente dentro da entidade e especificamente dentro da unidade de negócios onde o risco foi identificado): fraude e corrupção são mais prováveis em entidades que têm cultura de integridade pobre. A cultura de integridade da entidade deve ser considerada separadamente à sua cultura de controles internos, que seriam levadas em conta quando se considera o risco de controle interno.

O risco pode ser conduzido usando análise qualitativa (com base descritiva e métodos não numéricos), semiquantitativa (na qual os valores são atribuídos a escalas descritivas) ou quantitativa (utilização de escalas numéricas), tanto para consequência quanto para probabilidade.

Abordagens gráficas podem ser usadas para ilustrar posições relativas e auxiliar na posterior avaliação dos riscos.

(D) *Avaliação dos riscos*

Avalia-se os riscos de fraude e corrupção para facilitar as decisões sobre as necessidades e prioridades para tratá-los. Tal tomada de decisão é guiada por esses critérios e desenvolvida como parte do estabelecimento de contexto nas fases iniciais do processo de gestão de riscos. Esses critérios podem incluir:

- nível de risco avaliado;
- rankings relativos dos riscos;
- potenciais consequências se o risco ocorrer, ou o acumulado de consequências de vários eventos;
- probabilidade dos eventos ou dos seus resultados;
- níveis de tolerância definidos; e
- grau ou o intervalo de incerteza na avaliação do risco.

A saída da avaliação deve apresentar riscos identificados que são toleráveis ou não e que necessitam de tratamento ou não. A avaliação pode, contudo, indicar que não há informação suficiente sobre qual decisão pode ser tomada nesse momento e que uma análise mais aprofundada é justificada.

(E) *Tratar os riscos*

Em "tratar os riscos" são tomadas as decisões sobre as opções de tratamento mais adequadas para serem perseguidas para cada risco de fraude ou corrupção. As opções de tratamento devem considerar os resultados positivos e negativos que podem surgir com a implementação de cada opção de tratamento. Sempre que uma abordagem como "análise de custo-benefício" for usada para auxiliar a tomada de decisão, cuidado deve ser tomado para assegurar que tanto resultados tangíveis (por exemplo financeiros) e não tangíveis sejam examinados. O intervalo de opções que devem ser consideradas inclui:

- evitar o risco por não iniciar ou suspender atividades que podem dar risco;
- alterar a probabilidade (reduzir) do evento ou das suas consequências negativas ocorrendo, por exemplo, melhorando as medidas de segurança defensivas;
- alterar as consequências (reduzir negativo, melhorar positivo) do evento, para exemplo, ter procedimentos de detecção e investigação robustos no lugar;
- compartilhar o risco, por exemplo, através de seguros de garantia de fidelidade ou o seguro de interrupção de negócio; e
- manter o risco, por exemplo, através da aceitação do risco residual de outras atividades tratadas.

As decisões tomadas para avaliação e tratamento do risco devem considerar o total de custo de risco da fraude ou corrupção em consideração, incluindo aumentos ou reduções nos gastos com controles, como resultado das opções de tratamento propostos, tais como:

- perdas diretas e colaterais decorrentes, caso ocorra o risco;
- custos dos controles de antecipação existente e opções de tratamento propostos, tais como:
  – avaliação contínua de risco;
  – prevenção;
  – dissuasão; e
  – detecção.
- Custos de reação a resposta ao risco deve resultar em:
  – Investigação de fraude ou corrupção;
  – Recuperação do valor perdido como resultado da efetivação do risco, incluindo quaisquer custos incorridos na questão legal; e

– Restauração da capacidade e da habilidade da entidade para os seus níveis pré-evento.

Todas as ações propostas pela equipe de avaliação de risco devem ser validadas com a administração ou a gerência sênior, conforme apropriado antes da implementação. É importante também desenvolver uma estratégia que irá garantir implementação abrangente e prever uma verificação periódica do progresso. Esse processo será acompanhado se a responsabilidade pessoal for alocada no momento do desenvolvimento do produto da ação. Essas estratégias geralmente formam a base do Plano de Controle de Corrupção e Fraude.

Anexo 11 – Exemplo de matriz para avaliação de treinamento anticorrupção

Extraído do *Guia de avaliação de risco de corrupção* da United Nations Global Compact Office (2013).

