NORMA
BRASILEIRA

ABNT NBR ISO 37001

Primeira edição
06.03.2017

Sistemas de gestão antissuborno — Requisitos com orientações para uso

Anti-bribery management systems — Requirements with guidance for use

ICS 03.100.01; 03.100.70

ISBN 978-85-07-06833-4

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO 37001:2017
53 páginas

Arquivo de impressão gerado em 13/04/2018 13:24:08 de uso exclusivo de CEPEL - CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA

ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

Sumário

Página

Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos ABNT são elaborados conforme as regras da ABNT Diretiva 2.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Ressalta-se que Normas Brasileiras podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os Órgãos responsáveis pelos Regulamentos Técnicos podem determinar outras datas para exigência dos requisitos desta Norma.

A ABNT NBR ISO 37001 foi elaborada pela Comissão de Estudo Especial de Antissuborno (ABNT/CEE-278). O Projeto circulou em Consulta Nacional conforme Edital nº 01, de 24.01.2017 a 22.02.2017.

Esta Norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO 37001:2016, que foi elaborada pelo *Project Committee Anti-bribery management systems* (ISO/PC 278), conforme ISO/IEC Guide 21-1:2005.

O Escopo em inglês desta Norma Brasileira é o seguinte:

Scope

This document specifies requirements and provides guidance for establishing, implementing, maintaining, reviewing and improving an anti-bribery management system. The system can be stand-alone or can be integrated into an overall management system. This document addresses the following in relation to the organization's activities:

— *bribery in the public, private and not-for-profit sectors;*

— *bribery by the organization;*

— *bribery by the organization's personnel acting on the organization's behalf or for its benefit;*

— *bribery by the organization's business associates acting on the organization's behalf or for its benefit;*

— *bribery of the organization;*

— *bribery of the organization's personnel in relation to the organization's activities;*

— *bribery of the organization's business associates in relation to the organization's activities;*

— *direct and indirect bribery (e.g. a bribe offered or accepted through or by a third party).*

Arquivo de impressão gerado em 13/04/2018 13:24:08 de uso exclusivo de CEPEL - CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA

This document is applicable only to bribery. It sets out requirements and provides guidance for a management system designed to help an organization to prevent, detect and respond to bribery and comply with anti-bribery laws and voluntary commitments applicable to its activities.

This document does not specifically address fraud, cartels and other anti-trust/competition offences, money-laundering or other activities related to corrupt practices, although an organization can choose to extend the scope of the management system to include such activities.

The requirements of this document are generic and are intended to be applicable to all organizations (or parts of an organization), regardless of type, size and nature of activity, and whether in the public, private or not-for-profit sectors. The extent of application of these requirements depends on the factors specified in 4.1, 4.2 and 4.5.

NOTE 1 See Clause A.2 for guidance.

NOTE 2 The measures necessary to prevent, detect and mitigate the risk of bribery by the organization can be different from the measures used to prevent, detect and respond to bribery of the organization (or its personnel or business associates acting on the organization's behalf). See A.8.4 for guidance.

Introdução

Suborno é um fenômeno generalizado. Ele causa sérias preocupações sociais, morais, econômicas e políticas, debilita a boa governança, dificulta o desenvolvimento e distorce a competição. Corrói a justiça, mina os direitos humanos e é um obstáculo para o alívio da pobreza. O suborno também aumenta o custo de fazer negócios, introduz incertezas nas transações comerciais, eleva o custo dos bens e serviços, diminui a qualidade dos produtos e serviços, o que pode levar à perda de vidas e propriedades, destrói a confiança nas instituições e interfere na operação justa e eficiente dos mercados.

Governos têm feito progresso ao abordar o suborno por meio de acordos internacionais, como o da "*Organization for Economic Co-operation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*" [15] e da "*United Nations Convention against Corruption*" [14], e por meio das suas leis nacionais. Na maioria das jurisdições, é um delito os indivíduos se envolverem em suborno, e existe uma tendência crescente de responsabilizar as organizações, bem como os indivíduos.

Apesar disto, apenas a lei não é suficiente para resolver o problema. As organizações têm, portanto, uma responsabilidade de contribuir proativamente para o combate do suborno. Isto pode ser alcançado por meio de um sistema de gestão antissuborno, que este Documento pretende fornecer, e por meio de uma liderança comprometida no estabelecimento de uma cultura de integridade, transparência, abertura e *compliance*. A natureza da cultura de uma organização é crucial para o sucesso ou falha de um sistema de gestão antissuborno.

É esperado que uma organização bem gerenciada tenha uma política de *compliance* apoiada por sistemas de gestão apropriados, para auxiliá-la no cumprimento das suas obrigações legais e no comprometimento com a integridade. Uma política antissuborno é um componente de uma política global de *compliance*. A política antissuborno e o sistema de gestão de apoio ajudam uma organização a evitar ou mitigar os custos, riscos e danos de envolvimento com suborno, promover a confiança nos negócios e melhorar a sua reputação.

Este Documento reflete as boas práticas internacionais e pode ser usado em quaisquer jurisdições. É aplicável às pequenas, médias e grandes organizações em todos os setores, incluindo os setores público, privado e sem fins lucrativos. Os riscos de suborno que uma organização enfrenta variam de acordo com fatores como o tamanho da organização, as localizações e setores nos quais a organização opera, a natureza, escala e complexidade das atividades da organização. Portanto, este Documento especifica a implementação pela organização de políticas, procedimentos e controles que sejam razoáveis e proporcionais, de acordo com os riscos de suborno que a organização enfrenta. O Anexo A fornece orientações sobre a implementação dos requisitos deste Documento.

A conformidade com este Documento não pode fornecer garantia de que nenhum suborno tenha ocorrido ou ocorrerá em relação à organização, uma vez que não é possível eliminar completamente o risco de suborno. Entretanto, este Documento pode ajudar a organização a implementar medidas razoáveis e proporcionais concebidas para prevenir, detectar e responder ao suborno.

Neste Documento são usadas as seguintes formas verbais:

— "deve" indica um requisito;

— "convém que" indica uma recomendação;

— "pode" indica uma permissão, possibilidade ou capacidade.

Informação assinalada como “NOTA” é uma orientação quanto ao entendimento ou esclarecimento de um requisito associado.

Este Documento está em conformidade com os requisitos da ISO para normas de sistemas de gestão. Estes requisitos incluem uma estrutura de alto nível, textos centrais idênticos e termos comuns com as definições centrais, concebidas para beneficiar os usuários que implementam múltiplas normas ISO de sistemas de gestão. Este Documento pode ser usado em conjunto com outras normas ISO de sistemas de gestão (por exemplo, ABNT NBR ISO 9001, ABNT NBR ISO 14001, ABNT NBR ISO 27001 e ISO 19600) e com normas de gestão (por exemplo, ABNT NBR ISO 26000 e ABNT NBR ISO 31000).

NOTA BRASILEIRA Existe uma versão traduzida pela ABNT da ISO 19600, *Sistema de gestão de compliance – Diretrizes.*

Arquivo de impressão gerado em 13/04/2018 13:24:08 de uso exclusivo de CEPEL - CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA

Sistemas de gestão antissuborno — Requisitos com orientações para uso

1 Escopo

Este Documento especifica requisitos e fornece orientações para o estabelecimento, implementação, manutenção, análise crítica e melhoria de um sistema de gestão antissuborno. O sistema pode ser independente ou pode ser integrado a um sistema de gestão global. Este Documento aborda o seguinte, em relação às atividades da organização:

— suborno nos setores público, privado e sem fins lucrativos;

— suborno pela organização;

— suborno pelo pessoal da organização atuando em nome da organização ou para seu benefício;

— suborno pelos parceiros de negócio da organização atuando em nome da organização ou para seu benefício;

— suborno da organização;

— suborno do pessoal da organização em relação às atividades da organização;

— suborno dos parceiros de negócio da organização em relação às atividades da organização;

— suborno direto ou indireto (por exemplo, uma propina oferecida ou aceita um suborno oferecido ou aceito por meio ou por uma terceira parte).

Este Documento é aplicável apenas a suborno. Ele estabelece requisitos e fornece orientações para um sistema de gestão concebido para ajudar uma organização a prevenir, detectar e responder ao suborno e cumprir com as leis antissuborno e comprometimentos voluntários aplicáveis às suas atividades.

Este Documento não aborda especificamente fraude, cartéis e outros delitos antitruste/anticoncorrencial, lavagem de dinheiro ou outras atividades relacionadas a práticas corruptas, embora uma organização possa escolher ampliar o escopo do sistema de gestão para incluir estas atividades.

Os requisitos deste Documento são genéricos e destinam-se a ser aplicáveis a todas as organizações (ou partes de uma organização), independentemente do tipo, tamanho e natureza da atividade, bem como se a organização é do setor público, privado ou sem fins lucrativos. A extensão da aplicação destes requisitos depende dos fatores especificados em 4.1, 4.2 e 4.5.

NOTA 1 Para orientações, ver Seção A.2.

NOTA 2 As medidas necessárias para prevenir, detectar e mitigar o risco de suborno pela organização podem ser diferentes das medidas usadas para prevenir, detectar e responder a suborno da organização (ou de seu pessoal ou parceiros de negócio atuando em nome da organização). Para orientações, ver A.8.4.

2 Referências normativas

Não existem referências normativas neste Documento.

3 Termos e definições

Para os efeitos deste Documento, aplicam-se os seguintes termos e definições.

A ISO e a IEC mantêm as bases de dados terminológicos para uso na normalização nos seguintes endereços:

— *ISO Online browsing platform*: disponível em http://www.iso.org/obp

— *IEC Electropedia*: disponível em http://www.electropedia.org/

3.1
suborno
oferta, promessa, doação, aceitação ou solicitação de uma vantagem indevida de qualquer valor (que pode ser financeiro ou não financeiro), direta ou indiretamente, e independente de localização(ões), em violação às leis aplicáveis, como um incentivo ou recompensa para uma pessoa que está agindo ou deixando de agir em relação ao *desempenho* (3.16) das suas obrigações

Nota 1 de entrada: A definição de suborno acima é genérica. O significado do termo "suborno" é definido pela lei antissuborno aplicável à *organização* (3.2) e pelo sistema de *gestão antissuborno* (3.5) concebido pela organização.

3.2
organização
pessoa ou grupo de pessoas que têm suas próprias funções com responsabilidades, autoridades e relações para alcançar seus *objetivos* (3.11)

Nota 1 de entrada: O conceito de organização inclui, mas não é limitado a, empreendedor individual, companhia, corporação, firma, empresa, autoridade, parceria, instituição de caridade ou instituição, ou parte ou combinação destes, seja incorporada ou não, pública ou privada.

Nota 2 de entrada: Para organizações com mais de uma unidade operacional, uma ou mais unidades operacionais podem ser definidas como uma organização.

3.3
parte interessada (termo preferido)
stakeholder (termo admitido)
pessoa ou *organização* (3.2) que pode afetar, ser afetada ou se perceber afetada por uma decisão ou atividade

Nota 1 de entrada: Uma parte interessada pode ser interna ou externa à organização.

3.4
requisito
necessidade que é declarada e obrigatória

Nota 1 de entrada: A definição básica de "requisito" nas normas ISO de sistemas de gestão é "necessidade ou expectativa que é declarada, geralmente implícita ou obrigatória. "Requisitos geralmente implícitos" não são aplicáveis no contexto da gestão antissuborno.

Nota 2 de entrada: "Geralmente implícita" significa que é costume ou prática comum para a organização e partes interessadas que a necessidade ou expectativa sob consideração esteja implícita.

Nota 3 de entrada: Um requisito especificado é aquele que é declarado, por exemplo, em uma informação documentada.

Arquivo de impressão gerado em 13/04/2018 13:24:08 de uso exclusivo de CEPEL - CENTRO DE PESQUISAS DE ENERGIA ELÉTRICA

3.5
sistema de gestão
conjunto de elementos inter-relacionados ou interativos de uma *organização* (3.2), para estabelecer *políticas* (3.10), *objetivos* (3.11) e *processos* (3.15) para alcançar esses objetivos

Nota 1 de entrada: Um sistema de gestão pode abordar uma única disciplina ou várias disciplinas.

Nota 2 de entrada: Os elementos do sistema de gestão incluem a estrutura da organização, papéis e responsabilidades, planejamento e operação.

Nota 3 de entrada: O escopo de um sistema de gestão pode incluir a totalidade da organização, funções específicas e identificadas da organização, seções específicas e identificadas da organização ou uma ou mais funções executadas por mais de uma organização.

3.6
Alta Direção
pessoa ou grupo de pessoas que dirige e controla uma *organização* (3.2) no nível mais alto

Nota 1 de entrada: A Alta Direção tem o poder de delegar autoridade e prover recursos na organização.

Nota 2 de entrada: Se o escopo do *sistema de gestão* (3.5) cobrir apenas parte de uma *organização*, então Alta Direção se refere àqueles que dirigem e controlam aquela parte da organização.

Nota 3 de entrada: Organizações podem ser estruturadas dependendo do marco legal sob o qual são obrigadas a operar e também de acordo com o seu porte, setor, etc. Algumas organizações têm tanto *Órgão Diretivo* (3.7) quanto *Alta Direção* (3.6), enquanto algumas organizações não tem responsabilidades divididas em vários órgãos. Estas variações, tanto com respeito à organização como às responsabilidades, podem ser consideradas quando aplicados os requisitos da Seção 5.

3.7
Órgão Diretivo
grupo ou orgão que tem a responsabilidade e autoridade finais pelas atividades, governança e políticas de uma *organização* (3.2), e ao qual a *Alta Direção* (3.6) se reporta e perante o qual a Alta Direção é responsabilizada

Nota 1 de entrada: Nem todas as organizações, particularmente organizações pequenas, têm um Órgão Diretivo separado da *Alta Direção* (ver 3.6, Nota 3 de entrada).

Nota 2 de entrada: Um Órgão Diretivo pode incluir, porém não está limitado ao, conselho de administração, comitês do conselho, conselho de supervisão, curadores ou supervisores.

NOTA BRASILEIRA	O conselho de supervisão é também conhecido como conselho fiscal.

3.8
função de *compliance* antissuborno
pessoa(s) com responsabilidade e autoridade para a operação do *sistema de gestão* (3.5) antissuborno

3.9
eficácia
extensão na qual atividades planejadas são realizadas e resultados planejados são alcançados

3.10
política
intenções e direção de uma *organização* (3.2), como formalmente expressos pela sua *Alta Direção* (3.6) ou por seu *Órgão Diretivo* (3.7)

3.11
objetivo
resultado a ser alcançado

Nota 1 de entrada: Um objetivo pode ser estratégico, tático ou operacional.

Nota 2 de entrada: Objetivos podem se relacionar a diferentes disciplinas (como finanças, vendas e *marketing*, aquisição, saúde e segurança e metas ambientais) e podem se aplicar a diferentes níveis (como estratégico, organizacional, do projeto, do produto e dos *processos* (3.15)).

Nota 3 de entrada: Um objetivo pode ser expresso de outras formas, por exemplo, como um resultado pretendido, um propósito, um critério operacional, como um objetivo antissuborno, ou pelo uso de outras palavras com significado similar (por exemplo, finalidade, meta ou alvo).

Nota 4 de entrada: No contexto de sistemas de gestão antissuborno, objetivos antissuborno são estabelecidos pela *organização* (3.2), coerentemente com a *política antissuborno* (3.10), para alcançar resultados específicos.

3.12
risco
efeito da incerteza nos *objetivos* (3.11)

Nota 1 de entrada: Um efeito é um desvio do esperado – positivo ou negativo.

Nota 2 de entrada: Incerteza é o estado, ainda que parcial, de deficiência de informação relacionada ao entendimento ou conhecimento de um evento, sua consequência ou probabilidade.

Nota 3 de entrada: O risco é muitas vezes caracterizado pela referência aos eventos potenciais (como definido no ABNT ISO Guia 73:2009, 3.5.1.3) e às consequências (como definido no ABNT ISO 73:2009, 3.6.1.3), ou uma combinação destes.

Nota 4 de entrada: O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (*likelihood*) (como definido no ABNT ISO Guia 73:2009, 3.6.1.1) de ocorrência associada.

3.13
competência
capacidade de aplicar conhecimento e habilidades para alcançar resultados pretendidos

3.14
informação documentada
informação que se requer que seja controlada e mantida por uma *organização* (3.2) e o meio no qual ela está contida

Nota 1 de entrada: Informação documentada pode estar em qualquer formato e meio e pode ser proveniente de qualquer fonte.

Nota 2 de entrada: Informação documentada pode se referir a:

— *sistema de gestão* (3.5), incluindo *processos* (3.15) relacionados;

— informação criada para a organização operar (documentação);

— evidência de resultados alcançados (*registros*).

3.15
processo
conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas

3.16
desempenho
resultado mensurável

Nota 1 de entrada: Desempenho pode se relacionar tanto às constatações quantitativas quanto às qualitativas.

Nota 2 de entrada: Desempenho pode se relacionar à gestão de atividades, *processos* (3.15), produtos (incluindo serviços), sistemas ou *organizações* (3.2).

3.17
terceirizar (verbo)
fazer um arranjo onde uma *organização* (3.2) externa desempenha parte de uma função ou *processo* (3.15) de uma organização

Nota 1 de entrada: Uma organização externa está fora do escopo do *sistema de gestão* (3.5), apesar de a função ou processo terceirizado estar dentro do escopo.

Nota 2 de entrada: O texto principal das normas ISO de sistemas de gestão contém uma definição e um requisito em relação à terceirização, os quais não são utilizados neste Documento, uma vez que os provedores terceirizados estão incluídos na definição de parceiros de negócio (3.2).

3.18
monitoramento
determinação da situação de um sistema, um *processo* (3.15) ou uma atividade

Nota 1 de entrada: Para determinar a situação, pode haver a necessidade de verificar, supervisionar ou observar criticamente.

3.19
medição
processo (3.15) para determinar um valor

3.20
auditoria
processo (3.15) sistemático, independente e documentado, para obter evidência de auditoria e avaliá-la objetivamente, para determinar a extensão na qual os critérios de auditoria são atendidos

Nota 1 de entrada: Uma auditoria pode ser uma auditoria interna (primeira parte) ou uma auditoria externa (segunda parte ou terceira parte) e pode ser uma auditoria combinada (combinando duas ou mais disciplinas)

Nota 2 de entrada: Uma auditoria interna é conduzida pela própria *organização* (3.2), ou por uma parte externa em seu nome.

Nota 3 de entrada: “Evidência de auditoria” e “critérios de auditoria” estão definidos na ABNT NBR ISO 19011.

3.21
conformidade
atendimento de um *requisito* (3.4)

3.22
não conformidade
não atendimento de um *requisito* (3.4)

3.23
ação corretiva
ação para eliminar a causa de uma *não conformidade* (3.22) e para prevenir recorrência

3.24
melhoria contínua
atividade recorrente para elevar o *desempenho* (3.16)

3.25
pessoal
diretores, administradores, contratados ou trabalhadores temporários e voluntários da *organização* (3.2)

Nota 1 de entrada: Diferentes tipos de pessoal apresentam diferentes tipos e graus de *risco* (3.12) de suborno e, portanto, podem ser tratados diferentemente pelos procedimentos de gestão de risco de suborno e pelo processo de avaliação de riscos de suborno da organização.

Nota 2 de entrada: Para orientações sobre contratados ou trabalhadores temporários, ver A.8.5.

3.26
parceiro de negócio
parte externa com a qual a organização (3.2) tem, ou planeja estabelecer, alguma forma de relacionamento de negócio

Nota 1 de entrada: Parceiro de negócio inclui, mas não está limitado a, clientes*, joint ventures,* parceiros de *joint ventures,* parceiros de consórcio, provedores terceirizados, contratados, consultores, subcontratados, fornecedores, vendedores, conselheiros, agentes, distribuidores, representantes, intermediários e investidores. Esta definição é deliberadamente ampla e convém que seja interpretada em consonância com o perfil de *risco* (3.12) de suborno da organização, para que seja aplicada aos parceiros de negócio que possam razoavelmente expor a organização a riscos de suborno.

Nota 2 de entrada: Diferentes tipos de parceiro de negócio apresentam diferentes tipos e graus de risco de suborno, e uma *organização* (3.2) terá diferentes graus de capacidade para influenciar os diferentes tipos de parceiro de negócio. Diferentes tipos de parceiro de negócio podem ser tratados diferentemente pelo processo de avaliação de riscos de suborno da organização e pelos procedimentos de gestão de risco de suborno.

Nota 3 de entrada: Referência a “negócio”, neste Documento, pode ser interpretada de forma ampla, para significar aquelas atividades que são pertinentes ao propósito da existência da organização.

3.27
agente público
pessoa detentora de cargo legislativo, administrativo ou judicial, seja por nomeação, eleição ou sucessão, ou qualquer pessoa que exerça uma função pública, inclusive para um órgão público ou uma empresa pública, ou qualquer agente ou oficial de uma organização pública nacional ou internacional, ou qualquer candidato a cargo público

Nota 1 de entrada: Para exemplos de indivíduos que possam ser considerados agentes públicos, ver Seção A.21.

3.28
terceira parte
pessoa ou organismo (órgão) que é independente da *organização* (3.2)

Nota 1 de entrada: Todos os parceiros de negócio (3.26) são terceiras partes, mas nem todas as terceiras partes são parceiros de negócio.

3.29
conflito de interesse
situação onde os negócios, finanças, famílias, interesses políticos ou pessoais podem interferir no julgamento de pessoas no exercício das suas obrigações para a *organização* (3.2)

3.30
due diligence
processo (3.15) para aprofundar a avaliação da natureza e extensão dos *riscos* (3.12) de suborno e ajudar as *organizações* (3.2) a tomar decisões em relação a transações, projetos, atividades, *parceiros de negócio* (3.26) e pessoal específico

4 Contexto da organização

4.1 Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são pertinentes para o seu propósito e que afetam sua capacidade de alcançar os objetivos do seu sistema de gestão antissuborno. Estas questões incluem, sem limitação, os seguintes fatores:

a) tamanho, estrutura e delegação de autoridade para tomada de decisão da organização;

b) localizações e setores nos quais a organização opera ou antecipa a operação;

c) natureza, escala e complexidade das operações e atividades da organização;

d) modelo de negócio da organização;

e) entidades sobre as quais a organização tenha controle e entidades que exerçam controle sobre a organização;

f) parceiros de negócio da organização;

g) natureza e extensão das interações com agentes públicos; e

h) obrigações e deveres estatutários, regulatórios, contratuais e profissionais aplicáveis.

NOTA Uma organização tem controle sobre outra organização se ela controlar direta ou indiretamente a gestão da organização (ver A.13.1.3).

4.2 Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

a) as partes interessadas que são pertinentes para o sistema de gestão antissuborno;

b) os requisitos pertinentes destas partes interessadas.

NOTA Na identificação dos requisitos das partes interessadas, uma organização pode distinguir entre requisitos mandatórios e as expectativas não mandatórias e os comprometimentos voluntários das partes interessadas.

4.3 Determinando o escopo do sistema de gestão antissuborno

A organização deve determinar os limites e a aplicabilidade do sistema de gestão antissuborno para estabelecer o seu escopo.

Ao determinar esse escopo, a organização deve considerar:

a) as questões internas e externas referidas em 4.1;

b) os requisitos referidos em 4.2; e

c) os resultados da avaliação de riscos de suborno referidos em 4.5.

O escopo deve estar disponível como informação documentada.

NOTA Para orientações, ver Seção A.2.

4.4 Sistema de gestão antissuborno

A organização deve estabelecer, documentar, implementar, manter e, de forma contínua, analisar criticamente e, onde necessário, melhorar o sistema de gestão antissuborno, incluindo os processos necessários e as suas interações, de acordo com os requisitos deste Documento.

O sistema de gestão antissuborno deve conter medidas concebidas para identificar e avaliar o risco, bem como prevenir, detectar e responder ao suborno.

NOTA 1 Não é possível eliminar completamente o risco de suborno, e nenhum sistema de gestão antissuborno será capaz de prevenir e detectar o suborno como um todo.

O sistema de gestão antissuborno deve ser razoável e proporcional, levando-se em conta os fatores referidos em 4.3.

NOTA 2 Para orientações, ver Seção A.3.

4.5 Processo de avaliação de riscos de suborno

4.5.1 A organização deve realizar regularmente o processo de avaliação de riscos de suborno que devem:

a) identificar os riscos de suborno que a organização possa antecipar de forma razoável, em função dos fatores listados em 4.1;

b) analisar, avaliar e priorizar os riscos de suborno identificados;

c) avaliar a adequação e eficácia dos controles existentes da organização para mitigar os riscos de suborno avaliados.

4.5.2 A organização deve estabelecer critérios para avaliar seu nível de risco de suborno, que deve levar em conta as políticas e os objetivos da organização.

4.5.3 O processo de avaliação de riscos de suborno deve ser analisado criticamente:

a) em uma base regular, de modo que mudanças e novas informações possam ser apropriadamente avaliadas com base no tempo e frequência definidos pela organização;

b) no caso de uma mudança significativa da estrutura ou atividades da organização.

4.5.4 A organização deve reter informação documentada que demonstre que o processo de avaliação de riscos de suborno tem sido realizado e usado para conceber ou melhorar o sistema de gestão antissuborno.

NOTA Para orientações, ver Seção A.4.

5 Liderança

5.1 Liderança e comprometimento

5.1.1 Órgão Diretivo

Quando a organização tem um Órgão Diretivo, este órgão deve demonstrar liderança e comprometimento com respeito ao sistema de gestão antissuborno para:

a) aprovar a política antissuborno da organização;

b) assegurar que a estratégia da organização e a política antissuborno estão alinhadas;

c) receber e analisar criticamente, a intervalos planejados, informações sobre o conteúdo e a operação do sistema de gestão antissuborno da organização;

d) requerer que os recursos adequados e apropriados necessários para a operação eficaz do sistema de gestão antissuborno estejam alocados e atribuídos;

e) exercer razoável supervisão sobre a implementação do sistema de gestão antissuborno da organização pela Alta Direção e a sua eficácia.

Estas atividades devem ser realizadas pela Alta Direção, se a organização não tiver um Órgão Diretivo.

5.1.2 Alta Direção

A Alta Direção deve demostrar liderança e comprometimento com relação ao sistema de gestão antissuborno para:

a) assegurar que o sistema de gestão antissuborno, incluindo a política e os objetivos, esteja estabelecido, implementado, mantido e analisado criticamente para abordar de forma adequada os riscos de suborno da organização;

b) assegurar a integração dos requisitos do sistema de gestão antissuborno nos processos da organização;

c) disponibilizar recursos adequados e apropriados para a operação eficaz do sistema de gestão antissuborno;

d) comunicar interna e externamente sobre a política antissuborno;

e) comunicar internamente a importância de uma gestão eficaz antissuborno e da conformidade com os requisitos do sistema de gestão antissuborno;

f) assegurar que o sistema de gestão antissuborno esteja apropriadamente concebido para alcançar seus objetivos;

g) dirigir e apoiar o pessoal para contribuir com a eficácia do sistema de gestão antissuborno;

h) promover uma cultura antissuborno apropriada dentro da organização;

i) promover a melhoria contínua;

j) apoiar outros papéis pertinentes da gestão para demostrar como sua liderança na prevenção e detecção do suborno se aplica às áreas sob sua responsabilidade;

k) encorajar o uso de procedimentos de relato para subornos suspeitos e reais (ver 8.9);

l) assegurar que o pessoal não sofra retaliação, discriminação ou ação disciplinar (ver 7.2.2.1 d) por relatos feitos de boa-fé ou com base em uma razoável convicção de violação ou suspeita de violação da política antissuborno da organização, ou por se recusar a participar do suborno, mesmo que tal recusa possa resultar na perda de um negócio para a organização (exceto quando o indivíduo participou da violação);

m) reportar para o Órgão Diretivo (se existir), a intervalos planejados, sobre o conteúdo e operação do sistema de gestão antissuborno e de alegações de subornos sistemáticos ou graves.

NOTA Para orientações, ver Seção A.5.

5.2 Política antissuborno

A Alta Direção deve estabelecer, manter e analisar criticamente uma política antissuborno que:

a) proíba o suborno;

b) requeira o cumprimento das leis antissuborno que são aplicáveis à organização;

c) seja apropriada ao propósito da organização;

d) proveja uma estrutura para estabelecer, analisar criticamente e alcançar os objetivos antissuborno;

e) inclua um comprometimento para satisfazer os requisitos do sistema de gestão antissuborno;

f) encoraje o levantamento de preocupações com base na boa-fé ou em uma razoável convicção na confiança, sem medo de represália;

g) inclua um comprometimento para a melhoria contínua do sistema de gestão antissuborno;

h) explique a autoridade e independência da função de *compliance* antissuborno; e

i) explique as consequências do não cumprimento da política antissuborno.

A política antissuborno deve:

— estar disponível como informação documentada;

— ser comunicada nos idiomas apropriados dentro da organização e também para os parceiros de negócio que representem mais do que um baixo risco de suborno;

— estar disponível para as partes interessadas pertinentes, conforme apropriado.

5.3 Papéis, responsabilidades e autoridades organizacionais

5.3.1 Papéis e responsabilidades

A Alta Direção deve ter total responsabilidade pela implementação e conformidade com o sistema de gestão antissuborno, conforme descrito em 5.1.2.

A Alta Direção deve assegurar que as responsabilidades e autoridades para os papéis relevantes sejam atribuídas e comunicadas dentro e em todos os níveis da organização.

Gestores de todos os níveis devem ser responsáveis por requerer que os requisitos do sistema de gestão antissuborno sejam aplicados e cumpridos nos seus departamentos ou funções.

O Órgão Diretivo (se existir), a Alta Direção e todo o pessoal devem ser responsáveis por entender, cumprir e aplicar os requisitos do sistema de gestão antissuborno que se referem aos seus papéis na organização.

5.3.2 Função de *compliance* antissuborno

A Alta Direção deve atribuir a uma função de *compliance* antissuborno a responsabilidade e autoridade para:

a) supervisionar a concepção e a implementação pela organização do sistema de gestão antissuborno;

b) prover aconselhamento e orientação para o pessoal sobre o sistema de gestão antissuborno e as questões relativas ao suborno;

c) assegurar que o sistema de gestão antissuborno esteja em conformidade com os requisitos deste Documento;

d) reportar o desempenho do sistema de gestão antissuborno ao Órgão Diretivo (se existir) e à Alta Direção e outras funções de *compliance*, como apropriado.

A função de *compliance* antissuborno deve ser adequadamente provida de recursos e atribuída a pessoa(s) que tenha(m) competência, posição, autoridade e independência apropriadas.

A função de *compliance* antissuborno deve ter acesso direto e imediato ao Órgão Diretivo (se existir) e à Alta Direção, caso qualquer questão ou preocupação necessite ser levantada em relação ao suborno ou ao sistema de gestão antissuborno.

A Alta Direção pode atribuir alguma ou toda a função de *compliance* antissuborno a pessoas externas à organização. Neste caso, a Alta Direção deve assegurar que pessoal específico tenha responsabilidade e autoridade sobre aquelas partes da função, atribuídas externamente.

NOTA Para orientações, ver Seção A.6.

5.3.3 Tomada de decisão delegada

Onde a Alta Direção delegar para o pessoal a autoridade para tomar decisões em relação às quais existe mais do que um baixo risco de suborno, a organização deve estabelecer e manter um processo de tomada de decisão ou um conjunto de controles que requeira que o processo de decisão e o nível

de autoridade do(s) tomador(es) da decisão sejam apropriados e livres de conflitos de interesse reais ou potenciais. A Alta Direção deve assegurar que estes processos sejam periodicamente analisados criticamente e como parte do seu papel e responsabilidade para a implementação e a conformidade com o sistema de gestão antissuborno descrito em 5.3.1.

NOTA A delegação da tomada de decisão não exime a Alta Direção ou o Órgão Diretivo (se existir) das suas obrigações e responsabilidades, como descritas em 5.1.1, 5.1.2 e 5.3.1, nem necessariamente serão transferidas potenciais responsabilidades legais para o pessoal delegado.

6 Planejamento

6.1 Ações para abordar riscos e oportunidades

Ao planejar o sistema de gestão antissuborno, a organização deve considerar as questões referidas em 4.1, os requisitos referidos em 4.2, os riscos identificados em 4.5 e as oportunidades para melhoria, que precisam ser abordados para:

a) fornecer garantia razoável que o sistema de gestão antissuborno pode alcançar seus objetivos;

b) prevenir ou reduzir efeitos indesejados pertinentes aos objetivos e à política antissuborno;

c) monitorar a eficácia do sistema de gestão antissuborno;

d) alcançar a melhoria contínua.

A organização deve planejar:

— ações para abordar estes riscos de suborno e oportunidades para melhoria;

— como:

  — integrar e implementar essas ações nos processos do seu sistema de gestão antissuborno;

  — avaliar a eficácia dessas ações.

6.2 Objetivos antissuborno e planejamento para alcançá-los

A organização deve estabelecer objetivos do sistema de gestão antissuborno nas funções e níveis pertinentes.

Os objetivos do sistema de gestão antissuborno devem:

a) ser consistentes com a política antissuborno;

b) ser mensuráveis (se praticável);

c) levar em conta fatores aplicáveis referidos em 4.1, os requisitos descritos em 4.2 e os riscos de suborno identificados em 4.5;

d) ser alcançáveis;

e) ser monitoráveis;

f) ser comunicados de acordo com 7.4;

g) ser atualizados, como apropriado.

A organização deve reter informação documentada sobre os objetivos do sistema de gestão antissuborno.

Ao planejar como alcançar os seus objetivos do sistema de gestão antissuborno, a organização deve determinar:

— o que será feito;

— quais recursos serão requeridos;

— quem será responsável;

— quando os objetivos serão alcançados;

— como os resultados serão avaliados e relatados

— quem irá impor as sanções ou penalidades.

7 Apoio

7.1 Recursos

A organização deve determinar e fornecer recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão antissuborno.

NOTA Para orientações, ver Seção A.7.

7.2 Competência

7.2.1 Generalidades

A organização deve:

a) determinar a competência necessária de pessoa(s) que realiza(m) trabalho(s) sob o seu controle e que afeta(m) o seu desempenho antissuborno;

b) assegurar que essas pessoas sejam competentes com base em educação, treinamento ou experiência apropriados;

c) onde aplicável, tomar ações para adquirir e manter a competência necessária e avaliar a eficácia das ações tomadas;

d) reter informação documentada apropriada como evidência de competência.

NOTA Ações aplicáveis podem incluir, por exemplo, a provisão de treinamento, o *coaching*, a mudança de atribuições do pessoal ou parceiros de negócio; ou empregá-los ou contratá-los.

7.2.2 Processo de contratação de pessoal

7.2.2.1 Em relação a todo o seu pessoal, a organização deve implementar procedimentos tais que:

a) as condições de contratação requeiram que o pessoal cumpra com a política antissuborno e com o sistema de gestão antissuborno, e que seja dado à organização o direito de adotar medidas disciplinares no caso de não cumprimento;

b) dentro de um período de tempo razoável do início da sua contratação, o pessoal receba uma cópia ou que seja fornecido acesso à política antissuborno e treinamento em relação a essa política;

c) a organização tenha procedimentos que permitam tomar ações disciplinares apropriadas contra o pessoal que viole a política antissuborno ou o sistema de gestão antissuborno;

d) o pessoal não sofra retaliação, discriminação ou ações disciplinares (por exemplo, ameaças, isolamento, rebaixamento, impedimento de promoção, transferência, demissão, assédio, vitimização ou outras formas de intimidação) por:

   1) recusar-se a participar ou declinar de qualquer atividade em relação à qual tenha razoavelmente julgado que haja mais do que um baixo risco de suborno que não tenha sido mitigado pela organização; ou

   2) preocupações levantadas ou relatos feitos de boa-fé ou com base em uma convicção razoável de tentativas, reais ou suspeitas de suborno ou de violação da política antissuborno ou do sistema de gestão antissuborno (exceto nos casos em que o indivíduo participou da violação).

7.2.2.2 Em relação a todas as posições que estão expostas a mais do que um baixo risco de suborno, como determinado no processo de avaliação de riscos de suborno (ver 4.5), e à função de *compliance* antissuborno, a organização deve implementar procedimentos que prevejam que:

a) *a due diligence* (ver 8.2) seja conduzida nas pessoas antes de elas serem contratadas, e no pessoal antes de serem transferidos ou promovidos pela organização, para verificar, tanto quanto possível, se é apropriado contratá-los ou realocá-los e se é razoável acreditar que eles cumprirão com a política antissuborno e com os requisitos do sistema de gestão antissuborno;

b) os prêmios por desempenho, metas de desempenho e outros elementos de incentivo de remuneração são analisados criticamente de forma periódica, para verificar a existência de salvaguardas razoáveis implementadas para impedi-los de incentivar o suborno;;

c) o pessoal, a Alta Direção e o Órgão Diretivo (se existir) firmem uma declaração a intervalos razoáveis e proporcionais ao risco de suborno identificado, confirmando o seu cumprimento com a política antissuborno.

NOTA 1 A declaração de *compliance* antissuborno pode ser independente ou pode ser um componente de um processo de declaração de *compliance* mais abrangente.

NOTA 2 Para orientações, ver Seção A.8.

7.3 Conscientização e treinamento

A organização deve prover treinamento e conscientização antissuborno apropriados e adequados para o pessoal. Estes treinamentos devem abordar as seguintes questões, como apropriado, levando-se em conta os resultados do processo de avaliação de risco de suborno (ver 4.5):

a) a política antissuborno, os procedimentos e o sistema de gestão antissuborno da organização, e sua obrigação de cumpri-los;

b) os riscos de suborno e os danos causados a eles e à organização que podem resultar do suborno;

c) as circunstâncias nas quais o suborno pode ocorrer em relação às suas obrigações, e como reconhecer essas circunstâncias;

d) como reconhecer e responder às solicitações ou ofertas de propina;

e) como eles podem ajudar a prevenir e evitar suborno, e reconhecer indicadores-chave de riscos de suborno;

f) sua contribuição para a eficácia do sistema de gestão antissuborno, incluindo os benefícios de melhoria do desempenho antissuborno e de relatar suspeitas de subornos;

g) as implicações e potenciais consequências de não estar em conformidade com os requisitos do sistema de gestão antissuborno;

h) como e para quem eles são capazes de relatar quaisquer preocupações (ver 8.9);

i) informações sobre treinamento e recursos disponíveis.

O pessoal deve receber conscientização e treinamento antissuborno regularmente (a intervalos planejados definidos pela organização), como apropriado aos seus papéis, aos riscos de suborno a que eles estão expostos e a quaisquer mudanças de circunstâncias. Os programas de conscientização e treinamento devem ser atualizados periodicamente, quando necessário para refletir novas informações pertinentes.

Levando-se em conta os riscos de suborno identificados (ver 4.5), a organização deve também implementar procedimentos abordando a conscientização e o treinamento antissuborno para os parceiros de negócio que atuam em nome da organização ou para o seu benefício, e que podem representar mais do que um baixo risco de suborno para a organização. Estes procedimentos devem identificar os parceiros de negócio para os quais a conscientização e o treinamento sejam necessários, seu conteúdo e os meios pelos quais o treinamento deve ser fornecido.

A organização deve reter informação documentada sobre os procedimentos de treinamento, o conteúdo do treinamento e quando e para quem ele foi dado.

NOTA 1 Os requisitos de conscientização e treinamento para os parceiros de negócio podem ser comunicados por meio de requisitos contratuais ou similares, e ser implementados pela organização, pelo parceiro de negócio ou por outras partes indicadas para este propósito.

NOTA 2 Para orientações, ver Seção A.9.

7.4 Comunicação

7.4.1 A organização deve determinar as comunicações internas e externas pertinentes para o sistema de gestão antissuborno, incluindo:

a) o que ela irá comunicar;

b) quando comunicar;

c) com quem comunicar;

d) como comunicar;

e) quem irá comunicar;

f) os idiomas nos quais se comunicar.

7.4.2 A política antissuborno deve estar disponível para todo o pessoal da organização e aos parceiros de negócio, ser comunicada diretamente tanto para o pessoal quanto para os parceiros de negócio que representem mais do que um baixo risco de suborno, e deve ser publicada por meio de todos os canais de comunicação, internos e externos, da organização, conforme apropriado.

7.5 Informação documentada

7.5.1 Generalidades

O sistema de gestão antissuborno da organização deve incluir:

a) informação documentada requerida por este Documento;

b) informação documentada determinada pela organização como sendo necessária para a eficácia do sistema de gestão antissuborno.

NOTA 1 A extensão da informação documentada para um sistema de gestão antissuborno pode diferir de uma organização para outra devido:

— ao porte da organização e seu tipo de atividades, processos, produtos e serviços;

— à complexidade dos processos e suas interações;

— à competência do pessoal.

NOTA 2 A informação documentada pode ser retida separadamente como parte do sistema de gestão antissuborno, ou pode ser retida como parte de outros sistemas de gestão (por exemplo, *compliance*, financeiro, comercial, auditoria etc.).

NOTA 3 Para orientações, ver Seção A.17.

7.5.2 Criando e atualizando

Ao criar e atualizar informação documentada, a organização deve assegurar apropriadamente:

a) identificação e descrição (por exemplo, título, data, autor ou um número de referência);

b) formato (por exemplo, idioma, versão de *software*, gráficos) e meio (por exemplo, papel, eletrônico);

c) análise crítica e aprovação quanto à adequação e suficiência.

7.5.3 Controle da informação documentada

A informação documentada requerida pelo sistema de gestão antissuborno e por este Documento deve ser controlada para assegurar que:

a) ela esteja disponível e adequada ao uso, onde e quando necessária;

b) ela esteja protegida adequadamente (por exemplo, contra perda de confidencialidade, uso impróprio ou perda de integridade).

Para o controle de informação documentada, a organização deve abordar as seguintes atividades, como aplicável:

— distribuição, acesso, recuperação e uso;

— armazenamento e preservação, incluindo a preservação da legibilidade;

— controle de alterações (por exemplo, controle de versão);

— retenção e disposição.

A informação documentada de origem externa, determinada pela organização como necessária para o planejamento e operação do sistema de gestão antissuborno, deve ser identificada, como apropriado, e controlada.

NOTA Acesso pode implicar uma decisão relativa à permissão para somente ver a informação documentada, ou a permissão e autoridade para ver e alterar a informação documentada.

8 Operação

8.1 Planejamento e controle operacionais

A organização deve planejar, implementar, analisar criticamente e controlar os processos necessários para atender aos requisitos do sistema de gestão antissuborno, e implementar as ações determinadas em 6.1 para:

a) estabelecer critérios para os processos;

b) implementar controle dos processos de acordo com os critérios;

c) manter informação documentada na extensão necessária para se ter confiança de que os processos foram conduzidos como planejado.

Estes processos devem incluir os controles específicos referenciados em 8.2 a 8.10.

A organização deve controlar mudanças planejadas e analisar criticamente as consequências de mudanças não intencionais, tomando ações para mitigar quaisquer efeitos adversos, como necessário.

A organização deve assegurar que os processos terceirizados sejam controlados.

NOTA O texto central das normas ISO de sistemas de gestão contém um requisito em relação à terceirização, o qual não é usado neste Documento, já que os provedores terceirizados estão incluídos na definição de parceiros de negócio.

8.2 *Due diligence*

Quando o processo de avaliação dos riscos de suborno da organização, como realizado em 4.5, avaliar mais do que um baixo risco de suborno em relação a:

a) categorias específicas de transações, projetos ou atividades,

b) relacionamentos planejados ou em andamento com categorias específicas de parceiros de negócio, ou

c) categorias específicas de pessoal em determinadas posições (ver 7.2.2.2),

a organização deve avaliar a natureza e a extensão do risco de suborno em relação a transações, projetos, atividades, parceiros de negócio e pessoal específicos, que se encontram dentro destas categorias. Este processo de avaliação deve incluir qualquer *due diligence* necessária para obter informação suficiente para avaliar o risco de suborno. A *due diligence* deve ser atualizada em uma frequência definida para que as alterações e novas informações possam ser levadas em consideração apropriadamente.

NOTA 1 A organização pode concluir que é desnecessário, não razoável ou desproporcional realizar a *due diligence* em certas categorias de pessoal e parceiros de negócio.

NOTA 2 Os fatores listados em a), b) e c) anteriores não são exaustivos.

NOTA 3 Para orientações, ver Seção A.10.

8.3 Controles financeiros

A organização deve implementar controles financeiros que gerenciem os riscos de suborno.

NOTA Para orientações, ver Seção A.11.

8.4 Controles não financeiros

A organização deve implementar controles não financeiros que gerenciem os riscos de suborno em áreas como compras, operação, vendas, comercial, recursos humanos, atividades legais e regulatórias.

NOTA 1 Qualquer transação particular, atividade ou relacionamento pode estar sujeito tanto a controles financeiros quanto a controles não financeiros.

NOTA 2 Para orientações, ver Seção A.12.

8.5 Implementação de controles antissuborno por organizações controladas e por parceiros de negócio

8.5.1 A organização deve implementar procedimentos que requeiram que todas as outras organizações sobre as quais ela tem controle:

a) implementem o sistema de gestão antissuborno da organização, ou

b) implementem seus próprios controles antissuborno,

em cada caso, apenas na extensão razoável e proporcional, considerando os riscos de suborno a que a organização controlada está sujeita, levando-se em conta o processo de avaliação de riscos de suborno realizado de acordo com 4.5.

NOTA Uma organização tem controle sobre outra organização se ela controlar, direta ou indiretamente, a gestão da organização (ver A.13.1.3).

8.5.2 Em relação aos parceiros de negócio não controlados pela organização para os quais o processo de avaliação de riscos de suborno (ver 4.5) ou a *due diligence* (ver 8.2) tenham identificado mais do que um baixo risco de suborno, e onde os controles antissuborno implementados pelos parceiros de negócio associados possam ajudar a mitigar os riscos de suborno pertinentes, a organização deve implementar procedimentos conforme descrito a seguir:

a) a organização deve determinar se o parceiro de negócio tem implementado controles antissuborno que gerenciem os riscos de suborno pertinentes;

b) quando um parceiro de negócio não tem controles antissuborno implementados, ou não seja possível verificar se estão implementados:

   1) a organização deve, onde possível, requerer que o parceiro de negócio implemente controles antissuborno em relação às atividades, projetos ou transações pertinentes; ou

   2) quando não for possível requerer que o parceiro de negócio implemente controles antissuborno, este deve ser um fator a ser levado em consideração, quando da avaliação de riscos de suborno da relação com este parceiro de negócio (ver 4.5 e 8.2), bem como a maneira como a organização gerencia estes riscos (ver 8.3, 8.4 e 8.5).

NOTA Para orientações, ver Seção A.13.

8.6 Comprometimentos antissuborno

Para os parceiros de negócio que possam representar mais do que um baixo risco de suborno, a organização deve implementar procedimentos que requeiram que, onde possível:

a) o parceiro de negócio se comprometa em prevenir o suborno em seu nome ou para o benefício do parceiro de negócio em conexão com a transação, a atividade, o projeto ou relacionamentos pertinentes;

b) a organização seja capaz de encerrar o relacionamento com o parceiro de negócio no caso de suborno em seu nome ou para o benefício do parceiro de negócio em conexão com a transação, a atividade, o projeto ou relacionamentos pertinentes;

Quando não for possível, atender aos requisitos das alíneas a) ou b) anteriores, então este deve ser um fator a ser levado em consideração quando da avaliação do risco de suborno da relação com este parceiro de negócio (ver 4.5 e 8.2), bem como a maneira em que a organização gerencia estes riscos (ver 8.3, 8.4, e 8.5).

NOTA Para orientações, ver Seção A.14.

8.7 Presentes, hospitalidade, doações e benefícios similares

A organização deve implementar procedimentos que sejam concebidos para prevenir a oferta, fornecimento ou aceitação de presentes, hospitalidade, doações e benefícios similares onde a oferta, fornecimento ou aceitação são ou poderiam ser razoavelmente percebidos como suborno.

NOTA Para orientações, ver Seção A.15.

8.8 Gerenciando controles de inadequação de antissuborno

Sempre que a *due diligence* (ver 8.2), realizada em uma transação, projeto, atividade ou relacionamento específicos com um parceiro de negócio, estabelecer que os riscos de suborno não podem ser gerenciados por controles antissuborno existentes e a organização não puder ou não desejar implementar controles antissuborno adicionais ou ampliá-los, ou ainda tomar outras medidas apropriadas (como a mudança da natureza da operação, projeto, atividade ou relacionamento) para permitir que a organização gerencie os riscos de suborno pertinentes, a organização deve:

a) no caso de transação, projeto, atividade ou relacionamento existentes, tomar medidas apropriadas para os riscos de suborno e a natureza da transação, projeto, atividade ou relacionamento, para encerrar, descontinuar, suspender ou cancelar assim que possível;

b) no caso de novas propostas de transação, projeto, atividade ou relacionamento, adiar ou recusar a dar continuidade a elas.

8.9 Levantando preocupações

A organização deve implementar procedimentos que:

a) incentivem e permitam que o pessoal relate de boa-fé, ou com base em uma tentativa razoável de convicção, suspeita ou real de suborno, ou qualquer violação ou fragilidade fraqueza do sistema de gestão antissuborno para a função de *compliance* antissuborno ou ao pessoal apropriado (seja diretamente ou por meio de uma terceira parte apropriada);

b) exceto na extensão necessária para avançar em uma investigação, requeiram que a organização trate os relatos de forma confidencial para proteger a identidade de quem relatou e de outros envolvidos ou mencionados no relato;

c) permitam o relato de forma anônima;

d) proíbam retaliação e protejam aqueles que façam o relato da retaliação, após eles, de boa-fé ou com base em uma convicção razoável, terem levantado ou relatado uma preocupação sobre uma tentativa de suborno, real ou suspeita, ou violação da política antissuborno ou do sistema de gestão antissuborno;

e) permitam que o pessoal receba orientações de pessoa apropriada sobre o que fazer, se confrontado com uma preocupação ou situação que possa envolver suborno.

A organização deve assegurar que todo o pessoal esteja ciente dos procedimentos de relato e seja capaz de usá-los, e esteja ciente dos seus direitos e proteções nos termos dos procedimentos.

NOTA 1 Estes procedimentos podem ser os mesmos, ou fazer parte daqueles usados para relatar outras questões de preocupação (por exemplo, segurança, práticas inadequadas, transgressões ou outros riscos sérios).

NOTA 2 A organização pode usar um parceiro de negócio para gerenciar o sistema de relato em seu nome.

NOTA 3 Em algumas jurisdições, os requisitos em b) e c) anteriores são proibidos por lei. Nestes casos, a organização documenta a sua incapacidade de cumprimento.

8.10 Investigando e lidando com suborno

A organização deve implementar procedimentos que:

a) requeiram uma avaliação e, onde apropriado, investigação de qualquer suborno, ou violação da política antissuborno ou do sistema de gestão antissuborno, que seja relatado, detectado ou razoavelmente suspeito;

b) requeiram ação apropriada no caso em que a investigação revele qualquer suborno, ou violação da política antissuborno ou do sistema de gestão antissuborno;

c) deem poder e capacidade aos investigadores;

d) requeiram cooperação na investigação por pessoal pertinente;

e) requeiram que a situação e os resultados da investigação sejam relatados para a função de *compliance* antissuborno e para outras funções de *compliance*, como apropriados;

f) requeiram que a investigação seja conduzida de forma confidencial e que os resultados da investigação sejam confidenciais.

A investigação deve ser conduzida e relatada pelo pessoal que não participa do papel ou da função que está sendo investigada. A organização pode indicar um parceiro de negócio para conduzir a investigação e relatar os resultados ao pessoal que não participa da função ou do papel que está sendo investigado.

NOTA 1 Para orientações, ver Seção A.18.

NOTA 2 Em algumas jurisdições, o requisito em f) anterior é proibido por lei. Neste caso, a organização documenta sua incapacidade de cumprimento.

9 Avaliação do desempenho

9.1 Monitoramento, medição, análise e avaliação

A organização deve determinar:

a) o que precisa ser monitorado e medido;

b) quem é responsável pelo monitoramento;

c) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

d) quando o monitoramento e a medição devem ser realizados;

e) quando os resultados de monitoramento e medição devem ser analisados e avaliados;

f) para quem e como estas informações devem ser reportadas.

A organização deve reter informação documentada apropriada como evidência dos métodos e dos resultados.

A organização deve avaliar o desempenho antissuborno, a eficiência e a eficácia do sistema de gestão antissuborno.

NOTA Para orientações, ver Seção A.19.

9.2 Auditoria interna

9.2.1 A organização deve conduzir auditorias internas a intervalos planejados, para prover informação sobre se o sistema de gestão antissuborno:

a) está em conformidade com:

   1) os requisitos da própria organização para o seu sistema de gestão antissuborno;

   2) os requisitos deste Documento;

b) está implementado e mantido eficazmente.

NOTA 1 Orientações sobre sistemas de gestão de auditoria são fornecidas na ABNT NBR ISO 19011.

NOTA 2 O escopo e a escala das atividades da auditoria interna da organização podem variar, dependendo de uma variedade de fatores, incluindo o tamanho da organização, a estrutura, a maturidade e as localizações.

9.2.2 A organização deve:

a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios, os quais devem levar em consideração a importância dos processos pertinentes e os resultados de auditorias anteriores;

b) definir os critérios de auditoria e o escopo para cada auditoria;

c) selecionar auditores competentes e conduzir auditorias para assegurar objetividade e imparcialidade do processo de auditoria;

d) assegurar que os resultados das auditorias sejam reportados para a gerência pertinente, a função de *compliance* antissuborno, Alta Direção e, como apropriado, ao Órgão Diretivo (se existir);

e) reter informação documentada como evidência da implementação do programa de auditoria e dos resultados de auditoria.

9.2.3 Estas auditorias devem ser razoáveis, proporcionais e baseadas em risco. Tais auditorias devem consistir em processos de auditoria interna ou outros procedimentos que analisem criticamente, procedimentos, controles e sistemas para:

a) suborno ou suspeita de suborno;

b) violação da política antissuborno ou dos requisitos do sistema de gestão antissuborno;

c) falha do parceiro de negócio em atender aos requisitos antissuborno aplicáveis à organização;

d) fragilidades no sistema de gestão antissuborno ou oportunidades para sua melhoria.

9.2.4 Para assegurar a objetividade e imparcialidade destes programas de auditoria, a organização deve assegurar que estas auditorias sejam conduzidas por um dos seguintes:

a) uma função independente ou pessoal estabelecido ou designado para este processo; ou

b) a função de *compliance* antissuborno (a menos que o escopo da auditoria inclua uma avaliação do próprio sistema de gestão antissuborno, ou trabalho similar pelo qual a função de *compliance* antissuborno é responsável); ou

c) uma pessoa apropriada de um departamento ou outra função diferente daquela que está sendo auditada; ou

d) uma terceira parte apropriada; ou

e) um grupo que contemple quaisquer das opções a) a d).

A organização deve assegurar que nenhum auditor audite sua própria área de trabalho.

NOTA Para orientações, ver Seção A.16.

9.3 Análise crítica pela Direção

9.3.1 Análise crítica pela Alta Direção

A Alta Direção deve analisar criticamente o sistema de gestão antissuborno da organização, a intervalos planejados, para assegurar a sua contínua adequação, suficiência e eficácia.

A análise crítica pela Alta Direção deve incluir consideração de:

a) situação de ações de análises críticas de direções anteriores;

b) mudanças em questões externas e internas que sejam pertinentes para o sistema de gestão antissuborno;

c) informação sobre o desempenho do sistema de gestão antissuborno, incluindo tendências em:

   1) não conformidades e ações corretivas;

   2) resultados de monitoramento e medição;

   3) resultados de auditoria;

   4) relatos de suborno;

   5) investigações;

   6) natureza e extensão dos riscos de suborno a que a organização está sujeita;

d) eficácia das ações tomadas para abordar os riscos de suborno;

e) oportunidades para melhoria contínua do sistema de gestão antissuborno, como referido em 10.2.

As saídas da análise crítica pela Alta Direção devem incluir decisões relacionadas com oportunidades para melhoria contínua e qualquer necessidade de mudanças no sistema de gestão antissuborno.

Um resumo dos resultados da análise crítica pela Alta Direção deve ser reportado ao Órgão Diretivo (se existir).

A organização deve reter informação documentada como evidência dos resultados de análises críticas pela Alta Direção.

9.3.2 Análise crítica pelo Órgão Diretivo

O Órgão Diretivo (se existir) deve conduzir análises críticas periódicas do sistema de gestão antissuborno, baseadas na informação fornecida pela Alta Direção e pela função de *compliance* antissuborno, e qualquer outra informação que o Órgão Diretivo solicite ou obtenha.

A organização deve reter as informações documentadas resumidas como evidência dos resultados das análises críticas pelo Órgão Diretivo.

9.4 Análise crítica pela função de *compliance* antissuborno

A função de *compliance* antissuborno deve avaliar, em uma base contínua, se o sistema de gestão antissuborno está:

a) adequado para gerenciar eficazmente os riscos de suborno enfrentados pela organização;

b) sendo eficazmente implementado.

A função de *compliance* antissuborno deve reportar a intervalos planejados e em uma base *ad hoc*, como apropriado, para o Órgão Diretivo (se existir) e para a Alta Direção, ou para um comitê adequado do Órgão Diretivo ou da Alta Direção, sobre a adequação e implementação do sistema de gestão antissuborno, incluindo os resultados de investigações e auditorias.

NOTA 1 A frequência de tais relatórios depende dos requisitos da organização, mas é recomendado que seja pelo menos anualmente.

NOTA 2 A organização pode usar um parceiro de negócio para auxiliar na análise crítica, desde que as observações do parceiro de negócio sejam comunicadas de forma apropriada para a função de *compliance* antissuborno, para a Alta Direção e, como apropriado, para o Órgão Diretivo (se existir).

10 Melhoria

10.1 Não conformidade e ação corretiva

Ao ocorrer uma não conformidade, a organização deve:

a) reagir prontamente à não conformidade e, como apropriado:

   1) tomar medidas para controlá-la e corrigi-la;

   2) lidar com as consequências;

b) avaliar a necessidade de ação para eliminar as causas da não conformidade, a fim de que ela não se repita ou ocorra em outro lugar, ou seja:

   1) analisar criticamente a não conformidade;

   2) determinar as causas da não conformidade;

   3) determinar se não conformidades similares existem, ou podem potencialmente ocorrer;

c) implementar qualquer ação necessária;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas;

e) realizar mudanças no sistema de gestão antissuborno, se necessário.

As ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas.

A organização deve reter informação documentada como evidência:

— da natureza das não conformidades e quaisquer ações subsequentes tomadas;

— dos resultados de qualquer ação corretiva.

NOTA Para orientações, ver Seção A.20.

10.2 Melhoria contínua

A organização deve melhorar continuamente a adequação, suficiência e eficácia do sistema de gestão antissuborno.

NOTA Para orientações, ver Seção A.20.

Anexo A
(informativo)

Orientações para utilização deste Documento

A.1 Generalidades

As orientações deste Anexo são apenas ilustrativas. O objetivo deste Anexo é indicar para algumas áreas específicas o tipo de ações que uma organização pode adotar ao implementar seu sistema de gestão antissuborno. Este Anexo não é destinado a ser abrangente ou prescritivo, nem é necessário que uma organização implemente os passos a seguir para que tenha um sistema de gestão antissuborno que atenda aos requisitos deste Documento. Convém que os passos que uma organização adote sejam razoáveis e proporcionais em relação à natureza e extensão dos riscos de suborno enfrentados pela organização (ver 4.5 e os fatores de 4.1 e 4.2).

Orientações adicionais sobre boas práticas no sistema de gestão antissuborno são fornecidas em publicações listadas na Bibliografia.

A.2 Escopo do sistema de gestão antissuborno

A.2.1 Sistema de gestão antissuborno independente ou integrado

A organização pode escolher implementar este sistema de gestão antissuborno como um sistema separado ou como uma parte integrada de um sistema global de *compliance* (neste caso, a organização pode se referir para orientação à ISO 19600). A organização pode ainda escolher implementar o sistema de gestão antissuborno em paralelo ou como parte de outros sistemas de gestão, como os da qualidade, meio ambiente e segurança da informação (neste caso, a organização pode fazer referência às ABNT NBR ISO 9001, ABNT NBR ISO 14001 e ABNT NBR ISO/IEC 27001), bem como às ABNT NBR ISO 26000 e ABNT NBR ISO 31000).

A.2.2 Facilitação e pagamentos de extorsão

A.2.2.1 Pagamento de facilitação é a expressão às vezes atribuída a um pagamento ilegal ou não oficial, realizado em troca de serviços que o pagador teria legalmente direito de receber sem a realização deste pagamento. É normalmente um pagamento de pequeno valor, realizado a um agente público ou pessoa com função de aprovação, a fim de assegurar ou acelerar a realização de uma ação de rotina ou necessária, como a emissão de visto, permissão de trabalho, desembaraço de mercadorias ou instalação de telefone. Apesar de os pagamentos de facilitação serem, frequentemente, considerados diferentes em sua natureza de, por exemplo, pagamento de suborno para obtenção de negócios, eles são considerados ilegais na maioria dos lugares e são tratados como propina para fins deste Documento, e, portanto, convém que sejam proibidos pelo sistema de gestão antissuborno da organização.

A.2.2.2 Um pagamento de extorsão é quando o dinheiro é forçosamente extraído das pessoas por ameaças reais, ou percebidas à saúde, segurança ou liberdade, e está fora do escopo deste Documento. A segurança e a liberdade de uma pessoa são primordiais, e muitos sistemas jurídicos não criminalizam a realização de um pagamento por alguém que, razoavelmente, tema por sua saúde,

segurança ou liberdade, ou de outros. A organização pode ter uma política que permita um pagamento pelo pessoal em circunstâncias onde eles estejam em perigo iminente à sua saúde, segurança ou liberdade, ou de outros.

A.2.2.3 Convém que a organização forneça orientações específicas ao pessoal que pode ser confrontado com pedidos ou demandas para estes pagamentos, sobre como evitá-los ou lidar com eles. Tais orientações podem incluir, por exemplo:

a) especificar a ação a ser tomada por qualquer pessoal confrontado com o pedido de pagamento:

   1) no caso de pagamento de facilitação, solicitar prova de que o pagamento é legítimo e requerer um recibo oficial e, caso não haja comprovação satisfatória, recusar o pagamento;

   2) no caso de pagamento mediante extorsão, realizar o pagamento se sua saúde, segurança ou liberdade, ou de outrem, estiver ameaçada;

b) especificar a ação a ser adotada pelo pessoal que tenha realizado um pagamento de facilitação ou mediante extorsão:

   1) efetuar o registro do evento;

   2) reportar o evento para um gerente apropriado ou para a função de *compliance* antissuborno;

c) especificar a ação a ser adotada pela organização quando o pessoal tiver efetuado o pagamento de facilitação ou de extorsão:

   1) designar um gerente apropriado para investigar o evento (preferencialmente a função de *compliance* antissuborno ou um gerente que seja independente do departamento ou da função do pessoal);

   2) registrar corretamente os pagamentos na contabilidade da organização;

   3) se apropriado, ou se requerido por lei, reportar o pagamento às autoridades pertinentes.

A.3 Razoável e proporcional

A.3.1 O suborno é geralmente dissimulado. Pode ser difícil de prevenir, detectar e responder. Reconhecendo essas dificuldades, a intenção geral deste Documento é que o Órgão Diretivo (se existir) e a Alta Direção de uma organização precisem:

— ter um comprometimento genuíno para prevenir, detectar e responder a subornos relacionados ao negócio ou a atividades da organização;

— com intenção genuína, implementar medidas na organização que sejam concebidas para prevenir, detectar e responder a suborno.

As medidas não podem ser tão caras, onerosas e burocráticas que sejam inacessíveis ou tornem o negócio inviável, tampouco podem ser tão simples e ineficazes que o suborno possa ocorrer facilmente. As medidas precisam ser apropriadas ao risco de suborno e convém que tenham chance razoável de sucesso em seu objetivo de prevenir, detectar e responder a suborno.

A.3.2 Apesar das medidas antissuborno que precisam ser implementadas serem relativamente bem reconhecidas pelas boas práticas internacionais, e de algumas estarem refletidas como requisitos neste Documento, os detalhes reais das medidas a serem implementadas diferem amplamente de acordo com as circunstâncias pertinentes. É impossível prescrever em detalhes o que convém que a organização faça em circunstância particular. A qualificação “razoável e proporcional” foi introduzida neste Documento para que toda circunstância possa ser julgada de acordo com seu próprio mérito.

A.3.3 Os exemplos a seguir fornecem uma orientação sobre como a qualificação de “razoável e proporcional” pode ser aplicada em relação a diferentes circunstâncias.

a) Uma organização multinacional muito grande poderia precisar lidar com múltiplos níveis de gestão e milhares de pessoas. Assim, seu sistema de gestão antissuborno tipicamente precisa ser bastante mais detalhado do que o de uma pequena organização e com poucas pessoas.

b) Uma organização que tenha atividades em um local com mais do que alto risco de suborno precisará normalmente do processo de avaliação de riscos de suborno e procedimentos de *due dilligence* mais abrangentes, e um nível mais elevado de controle antissuborno sobre suas transações de negócios naquele local em que uma organização que tenha atividades somente em locais com mais do que baixo risco de suborno, onde o suborno é relativamente raro.

c) Apesar de o risco de suborno existir em relação a muitas transações ou atividades, é provável que o processo de avaliação de risco de suborno, os procedimentos de *due dilligence* e os controles antissuborno implementados por uma organização envolvida em uma grande, valiosa transação, ou em atividades envolvendo uma ampla gama de parceiros de negócio sejam mais abrangentes que aqueles implementados por uma organização em relação a um negócio que envolve vender itens de pequeno valor a múltiplos clientes ou múltiplas pequenas transações com uma única parte.

d) Uma organização com vasta gama de parceiros de negócio pode concluir, como parte de seu processo de avaliação de risco de suborno, que seja improvável que certas categorias de parceiros de negócio, clientes de varejo, apresentem mais do que um baixo risco de suborno, e levar isso em conta na concepção e implementação do seu sistema de gestão antissuborno. Por exemplo, é improvável que a *due diligence* seja necessária ou que seja um controle proporcional e razoável, em relação aos clientes do varejo que estão comprando da organização itens como produtos de consumo.

A.3.4 Embora exista risco de suborno em relação a muitas transações, convém que uma organização implemente um nível mais abrangente de controle antissuborno sobre uma transação de alto risco de suborno do que sobre uma transação de baixo risco de suborno. Neste contexto, é importante compreender que a identificação e a aceitação de um baixo risco de suborno não significam que a organização aceita o fato de o suborno ocorrer, ou seja, o risco de ocorrência do suborno (se uma propina pode ocorrer) não é o mesmo que a ocorrência do suborno (o fato a propina propriamente dita). A organização pode ter “tolerância zero” para a ocorrência de suborno, enquanto ainda envolver negócios e situações em que haja baixo risco de suborno, ou mais do que um baixo risco (desde que sejam aplicadas medidas de mitigação adequadas). Orientação adicional sobre controles específicos é fornecida a seguir.

A.4 Processo de avaliação de riscos de suborno

A.4.1 A intenção do processo de avaliação de riscos de suborno requerida em 4.5 é possibilitar à organização a constituição de uma base sólida para o seu sistema de gestão antissuborno. Esta avaliação identifica os riscos de suborno que serão focados pelo sistema, ou seja, os riscos de suborno considerados prioritários pela organização para mitigação do risco de suborno, implementação de controle, alocação de pessoal de *compliance* antissuborno, recursos e atividades.

A seguir é fornecido um exemplo de como uma organização pode optar por realizar este processo de avaliação.

a) Selecionar o critério para a avaliação do risco de suborno. Por exemplo, a organização pode selecionar um critério em três níveis, (por exemplo, “baixo”, “médio” e “alto”), um mais detalhado em cinco ou sete níveis, ou uma abordagem ainda mais detalhada. Os critérios frequentemente levarão em consideração vários fatores, incluindo a natureza do risco de suborno, a probabilidade de ocorrência do suborno e a magnitude das consequências, que convém que ocorram.

b) Avaliar os riscos de suborno apresentados pelo tamanho e estrutura da organização. Uma pequena organização, baseada em um único local com controles de gestão centralizados nas mãos de poucas pessoas, pode ser capaz de controlar o seu risco de suborno mais facilmente do que uma organização muito grande com uma estrutura descentralizada e operando em muitos locais;

c) Examinar os locais e setores em que a organização opera ou prevê operar e avaliar o nível de risco de suborno que estes locais e setores podem apresentar. Um índice de suborno apropriado pode ser usado para auxiliar neste processo de avaliação. Locais ou setores com mais do que alto risco de suborno podem ser considerados pela organização, por exemplo, como de risco “médio” ou “alto”, o que pode resultar na organização impor um nível mais elevado de controles aplicáveis às suas atividades nestes locais ou setores;

d) Examinar a natureza, escala e complexidade dos tipos de atividades e operações da organização.

   1) Pode, por exemplo, ser mais fácil controlar o risco de suborno em uma organização que realiza uma pequena operação de produção em um único local, do que em uma organização que esteja envolvida em inúmeros projetos de construção de grande porte em várias localidades.

   2) Algumas atividades podem acarretar riscos de suborno específicos, por exemplo, acordos de contrapartidas por meio dos quais o governo adquire produtos ou serviços e exige que o fornecedor reinvista alguma proporção do valor do contrato no país da aquisição. Convém que a organização tome medidas apropriadas para prevenir que os acordos de contrapartida constituam suborno.

e) Examinar os tipos existentes e potenciais de parceiros de negócio da organização por categoria e avaliar o risco de suborno, em princípio, que eles apresentam. Por exemplo:

   1) A organização pode ter um grande número de clientes que compram seus produtos de valor muito baixo, e que, na prática, representam um mínimo risco de suborno para a organização. Neste caso, a organização pode considerar estes clientes como de baixo risco de suborno e pode determinar que estes clientes não precisam ter quaisquer controles antissuborno específicos a eles relacionados. Alternativamente, a organização pode lidar com clientes que compram produtos de valor muito elevado e que podem representar um risco de suborno significativo (por exemplo, o risco de demandarem suborno da organização como contrapartida de pagamentos, aprovações). Estes tipos de clientes podem ser considerados, por exemplo, como “médio” ou “alto” risco de suborno, e podem requerer um nível mais alto de controles antissuborno pela organização.

   2) Diferentes categorias de fornecedores podem representar distintos níveis de risco de suborno. Por exemplo, os fornecedores com um escopo muito grande de trabalho, ou que poderiam estar em contato com os clientes da organização, ou agentes públicos pertinentes, podem representar “médio” ou “alto” risco de suborno. Algumas categorias de fornecedores podem ser de “baixo” risco, por exemplo, fornecedores baseados em locais de baixo risco de suborno que não têm interface com agentes públicos pertinentes para a transação ou clientes da organização. Algumas categorias de fornecedores podem representar um risco “muito baixo” de suborno, por exemplo, fornecedores de pequenas quantidades de itens de baixo valor,

serviços de compras *on-line* para viagens aéreas ou hotéis etc. A organização pode concluir que os controles antissuborno específicos não precisam ser implementados em relação a estes fornecedores de baixo ou muito baixo risco de suborno.

3) Agentes ou intermediários que interagem com os clientes da organização ou agentes públicos que atuam em nome da organização, provavelmente representam um “médio” ou “alto” risco de suborno, especialmente se eles forem pagos com base em comissão ou taxa de sucesso.

f) Examinar a natureza e a frequência de interações com agentes públicos nacionais ou estrangeiros que possam representar um risco de suborno, por exemplo, interações com agentes públicos responsáveis pela emissão de licenças e aprovações podem representar um risco de suborno.

g) Examinar as obrigações e deveres legais, regulatórios, contratuais e profissionais aplicáveis, por exemplo, a proibição ou limitação de entretenimento de agentes públicos ou da utilização de agentes.

h) Considerar a extensão na qual a organização é capaz de influenciar ou controlar os riscos avaliados.

Os riscos de suborno acima se inter-relacionam. Por exemplo, os fornecedores da mesma categoria podem representar riscos de suborno diferentes, dependendo do local em que eles operem.

A.4.2 Tendo avaliado os riscos de suborno pertinentes, a organização pode, então, determinar o tipo e o nível de controles antissuborno a serem aplicados a cada categoria de risco e pode avaliar se os controles existentes são adequados. Se não, os controles podem ser devidamente melhorados. Por exemplo, um nível de controle mais elevado provavelmente será implementado com relação a locais ou categorias de parceiros de negócio de mais do que alto risco de suborno. A organização pode determinar que é aceitável ter um nível de controle baixo sobre atividades ou parceiros de negócio com baixo risco de suborno. Alguns dos requisitos deste Documento excluem expressamente a necessidade de aplicar esses requisitos a atividades de baixo risco de suborno ou parceiros de negócio (embora a organização possa optar por aplicá-los, se assim desejar).

A.4.3 A organização pode modificar a natureza da transação, projeto, atividade ou relacionamento de tal forma que a natureza e a extensão do risco de suborno sejam reduzidas a um nível que possam ser adequadamente gerenciadas pela existência de controles de riscos antissuborno, adicionais ou melhorados.

A.4.4 Este exercício de processo de avaliação de riscos de suborno não se destina a ser um exercício extenso ou excessivamente complexo, e os resultados do processo de avaliação não necessariamente se provarão corretos (por exemplo, uma transação avaliada como de baixo risco de suborno pode vir a ter a ocorrência de suborno). Na medida do possível, convém que os resultados do processo de avaliação de riscos de suborno reflitam os reais riscos de suborno enfrentados pela organização. Convém que o exercício seja concebido como uma ferramenta para ajudar a organização a avaliar e priorizar seu risco de suborno, e convém que seja analisado criticamente e revisado regularmente com base em mudanças na organização ou circunstâncias (por exemplo, novos mercados ou produtos, requisitos legais, experiências adquiridas).

NOTA Orientações adicionais são fornecidas na ABNT NBR ISO 31000.

A.5 Papéis e responsabilidades do Órgão Diretivo e da Alta Direção

A.5.1 Muitas organizações têm alguma forma de Órgão Diretivo (por exemplo, como um conselho de administração ou de supervisão) que tem responsabilidades gerais de supervisão no que diz respeito à organização. Estas responsabilidades incluem a supervisão sobre o sistema de gestão antissuborno da organização. No entanto, o Órgão Diretivo geralmente não exerce a direção do dia

a dia das atividades da organização: este é o papel da diretoria executiva (por exemplo, o presidente, diretor de operações), a qual é referida neste Documento como “Alta Direção”. No que diz respeito ao sistema de gestão antissuborno, convém que o Órgão Diretivo esteja bem informado sobre o conteúdo e a operação do sistema de gestão, e convém que exerça uma supervisão razoável com relação à adequação, eficácia e implementação do sistema de gestão. Convém que receba periodicamente informações com relação ao desempenho do sistema de gestão por meio do processo de análise crítica da direção (que pode caber a todo o corpo diretivo, ou a um comitê do corpo diretivo, como o comitê de auditoria). A este respeito, convém que a função de *compliance* antissuborno seja capaz de reportar informações sobre o sistema de gestão diretamente para o Órgão Diretivo (ou ao comitê apropriado).

A.5.2 Algumas organizações, particularmente as menores, não têm um órgão diretivo independente, ou os papéis do órgão diretivo e da diretoria executiva podem ser combinados em um grupo ou mesmo um indivíduo. Nestes casos, o grupo ou o indivíduo terá as responsabilidades atribuídas neste Documento à Alta Direção e ao Órgão Diretivo.

NOTA Comprometimento da liderança é frequentemente chamado de “*tone at the top*” ou de “*tone from the top*”.

A.6 Função de *compliance* antissuborno

A.6.1 O número de pessoas trabalhando na função de *compliance* antissuborno depende de fatores como o tamanho da organização, a extensão do risco de suborno que a organização enfrenta, e a carga de trabalho resultante da função. Em uma organização pequena, é provável que a função de *compliance* antissuborno seja uma pessoa a quem foi atribuída a responsabilidade em tempo parcial, e que consiga combinar esta com outras responsabilidades. Quando a extensão do risco de suborno e a carga de trabalho resultante justifiquem, a função de *compliance* antissuborno pode ser uma pessoa a quem seja atribuída a responsabilidade em tempo integral. Em organizações de grande porte, a função provavelmente será ocupada por várias pessoas. Algumas organizações podem atribuir a responsabilidade a um comitê que incorpore uma gama de competências pertinentes. Algumas organizações podem optar por usar uma terceira parte para realizar parte ou toda a função de *compliance* antissuborno, e isso é aceitável, desde que um gerente apropriado da organização mantenha responsabilidade global e autoridade sobre a função de *compliance* antissuborno, e supervisione os serviços prestados pela terceira parte.

A.6.2 Este Documento requer que a função de *compliance* antissuborno seja provida por pessoa(s) com competência, *status*, autoridade e independência apropriadas. A este respeito:

a) “competência” significa que o pessoal pertinente tem educação, treinamento ou experiência apropriados, a habilidade pessoal para lidar com os requisitos de seus papéis e a capacidade de aprender sobre o papel e desempenhá-lo apropriadamente;

b) “*status*” significa que provavelmente o pessoal está suscetível a ouvir e respeitar as opiniões do pessoal responsável pela conformidade atribuída;

c) “autoridade” significa que à(s) pessoa(s) pertinente(s) a quem for atribuída a responsabilidade de *compliance* tenham sido concedidos poderes suficientes pelo Órgão Diretivo (se houver) e pela Alta Direção, de maneira a assumir as responsabilidades de *compliance* eficazmente;

d) “independência” significa que a(s) pessoa(s) pertinente(s) a quem é(são) atribuída(s) a(s) responsabilidade(s) de *compliance* não é (são), tanto quanto possível, envolvida(s) pessoalmente nas atividades da organização que estejam expostas a riscos de suborno. Isto pode ser mais

facilmente obtido quando a organização nomeia uma pessoa para lidar com o papel em tempo integral, mas é mais difícil para uma organização menor que tenha designado uma pessoa para combinar o papel de *compliance* com outras atribuições. Quando a função de *compliance* antissuborno é desempenhada por tempo parcial, convém que o papel não seja desempenhado por uma pessoa que possa estar exposta ao suborno quando desempenhando a sua função principal. No caso de uma organização muito pequena, onde possa ser mais difícil se alcançar a independência, convém que a pessoa apropriada, no melhor de sua capacidade, separe suas outras responsabilidades das responsabilidades de *compliance,* de modo a se tornar imparcial.

A.6.3 É importante que a função de *compliance* antissuborno tenha acesso direto à Alta Direção e ao Órgão Diretivo (se houver), a fim de comunicar informação que seja pertinente. Convém que esta função não tenha que reportar exclusivamente a outro gerente na cadeia, o qual se reporte à Alta Direção, considerando que esta condição aumenta o risco de que a mensagem passada pela função de *compliance* antissuborno não seja total ou claramente recebida pela Alta Direção. Convém que a função de *compliance* antissuborno também tenha uma relação de comunicação direta com o Órgão Diretivo (se houver), sem ter que passar pela Alta Direção. Isso pode ser tanto para o Órgão Diretivo completamente constituído (por exemplo, um conselho de administração ou um conselho de supervisão) ou pode ser a um comitê especialmente delegado pelo Órgão Diretivo ou Alta Direção (por exemplo, um comitê de auditoria ou de ética).

A.6.4 A principal responsabilidade da função de *compliance* antissuborno é supervisionar a concepção e a implementação do sistema de gestão antissuborno. Convém que isso não seja confundido com a responsabilidade direta pelo desempenho antissuborno da organização e cumprimento das leis antissuborno aplicáveis. Cada um é responsável por conduzir-se de forma ética e cumpridora, incluindo a conformidade com os requisitos do sistema de gestão antissuborno da organização e as leis antissuborno. É particularmente importante que a gerência assuma o papel de liderança para alcançar o *compliance*, pelas partes da organização, sobre as quais tem responsabilidade.

NOTA Orientações adicionais são fornecidas na ISO 19600.

A.7 Recursos

Os recursos necessários dependem de fatores como o tamanho da organização, a natureza de suas operações e os riscos de suborno que enfrenta. Os recursos podem incluir, por exemplo:

a) **Recursos humanos:** Convém que exista pessoal suficiente que seja capaz de dedicar tempo suficiente para suas responsabilidades antissuborno pertinentes, a fim de que o sistema de gestão antissuborno possa funcionar eficazmente. Isto inclui a atribuição de pessoal suficiente (interno ou externo) para a função de *compliance* antissuborno.

b) **Recursos físicos:** Convém que existam recursos físicos necessários na organização, inclusive para a função de *compliance* antissuborno, de modo que o sistema de gestão de antissuborno funcione eficazmente, por exemplo, espaço de escritório, mobiliário, equipamentos de computador (*hardware e software*), materiais de treinamento, telefones, artigos de papelaria etc.

c) **Recursos financeiros:** Convém que exista um orçamento suficiente, inclusive para a função de *compliance* antissuborno, de modo que o sistema de gestão de antissuborno funcione eficazmente.

A.8 Procedimentos de contratação de pessoal

A.8.1 *Due diligence* em pessoas

Ao proceder à *due diligence* em pessoas, antes de admiti-las, a organização, dependendo da funções propostas e dos correspondentes riscos de suborno, pode tomar ações como:

a) discutir a política antissuborno da organização com potencial candidato em uma entrevista e formar uma opinião se o pessoal parece entender e aceitar a importância do *compliance*;

b) adotar medidas razoáveis, a fim de verificar se as qualificações do potencial candidato são precisas;

c) adotar medidas razoáveis para obtenção de referências satisfatórias sobre o potencial candidato de empregadores anteriores;

d) adotar medidas razoáveis para determinar se o potencial candidato se envolveu com subornos;

e) adotar medidas razoáveis para verificar se a organização não está oferecendo o emprego ao potencial candidato como contrapartida por haver, em seu emprego anterior, favorecido indevidamente à organização;

f) verificar se a finalidade do oferecimento do emprego ao potencial candidato não é a de assegurar tratamento favorável indevido à organização;

g) adotar medidas razoáveis para identificar a relação potencial do potencial candidato com agentes públicos.

A.8.2 Bônus de desempenho

Arranjos para compensação, incluindo bônus e incentivos, podem encorajar, mesmo que não intencionalmente, o pessoal a participar de subornos. Por exemplo, se um gerente receber um bônus baseado na celebração de um contrato para a organização, ele pode ser tentado a pagar uma propina, ou a fazer vista grossa para um agente ou um parceiro de *joint venture* que esteja pagando uma propina, para assegurar a celebração do contrato. O mesmo resultado pode ocorrer se muita pressão for feita sobre o gerente para conseguir resultados (por exemplo, se o gerente puder ser demitido por não conseguir alcançar metas de vendas mais ambiciosas). A organização precisa prestar cuidadosa atenção a estes aspectos da compensação, para assegurar que, de forma razoável, não atuem como incentivos a subornos.

As avaliações de pessoal, promoções, bônus e outras recompensas podem ser usadas como incentivos para o pessoal agir de acordo com a política de antissuborno e o sistema de gestão antissuborno da organização. Contudo, a organização precisa ser cautelosa neste caso, porque a ameaça da perda de bônus etc. pode resultar na ocultação de falhas pelo pessoal no sistema de gestão antissuborno.

Convém que o pessoal esteja ciente de que a violação do sistema de gestão antissuborno não é aceitável para melhorar seus resultados em outras áreas (por exemplo, alcançar a meta de vendas) e convém que resulte em ação corretiva e/ou disciplinar.

A.8.3 Conflitos de interesse

Convém que a organização identifique e avalie o risco de conflito de interesses interno e externo. Convém que a organização informe a todo seu pessoal, de maneira clara, o dever de relatar qualquer conflito de interesse, real ou potencial, como conexão familiar, financeira ou outra direta ou indireta, que esteja relacionada à sua linha de trabalho. Isto auxilia a organização a identificar situações nas quais seu pessoal possa facilitar ou falhar em prevenir ou relatar subornos, por exemplo.

a) quando o gerente de vendas da organização possui relação com o gerente de compras do cliente, ou

b) quando um gerente de linha da organização possui interesse financeiro pessoal em negócios do concorrente.

Convém que a organização mantenha preferencialmente registro de qualquer circunstância de conflitos de interesse, reais ou potenciais, bem como das ações adotadas para mitigar o conflito.

A.8.4 Suborno pelo pessoal da organização

A.8.4.1 As medidas necessárias para prevenir, detectar e considerar os riscos de o pessoal da organização subornar outros em nome da organização (“suborno de dentro para fora”) podem diferir de medidas utilizadas para prevenir, detectar e abordar riscos de suborno por pessoas da organização (“suborno de fora para dentro”). Por exemplo, a capacidade de identificar e mitigar riscos de suborno de fora para dentro pode ser significativamente restringida à disponibilidade de informação não controlada pela organização (por exemplo, conta bancária pessoal de empregado e dados de transações de cartão de crédito), lei aplicável (por exemplo, legislação de privacidade) ou outros fatores. Como consequência, o número e as modalidades de controles disponíveis pela organização para mitigar os riscos de suborno de dentro para fora podem superar em quantidade os controles que podem ser implementados para mitigar riscos de suborno de fora para dentro.

A.8.4.2 O suborno do pessoal da organização tem maior probabilidade de ocorrer em relação ao pessoal que é capaz de tomar ou influenciar decisões em nome da organização (por exemplo, um gerente de compras que pode celebrar contratos; um supervisor que pode aprovar um trabalho realizado; um gerente que pode indicar pessoal ou aprovar salários ou bônus; um assistente que prepare documentos para obtenção de licenças, permissões). Como o suborno tende a ser aceito por pessoal que esteja fora do alcance dos sistemas de controles da organização, a capacidade da organização de prevenir ou detectar estas propinas pode ser limitada.

A.8.4.3 Em complementação às medidas referidas em A.8.1 e A.8.3, o risco de suborno de fora para dentro poderia ser mitigado pelos seguintes requisitos deste Documento que tratam deste risco:

a) convém que a política antissuborno da organização (ver 5.2) proíba explicitamente a solicitação e aceitação de propinas pelo pessoal da organização e qualquer um que trabalhe em seu nome;

b) convém que orientações e materiais de treinamento (ver 7.3) reforcem a proibição de solicitação e aceitação de propinas, e incluam:

   1) orientações para reportar preocupações sobre suborno (ver 8.9);

   2) ênfase na política de não retaliação da organização (ver 8.9).

c) convém que a política de presentes e hospitalidade da organização (ver 8.7) limite a aceitação de presentes e hospitalidades pelo pessoal;

d) a publicação da política antissuborno da organização em seu website e detalhes de como reportar suborno ajudam a definir as expectativas com parceiros de negócio, de modo a diminuir a probabilidade de que um parceiro de negócio ofereça, ou o pessoal da organização solicite ou aceite, uma propina;

e) controles (8.3 e 8.4) que requerem, por exemplo, uso de fornecedores aprovados, procedimentos de contratação por concorrência com pelo menos duas assinaturas em celebrações de contrato, aprovações de trabalho etc. reduzem o risco de premiações, aprovações, pagamentos ou benefícios oriundos de corrupção.

NOTA BRASILEIRA O termo "*contract award,*" para melhor entendimento, foi traduzido como "celebração de contrato", podendo também significar nomeação de contrato.

A.8.4.4 A organização pode também implementar procedimentos de auditoria para identificar formas pelas quais seu pessoal possa explorar fragilidades de controles para ganhos pessoais. Exemplos de procedimentos poderiam incluir:

a) análise crítica da folha de pagamento para identificação de registros de pessoal-fantasma e pessoal em duplicidade;

b) análise crítica dos registros de despesas de seu pessoal a trabalho para identificar dispêndios não usuais;

c) comparação de informações de folhas de pagamento de pessoal (por exemplo, número de contas bancárias pessoais e endereços) com as contas bancárias e endereços disponíveis na lista de fornecedores da organização, a fim de identificar cenários de potenciais conflitos de interesse.

A.8.5 Contratados ou trabalhadores temporários

Em alguns casos, contratados ou trabalhadores temporários podem ser disponibilizados para a organização por fornecedor de mão de obra ou outro parceiro de negócio. Neste caso, convém que a organização determine que o risco de suborno representado pelos contratados ou trabalhadores temporários (se houver) seja devidamente resolvido pelo tratamento dos contratados ou trabalhadores temporários como o seu próprio pessoal para fins de controle e treinamento, ou sejam impostos controles apropriados por meio do parceiro de negócios que disponibiliza os contratados ou trabalhadores temporários.

A.9 Conscientização e treinamento

A.9.1 A finalidade do treinamento é ajudar a assegurar que o pessoal pertinente compreenda, como apropriado, o seu papel dentro ou com a organização:

a) os riscos de suborno que eles e sua organização enfrentam;

b) a política antissuborno;

c) os aspectos do sistema de gestão antissuborno pertinentes ao seu papel;

d) quaisquer ações preventivas e de relato necessárias, que precisem ser adotadas em relação a qualquer risco ou suspeita de suborno.

A.9.2 A formalidade e a extensão do treinamento dependem do tamanho da organização e dos riscos de suborno enfrentados. Poderia ser conduzido como um módulo *on-line* ou métodos presenciais (por exemplo, sessões de aula, *workshops*, mesas redondas para discussões entre pessoas pertinentes ou sessões individuais). O método do treinamento é menos importante que o resultado, o conveniente é que todo o pessoal pertinente compreenda as questões referidas em A.9.1.

A.9.3 Treinamentos presenciais são recomendados para o Órgão Diretivo (se existir) e todo o pessoal (independentemente de suas posições ou hierarquia na organização) ou parceiros de negócio que estejam envolvidos em operações e procedimentos com mais que baixo risco de suborno.

A.9.4 Se a(s) pessoa(s) pertinente(s) designada(s) para a função de *compliance* antissuborno não tiver(em) experiência suficiente, convém que a organização providencie os treinamentos necessários para que ele ou ela desempenhe(m) a função de *compliance* antissuborno adequadamente.

A.9.5 O treinamento pode, de forma independente, tratar apenas de antissuborno, ou pode ser parte de um treinamento geral de *compliance* e ética ou do programa de integração.

A.9.6 O conteúdo do treinamento pode ser adaptado às funções do pessoal. O pessoal que não enfrenta riscos significativos de suborno em suas funções poderia receber um treinamento bastante simples sobre as políticas da organização, para que compreenda a política e saiba como agir, caso se depare com uma potencial violação. Convém que o pessoal cujo papel envolva um alto risco de suborno receba treinamento mais detalhado.

A.9.7 Convém que o treinamento seja repetido frequentemente, o tanto quanto necessário, para que o pessoal se mantenha atualizado com as políticas e procedimentos da organização, qualquer evolução em relação ao seu papel e quaisquer alterações regulatórias.

A.9.8 Aplicar os requisitos de conscientização e de treinamento aos parceiros de negócio identificados em 7.3 representa desafios específicos, porque os contratados de tais parceiros de negócio geralmente não trabalham diretamente para a organização, e a organização normalmente não tem acesso direto a estes contratados para efeitos de treinamento. O treinamento de fato dos contratados que trabalham para os parceiros de negócio será normalmente realizado pelos parceiros de negócio ou por outras partes contratadas para esta finalidade. É importante que os contratados que trabalham para os parceiros de negócio, que possam representar mais que um baixo risco de suborno para a organização, estejam cientes da questão e recebam treinamento, de forma razoável, destinado a reduzir este risco. O conteúdo de 7.3 requer que a organização ao menos identifique, nos parceiros de negócio, para quais contratados convém que seja ministrado treinamento antissuborno, qual o seu conteúdo mínimo e como ele será conduzido. O treinamento em si pode ser fornecido pelos parceiros de negócio, por outras partes definidas ou, se a organização escolher, por ela própria. A organização pode comunicar estas obrigações a seus parceiros de negócio de diversas maneiras, inclusive como parte de acordos contratuais.

A.10 *Due diligence*

A.10.1 O propósito de se conduzir uma *due diligence* em determinadas transações, projetos, atividades, parceiros de negócio ou no pessoal da organização é aprofundar a avaliação do escopo, escala e natureza dos riscos de suborno identificados como mais que um baixo risco de suborno, como parte do processo de avaliação de risco da organização (4.5). Serve também ao propósito de agir como um controle adicional direcionado à prevenção e detecção de risco de suborno, e informa a decisão da organização sobre a possibilidade de adiar, descontinuar, interromper ou rever estas transações, projetos ou relacionamentos com parceiros de negócio ou seu pessoal.

A.10.2 Fatores que a organização pode considerar úteis para avaliar projetos, transações e atividades incluem:

a) estrutura, natureza e complexidade (por exemplo, vendas diretas e indiretas, nível de descontos, procedimentos de contratação e celebração de contratos);

b) formas acordadas para financiamento e pagamento;

c) escopo do engajamento da organização e disponibilidade de recursos;

d) nível de controle e visibilidade;

e) parceiros de negócio e outras terceiras partes envolvidas (incluindo agentes públicos);

f) ligações entre quaisquer das partes em e) anterior e agentes públicos;

g) competências e qualificações das partes envolvidas;

h) reputação do cliente;

i) localização;

j) relatórios no mercado ou na imprensa.

A.10.3 Com relação à possível *due diligence* em parceiros de negócio:

a) fatores que a organização pode considerar úteis para avaliar os parceiros de negócio incluem:

   1) se o parceiro de negócio constitui uma entidade legítima de negócios, como demonstrado por indicadores como documentos de registro societário, contabilidade anual registrada, número de identificação fiscal (CNPJ/MF), listagem em bolsa de valores;

   2) se o parceiro de negócio tem as qualificações, experiência e recursos necessários para conduzir os negócios para os quais está sendo contratado;

   3) se e em que extensão o parceiro de negócio tem um sistema de gestão antissuborno;

   4) se o parceiro de negócio possui uma reputação relacionada a suborno, fraude, desonestidade ou má conduta similar, ou se tem sido investigado, condenado, sancionado ou impedido em razão de suborno ou conduta criminal similar;

   5) a identidade dos acionistas (inclusive do(s) beneficiário(s) final(is)) e da Alta Direção do parceiro de negócio, e se eles:

      i) têm uma reputação para suborno, fraude, desonestidade ou má conduta similar;

      ii) têm sido investigados, condenados, sancionados ou impedidos em razão de suborno ou conduta criminal semelhante;

      iii) têm qualquer vínculo direto ou indireto com os clientes da organização ou com agentes públicos pertinentes, que podem conduzir ao suborno (isto pode incluir pessoas que não são propriamente agentes públicos, mas que podem direta ou indiretamente estar relacionadas a agentes públicos, candidatos a cargos públicos etc.);

6) estrutura das transações e das formas de pagamento acordadas.

b) a natureza, o tipo e extensão da *due dilligence* conduzida dependerá de fatores como capacidade da organização de obter informações suficientes, os custos para obtenção das informações, e a extensão do risco de suborno possível imposto pela relação;

c) convém que os procedimentos de *due diligence* implementados pela organização em seus parceiros de negócios sejam consistentes em todos os níveis de risco de suborno similares. Parceiros de negócios com alto risco de suborno, em locais ou mercados onde haja um alto risco de suborno, são suscetíveis de requerer um nível significativamente mais elevado de *due diligence* do que de parceiros de negócios em locais ou mercado com baixo risco de suborno.

d) diferentes tipos de parceiros de negócio tendem a requerer diferentes níveis de *due diligence*. Por exemplo:

1) da perspectiva de potencial responsabilidade legal e financeira da organização, parceiros de negócio representam um alto risco de suborno à organização. Por exemplo, um agente envolvido em apoiar uma organização a obter a celebração de um contrato pode pagar uma propina a um gerente do cliente da organização, para ajudar a organização a ganhar o contrato, e isso pode resultar na responsabilização da organização pela conduta corrupta do agente. Como resultado, é provável que a *due diligence* da organização sobre o agente, seja a mais abrangente possível. Por outro lado, é menos provável que um fornecedor vendendo equipamento ou material para a organização e que não tenha envolvimento com os clientes da organização ou com agentes públicos que sejam pertinentes para as atividades da organização, seja menos capaz de pagar um suborno em nome da organização ou para o seu benefício e, portanto, o nível de *due diligence* neste fornecedor pode ser menor;

2) o nível de influência que a organização tem sobre seu parceiro de negócio também afeta a capacidade da organização de obter informações diretamente dos parceiros de negócio como parte da sua *due diligence*. Pode ser relativamente fácil para uma organização requerer que seus agentes e parceiros em *joint venture* forneçam ampla informação sobre si mesmos como parte de um exercício de *due diligence*, antes de a organização se comprometer a trabalhar com eles, considerando que a organização tem um grau de escolha sobre a quem contratar nesta situação. No entanto, pode ser mais difícil para uma organização requerer que um comprador ou cliente forneça informações sobre si ou preencha questionários de *due diligence*. Esta condição pode ser devido à organização não possuir influência suficiente sobre um comprador ou cliente, ou ser capaz de fazê-lo (por exemplo, onde a organização está envolvida em um concurso público de prestação de serviços ao cliente);

e) a *due diligence* realizada pela organização em seus parceiros de negócio pode incluir, por exemplo:

1) questionário enviado aos parceiros de negócio em que seja solicitado que responda a questões relacionadas a A.10.3 a);

2) pesquisa de *internet* sobre os parceiros de negócio, seus acionistas e sua Alta Direção, a fim de identificar qualquer informação relacionada a suborno;

3) pesquisas apropriadas em fontes governamentais, judiciais e internacionais para busca de informações pertinentes;

4) examinar listas disponíveis publicamente de organizações impedidas ou proibidas de contratar organizações públicas ou governamentais, mantidas por governos locais ou nacionais ou instituições multilaterais, como o Banco Mundial;

5) fazer pesquisas de outras partes apropriadas sobre a reputação ética do parceiro de negócio (por exemplo, para explicar qualquer informação adversa);

6) designar outras pessoas físicas ou jurídicas com experiência pertinente para auxiliar na condução do processo de *due diligence*;

f) O parceiro de negócio pode ser perguntado sobre o resultado inicial da *due diligence* (por exemplo, para explicar uma informação adversa).

A.10.4 *Due diligence* não é uma ferramenta perfeita. A ausência de informações negativas não necessariamente significa que o parceiro de negócio não possa causar risco de suborno. Informações negativas não necessariamente significam que o parceiro de negócio cause um risco de suborno. Entretanto, os resultados precisam ser cautelosamente avaliados e um julgamento racional realizado pela organização com base nos fatos disponíveis. A intenção geral é que a organização elabore perguntas razoáveis e proporcionais ao parceiro de negócio, levando em conta as atividades que o parceiro de negócio poderia realizar e o risco de suborno inerente a estas atividades, para então formar um julgamento racional sobre o nível de risco de suborno a que a organização estará exposta se trabalhar com o parceiro de negócio.

A.10.5 *Due diligence* sobre o pessoal está coberta em A.8.1

A.11 Controles financeiros

Controles financeiros são sistemas de gestão e processos implementados pela organização para gerenciar adequadamente suas transações financeiras e registrar estas transações precisamente e em tempo hábil. Dependendo do porte da organização e da transação, os controles financeiros implementados pela organização que podem reduzir o risco de suborno incluem, por exemplo:

a) implementar a separação de funções, de modo que a mesma pessoa não possa ao mesmo tempo iniciar e aprovar um pagamento;

b) implementar níveis escalonados apropriados de autoridade para aprovação de pagamentos (para que transações maiores requeiram a aprovação de um gerente mais sênior);

c) verificar se a indicação do beneficiário e o trabalho ou serviços executados foram aprovados pelos mecanismos de aprovação pertinentes da organização;

d) requerer pelo menos duas assinaturas para aprovações de pagamentos;

e) requerer a documentação apropriada de apoio para ser anexada às aprovações de pagamento;

f) restringir o uso de dinheiro em espécie e implementar métodos efetivos de controle de fluxo de caixa;

g) requerer que categorizações e descrições de pagamentos na contabilidade sejam corretas e claras;

h) implementar uma análise crítica periódica da gestão de transações financeiras significativas;

i) implementar auditorias financeiras independentes e periódicas, e substituir, em bases regulares, a pessoa física ou a organização que conduz a auditoria.

