REVISTA METROPOLITANA DE GOVERNANCA CORPORATIVA - ISSN: 2447-8024

PRODUTO TECNOLOGICO

Este produto possui a finalidade de ser uma ferramenta útil e aplicada para as empresas e profissionais. Nesta proposta, o seu conteúdo se apresenta de forma pragmática e objetiva, e busca utilizar a estrutura de comunicação comum ao ambiente das organizações.

Este material não apresenta o arcabouço teórico comum aos trabalhos acadêmicos, no entanto eles foram elementos fundamentais para o desenvolvimento deste produtos. O referencial teórico que sustenta esta proposta pode ser identificado na pesquisa abaixo indicada.

Dissertação de mestrado – REESTRUTURAÇÃO DO COMPLIANCE EM CONSTRUTORA ENVOLVIDA EM ESCÂNDALO DE CORRUPÇÃO, que pode ser consultada pelo link → http://arquivo.fmu.br/prodisc/mestradoadm/abf.pdf

Se posicionam como autores desta Ferramenta:
Adilson de Brito Farias– Desenvolveu a pesquisa durante seu mestrado.
Celso Machado Júnior – Orientador da pesquisa.

FINALIDADE DESTE PRODUTO TECNOLÓGICO

Este Produto Tecnológico se posiciona como uma ferramenta destinada a auxiliar os gestores e membros do Conselho de Administração, a elaborar o seu próprio Manual de Sistema de Gestão de *Compliance*, para a empresa em que atuam. A estrutura utilizada se assemelha a das Normas ABNT NBR ISO 9001 – Sistemas de Gestão da Qualidade e ABNT NBR ISO 14001:2015 - Sistemas da gestão ambiental Requisitos com orientações para uso. A adoção deste formato possui por finalidade a implantação destes conceitos e empresas que já possuam estes sistemas de gestão implantados e ainda seguir padrão comum ao das normas da Associação Brasileira de Normas Técnicas – ABNT. Adicionalmente este manual busca ser elemento complementar as normas ISO 19600:2014, *Sistema de gestão de compliance - Diretrizes* e ABNT NBR ISO 37001:2017, *Sistemas de gestão antissuborno - Requisitos com orientações para o uso*

Este documento passou por um processo de revisão do editor da revista, e por mais dois revisores. Os revisores que participaram do processo de avaliação, se posicionam como profissionais atuantes na área, e que potencialmente se beneficiariam do uso desta ferramenta.

Atenciosamente.
Celso Machado Jr.
Editor da Revista Metropolitana
de Governança Corporativa.

1 Escopo

Este Documento estabelece os requisitos necessários para um sistema de gestão de *compliance* e as obrigações inerentes a sua implementação nas organizações.

2 Referência normativa

ISO 19600:2014, *Sistema de gestão de compliance – Diretrizes*
ABNT NBR ISO 37001:2017, *Sistemas de gestão antissuborno – Requisitos com orientações para o uso*

3 Termos e definições

Para os efeitos deste documento, aplicam-se os termos e definições da ISO 19600:2014.

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 de *compliance*. 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.

4.2 Entendendo as necessidades e expectativas das partes interessadas

A organização deve determinar:

a) as partes interessadas que são pertinentes ao sistema de gestão de *compliance*;

b) os requisitos destas partes interessadas.

4.3 Determinando o escopo do sistema de gestão de *compliance*

A organização deve determinar os limites e a aplicabilidade do sistema de gestão de *compliance* para estabelecer o seu escopo. Ao determinar esse escopo, a organização deve considerar:

a) as questões externas e internas referidas em 4.1;

b) os requisitos referidos em 4.2 e 4.5.1;

c) os resultados da avaliação de risco de *compliance* referidos em 4.6.

O escopo deve estar disponível como informação documentada.

4.4 Sistema de gestão de *compliance*

O sistema de gestão de *compliance* deve conter controles concebidos para tratar o risco de *compliance*, bem como prevenir, detectar e reagir ao descumprimento da política de *compliance* e do sistema de gestão de *compliance*.