A. Matriz de pontuação de treinamento anticorrupção

#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
1	O treinamento anticorrupção visa públicos relevantes?	3	3	Todos- 3, Alguns- 2, Poucos- 1
2	É fornecido em línguas pertinentes?	2	3	Todas- 3, Algumas- 2, Poucas ou Não- 1
3	O treinamento anticorrupção é obrigatório?	1	2	Sim, para todos- 3, Alguns funcionários- 2 Não- 1
4	O treinamento está incluído na orientação de novos funcionários ou conduzido geralmente dentro de 3 a 6 meses a contar do início do emprego?	2	1	Sim, em 3 meses- 3, entre 3 e 6 meses-2, depois de 6 meses- 1

A. Matriz de pontuação de treinamento anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
5	O treinamento é suficientemente conduzido periodicamente?	2	2	Anual:- 3, A cada 2 anos- 2, A cada 2+ anos ou Não- 1
6	Qual é a qualidade do conteúdo de treinamento?	2	3	Boa- 3, Satisfatória- 2, Fraca- 1 Observação: as considerações sobre qualidade podem incluir: a presença de tópicos relevantes essenciais, tom da alta administração, interatividade, facilidade de navegação, apresentação visual, nível linguísticos, clareza de conteúdo, etc.. Esses critérios podem ser pontuados formalmente e separadamente para atingir a pontuação de qualidade de conteúdo ou usados como guia de qualidade para o avaliador, para ajudá-lo a atribuir uma pontuação precisa a esses critérios de qualidade de conteúdo.
7	O treinamento inclui um formulário de certificação da política ou confirmação escrita?	3	1	Sim-3, Não- 1
8	O treinamento inclui teste?	3	2	Sim-3, Não- 1
9	Os resultados do teste são acompanhados e mantidos?	3	1	Sim-3, Não- 1
10	A conclusão do treinamento é acompanhada e esses registros são mantidos?	3	2	Sim-3, Não- 1
11	Qual é a taxa de conclusão do treinamento do público alvo?	3	3	Acima de 66%- 3, 33%–66%- 2, menos de 33%- 1
12	Há consequências disciplinares por não conclusão do treinamento?	1	1	Sim-3, Não- 1

A. Matriz de pontuação de treinamento anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
13	A conclusão do treinamento é parte da avaliação de desempenho anual do funcionário?	1	1	Sim-3, Alguns(por exemplo, apenas gerentes)- 2, Não- 1
14	Qual é a qualidade do plano de treinamento escrito?	2	2	Boa- 3, Média- 2, Fraca- 1 Obs.: Considerações sobre a qualidade podem incluir prazos anuais e estratégicos plurianuais, metas e objetivos declarados, públicos meta definidos, currículo detalhado, taxas de conclusão meta declaradas, frequência planejada, modalidade de entrega, escalas de instalação, indicadores-chaves de desempenho (KPIs), se o plano foi desenvolvido em consulta com outras funções, etc.
15	A eficiência do desempenho do programa de treinamento é avaliada periodicamente?	1	2	Sim, no mínimo anualmente- 3, a cada 2-3 anos-2 , a cada 3+ anos ou Não- 1
16	Os resultados da avaliação do programa de treinamento são usados para modificar o escopo do programa de treinamento?	1	1	Sim- 3, Não- 1
17	Qual é a qualidade do relatório de desempenho do programa de treinamento?	2	1	Boa- 3, Média- 2, Fraca- 1 Considerações sobre qualidade podem incluir ver se os relatórios são completados/ detalhados adequadamente, informam KPIs, são regularmente fornecidos para a autoridade apropriada na empresa.

A. Matriz de pontuação de treinamento anticorrupção				
#	Critérios de classificação de controle	Pontuação (simulada/ amostra de pontuação inserida)	Peso (Muito importante: 3, Importante: 2, menos importante: 1)	Guia de critérios de pontuação
18	Qual é a qualidade das iniciativas de comunicação que acompanham o treinamento formal? (por exemplo, material impresso, e-mails, vídeos, podcasts, blogs, recursos de intranet, etc.)	2	3	Boa- 3, Média- 2, Fraca- 1 (Observe que as considerações podem incluir cobertura de tópicos, disponibilidade linguística, frequência, tom da alta administração, administração intermediária, clareza de conteúdo e faixa dos veículos de entrega usados)
19	O programa de treinamento em geral é adequado para criar boa conscientização da matéria em questão entre os funcionários relevantes?	2		Sim- 3, Mais ou menos- 2, Não- 1 (Observação: essa é uma pergunta de verificações e balanços A pontuação deve ser consistente com as pontuações médias acima. As considerações podem incluir feedback do gerente/funcionário, e/ ou avaliação de outra parte)
PONTUAÇÃO PONDERADA TOTAL (escala de 1 a 3)				2.15