A.12 Controles não financeiros

Controles não financeiros são sistemas de gestão e processos implementados pela organização para ajudar a assegurar que as compras, o operacional, o comercial e outros aspectos não financeiros de suas atividades têm sido gerenciados adequadamente.

a) usar empreiteiras, subfornecedores, fornecedores e consultores aprovados, que tenham passado por um processo de pré-qualificação, onde a probabilidade de suas participações em suborno seja avaliada; este processo pode incluir *due diligence* do tipo descrito na Seção A.10;

b) avaliar:

   1) a necessidade e legitimidade dos serviços a serem fornecidos pelo parceiros de negócio da organização (excluindo clientes);

   2) se os serviços foram devidamente executados;

   3) se quaisquer pagamentos a serem realizados aos parceiros de negócio são razoáveis e proporcionais, levando em conta aqueles serviços. Isto é particularmente importante para evitar o risco de o parceiro de negócio utilizar parte do pagamento realizado pela organização para pagar uma propina em seu nome ou para o seu benefício. Por exemplo, se um agente for indicado pela organização para auxiliar nas vendas e a ele for paga uma comissão ou honorários na celebração de um contrato para a organização, a organização precisa estar razoavelmente convencida de que o pagamento da comissão é razoável e proporcional, levando-se em conta os serviços legítimos efetivamente realizadas pelo agente, considerando o risco assumido pelo agente no caso de o contrato não ser celebrado. Se uma comissão ou honorários elevados desproporcionais forem pagos, há um aumento do risco de que parte possa ter sido utilizada indevidamente pelo agente para influenciar um agente público ou um empregado do cliente da organização para celebrar o contrato. A organização pode também requerer que seus parceiros de negócio forneçam a documentação que demonstre que os serviços foram prestados;

c) celebrar contratos, onde possível e razoável, somente após um justo e, quando apropriado, transparente processo de licitação competitiva entre no mínimo três concorrentes ter sido realizado;

d) requerer no mínimo duas pessoas para avaliarem as propostas e aprovarem a celebração do contrato;

e) implementar uma separação de responsabilidades, de modo que o pessoal que aprova a contratação seja diferente daquele que solicita a contratação e seja de um departamento ou função diferente daquele que gerencia o contrato ou que aprova o trabalho realizado sob o contrato;

f) requerer a assinatura de pelo menos duas pessoas nos contratos, e nos Documentos que alterem os termos de um contrato ou que aprovem o trabalho realizado ou os fornecimentos previstos no contrato;

g) adotar um nível de gerenciamento geral elevado sobre transações com potencial de alto risco de suborno;

h) proteger a integridade das ofertas e outras informações sensíveis do preço, restringindo o acesso às pessoas apropriadas;

i) fornecer ferramentas e modelos apropriados para apoiar o pessoal (por exemplo, orientação prática, fazer ou não fazer, tabelas de aprovação, lista de verificação, formulários, fluxos de trabalho de TI).

NOTA Exemplos adicionais de controles e orientações podem ser encontrados na ISO 19600.

A.13 Implementação do sistema de gestão antissuborno por organizações controladas e por parceiros de negócio

A.13.1 Generalidades

A.13.1.1 A razão para o requisito em 8.5 é que tanto as organizações controladas quanto os parceiros de negócio podem representar um risco de suborno para a organização. Os tipos de risco de suborno que a organização tem pretensão de evitar, nestes casos são, por exemplo:

a) uma subsidiária da organização pagando suborno e, como resultado, a organização poder ser responsabilizada;

b) uma *joint venture* ou parceiro de uma joint venture, pagando propina para ganhar um trabalho para uma *joint venture*, da qual a organização participa;

c) um gerente de compras de um cliente pedindo propina para a organização em troca de uma celebração de contrato;

d) um cliente da organização requerendo que a organização indique um subcontratado ou fornecedor específico em situações onde um gerente do cliente ou agente público possa se beneficiar pessoalmente com esta indicação;

e) um agente da organização pagando propina para um gerente do cliente da organização, em nome da organização;

f) um fornecedor ou subcontratado da organização pagando propina para o gerente de compras da organização em troca de uma celebração de contrato.

A.13.1.2 Se a organização controlada ou o parceiro de negócio tiver implementado controles antissuborno em relação a estes riscos, consequentemente o risco de suborno para a organização é normalmente reduzido.

Este requisito em 8.5 faz uma distinção entre aquelas organizações sobre as quais a organização tem controle e aquelas sobre as quais ela não tem controle. Para os propósitos deste requisito, uma organização tem controle sobre outra organização quando ela controla, direta ou indiretamente, a gestão da organização. Uma organização pode ter controle, por exemplo, sobre uma subsidiária, *joint venture* ou consórcio por meio da maioria dos votos do conselho, ou por meio de uma maior participação societária. Para fins deste requisito, uma organização não tem controle sobre outra organização somente pelo fato de colocar um grande volume de trabalho na outra organização.

A.13.2 Empresas controladas

A.13.2.1 É razoável esperar que a organização requeira que qualquer outra organização que ela controle implemente controles antissuborno razoáveis e proporcionais. Isto pode ser feito com a organização controlada, implementando o mesmo sistema de gestão antissuborno, como o implementado pela própria organização, ou pela organização controlada implementando os seus próprios controles antissuborno específicos. Convém que estes controles sejam razoáveis e proporcionais, levando-se em consideração o processo de avaliação de riscos de suborno que a organização realiza, de acordo com 4.5.

A.13.2.2 Quando um parceiro de negócio é controlado pela organização (por exemplo, uma *joint venture* sobre a qual a organização tem o controle da gestão), então este parceiro de negócio controlado se enquadra nos requisitos de 8.5.1.

A.13.3 Parceiros de negócio não controlados

A.13.3.1 Com relação aos parceiros de negócio que não são controlados pela organização, a organização pode não precisar seguir os passos requeridos em 8.5.2 para requisitar a implementação pelo parceiro de negócio de controles antissuborno nas seguintes circunstâncias:

a) onde o parceiro de negócio não representa risco ou representa um baixo risco de suborno; ou

b) onde o parceiro de negócio representa mais do que um baixo risco de suborno, mas os controles que poderiam ser implementados por este parceiro de negócio não ajudam a mitigar o risco pertinente (não há motivo em insistir para que o parceiro de negócio implemente controles que não ajudariam; entretanto, espera-se, neste caso, que a organização leve em consideração este fator em seu processo de avaliação de risco, para informar sua decisão a respeito de como prosseguir com a relação).

Isto reflete a razoabilidade e a proporcionalidade deste Documento.

A.13.3.2 Se o processo de avaliação de riscos de suborno (4.5) ou a *due diligence* (8.2) concluir que o parceiro de negócio não controlado causa mais do que um baixo risco de suborno, e que os controles antissuborno implementados pelo parceiro de negócio podem ajudar a mitigar estes riscos de suborno, então convém que a organização adote as seguintes medidas adicionais, no âmbito de 8.5:

a) A organização determina se o parceiro de negócio tem controles antissuborno apropriados que gerenciem os riscos de suborno pertinentes. Convém que a organização faça esta determinação após a realização de uma *due diligence* apropriada (ver Seção A.10). A organização está tentando verificar se estes controles gerenciam o risco de suborno pertinente para a transação entre a organização e o parceiro de negócio. A organização não precisa verificar se o parceiro de negócio possui controles sobre seus maiores riscos de suborno. Notar que convém que tanto a extensão dos controles quanto as medidas que a organização precisa tomar para verificar estes controles sejam razoáveis e proporcionais em relação ao risco de suborno pertinente. Se a organização determinar, na medida do possível, que o parceiro de negócio possui controles apropriados implementados, então o requisito de 8.5 está contemplado em relação a este parceiro do negócio. Ver A.13.3.4 para comentários sobre tipos de controles apropriados.

b) Se a organização identificar que o parceiro de negócio não possui controles antissuborno apropriados que possam gerenciar os riscos de suborno pertinentes, ou se não for possível verificar se ele possui estes controles aplicados, então a organização pode adotar as seguintes medidas adicionais:

    1) Se praticável fazer isto (ver A.13.3.3), a organização requer que o parceiro de negócio implemente controles antissuborno (ver A.13.3.4) em relação às transações, projetos ou atividades pertinentes.

    2) Quando não for possível (ver A.13.3.3) requerer que o parceiro de negócios implemente controles antissuborno, a organização leva em conta este fator quando da avaliação dos riscos de suborno que os parceiros de negócios podem representar e a maneira pela qual a organização gerencia estes riscos. Isto não significa que a organização não possa dar continuidade à transação ou ao relacionamento. Entretanto, convém que a organização considere, como parte da avaliação do risco de suborno, a probabilidade de o parceiro de negócio estar envolvido em suborno, e convém que a organização leve em conta a ausência de tais controles na sua avaliação global do risco de suborno. Se a organização acreditar que os riscos de suborno representados por este parceiro de negócio são inaceitavelmente altos, e se o risco de suborno não puder ser reduzido por outros meios (por exemplo, uma reestruturação da transação), então as disposições de 8.8 serão aplicáveis.

A.13.3.3 O fato de ser ou não praticável para a organização requerer que um parceiro de negócio não controlado implemente controles depende das circunstâncias. Por exemplo:

a) Normalmente isto será praticável quando a organização tiver um grau de influência significativo sobre o parceiro de negócio. Por exemplo, quando a organização indicar um agente para atuar em seu nome em uma transação, ou indicar um subcontratado com um grande escopo de trabalho. Neste caso, a organização normalmente será capaz de implementar controles antissuborno, como uma condição pela indicação.

b) Normalmente isto não é praticável quando a organização não tem um grau de influência significativo sobre o parceiro de negócio. Por exemplo:

   1) um cliente para um projeto;

   2) um subcontratado ou fornecedor específico indicado pelo cliente;

   3) um importante subcontratado ou fornecedor quando o poder de barganha deste fornecedor ou subcontratado for maior que o da organização (por exemplo, quando a organização está comprando componentes de um grande fornecedor, nos termos estabelecidos por ele.

c) Normalmente isto não é praticável quando o parceiro de negócio não possui recursos ou experiência técnica que seja capaz de implementar os controles.

A.13.3.4 Os tipos de controles requeridos pela organização dependem das circunstâncias. Convém que eles sejam razoáveis e proporcionais ao risco de suborno, e convém que incluam no mínimo os riscos de suborno pertinentes no seu escopo. Dependendo da natureza do parceiro de negócio e da natureza do risco de suborno que representa, a organização pode, por exemplo, tomar as seguintes medidas:

a) No caso de um parceiro de negócio com alto risco de suborno, com um amplo e complexo escopo de trabalho, a organização pode requerer que o parceiro de negócio tenha controles implementados equivalentes àqueles requeridos por este Documento, pertinentes aos riscos de suborno que representa para a organização.

b) No caso de um parceiro de negócio de médio porte e médio risco de suborno, a organização pode requerer que o parceiro de negócio tenha implementado alguns requisitos antissuborno mínimos com relação à transação, como uma política antissuborno, treinamento para seus contratados pertinentes, um gerente com a responsabilidade por *compliance* em relação à transação, controles sobre pagamentos-chave e um canal de comunicação.

c) No caso de parceiros de negócio menores que possuem um escopo de trabalho muito específico (por exemplo, um agente ou um fornecedor menor), a organização pode requerer treinamento para os contratados pertinentes e controles sobre pagamentos-chave, presentes e hospitalidade.

Os controles só precisam funcionar com relação à transação entre a organização e o parceiro de negócio (embora, na prática, o parceiro de negócio possa ter controles aplicados em relação ao seu negócio como um todo).

Os pontos anteriores são apenas exemplos. A questão importante é que a organização identifique os riscos-chave de suborno em relação à transação e requeira, na medida do possível, que o parceiro de negócio tenha implementado controles razoáveis e proporcionais sobre estes riscos-chave de suborno.

A.13.3.5 Normalmente, a organização irá impor estes requisitos sobre o parceiro de negócio não controlado, como uma precondição para trabalhar com este parceiro e/ou como parte do documento contratual.

A.13.3.6 Não é requerido que a organização verifique se o parceiro de negócio não controlado está cumprindo com todos estes requisitos. Entretanto, convém que a organização tome passos razoáveis para assegurar-se de que o parceiro está em conformidade (por exemplo, solicitando que o parceiro de negócio forneça cópias de suas políticas pertinentes). Em casos de alto risco de suborno (por exemplo, um agente), a organização pode implementar procedimentos de auditoria e/ou relatórios de monitoramento.

A.13.3.7 Como os controles antissuborno podem levar algum tempo para serem implementados, é razoável para uma organização conceder ao seu parceiro de negócio tempo para implementar estes controles. Convém que a organização continue a trabalhar com este parceiro de negócio neste ínterim, mas a ausência de tais controles pode ser um fator a considerar tanto no processo de avaliação de riscos quanto na *due diligence* realizados. Entretanto, convém que a organização considere requerer o direito de encerrar o contrato ou acordo pertinente, caso o parceiro de negócio não implemente efetivamente os controles requeridos em tempo hábil.

A.14 Comprometimentos antissuborno

A.14.1 Este requisito para obter comprometimentos antissuborno aplica-se somente em relação aos parceiros de negócio que representam mais do que um baixo risco de suborno.

A.14.2 O risco de suborno é provavelmente baixo em relação à transação, por exemplo:

a) quando a organização compra uma pequena quantidade de itens de valor muito baixo;

b) quando a organização faz a reserva de passagens aéreas ou hospedagem *online*, diretamente no *site* da companhia aérea ou hotel;

c) quando a organização fornece bens ou serviços de baixo valor diretamente para um cliente (por exemplo, alimentos, filmes, *tickets* etc.).

Nestes casos, a organização não seria requerida a ter comprometimentos antissuborno destes fornecedores ou clientes com baixo risco de suborno.

A.14.3 No caso em que um parceiro de negócio possa representar mais do que um baixo risco de suborno, convém que a organização, quando possível, obtenha o comprometimento antissuborno deste parceiro de negócio.

a) Normalmente, será possível requerer estes comprometimentos quando a organização tiver influência sobre o parceiro de negócio e, portanto, pode insistir que o parceiro de negócio esteja comprometido. A organização pode também ser capaz de requerer estes comprometimentos, por exemplo, onde a organização indica um agente para atuar em seu nome em uma transação ou indica um subcontratado com um amplo escopo de trabalho.

b) A organização pode não ter influência suficiente para requerer estes comprometimentos quando, por exemplo, estiver negociando com grandes clientes, ou quando a organização estiver comprando componentes de um grande fornecedor nas condições-padrão estabelecidas por ele. Nestes casos, a ausência de tais disposições não significa que não convém que o projeto ou relação sigam adiante, mas convém que a falta de comprometimento seja considerada um fator pertinente no processo de avaliação dos riscos de suborno e *due diligence* realizados de acordo com 4.5 e 8.2.

A.14.4 Convém que estes comprometimentos, na medida do possível, sejam obtidos por escrito. Isto pode ser feito na forma de um Documento de comprometimento separado ou como parte de um contrato entre a organização e o parceiro de negócio.

A.15 Presentes, hospitalidade, doações e benefícios similares

A.15.1 A organização precisa estar consciente de que presentes, hospitalidade, doações e demais benefícios podem ser entendidos por uma terceira parte (por exemplo, um concorrente, a imprensa, um promotor de justiça ou juiz) como um suborno, mesmo que nem o doador nem o recebedor tenham tido esta intenção. Portanto, um mecanismo de controle útil é evitar, na medida do possível, quaisquer presentes, hospitalidades, doações e outros benefícios que possam ser razoavelmente percebidos por uma terceira parte como tendo propósito de suborno.

A.15.2 Os benefícios citados em 8.7 podem incluir, por exemplo:

a) presentes, entretenimento e hospitalidade;

b) doações políticas ou de caridade;

c) viagem de representante do cliente ou de agente público;

d) despesas promocionais;

e) patrocínio;

f) benefícios para comunidade;

g) treinamentos;

h) associações de clube;

i) favores pessoais;

j) informação privilegiada e confidencial.

A.15.3 Em relação a presentes e hospitalidade, os procedimentos implementados pela organização podem, por exemplo, ser concebidos para:

a) controlar a extensão e frequência de presentes e hospitalidades por:

   1) total proibição de quaisquer presentes e hospitalidades; ou

   2) permissão de presentes e hospitalidades, porém limitando-os por referência a fatores como:

      i) uma despesa máxima (que pode variar dependendo do local e do tipo de presente e hospitalidade);

      ii) frequência (pequenos presentes e hospitalidade podem acumular grandes quantidades, se repetidos);

      iii) tempo (por exemplo, nem durante ou imediatamente antes ou depois de negociações de uma licitação);

      iv) razoabilidade (considerando localização, setor e senioridade do doador ou recebedor);

v) identidade do beneficiário (por exemplo, aqueles em posição de celebrar contratos ou aprovar licenças, certificados ou pagamentos);

vi) reciprocidade (ninguém na organização pode receber um presente ou hospitalidade de valor superior ao do presente que está autorizado a dar);

vii) o contexto legal e regulatório (alguns locais e organizações podem ter proibições ou controles próprios aplicados);

b) requerer aprovação prévia de presentes e hospitalidade acima de um valor ou frequência definidos por um gerente apropriado;

c) requerer que presentes e hospitalidade acima de um valor ou frequência definidos, sejam efetuados abertamente, formalmente documentados (por exemplo, em um livro de registros contábeis ou balancete) e supervisionados.

A.15.4 Em relação às doações políticas ou de caridade, patrocínio, despesas promocionais e benefícios para comunidade, os procedimentos implementados pela organização podem, por exemplo, ser concebidos para:

a) proibir pagamentos que são destinados a influenciar ou que podem ser percebidos de forma razoável como destinados a influenciar uma licitação ou outra decisão a favor da organização;

b) realizar *due diligence* no partido político, na instituição de caridade ou qualquer outro destinatário para assegurar que sejam legítimos e que não estejam sendo usados como um canal para suborno (isto pode incluir, por exemplo, pesquisas na *internet* ou outra investigação adequada para verificar se os gestores do partido político ou da instituição de caridade têm uma reputação para suborno ou conduta criminosa similar, ou se estão associados aos projetos da organização ou dos clientes);

c) requerer que um gerente apropriado aprove o pagamento;

d) requerer a divulgação pública do pagamento;

e) assegurar que o pagamento seja permitido pelas leis e regulamentos aplicáveis;

f) evitar fazer contribuições imediatamente antes, durante ou imediatamente após negociações contratuais.