4.5 Obrigações de *compliance*

4.5.1 Identificação das obrigações de *compliance*

A organização deve documentar suas obrigações de *compliance* de forma apropriada ao seu porte, complexidade, estrutura e operações. Exemplos de requisitos de *compliance* incluem:

- leis e regulamentos;
- permissões, licenças ou outras formas de autorização;
- ordens, regras ou diretrizes emitidas pelas agências reguladoras;
- decisões de tribunais de justiça ou tribunais administrativos;
- tratados, convenções e protocolos.
- acordos com grupos comunitários ou organizações não governamentais;
- acordos com as autoridades públicas e os clientes;
- requisitos organizacionais, como as políticas e os procedimentos;
- princípios voluntários ou códigos de prática;
- rotulagem voluntária ou compromissos ambientais;
- obrigações decorrentes de acordos contratuais com a organização;
- normas organizacionais e industriais pertinentes.

4.5.2 Manutenção das obrigações de *compliance*

As organizações devem dispor de processos para identificar novas leis e alterações de leis, regulamentos, códigos e outras obrigações de *compliance* para assegurar a sua continuidade.

4.6 Identificação, análise e avaliação dos riscos de *compliance*

4.6.1 A organização deve realizar regularmente o processo de avaliação de riscos de *compliance*, que devem:

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

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

c) avaliar a adequação e eficácia dos controles existentes da organização para tratar os riscos de *compliance* avaliados.

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

4.6.3 O processo de avaliação de riscos de *compliance* deve ser analisado criticamente:

a) em intervalos regulares, 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, novas atividades, iniciativas, produtos ou serviços;

c) em mudanças externas significativas, como circunstâncias econômico-financeiras, condições de mercado, passivos e relacionamento com as partes interessadas; d) nas alterações em obrigação de *compliance* (ver 4.5);

e) em casos de não *compliance*.

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

5 Liderança

5.1 Liderança e comprometimento

5.1.1 Órgão Diretivo (Conselho de Administração)

Quando a organização tem um Órgão Diretivo, este órgão deve demonstrar liderança e comprometimento em relação ao sistema de gestão de *compliance* para:

a) aprovar a política de *compliance* da organização;

b) assegurar que a estratégia da organização e a política de *compliance* estão alinhadas;

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

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

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

5.1.2 Alta Direção

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

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

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

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

d) comunicar interna e externamente sobre a política de *compliance*;

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

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

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

h) promover uma cultura de *compliance* apropriada dentro da organização;

i) promover a melhoria contínua do sistema de gestão de *compliance*;

j) apoiar outros papéis pertinentes da gestão para demostrar como sua liderança na prevenção e detecção do não cumprimento da política de *compliance*, ou do sistema de gestão de *compliance*, se aplica às áreas sob sua responsabilidade;

k) encorajar o uso de procedimentos de relato de má conduta ou de violações da política de *compliance* ou do sistema de gestão de *compliance*, seja suspeito ou real (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 de *compliance* da organização, ou por se recusar a descumprir a política de *compliance* ou o sistema de gestão de *compliance*, mesmo que tal recusa possa resultar na perda de um negócio para a organização;

m) reportar para o Órgão Diretivo (se existir), a intervalos planejados, sobre o conteúdo e operação do sistema de gestão de *compliance* e de alegações de má conduta ou de violação ao sistema de gestão de *compliance*, seja sistemático ou grave;

n) assegurar o alinhamento entre os objetivos operacionais e as obrigações de *compliance*.

5.2 Política de *compliance*

O Órgão Diretivo e a Alta Direção devem estabelecer, manter e analisar criticamente uma política de *compliance* que:

a) requeira o cumprimento das leis, regulamentações e outros requisitos aplicáveis e compromissos voluntários assumidos;

b) seja apropriada ao propósito da organização;

c) proveja uma estrutura para estabelecer, analisar criticamente e alcançar os objetivos de *compliance*;

d) inclua um comprometimento para satisfazer aos requisitos do sistema de gestão de *compliance*;

e) que defina as responsabilidades para gerenciar e relatar as questões de *compliance;*

f) defina o grau em que o *compliance* será incorporado nas políticas, procedimentos e processos;

g) que estabeleça o padrão de conduta e a responsabilização por prestar contas conforme requerido;

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

i) inclua um comprometimento para a melhoria contínua do sistema de gestão de *compliance*;

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

k) explique as consequências do não cumprimento com as políticas e procedimentos de *compliance*.

A política de *compliance* deve:

- estar disponível como informação documentada;
- ser comunicada nos idiomas apropriados dentro da organização e também para os parceiros de negócio que representem um risco de *compliance*;
- estar disponível para as partes interessadas pertinentes, conforme apropriado;
- ser atualizada, conforme requerido, para assegurar que ela permaneça irrelevante;
- ser estabelecida em alinhamento com os valores, os objetivos e a estratégia da organização.

5.3 Papéis, responsabilidades e autoridades organizacionais

5.3.1 Papéis e responsabilidades

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

A Alta Direção deve assegurar que as responsabilidades e as 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 de *compliance* 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 de *compliance* que se referem aos seus papéis na organização.

5.3.2 Função de *compliance*

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

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

b) prover aconselhamento e orientação para o pessoal sobre o sistema de gestão de *compliance*;

c) assegurar que o sistema de gestão de *compliance* da organização esteja em conformidade com os requisitos deste documento e que a organização esteja cumprindo com a obrigação de *compliance*;

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

e) identificar as obrigações de *compliance* com o apoio de recursos pertinentes e traduzir essa obrigação em políticas, procedimentos e processos;

f) integrar a obrigação de *compliance* nas políticas, procedimentos e processos existentes;

g) fornecer ou organizar apoio contínuo de treinamento em *compliance* para os empregados e, onde pertinente, para os parceiros de negócio, de modo a assegurar que todas as pessoas relevantes sejam treinadas regularmente;

h) promover a inclusão das responsabilidades de *compliance* em descrições de cargos e processos de gestão de desempenho de empregados;

i) estabelecer indicadores de desempenho de *compliance*, monitorando, medindo, analisando e avaliando esses indicadores.

j) desenvolver e implementar processos para a gestão da informação, como reclamações e/ou retroalimentação por meio de linhas diretas, um sistema de comunicação de irregularidades e de outros mecanismos de execução;

k) identificar riscos de *compliance* e gestão destes riscos de *compliance* relativos aos parceiros de negócio, como, por exemplo, os fornecedores, agentes, distribuidores, consultores e contratados.

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

A função de *compliance* 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 sistema de gestão de *compliance*.

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 um risco de *compliance*, 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.

5.3.4 Responsabilidade do empregado

Todos os empregados, incluindo gerentes e líderes devem:

a) aderir às obrigações de *compliance* da organização, que são relevantes para a sua posição e atribuições;

b) participar de treinamento de acordo com o sistema de gestão de *compliance*;

c) utilizar os recursos de *compliance* disponibilizados pela organização;

d) relatar preocupações, problemas e falhas relacionados ao *compliance*.

6 Planejamento

6.1 Ações para abordar os riscos de *compliance*

Durante o planejamento do sistema de gestão de *compliance*, a organização deve considerar as questões referidas em 4.1, os requisitos referidos em 4.2, os princípios da boa governança referidos em 4.4, as obrigações de *compliance* identificadas em 4.5 e os resultados da avaliação de risco de *compliance* referidos em 4.6 para determinar os riscos de *compliance* que necessitam ser abordados para:

— garantir que o sistema de gestão de *compliance* atinja o(s) seu(s) resultado(s) pretendido(s);

— prevenir, detectar e reduzir os efeitos indesejáveis;

— promover a melhoria contínua.

