COMPLIANCE, INVESTIGAÇÕES E GOVERNANÇA CORPORATIVA

COMPLIANCE EMPRESARIAL: POR QUE TER UM PROGRAMA NÃO BASTA

14 DE SETEMBRO DE 2026

AUTORES

RAPHAEL SORÉ
SÓCIO / SÃO PAULO

NATHÁLIA CORRÊA LEISER TAMER
ADVOGADA / SÃO PAULO

Compliance empresarial pode ser compreendido como o sistema pelo qual uma organização previne, detecta e responde a riscos de integridade. Essa definição é suficientemente clara para quem se aproxima do tema e suficientemente ampla para revelar sua complexidade. Afinal, prevenir, detectar e responder não são atividades isoladas. Elas dependem de decisões sobre governança, responsabilidades, recursos, controles, circulação de informações, apuração de fatos e remediação.

O ponto de partida mudou

A Lei Anticorrupção teve papel decisivo na consolidação dos programas de integridade no Brasil. A partir dela, e dos parâmetros desenvolvidos por autoridades nacionais e estrangeiras, difundiu-se uma estrutura que hoje é familiar: apoio da alta administração, avaliação de riscos, código de conduta, políticas, treinamentos, controles internos, canais de relatos, investigações, diligência de terceiros e monitoramento.

Essa consolidação foi necessária. Ela permitiu que empresas organizassem responsabilidades, criassem funções especializadas e desenvolvessem mecanismos internos antes pouco estruturados. Também estabeleceu referências para a avaliação de programas por autoridades, investidores, financiadores e parceiros comerciais. O amadurecimento da prática, porém, tornou insuficiente a simples verificação de que esses elementos existem.

Da presença dos elementos à coerência do sistema

A experiência demonstrou que programas formalmente semelhantes podem produzir resultados muito diferentes. Um código de conduta pode oferecer critérios para decisões sensíveis ou limitar-se a enunciar valores genéricos. Uma avaliação de riscos pode orientar prioridades e investimentos ou permanecer apartada da estratégia. Um canal pode permitir que a organização conheça problemas relevantes ou funcionar apenas como meio de recebimento e encaminhamento de relatos. Um processo de resposta pode levar à correção das causas de uma falha ou se limitar ao tratamento pontual de suas consequências.

A questão central, portanto, não é quantos instrumentos foram implementados, mas se há coerência entre o perfil da organização, os riscos identificados, as medidas adotadas e as evidências de seu funcionamento. É essa relação que permite distinguir um programa concebido para atender a uma referência formal de outro efetivamente incorporado à gestão do negócio.

O que torna um programa efetivo na prevenção, detecção e resposta a riscos?

> **Prevenir** exige compreender onde a organização está exposta e por que determinados riscos podem se materializar. Isso envolve examinar atividades, geografias, parceiros comerciais, estruturas de incentivo, processos decisórios e experiências anteriores. A partir dessa leitura, o programa deve definir responsabilidades e controles proporcionais. A sofisticação não está na multiplicação de aprovações, mas na escolha de medidas capazes de reduzir o risco sem desconsiderar a realidade operacional;

> **Detectar** depende da capacidade de receber e interpretar informações sobre desvios. Canais de relatos, controles financeiros, auditorias, monitoramento e análise de dados são fontes complementares. Sua utilidade está associada à qualidade das informações produzidas, aos critérios de escalonamento e à possibilidade de que os sinais relevantes cheguem, em tempo adequado, às pessoas com autoridade e independência para agir;

> **Responder** significa mobilizar, de forma proporcional, as instâncias e os instrumentos adequados ao problema identificado. Conforme a natureza do evento, a resposta pode envolver contenção imediata, correção de processos, revisão de controles, tratamento de impactos, comunicação a partes interessadas, interação com autoridades, medidas contratuais ou disciplinares e, quando necessário, investigação interna. O objetivo não é apenas encerrar uma ocorrência, mas recuperar a capacidade de gestão sobre o risco, documentar as decisões adotadas e reduzir a possibilidade de repetição.