A.15.5 Em relação a viagens do representante do cliente ou do agente público, os procedimentos implementados pela organização podem, por exemplo, ser concebidos para:

a) permitir somente um pagamento que seja autorizado pelos procedimentos do cliente ou órgão público, assim como por leis e regulamentos aplicáveis;

b) permitir somente viagens necessárias para a devida realização das funções do representante do cliente ou agente público (por exemplo, para inspecionar procedimentos de qualidade da organização em sua fábrica);

c) requerer que um gerente apropriado da organização aprove o pagamento;

d) requerer, se possível, que o supervisor ou empregador do agente público, ou o responsável pela função de *compliance* antissuborno seja notificado da viagem e hospitalidade a ser fornecida;

e) restringir pagamentos às despesas necessárias de viagem, hospedagem e alimentação, diretamente associadas a um itinerário de viagem razoável;

f) limitar o entretenimento a um nível razoável, de acordo com a política de presentes e hospitalidade da organização;

g) proibir pagamento de despesas de familiares ou amigos;

h) proibir pagamento de despesas de férias ou recreativas.

A.16 Auditoria interna

A.16.1 O requisito em 9.2 não significa que uma organização seja obrigada a ter sua própria função de auditoria interna separada. É requerido que a organização indique uma função ou pessoa adequada, competente e independente, com responsabilidade para conduzir esta auditoria. Uma organização pode usar uma terceira parte para operar o seu programa completo de auditoria interna, ou pode contratar uma terceira parte para implementar algumas partes de um programa existente.

A.16.2 A frequência da auditoria dependerá dos requisitos da organização. É provável que algumas amostras de projetos, contratos, procedimentos, controles e sistemas sejam selecionadas para auditoria anual.

A.16.3 A seleção das amostras pode ser baseada no risco e, sendo assim, por exemplo, um projeto com alto risco de suborno pode ser selecionado para ser auditado, ao invés de um projeto com baixo risco de suborno.

A.16.4 As auditorias normalmente precisarão ser planejadas com antecedência para que as partes pertinentes tenham os documentos necessários e em tempo hábil. Entretanto, em alguns casos, a organização pode considerar útil implementar uma auditoria na qual as partes a serem auditadas não sejam avisadas com antecedência.

A.16.5 Se uma organização tiver um Órgão Diretivo, este também pode orientar a organização na seleção e frequência de auditorias, se julgar necessário, a fim de exercer sua independência e ajudar a assegurar que as auditorias estejam focadas nas principais áreas de riscos de suborno da organização. O Órgão Diretivo também pode requerer acesso a todos os relatórios de auditoria e resultados, e que quaisquer auditorias que identifiquem certos tipos de questões de alto risco de suborno ou indicadores de risco de suborno, sejam a ele reportadas, quando a auditoria for concluída.

A.16.6 O objetivo da auditoria é fornecer uma garantia razoável ao Órgão Diretivo (se houver) e à Alta Direção de que o sistema de gestão antissuborno foi implementado e está funcionando eficazmente, para ajudar a prevenir e detectar o suborno, e para fornecer um impedimento a qualquer pessoal potencialmente corrupto (uma vez que eles estarão cientes de que seus projetos ou departamento podem ser selecionados para auditoria).

A.17 Informação documentada

A informação documentada, indicada em 7.5.1, pode incluir:

a) recebimento da política antissuborno pelo pessoal;

b) fornecimento da política antissuborno aos parceiros de negócio que causam mais do que um baixo risco de suborno;

c) políticas, procedimentos e controles do sistema de gestão antissuborno;

d) resultados da avaliação do risco de suborno (ver 4.5);

e) fornecimento de treinamento antissuborno (ver 7.3);

f) realização de *due diligence* (ver 8.2);

g) medidas tomadas para implementar o sistema de gestão antissuborno;

h) aprovações e registros de presentes, hospitalidades, doações e benefícios similares dados e recebidos (ver 8.7);

i) ações e resultados de preocupações levantadas com relação a:

   1) qualquer fragilidade do sistema de gestão antissuborno;

   2) incidentes de tentativa, suspeita ou suborno real;

j) resultados de monitoramento, investigação ou auditoria realizada pela organização ou por terceira parte.

A.18 Investigando e lidando com suborno

A.18.1 Este Documento requer que a organização implemente procedimentos apropriados sobre como investigar e lidar com quaisquer casos de suborno, ou violação dos controles antissuborno, que sejam reportados, detectados ou razoavelmente suspeitos. A forma como a organização investiga e lida com uma questão particular vai depender das circunstâncias. Cada situação é diferente, e convém que a resposta da organização seja razoável e proporcional às circunstâncias. Um relatório de uma importante questão com grande suspeita de suborno pode requerer uma ação mais rápida, significativa e detalhada do que uma pequena violação dos controles antissuborno. As sugestões a seguir são apenas orientações, e convém que não sejam consideradas prescritivas.

A.18.2 Convém que a função de *compliance* seja, preferencialmente, a destinatária de quaisquer relatórios com suspeita de suborno ou suborno real ou violação dos controles antissuborno. Se um relatório for enviado em primeira instância para outra pessoa, convém que os procedimentos da organização requeiram que este relatório seja repassado, o mais rápido possível, para a função de *compliance.* Em alguns casos, a função de *compliance* identificará uma suspeita ou violação.

A.18.3 Convém que o procedimento determine quem tem a responsabilidade para decidir como a questão será investigada e tratada. Por exemplo:

a) uma pequena organização pode implementar um procedimento sobre todas as questões, de qualquer magnitude, que convém que sejam relatadas diretamente pela função de *compliance* à Alta Direção para sua decisão de como responder.

b) uma grande organização pode implementar um procedimento de acordo com o qual:

   1) questões menores sejam tratadas pela função de *compliance*, com um relatório resumido sobre todas as questões menores, para a Alta Direção;

2) questões maiores sejam reportadas diretamente pela função de *compliance* para a Alta Direção, para sua decisão de como responder.

A.18.4 Convém, que após a identificação de qualquer questão, a Alta Direção ou a função de *compliance* (conforme apropriado) avalie os fatos conhecidos e a potencial gravidade da questão. Se eles ainda não tiverem fatos suficientes com os quais possam tomar uma decisão, convém iniciar uma investigação.

A.18.5 Convém que a investigação seja conduzida por uma pessoa que não esteja envolvida na questão. Pode ser a função de *compliance*, auditoria interna, outro gerente apropriado ou uma terceira parte apropriada. Convém que a pessoa que esteja investigando tenha autoridade, recursos e acesso apropriados à Alta Direção, a fim de permitir que a investigação seja realizada eficazmente. Convém também que a pessoa que está investigando tenha sido treinada ou tenha experiência anterior na condução de uma investigação. Convém que a investigação estabeleça prontamente os fatos e colete todas as evidências necessárias, por exemplo:

a) realizar inquéritos para determinar os fatos;

b) coletar toda documentação pertinente e outras evidências;

c) obter evidências de provas testemunhais;

d) onde for possível e razoável, requerer relatórios sobre os casos, por escrito e assinados pelas pessoas que os fizeram.

A.18.6 Durante a realização da investigação e de qualquer ação de acompanhamento, a organização necessita considerar os seguintes fatores pertinentes, por exemplo:

a) leis aplicáveis (pode ser necessária orientação jurídica);

b) a segurança do pessoal;

c) o risco de difamação ao fazer declarações;

d) a proteção da pessoa que faz o relato e de outros envolvidos ou mencionados no relatório (ver 8.9);

e) potencial responsabilidade criminal, civil e administrativa, perda financeira e dano de reputação à organização e pessoas;

f) qualquer obrigação legal ou benefício para a organização de se reportar às autoridades;

g) manutenção da confidencialidade da questão e da investigação, até que os fatos sejam estabelecidos;

h) a necessidade para a Alta Direção de requerer a cooperação total do pessoal na investigação.

A.18.7 Convém que os resultados da investigação sejam reportados à Alta Direção ou à função de *compliance*, como apropriado. Se os resultados forem reportados à Alta Direção, convém que eles também sejam reportados à função de *compliance* antissuborno.

A.18.8 Uma vez concluída a investigação pela organização e/ou se houver informação suficiente para tomar uma decisão, convém que a organização implemente ações de acompanhamento apropriadas. Dependendo das circunstâncias e da gravidade da questão, estas ações podem incluir uma ou mais

das seguintes:

a) encerrar, cancelar ou modificar o envolvimento da organização em um projeto, transação ou contrato;

b) reembolsar ou reivindicar qualquer benefício indevido obtido;

c) aplicar um processo disciplinar ao pessoal responsável (o que, dependendo da gravidade da questão, pode variar de uma advertência por um delito menor até a demissão por um delito mais grave);

d) reportar o problema às autoridades;

e) se um suborno ocorrer, tomar as ações necessárias para evitar ou lidar com as eventuais consequências legais do delito (por exemplo, contabilidade falsa que pode ocorrer onde um suborno é falsamente descrito nas contas, uma infração fiscal, onde um suborno é deduzido erroneamente da receita, ou lavagem de dinheiro, onde os produtos de um crime são tratados).

A.18.9 Convém que a organização analise criticamente seus procedimentos antissuborno para examinar se a questão ocorreu devido a alguma inadequação nos seus procedimentos e, se for o caso, convém tomar medidas urgentes e apropriadas para melhorar os seus procedimentos.

A.19 Monitoramento

O monitoramento do sistema de gestão antissuborno pode incluir, por exemplo, os seguintes aspectos:

a) eficácia dos treinamentos;

b) eficácia de controles, por exemplo, por saídas de amostras de ensaio;

c) eficácia na atribuição de responsabilidades para atender aos requisitos do sistema de gestão antissuborno;

d) eficácia na abordagem das falhas de *compliance* previamente identificadas; e

e) situações nas quais as auditorias internas não são realizadas conforme programado.

O monitoramento do desempenho de *compliance* pode incluir, por exemplo, os seguintes aspectos:

— não conformidade e “uma situação indesejável” (um incidente sem efeito adverso, quase acidente);

— situações nas quais os requisitos antissuborno não são atendidos;

— situações nas quais os objetivos não são alcançados; e

— situação da cultura de *compliance.*

NOTA Ver ISO 19600.

A organização pode realizar periodicamente autoavaliações, em toda a organização ou em partes dela, para avaliar a eficácia do sistema de gestão antissuborno (ver 9.2).

A.20 Mudanças no planejamento e na implementação do sistema de gestão antissuborno

A.20.1 Convém que a adequação e eficácia do sistema de gestão antissuborno seja avaliada em uma base contínua e regular, por diversos métodos, como análises críticas pelas auditorias internas (ver 9.2), análise crítica pela Alta Direção (ver 9.3) e função de *compliance* antissuborno (ver 9.4).

A.20.2 Convém que a organização considere os resultados e as saídas destas avaliações para determinar se existe uma necessidade ou oportunidade para mudar o sistema de gestão antissuborno.

A.20.3 Para ajudar a assegurar que a integridade do sistema de gestão antissuborno e sua eficácia sejam mantidas, convém que mudanças em elementos individuais do sistema de gestão considerem a dependência e o impacto desta mudança na eficácia do sistema de gestão como um todo.

A.20.4 Quando a organização determina a necessidade de alterações no sistema de gestão antissuborno, convém que estas mudanças sejam realizadas de maneira planejada, considerando o seguinte:

a) o propósito das mudanças e suas potenciais consequências;

b) a integridade do sistema de gestão antissuborno;

c) a disponibilidade de recursos;

d) a atribuição e reatribuição de responsabilidades e autoridades;

e) preço, extensão e prazo para implementação das mudanças.

A.20.5 Convém que aperfeiçoamentos do sistema de gestão antissuborno resultantes de medidas tomadas em razão de qualquer não conformidade (ver 10.1) e decorrentes de melhorias contínuas (10.2) sejam realizados sob a mesma abordagem, como estabelecido em A.20.4.

A.21 Agentes públicos

O termo agente público (3.27) é amplamente definido em muitas leis anticorrupção.

A lista a seguir não é exaustiva nem todos os exemplos são aplicáveis a todas as jurisdições. Ao avaliar seus riscos de suborno, convém que uma organização considere as categorias de agentes públicos com os quais ela trata ou pode vir a tratar.

O termo agente público pode incluir o seguinte:

a) titulares de cargos públicos em nível nacional, estadual, municipal ou de província, incluindo membros de órgãos legislativos, titulares de cargos executivo e judicial;

b) contratados de partidos políticos;

c) candidatos a cargos públicos;

d) funcionários do governo, incluindo funcionários de ministérios, agências governamentais; tribunais administrativos e quadros públicos;

e) agentes de organizações públicas internacionais, como, por exemplo, Banco Mundial, Nações Unidas, Fundo Monetário Internacional etc.,

f) contratados de empresas estatais, a menos que a empresa opere em uma base comercial normal no mercado, isto é, em uma base que é substancialmente igual à de uma empresa privada, sem subsídios preferenciais ou quaisquer outros privilégios (ver referência [17]).

Em muitas jurisdições, parentes e parceiros próximos de agentes públicos também são considerados agentes públicos, para os propósitos das leis anticorrupção.

A.22 Iniciativas antissuborno

Embora não seja um requisito deste Documento, a organização pode considerar útil participar ou considerar recomendações, sejam setoriais ou outras iniciativas antissuborno, que promovam ou publiquem boas práticas antissuborno pertinentes para as atividades da organização.

Bibliografia

[1] ABNT NBR ISO 9000, *Sistemas de gestão da qualidade – Fundamentos e vocabulário*

[2] ABNT NBR ISO 9001, *Sistemas de gestão da qualidade – Requisitos*

[3] ABNT NBR ISO 19011, *Diretrizes para auditoria de sistemas de gestão*

[4] ABNT NBR ISO 14001, *Sistemas de gestão ambiental – Requisitos com orientações para uso*

[5] ABNT NBR ISO/IEC 17000, *Avaliação da conformidade – Vocabulário e princípios gerais*

[6] ISO 19600, *Compliance management systems – Guidelines*

NOTA BRASILEIRA No Brasil, existe uma versão traduzida, a ISO 19600, *Sistema de gestão de compliance – Diretrizes*

[7] ABNT NBR ISO 22000, *Sistema de gestão da segurança de alimentos – Requisitos para qualquer organização na cadeia produtiva de alimentos*

[8] ABNT NBR ISO 26000, *Diretrizes sobre responsabilidade social*

[9] ABNT NBR ISO 27001, *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos*

[10] ABNT NBR ISO 31000, *Gestão de riscos – Princípios de diretrizes*

[11] ABNT NBR ISO GUIA 73, *Gestão de riscos – Vocabulário*

[12] ABNT ISO/IEC GUIA 2, *Normalização e atividades relacionadas – Vocabulário ge*ral

[13] BS 10500, *Specification for an anti-bribery management system*

[14] UNITED NATIONS. United Nations Convention against Corruption. New York. 2004. (Available at: http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf)

[15] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents. Paris: OECD. 2010. (http://www.oecd.org/corruption/oecdantibriberyconvention.htm)

[16] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Good Practice Guidance on Internal Controls, Ethics, and Compliance. Paris: OECD. 2010.

[17] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Commentaries on the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. 21 November 1997.

[18] UNITED NATIONS GLOBAL COMPACT / TRANSPARENCY INTERNATIONAL. Reporting guidance on the 10th principle against corruption.UN Global Compact. 2009

[19] INTERNATIONAL CHAMBER OF COMMERCE, TRANSPARENCY INTERNATIONAL, UNITED NATIONS GLOBAL COMPACT AND WORLD ECONOMIC FORUM. RESIST: Resisting Extortion and Solicitation in International Transactions. A company tool for employee training. 2010.

[20] INTERNATIONAL CHAMBER OF COMMERCE, Rules on Combating Corruption, Paris: ICC.2011

[21] TRANSPARENCY INTERNATIONAL. Business Principles for Countering Bribery and associated tools. Berlin: Transparency International. 2013.

[22] TRANSPARENCY INTERNATIONAL. Corruption Perceptions Index

[23] TRANSPARENCY INTERNATIONAL. Bribe Payers Index.

[24] WORLD BANK. Worldwide Governance Indicators.

[25] INTERNATIONAL CORPORATE GOVERNANCE NETWORK. ICGN Statement and Guidance on Anti-Corruption Practices. London: ICGN. 2009.

[26] WORLD ECONOMIC FORUM. Partnering Against Corruption Principles for Countering Bribery. An Initiative of the World Economic Forum in partnership with Transparency International and the Basel Institute on Governance. Geneva: World Economic Forum

[27] COMMITTEE OF THE SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO): Internal Control – Integrated Framework: May 2013