A organização deve planejar:

a) as ações para abordar os riscos de *compliance*;

b) integração e a implementação das ações em seus processos do sistema de gestão de *compliance*;

c) a avaliação da eficácia das ações mencionadas.

A organização deve reter informação documentada sobre as ações planejadas para abordar os riscos de *compliance*.

6.2 Objetivos de *compliance* e planejamento para alcançá-los

A organização deve estabelecer os seus objetivos do sistema de gestão de *compliance* em funções e níveis relevantes.

Os objetivos de *compliance* devem:

a) ser consistentes com a política de *compliance*;

b) ser mensuráveis (se possível);

c) levar em consideração os fatores aplicáveis referidos em 4.1, os requisitos descritos em 4.2, as obrigações de *compliance* identificadas em 4.5 e os riscos de *compliance* identificados em 4.6;

d) ser monitorados;

e) ser comunicados de acordo com 7.4;

f) ser atualizados e/ou revisados, caso necessário.

Ao planejar como alcançar seus objetivos de *compliance*, a organização deve determinar:

— o que será feito;

— os recursos que serão necessários;

— quem será responsável;

— quando será concluído;

— como os resultados serão avaliados e relatados.

A organização deve manter informação documentada sobre os objetivos de *compliance* e reter informação documentada como evidência sobre as ações planejadas para alcançá-los.

7 Apoio

7.1 Recursos

A organização deve determinar e fornecer os recursos necessários para o estabelecimento, desenvolvimento, implementação, avaliação, manutenção e melhoria contínua do sistema de gestão de *compliance* adequado ao seu porte, complexidade, estrutura e operações.

Os recursos incluem recursos humanos e financeiros, aconselhamento externo e habilidades especializadas, infraestrutura organizacional, material de referência contemporânea, sobre gestão de *compliance* e obrigações legais, desenvolvimento profissional e tecnologia.

7.2 Competência

7.2.1 Generalidades

A organização deve:

a) determinar as competências necessárias de pessoas que realizam trabalho sob o seu controle e que afetam o desempenho e a eficácia do sistema de gestão de *compliance*;

b) assegurar que essas pessoas sejam competentes, com base em educação, treinamento e/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 evidências de competência.

7.2.2 Processo de contratação de pessoal

7.2.2.1 Quadro geral

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

a) as condições de contratação requeiram que o pessoal cumpra a política de *compliance* e com o sistema de gestão de *compliance*, 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 após o início da sua contratação, o pessoal receba uma cópia ou que seja fornecido acesso à política de *compliance* 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 de *compliance* ou o sistema de gestão de *compliance*;

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 um risco de *compliance* que não tenha sido tratado 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 violação da política de *compliance* ou do sistema de gestão de *compliance* (exceto nos casos em que o indivíduo participou da violação).

7.2.2.2 Quadro de maior exposição ao risco de *compliance*

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

a) *a due diligence* 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 a política de *compliance* e os requisitos do sistema de gestão de *compliance*;

b) os prêmios por desempenho, metas de desempenho e outros elementos de incentivo de remuneração sejam analisados criticamente de forma periódica, para verificar a existência

de salvaguardas razoáveis implementadas para impedi-los de incentivar o descumprimento da política de *compliance* ou dos requisitos do sistema de gestão de *compliance*;

c) o pessoal, a Alta Direção e o Órgão Diretivo (se existir) firmem uma declaração a intervalos razoáveis e proporcionais ao risco de *compliance* identificado, confirmando o seu cumprimento com a política de *compliance* e com os requisitos do sistema de gestão de *compliance*.

7.3 Conscientização e treinamento

7.3.1 Generalidades

7.3.1.1 A organização deve assegurar a conscientização quanto ao cumprimento da política de *compliance* e do sistema de gestão de *compliance* , incluindo a provisão de treinamentos apropriados e adequados para o pessoal, incluindo a Alta Direção e o Órgão Diretivo (se existir). Os treinamentos e outros meios para se atingir a conscientização devem abordar as seguintes questões, como apropriado, levando-se em conta os resultados do processo de avaliação de risco de *compliance* (ver 4.6):

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

b) os riscos de *compliance* e os danos causados a eles e à organização que podem resultar do descumprimento da política de *compliance* ou do sistema de gestão de *compliance*;

c) as circunstâncias nas quais o descumprimento da política de *compliance* ou do sistema de gestão de *compliance* podem ocorrer em relação às suas obrigações, e como reconhecer essas circunstâncias;

d) como eles podem ajudar a prevenir e evitar o descumprimento da política de *compliance* ou do sistema de gestão de *compliance* e reconhecer indicadores-chave de riscos de *compliance*;

e) sua contribuição para a eficácia do sistema de gestão de *compliance*, incluindo os benefícios de melhoria do desempenho do sistema de gestão de *compliance* e de relatar suspeitas de descumprimento da política de *compliance* ou do sistema de gestão de *compliance*;

f) as implicações e potenciais consequências de não estar em conformidade com os requisitos do sistema de gestão de *compliance*;

g) como e para quem eles são capazes de relatar quaisquer preocupações;

h) informações sobre treinamento e recursos disponíveis.

7.3.1.2 O pessoal deve receber conscientização e treinamento na política de *compliance* regularmente (a intervalos planejados definidos pela organização), como apropriado aos seus papéis, aos riscos de *compliance* 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.

7.3.1.3 O treinamento deve ser adaptado às obrigações e aos riscos de *compliance* relacionados com os papéis e responsabilidades do pessoal, realizado por ocasião da sua admissão na

organização, alinhado com o programa e treinamento corporativo e incorporado nos planos de treinamentos anuais.

7.3.1.4 Um retreinamento em *compliance* deve ocorrer sempre que houver:

a) mudança de cargo ou responsabilidades;

b) mudanças em políticas, procedimentos e processos internos;

c) mudanças na estrutura da organização;

d) mudanças nas obrigações de *compliance*, especialmente nos requisitos legais ou das partes interessadas;

e) mudanças nas atividades, produtos ou serviços;

f) questões decorrentes do monitoramento, auditoria, análises críticas, reclamações e não cumprimento, incluindo retroalimentação das partes interessadas.

7.3.1.5 Levando-se em conta os riscos de *compliance* identificados (ver 4.6), a organização deve também implementar procedimentos abordando a conscientização e o treinamento na política de *compliance* e no sistema de gestão de *compliance* para os parceiros de negócio que atuam em nome da organização ou para o seu benefício, e que podem representar um risco de *compliance* 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.

7.3.2 Comportamento

O comportamento que cria e apoia o *compliance* deve ser incentivado e o comportamento que compromete o *compliance* não pode ser tolerado.

A Alta Direção deve:

a) incentivar o pessoal a aceitar a importância de alcançar os objetivos de *compliance* pelos quais são responsabilizados;

b) criar um ambiente onde o relato de não cumprimento com a política de *compliance* e com o sistema de gestão de *compliance* seja incentivado, assegurando que o pessoal que fez o relato estará a salvo de retaliação;

c) incentivar o pessoal a fazer sugestões que facilitem a melhoria contínua do desempenho de *compliance*;

d) assegurar que o *compliance* seja incorporado às iniciativas mais amplas da cultura e da mudança da cultura organizacional, incluindo os sistemas de avaliação de desempenho e reconhecimento;

e) assegurar que os objetivos e metas operacionais não comprometam o comportamento compatível.

7.3.3 Cultura de *compliance*

O desenvolvimento de uma cultura de *compliance* requer o comprometimento ativo, visível, consistente e sustentado da Alta Direção e do Órgão Diretivo (se existir) a um padrão comum de comportamento, publicado, e que seja requerido em todas as áreas da organização.

7.4 Comunicação

7.4.1 A organização deve determinar as comunicações internas e externas pertinentes para o sistema de gestão de *compliance*, 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 de *compliance* 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 um risco de *compliance* , 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 de *compliance* 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 de *compliance*.

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 de *compliance*, às obrigações de *compliance* e implementar as ações determinadas em 6.1 ao:

— estabelecer critérios para os processos;

— implementar um controle de processos de acordo com os critérios;

— manter informação documentada, na extensão necessária, para ter a confiança de que os processos foram realizados conforme o planejado.

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

8.2 Processos terceirizados

A organização deve assegurar que os processos terceirizados sejam controlados e monitorados.

Se houver qualquer terceirização das atividades da organização, é requerida para este caso a realização de uma *due diligence* para assegurar o cumprimento com as politicas e procedimentos de *compliance* da organização. Os controles sobre parceiros de negócio também devem estar em vigor para assegurar que o contrato seja cumprido de forma eficaz.

A organização deve considerar os riscos de *compliance* relacionados com os processos de terceira parte.

8.3 *Due diligence*

Quando o processo de avaliação dos riscos de *compliance* da organização, for realizado conforme descrito em 4.6, avaliar que existe um risco de *compliance* maior do que o que a organização está disposta a aceitar em relação a:

a) categorias específicas de transações, projetos ou atividades, processos, iniciativas, produtos e serviços;

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

c) categorias específicas de pessoal em determinadas posições.

d) A organização deve avaliar a natureza e a extensão do risco de *compliance* 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 *compliance*.

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.

9.2 Auditoria interna

9.2.1 A organização deve conduzir auditorias internas a intervalos planejados, para prover as seguintes informações sobre se o sistema de gestão de *compliance*:

a) está em conformidade com:

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

   2) os requisitos deste Documento;

b) está implementado e mantido de maneira eficaz.

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*, 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.

9.3 Análise Crítica pela Alta Direção e pelo Órgão Diretivo (se existir)

9.3.1 Análise crítica pela Alta Direção

A Alta Direção deve analisar criticamente o sistema de gestão de *compliance* 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 de *compliance*;

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

   1) não conformidades e ações corretivas;

2) resultados de monitoramento e medição;

3) resultados de auditoria;

4) relatos de violação da política de *compliance* ou do sistema e gestão de *compliance*; 5) investigações;

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

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

e) oportunidades para melhoria contínua do sistema de gestão de *compliance*, 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 de *compliance*.

10 Melhorias

10.1 Não conformidade, não cumprimento e ação corretiva

Quando uma não conformidade e/ou não cumprimento ocorrer, a organização deve:

a) reagir prontamente à não conformidade e/ou ao não cumprimento e, conforme o caso:

1) tomar medidas para controlar e corrigir; e/ou

2) lidar com as consequências;

b) avaliar a necessidade de ações para eliminar as causas fundamentais da não conformidade e/ou do não cumprimento, a fim de que não se repita ou ocorra em outros lugares, ao:

1) analisar criticamente a não conformidade e/ou não cumprimento;

2) determinar as causas de não conformidade e/ou não cumprimento;

3) determinar se existem não conformidades e/ou não cumprimentos similares, ou se poderiam potencialmente ocorrer;

c) implementar qualquer ação necessária;

d) analisar criticamente a eficácia das ações corretivas tomadas;

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

As ações corretivas devem ser apropriadas aos efeitos das não conformidades e/ou não cumprimentos encontrados.

10.2 Melhoria contínua

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

A organização deve considerar os resultados de análise e avaliação e as saídas de análise crítica pela função de *compliance*, Alta Direção e pelo Órgão Diretivo (se existir), para determinar se existem necessidades ou oportunidades que devem ser abordadas como parte da melhoria contínua.

Bibliografia

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

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

[3] ABNT NBR ISO 31000, *Gestão de riscos – Diretrizes*

[4] ISO 19600, *Sistema de gestão de compliance – Diretrizes*