A ampliação do campo da integridade e a coordenação entre especialidades

Os programas de integridade se desenvolveram, em grande medida, a partir do enfrentamento da corrupção e da fraude. As metodologias então consolidadas — avaliação de riscos, controles internos, diligência de terceiros, canais de relatos, investigações e remediação — mostraram-se úteis diante de outros riscos empresariais. Essa

evolução não criou uma especialidade única para matérias distintas; tornou mais evidente a necessidade de coordenar competências distribuídas pela organização.

Quando um risco apresenta dimensões jurídicas, operacionais, financeiras, humanas ou socioambientais, diferentes áreas precisam atuar a partir de responsabilidades claras e informações consistentes. A contribuição do programa está em estabelecer essa governança: definir quem identifica e avalia o risco, quem desenha e executa os controles, como os sinais relevantes são escalonados e a quem cabe decidir sobre a resposta.

O desenho, portanto, deve partir do contexto da organização, e não de uma taxonomia abstrata. Uma empresa industrial com extensa cadeia de fornecedores, interação com comunidades e operações em diferentes jurisdições apresenta riscos, fontes de informação e necessidades de coordenação distintos daqueles de uma organização de serviços. O programa precisa refletir essas diferenças e acompanhar a forma como a empresa efetivamente opera e se relaciona.

Direitos humanos, sustentabilidade e cadeia de valor

Essa necessidade de coordenação é particularmente clara nas agendas de direitos humanos, sustentabilidade e cadeia de valor. Uma das mudanças mais relevantes da prática empresarial foi a ampliação do olhar para além dos atos diretamente praticados pela pessoa jurídica. Os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos e os parâmetros internacionais de conduta empresarial responsável exigem que as organizações considerem os impactos que possam causar, para os quais possam contribuir ou aos quais estejam diretamente ligadas por suas relações comerciais.

Esse movimento amplia a própria compreensão da diligência de terceiros. A verificação reputacional permanece relevante, mas não esgota o trabalho. Conforme o risco, pode ser necessário compreender a cadeia, priorizar relações e impactos, estabelecer compromissos contratuais, estruturar mecanismos de monitoramento e definir respostas para problemas identificados. Na agenda de sustentabilidade, a mesma lógica alcança a confiabilidade de compromissos e divulgações: afirmações públicas precisam corresponder a processos, dados, responsabilidades e controles capazes de sustentá-las.

A atuação coordenada não transfere para a área de Compliance a responsabilidade técnica por todas essas matérias. Seu papel é contribuir para que a organização estabeleça critérios comuns de governança e assegure que a especialização de cada função não resulte em fragmentação da análise, lacunas de responsabilidade ou decisões tomadas sem acesso às informações relevantes.

Como avaliar a efetividade e maturidade de um programa de integridade?

Normas ISO, diretrizes da Controladoria-Geral da União e referências internacionais convergem quanto à necessidade de que programas sejam baseados em risco, recebam recursos adequados, estejam integrados à operação e sejam periodicamente avaliados. A efetividade não é aferida por um único indicador. Ela resulta da análise conjunta do desenho do programa, de sua aplicação e de sua capacidade de produzir informações, decisões e resultados consistentes.

Para organizações maduras, isso exige examinar, entre outros pontos, se os riscos de integridade influenciam decisões estratégicas; se a liderança recebe informações qualitativas, e não apenas indicadores de atividade; se os controles permanecem proporcionais às exposições; se os incentivos são compatíveis com as condutas esperadas; se terceiros são acompanhados de acordo com o risco; se sinais de alerta recebem tratamento adequado; e se falhas identificadas resultam em contenção, remediação e aperfeiçoamento.

Por que o programa de integridade precisa ser um sistema em revisão permanente?

Programas de integridade não eliminam a possibilidade de desvios, nem devem ser avaliados a partir dessa promessa. Sua função é reduzir a probabilidade de ocorrências razoavelmente previsíveis, aumentar a capacidade de identificá-las e permitir que a organização responda com base em critérios, fatos e responsabilidades previamente definidos.

O programa também precisa acompanhar mudanças no negócio. Expansões, aquisições, reorganizações, novas jurisdições, alterações na cadeia de fornecimento, pressão por resultados e experiências concretas modificam o perfil de risco. A maturidade está na capacidade de reconhecer essas mudanças, preservar o que funciona e revisar, com método, o que já não responde às necessidades da organização.