Anexo 12 – Quesitos para avaliação do comprometimento da organização no combate a fraude e corrupção

Para uma avaliação do sistema de prevenção e detecção de fraudes da organização, avalie cada questão ou atividade abaixo e julgue conforme a escala. As questões ou atividades que obtiverem nota vermelha ou amarela, um plano de ação deve ser elaborado para trazê-los para o verde. Extraído e adaptado do Institute of Internal Auditors (2008).

Vermelho indica a questão ou atividade que precisa de reforço substancial para trazer o risco de fraude para níveis aceitáveis.

Amarelo indica a questão ou atividade que precisa de algum reforço para trazer o risco de fraude para níveis aceitáveis.

Verde indica a questão ou atividade que mantém o risco de fraude pelo menos abaixo do nível aceitável.

Questão ou atividade para prevenção ou detecção de fraude	Nota
A cultura da organização é forte o suficiente para estabelecer uma tolerância zero às fraudes.	
A alta administração demonstra consistentemente comportamento ético que inspire nos liderados confiança e o sentimento de intolerância a fraudes.	
O código de ética existe, é divulgado e é conhecido pelos servidores e partes interessadas.	
O código de conduta existe, é divulgado e é conhecido pelos servidores e partes interessadas.	
As condutas antiéticas são analisadas e sancionadas pela comissão de ética.	
Existe um plano de combate a fraude e corrupção aprovado pela alta administração.	
A gestão de riscos da organização leva em consideração o risco de fraude e analisa e recomenda controles ou sua melhoria.	
As estruturas descentralizadas, órgãos desconcentrados ou subsidiárias, da organização possuem os mesmos controles preventivos da matriz.	
A auditoria interna leva em consideração o risco de fraude no plano de auditoria.	
A auditoria interna tem independência da alta gerência e se reporta diretamente a alta administração.	
A estrutura da auditoria interna é compatível com o porte da organização e atua seguindo os padrões profissionais, com pessoal com competência apropriada para as atividades.	
A auditoria interna conduz ou participa de investigações de potenciais casos de fraude.	
Existe política de segregação de função e rotação de pessoal que está em funcionamento e tem sido efetiva.	
A gestão de recursos humanos analisa antecedentes para cargos de livre nomeação.	
Na capacitação de novos servidores e na capacitação periódica de todos estão incluídos aspectos de ética, integridade, conflito de interesse e prevenção da fraude.	
Os servidores e partes interessadas estão conscientes da política de tolerância zero à fraude e sabem o que fazer caso fiquem sabendo de alguma suspeita de fraude.	
As responsabilidades por prevenção e detecção estão definidas.	
Os *red flags* foram mapeados.	
Controles contínuos estão em operação para impedir ou alertar transações suspeitas.	
São utilizadas ferramentas de análise dadas para detectar transações anormais.	
Os indicadores de desempenho da organização incluem métricas que valorem os aspectos éticos e de integridade.	
Existem indicadores para monitorar a efetividade dos controles preventivos e detectivos.	

Questão ou atividade para prevenção ou detecção de fraude	Nota
A alta administração monitora os resultados alcançados com os controles preventivos e detectivos e suporta as medidas necessárias para melhorá-los.	
Existe o canal de denúncia, que está em operação, e os servidores e partes interessadas sabem dele.	
O sigilo da denúncia e a proteção contra represália são do conhecimento de todos e efetivamente funcionam.	
As denúncias são analisadas e catalogadas num repositório.	
Existe unidade antifraude que está operacional e avalia e investiga as denúncias.	
Existe um plano de resposta à fraude.	
Existem servidores treinados para compor equipe de investigação.	
Os responsáveis por fraudes são identificados e punidos.	
Os prejuízos são identificados, valorados e recuperados.	
Os casos de fraudes são identificados, e as medidas tomadas e os resultados são divulgados.	
Divulga-se para servidores e partes interessadas que controles preventivos e detectivos estão em vigor, mas sem adentrar nas questões técnicas.	

Anexo 13 – Exemplos de indicadores de fraude *(red flags)*

Extraído e adaptado do National Audit Office (2008).

Cada organização, pela sua singularidade, vai apresentar um conjunto específico de *red flags*. Cabe a ela o exercício de mapear os seus *red flags*. Como já dito, um *red flag* não necessariamente é uma fraude, mas apenas fornece possíveis sinais de alerta para uma fraude. Ou seja, identificado um *red flag*, precisa-se averiguar o que está acontecendo. Entretanto, o ideal é que o processo e o controle evitem essas ocorrências.

Ainda que cada organização tenha o seu conjunto de *red flags*, alguns processos são comuns a muitas organizações e, portanto, compartilham muitos *red flags*. Abaixo alguns exemplos de *red flags* em algumas atividades rotineiras.

- Conluio entre licitantes nas compras públicas
  - » Evidência ou indício de relação estreita entre licitantes;
  - » Competição limitada no setor;
  - » Todas as propostas são bem acima do orçamento da licitação;
  - » Empresas esperadas não dão lances;
  - » Vencedor da licitação subcontrata licitante perdedor ou não licitante;

- » Existe um padrão nos lances vencedores e perdedores;
- » Apenas um licitante atende às especificações, os demais apresentam propostas falhas.

- Conluio entre comprador e licitante
  - » O pessoal responsável pelas compras tem relação com o licitante vencedor;
  - » O licitante oferece presentes ou benefícios para o comprador;
  - » Especificação da licitação identifica o produto do licitante vencedor;
  - » Especificação do contrato altera após o licitante favorecido ser contratado;
  - » Desqualificação de licitante sem razão motivada;
  - » Contrato adjudicado à empresa desconhecida;
  - » Licitantes perdedores manifestam-se publicamente contra a licitação.

- Fornecedor único
  - » Excesso de dispensa de licitação;
  - » Uma empresa é favorecida;
  - » Empresa sem histórico no ramo.

- Execução contratual
  - » Aceite de faturas sem a fiscalização adequada;
  - » Excesso de lucro ou falta de transparência da margem líquida;
  - » Modelo do contrato deixa margem para manipulação da medição;
  - » Evidência de baixo desempenho por meio de dados públicos, denúncias, pesquisa de satisfação ou notícias;
  - » Sanções não aplicadas mesmo com o baixo desempenho;
  - » Pouco contato entre contratante e contratado.

- Sistemas de pagamento
  - » A mesma pessoa que lança o pagamento autoriza;
  - » Aumento de ressarcimento ou pagamento para indivíduos;
  - » Transações feitas em horários e frequências estranhas, valores inusuais ou para destinatários excêntricos.

- » Controle interno que não é aplicado ou comprometido por pessoas mais experientes;
- » Discrepância nos registros contábeis e reconciliação com itens inexplicávies;
- » Excesso de créditos suspeitos;
- » Ativo físico extraviado;
- » Evidência de alteração em documentos ou duplicações.

- Controles internos
  - » Conflito de interesse no processo. Uma pessoa tem o controle do processo do começo ao fim;
  - » Conluio de servidores, onde há pouco ou nenhuma supervisão;
  - » Manipulação deliberada de demonstrações financeiras e/ou extravio dos arquivos de auditoria.

Responsabilidade pelo conteúdo
Secretaria-Geral de Controle Externo (Segecex)
Coordenação-Geral de Controle Externo dos Serviços
Essenciais ao Estado e das Regiões Sul e C.Oeste (Coestado)
Secretaria de Métodos e Suporte ao Controle Externo (Semec)

Projeto gráfico, diagramação e capa
Secretaria-Geral da Presidência (Segepres)
Secretaria de Comunicação (Secom)
Núcleo de Criação e Editoração (NCE)

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria-Geral de Controle Externo (Segecex)
SAFS Quadra 4, Lote 1
Edifício Anexo III, Salas 453 e 450
70.042-900 Brasília - DF
Tel.: (61) 3316 7322
segecex@tcu.gov.br

Ouvidoria
Tel.: 0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Sesap/Segedam

MISSÃO
Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo.

VISÃO
Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável.