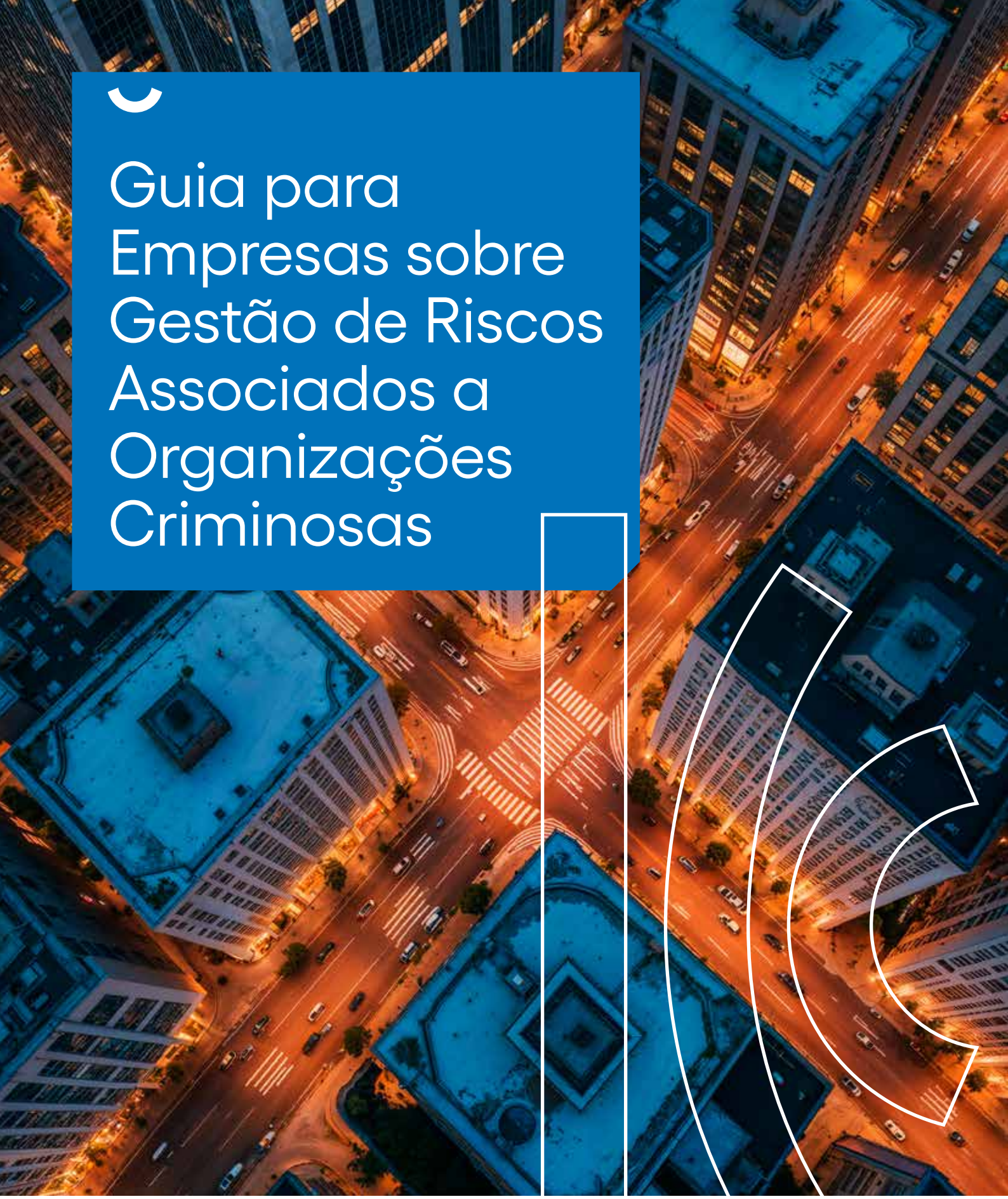
Guia para Empresas sobre Gestão de Riscos Associados a Organizações Criminosas



Realização

ICC Brasil

Colaboração

CONTROLADORIA-GERAL DA UNIÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Guia para Empresas sobre Gestão de Riscos Associados a Organizações Criminosas

ICC Brasil, com a colaboração da Controladoria-Geral da União (CGU)
Abril de 2026

Índice

Definições

Este Guia foi elaborado com base em normas como:

- Lei nº 12.846/2013 (Lei Anticorrupção), e seu Decreto Regulamentador nº 11.129/2022;
- Lei nº 9.613/1998 (Lei de Lavagem de Capitais e Financiamento ao Terrorismo);
- Lei nº 13.260/2016, Lei nº 13.709/2018 (Lei Geral de Proteção de Dados);
- Lei nº 12.850/2013 (Lei das Organizações Criminosas);
- Lei nº 9.296/1996 (Lei das Interceptações);
- Resolução COAF nº 36/2021;
- Carta Circular BACEN nº 4.001/2020;
- Circular BACEN nº 3.978/2020;
- Resolução BACEN nº 150/2021;
- Instrução Normativa BACEN nº 262/2022;
- Resolução BACEN nº 44/2020;
- Comunicado GAFI/FATF nº 43.419/2025;
- Lei nº 13.810/2019 (Sanções do Conselho de Segurança das Nações Unidas);
- Decreto nº 9.825/2019;
- Circular SUSEP nº 612/2020;
- Resolução CNSP nº 393/2020;
- Resolução CVM nº 50/2021;
- Resolução CMN nº 4.968/2021,
- Instrução Previc nº 34/2020; e
- Decreto nº 10.270/2020 (Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, de Financiamento do Terrorismo e de Financiamento da Proliferação de Armas de Destruição em Massa).

Glossário:

BACEN significa Banco Central do Brasil;

CGU significa Controladoria-Geral da União;

COAF significa Conselho de Controle de Atividades Financeiras;

CMN significa Conselho Monetário Nacional;

CNSP significa Conselho Nacional de Seguros Privados;

CVM significa Conselho de Valores Mobiliários;

Decreto Regulamentador significa o Decreto nº 11.129/2022, que regulamenta a Lei nº 12.846 (Lei Anticorrupção);

FINCEN (*Financial Crimes Enforcement Network*) significa Rede de Combate a Crimes Financeiros; e

GAFI/FATF significa Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo;

ICC (*International Chamber of Commerce*) significa Câmara Internacional de Comércio;

ISO 37002 é uma norma internacional que fornece diretrizes para a implantação, operação e melhoria contínua de sistemas de gestão de denúncias;

KCIs (*key control indicators*) significam indicadores-chave de controle;

KPIs (*key performance indicators*) significam indicadores-chave de desempenho;

KRIs (*key risk indicators*) significam indicadores-chave de risco;

OFAC (*Office of Foreign Assets Control*) significa Escritório de Controle de Ativos Estrangeiros;

Lei Anticorrupção significa a Lei nº 12.846/2013;

PLD/FT significa prevenção à lavagem de dinheiro e ao financiamento do terrorismo;

PREVIC significa Superintendência Nacional de Previdência Complementar;

SUSEP significa Superintendência de Seguros Privados;

US persons (Pessoas dos Estados Unidos da América) significa indivíduos ou entidades sujeitas às leis tributárias dos EUA, incluindo cidadãos (nascidos ou naturalizados), portadores de *Green Card*, residentes fiscais com presença física substancial no país, e empresas/trusts constituídos nos Estados Unidos; e

Wolfsberg Group é uma associação voluntária formada pelos principais bancos internacionais, dedicada ao desenvolvimento de padrões globais para prevenção à lavagem de dinheiro, combate ao financiamento do terrorismo e práticas responsáveis de integridade nos serviços financeiros.

Créditos

Este documento é um Guia elaborado pela ICC Brasil, com o apoio da CGU. Seu conteúdo não reflete, necessariamente, as opiniões individuais das organizações que integram a rede de relacionamento da ICC Brasil.

Direitos Reservados

ICC Brasil. *Guia para Empresas sobre Gestão de Riscos Associados a Organizações Criminosas*. São Paulo: ICC Brasil, 2026.

Este documento foi elaborado com contribuições de empresas associadas à ICC Brasil e coordenado por:

ICC Brasil

Equipe Executiva

Gabriella Dorlhiac, Diretora-Executiva

Paula Costim, Head de Policy

Paula Scalco, Gerente de Novos Negócios

Guilherme Rabel, Analista Júnior de Policy

Liderança da Comissão de Integridade e Responsabilidade Corporativa e da Task Force Integridade Frente ao Crime Organizado

José Alexandre Buaiz Neto, Chair da Comissão

Ana Paula Carracedo, Vice-Chair da Comissão

Chantal Pillet, Vice-Chair da Comissão e Co-Líder da Task Force

Karina Martins, Vice-Chair da Comissão e Co-Líder da Task Force

Carlos Flávio Lopes, Co-Líder da Task Force

Paula Mader, Co-Líder da Task Force

Luisa Mesquita, Coordenadora da Task Force

Marina Fronterotta, Coordenadora da Task Force

Com a colaboração de:

CONTROLADORIA-GERAL DA UNIÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Marcelo Pontes Vianna, Secretário de Integridade Privada

Cristine Köhler Ganzenmüller, Diretora de Promoção e Avaliação de Integridade Privada

Monique Cerqueira Zuidema, Coordenadora-Geral de Promoção de Integridade Privada

Sergio Filgueiras de Paula, Coordenador-Geral de Avaliação de Integridade Privada

Andre Spencer de Souza Holanda, Auditor Federal de Finanças e Controle

Isabella Brito, Chefe de Serviço da Coordenação-Geral de Promoção de Integridade Privada

Prefácio

O impacto das organizações criminosas sobre as atividades empresariais tem se consolidado como um tema central na agenda estratégica do setor privado. Trata-se de um fenômeno que afeta diretamente o ambiente de negócios, colocando em risco a integridade das empresas, e, por consequência, sua competitividade no Brasil e no exterior. Esse risco não se limita às atividades conduzidas nos escritórios e nas estruturas corporativas das empresas, estendendo-se também ao transporte aéreo, marítimo e terrestre, o que confere ao tema especial relevância para o debate sobre o ambiente de negócios no Brasil e a inserção internacional do país.

A crescente gravidade e complexidade desse cenário evidenciou a necessidade de aprofundamento da reflexão sobre o tema e impulsionou a ICC Brasil a promover um esforço estruturado de escuta e diálogo com lideranças empresariais e com a rede de empresas de seu ecossistema. A partir dessa mobilização e, em interlocução com representantes de diferentes setores, tornou-se possível compreender com maior clareza as principais preocupações, vulnerabilidades e limitações enfrentadas pelas empresas diante desse risco.

As informações reunidas ao longo desse processo indicam que a atuação das organizações criminosas exige das empresas abordagens mais estruturadas, minuciosas e integradas em todo o seu processo produtivo, capazes de fortalecer a prevenção, aprimorar a gestão de riscos e qualificar a resposta a incidentes ao longo das cadeias de valor. Esse contexto também evidencia que o enfrentamento dessas ameaças demanda articulação estratégica entre os setores privado e público, de modo a ampliar a compreensão mútua sobre os desafios envolvidos e favorecer a construção de caminhos de colaboração.

É nesse contexto que a ICC Brasil, em colaboração com a Controladoria-Geral da União (CGU), desenvolveu este Guia. A publicação, resultado da troca de experiências e conhecimento entre integrantes da ICC Brasil e da CGU, tem como propósito apoiar as empresas na compreensão desse fenômeno e em sua preparação para lidar com a potencial presença e influência de organizações criminosas em suas operações, contribuindo para o fortalecimento do *compliance* como instrumento estratégico de proteção da atividade econômica formal.

1 Introdução

O combate à corrupção, à lavagem de dinheiro e às organizações criminosas constitui uma agenda estratégica para o Brasil e para as empresas brasileiras, visto que impacta diretamente a economia real, a competitividade e credibilidade do país e a governança pública e privada. As organizações criminosas operam e expandem suas atividades ilícitas burlando mecanismos de fiscalização e de aplicação da lei, adotando, por exemplo, estratégias como a incorporação de estruturas empresariais aparentemente lícitas, a aquisição gradual ou a tomada de controle de empresas já estabelecidas e o uso de pessoas interpostas em novos negócios para ocupar a titularidade real de ativos e operações.

Estão presentes, também, em outras práticas, como lavagem de dinheiro, roubo de cargas, crimes digitais e ambientais e infiltração em cadeias produtivas. Por utilizarem, paralelamente, um histórico legítimo, a complexidade da detecção aumenta. A infiltração dessas práticas compromete a reputação de países e empresas, desafia estruturas de *compliance*, gera insegurança jurídica e fragiliza a estabilidade regulatória e econômica.

O que se percebe é que as organizações criminosas buscam, cada vez mais, se infiltrar nas várias esferas públicas e privadas para aumentar sua influência e atuação. Até por isso, é fundamental a cooperação entre os setores público e privado para buscar meios integrados e estruturados para lidar com os riscos.

Nesse contexto, o Guia para Empresas sobre Gestão de Riscos Associados a Organizações Criminosas busca conscientizar o setor privado sobre a presença e a influência de organizações criminosas nas cadeias produtivas, de fornecedores e de clientes das empresas. O documento também oferece orientações para auxiliar na gestão de riscos associados a práticas ilícitas que afetam a economia formal.

Partindo do reconhecimento de que o setor privado exerce um papel estratégico na identificação, prevenção e gestão desses riscos, este Guia adota uma abordagem não normativa e não exaustiva. Seu objetivo é apresentar considerações e proposições iniciais sobre governança, gestão de incidentes e tomada de decisão; exemplos de cenários práticos de como organizações criminosas podem se infiltrar em operações empresariais; e reflexões sobre as limitações e os desafios enfrentados pelas companhias, em especial as áreas de *compliance*. As orientações partem do entendimento de que mecanismos formais de controle e de *compliance* esbarram nas dinâmicas informais, assimétricas e transnacionais das organizações criminosas.

As diretrizes apresentadas podem ser utilizadas como referência para empresas de diferentes portes e setores, reguladas ou não, expostas direta ou indiretamente a riscos relacionados a atividades ilícitas. A aplicação do documento pressupõe adaptação às especificidades de cada companhia, conforme seu contexto de negócios, setor de atuação, perfil de risco e nível de maturidade em governança e *compliance*. As recomendações devem ser compreendidas como proposições para o fortalecimento de processos internos de identificação e mitigação desses riscos, e não como soluções definitivas, obrigações ou padrões vinculantes.

A velocidade de adaptação das organizações criminosas é extremamente alta, o que torna evidente a necessidade de acompanhamento contínuo e de atualização das medidas indicadas neste Guia. A proposta apresentada consiste em organizar situações exemplificativas que possam auxiliar na abordagem do tema. Ao identificar a problemática e apontar possíveis medidas a serem adotadas, este Guia se apresenta como uma referência para empresas direta ou indiretamente expostas à atuação do crime organizado.

2 Contexto, Diagnóstico e Natureza dos Riscos

O ambiente empresarial brasileiro tem registrado um aumento expressivo dos riscos associados à atuação de organizações criminosas. Estima-se que essas organizações movimentaram cerca de R$ 350 bilhões entre 2022 e 2024[1]. Trata-se, portanto, de um impacto sistêmico, que afeta a arrecadação, a concorrência e a integridade dos mercados.

Ao se tornar cada vez mais ousado e profissionalizado, o crime organizado não se limita à ocultação de recursos: busca infiltrar-se em negócios legítimos, utilizando-se de veículos e estruturas societárias complexas, como mecanismos de integração econômica.

Nesse contexto, instrumentos como fundos de investimento, estruturas de *private equity*, *fintechs*, *holdings*, veículos *offshore*, operações de M&A, franquias e novos prestadores de serviços passam a ser utilizados não apenas para movimentar recursos, mas para converter capital ilícito em receitas formais, dividendos e ganhos de capital, com aparência de legitimidade. O que se percebe é que as organizações criminosas se utilizam cada vez mais de meios lícitos - como operações de M&A, por exemplo - para promover a lavagem ou "regularização" de recursos provenientes de atividades criminosas.

A infiltração estrutural do crime organizado em negócios legítimos representa um risco sistêmico relevante, pois favorece a lavagem de dinheiro, a captura da governança, a distorção da concorrência, a influência econômica de grupos ilícitos, a normalização de fluxos ilícitos e o comprometimento da reputação e da sustentabilidade da empresa.

1 **FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. *Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil*. Coordenação: Nivio Nascimento; Eduardo Pazinato. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/c5a85bb2-214a-4288-abf5-fcc619612777/content. Acesso em: 6 abr. 2026.

Esses riscos não se limitam a perdas financeiras diretas. Mesmo relações indiretas com atividades ilícitas podem acarretar perdas financeiras e implicações jurídicas, além de comprometer a reputação das empresas, afetar a continuidade das operações, enfraquecer a integridade institucional em toda a cadeia e, possivelmente, colocar em risco a segurança dos colaboradores. Surgem questões recorrentes sobre como mapear fatores de risco (*red flags*), monitorar o mercado, identificar indícios de sua materialização, acionar as instâncias competentes e atuar de forma tempestiva nos negócios e junto às contrapartes envolvidas.

As manifestações mais frequentes envolvem evasão fiscal[2]; evasão de sanções comerciais; lavagem de dinheiro; fraudes; corrupção; roubo e furto de cargas; contrabando; violação de propriedade intelectual e comércio ilícito de produtos falsificados; uso indevido de estruturas logísticas e ataques cibernéticos. Entre as práticas adotadas pelas organizações criminosas destacam-se a sonegação por meio de declarações fictícias; vendas sem nota fiscal; operações interestaduais simuladas; desvio de finalidade em importações e exportações; além da inadimplência estruturada; que inclui empresas de fachada; devedores contumazes e esquemas de lavagem de dinheiro.

Apesar de avanços pontuais nos esforços das companhias e órgãos de fiscalização, ainda há fragilidades na adoção de práticas preventivas mais amplas e contínuas, especialmente na capacidade de identificar conexões suspeitas ao longo da cadeia de valor.

As empresas precisam estabelecer um processo estruturado e periódico de avaliação de riscos, mantendo em funcionamento instrumentos de gestão, controles internos e mecanismos eficazes de monitoramento de possíveis *red flags* ao longo da cadeia de valor dos negócios, tendo como referência, por exemplo, riscos de lavagem de dinheiro, corrupção, extravio de ativos, manipulação de informações contábeis e financeiras e riscos cibernéticos, entre outros.

2 A evasão fiscal deve ser compreendida como dimensão central na agenda de integridade e no enfrentamento dos fluxos ilícitos. Estruturas criminosas recorrem sistematicamente a mecanismos de sonegação, subdeclaração de receitas, notas fiscais ideologicamente falsas, triangulação interestadual e ocultação de beneficiários econômicos para reduzir artificialmente sua carga tributária e financiar atividades ilícitas. A redução da evasão fiscal, portanto, não é apenas um objetivo arrecadatório, mas componente essencial para mitigar distorções concorrenciais, fortalecer ambientes regulatórios e diminuir o espaço econômico disponível para organizações criminosas.

Entre as empresas reguladas, observa-se um grau mais elevado de maturidade. Essas companhias costumam contar com estruturas formais de gestão de riscos de *compliance*, auditorias, políticas documentadas e programas regulares de comunicação e treinamento. Ainda assim, persistem oportunidades de aprimoramento na ampliação das diligências, na realização de análises mais aprofundadas sobre potenciais parceiros, na consideração das características específicas das regiões onde operam, na identificação de beneficiários finais e na efetividade e tempestividade do monitoramento de terceiros ao longo da parceria ou da prestação de serviços, por parte dos próprios contratantes, em conjunto com suas estruturas de *compliance*.

Nas empresas não reguladas, é comum a existência de áreas ou executivos responsáveis por *compliance* e de políticas de integridade básicas. No entanto, práticas como verificações estruturadas de antecedentes e monitoramento contínuo ainda são aplicadas de forma limitada. A ausência de protocolos específicos para situações críticas, como extorsão ou ameaças externas, evidencia a necessidade de evolução para modelos mais sofisticados de prevenção e resposta.

Além disso, ainda é limitada a atenção dedicada aos riscos de lavagem de dinheiro. Muitos programas de *compliance* permanecem concentrados em temas anticorrupção ou em preocupações estritamente reputacionais. Aspectos como conflito de interesses, tráfico de influência e infiltração criminosa tendem a ser tratados de forma isolada, mesmo quando fazem parte de uma mesma dinâmica de risco.

Também se observa um aumento nos casos de cooptação de colaboradores, frequentemente por meio de ofertas financeiras elevadas direcionadas a funções estratégicas. A identificação precoce dessas situações é dificultada pela falta de indicadores objetivos, por políticas discretas de identificação e monitoramento, pela tímida inserção de mecanismos de *compliance* no dia a dia dos negócios, pela falta de confiança nos canais de denúncia e pela ausência de protocolos claros de proteção aos empregados. Abaixo apresentamos cenários por setor e indústria.

Indústrias:

- Vulnerabilidades específicas em atividades de transporte, logística e serviços terceirizados;
- Pontos de acesso menos visíveis, que escapam com maior facilidade aos controles corporativos tradicionais;
- Metodologias de classificação de risco (*risk scoring*) e de monitoramento contínuo ainda incipiente (especialmente quando comparada ao setor financeiro);
- Cadeias produtivas longas e fragmentadas, caracterizada pela multiplicidade de terceirizados e subcontratados;
- Heterogeneidade operacional entre sítios e regiões;
- Dados distribuídos em sistemas pouco interoperáveis;
- Informações de fornecedores de qualidade irregular e baixa formalização;
- Maior risco de recebimento ou movimentação não intencional de recursos de origem ilícita; e
- Exposição a estruturas societárias opacas e a beneficiários finais ocultos[3].

Setor de Combustíveis

- Roubo e furto de cargas;
- Adulteração, fraude de qualidade e fraude volumétrica;
- Atuação de formuladoras e batedeiras clandestinas;
- Formação de cartéis e outras violações concorrenciais;
- Operação de postos piratas; e
- Crescente interesse de organizações associadas ao narcotráfico.

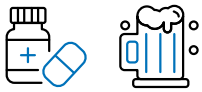
Setor Florestal

- Invasão de áreas produtivas com uso de armamento pesado;
- Comercialização ilegal de terras;
- Furto de madeira para produção clandestina de carvão;
- Envio de cargas para áreas sob controle do crime, inclusive como forma de testar desvios associados a rotas internacionais; e
- Aumento de ataques a cargas e tentativas de contaminação de contêineres no ambiente portuário.

Setor financeiro (bancos e meios de pagamento)

- Exposição contínua a movimentações ilícitas;
- Assimetria entre a capacidade de adaptação das organizações criminosas e os recursos destinados pelas empresas à prevenção e à resposta;
- Impacto da profissionalização do crime cibernético; e
- Desafios associados à *fintechs* e à atuação transversal de grupos criminosos em diferentes setores da economia.

3 Nos termos do art. 53 da Instrução Normativa RFB nº 2.290/2025, considera-se beneficiário final a pessoa natural que, em última instância, de forma direta ou indireta, detenha a propriedade, exerça o controle ou influência significativa sobre a entidade, bem como a pessoa natural em nome de quem uma transação seja realizada. A definição adota, portanto, uma perspectiva material, voltada à identificação de quem efetivamente se beneficia, comanda ou influencia a estrutura societária ou a operação, ainda que essa posição não se revele de maneira imediata na documentação formal.



Setor de medicamentos e bebidas

- Intensificação de falsificação, contrabando e circulação irregular de produtos regulados;
- Mercados paralelos favorecidos pelo alto valor econômico dos produtos;
- Expansão de canais digitais não autorizados, dificultando o rastreamento das operações; e
- Crescente preocupação com desvio de insumos.

A falsificação de produtos constitui relevante fonte de receita para organizações criminosas, frequentemente associada a outras práticas ilícitas, como lavagem de dinheiro, roubo e furto de cargas, contrabando e evasão fiscal. Esses grupos exploram cadeias produtivas complexas, redes logísticas internacionais e lacunas regulatórias para inserir mercadorias falsificadas no mercado, inclusive por meio de remessas fracionadas e da produção descentralizada próxima aos centros consumidores. Segundo estimativas da OCDE, o comércio global de bens falsificados alcançou o equivalente a cerca de 2,3% das importações mundiais, o que evidencia a escala e o grau de sofisticação dessas atividades ilícitas[4].

Entre os setores mais afetados estão vestuário, calçados, artigos de couro, eletrônicos, cosméticos, joias, brinquedos, produtos farmacêuticos, veículos, bebidas e alimentos. No contexto brasileiro, destacam-se também casos de adulteração de bebidas alcoólicas, com riscos à saúde pública, e fraudes envolvendo insumos agrícolas, como fertilizantes adulterados, que podem comprometer a produtividade e, por consequência, afetar a segurança alimentar[5]. A falsificação alcança tanto bens de consumo quanto outros produtos protegidos por direitos de propriedade intelectual. Além dos prejuízos econômicos e dos impactos sobre a integridade dos mercados, a circulação de produtos falsificados representa riscos significativos à saúde e à segurança dos consumidores, especialmente nos setores farmacêutico, cosmético, alimentício, de brinquedos e de peças automotivas. Esse fenômeno compromete a concorrência leal, fragiliza os mecanismos de regulação e fiscalização e fragiliza a confiança nas relações de consumo.

4 **ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD); EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE (EUIPO)**. *Mapping Global Trade in Fakes 2025: global trends and enforcement challenges*. Paris: OECD Publishing, 2025. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/mapping-global-trade-in-fakes-2025_5c812e3c/94d3b29f-en.pdf. Acesso em: 6 abr. 2026.

5 **BRASIL**. Ministério da Justiça e Segurança Pública. *Nota oficial — Sistema do Governo Federal registra nove casos de intoxicação por metanol*. Brasília, DF, 26 set. 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/nota-oficial-2014-sistema-do-governo-federal-registra-nove-casos-de-intoxicacao-por-metanol. Acesso em: 6 abr. 2026; **BRASIL**. Ministério da Agricultura e Pecuária. Mapa apreende mais de 5 mil litros de fertilizantes irregulares no interior de São Paulo. Brasília, DF, 26 mar. 2026. Disponível em: https://www.gov.br/agricultura/pt-br/assuntos/noticias/mapa-apreende-mais-de-5-mil-litros-de-fertilizantes-irregulares-no-interior-de-sao-paulo. Acesso em: 6 abr. 2026.

Além disso, é importante destacar que, nos **setores intensivos em mão de obra**, ações corretivas podem levar à desmobilização de fornecedores e à interrupção de contratos - medidas que, além de comprometer a continuidade das operações, afetam cadeias inteiras e produzem impactos sociais relevantes. Medidas mitigadoras são importantes para afastar o risco de desmobilização e suas consequências.

Desde 2022, as principais movimentações monetárias ilícitas concentram-se em quatro frentes: comercialização ilegal de combustíveis (R$ 61,4 bilhões), comercialização ilegal de bebidas (R$ 56,9 bilhões), extração e produção ilegal de ouro (R$ 18,2 bilhões), e comércio ilegal de tabaco e cigarros (R$ 10,3 bilhões)[6].

Outros setores relevantes que merecem atenção incluem agências de automóveis, mercado imobiliário, empresas de construção civil, casas de câmbio, empresas de transporte coletivo (como ônibus), organizações religiosas, organizações sociais de saúde pública, serviços de coleta de lixo, mineração, empresas de apostas, infraestrutura, portuário e entidades vinculadas a clubes de futebol. Embora alguns setores apresentem maior relevância ou vulnerabilidade no contexto analisado, a exposição à atuação de organizações criminosas não se limita a eles, podendo atingir, em maior ou menor grau, empresas de todos os setores da economia.

Diante desse contexto, o diagnóstico parte do reconhecimento de que os riscos associados às organizações criminosas são dinâmicos e pervasivos. As estratégias de prevenção, detecção e resposta devem ser aprimoradas de forma contínua, à medida que novos padrões de atuação e vulnerabilidades se tornam evidentes. O fortalecimento da resiliência empresarial depende da consolidação de uma cultura ética e que trate a prevenção às organizações criminosas como parte integrante da gestão e da governança.

Papel crítico de M&A e Relações com Investidores (RI)

Como peças-chave nos controles de governança e *compliance* voltados à prevenção da infiltração do crime organizado, as áreas de M&A e RI ocupam posições sensíveis à entrada de capital ilícito e devem atuar como primeira linha de defesa e de governança.

A evolução do crime organizado indica uma mudança de paradigma: o capital ilícito deixou de buscar apenas ocultação e passou a buscar integração, escala e influência dentro da economia formal, em quase todos os setores. As organizações criminosas perceberam que podem ampliar seus resultados financeiros e, ao mesmo tempo, tornar sua detecção mais difícil ao atuar como se integrassem o mercado lícito.

A incapacidade das companhias de formular as perguntas certas sobre substância econômica, governança e conduta na relação com parceiros as tornam vulneráveis não apenas a riscos regulatórios, mas à captura silenciosa de sua própria estrutura.

A gestão dos riscos associados às organizações criminosas deve incidir com atenção sobre investidores, garantidores e financiadores, para além da supervisão ativa de fornecedores e clientes. Gerenciar o risco de captura pelo crime organizado depende da capacidade da companhia de questionar a razoabilidade e a coerência econômica das operações, bem como de manter uma postura de tolerância zero em relação à opacidade estrutural.

6 **FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. *Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil*. Coordenação: Nivio Nascimento; Eduardo Pazinato. São Paulo: Fórum Brasileiro de Segurança Pública, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/c5a85bb2-214a-4288-abf5-fcc619612777/content. Acesso em: 6 abr. 2026.

3 Proposições de Governança para Gestão de Riscos

3.1. Proposições do Processo de Governança e *Compliance*

Para traçar proposições de medidas que visam proteger uma empresa diante de um risco que possa afetar sua capacidade de atingir suas finalidades, é particularmente útil revisitar alguns conceitos relacionados à integridade.

Nos últimos anos, a literatura especializada e as regulamentações governamentais convencionaram o uso do termo "programa de integridade" para denominar o conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes, com objetivo de prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos, bem como fomentar e manter uma cultura de integridade no ambiente organizacional. Por ser um processo dinâmico, o programa de integridade precisa se adaptar continuamente a novos riscos e contextos, o que demanda revisões periódicas e a adoção de medidas adicionais sempre que necessário.

A CGU define o programa de integridade como sendo o conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e conduta, políticas e diretrizes, com o objetivo de (i) prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira; e (ii) fomentar e manter uma cultura de integridade no ambiente organizacional, conforme art. 56, do Decreto 11.129/2022, que regulamentou a Lei Anticorrupção.

Mais recentemente, ganhou força o conceito de “sistemas de integridade”, elaborado pelo Instituto Brasileiro de Governança Corporativa (IBGC)[7]. O conceito traz uma visão de que o programa de integridade é um dos componentes desse sistema, na medida em que o sistema busca ser uma estrutura dinâmica que abrange todas as unidades internas, programas, processos, atividades e políticas que interagem para garantir que a companhia opere de forma ética e em conformidade com seu propósito, valores, objetivos e a legislação pertinente.

7 **INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC)**. *Sistema de integridade: fundamentos e boas práticas*. São Paulo: IBGC, 2025. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24725&assessment=1. Acesso em: 6 abr. 2026.

A partir dessa abordagem, propõe-se que a empresa considere não apenas estratégias de aprofundamento, interlocução e auditoria de evidências relacionadas à prestação de serviços e/ou às atividades previstas no contrato, mas também o fortalecimento da cultura ética e da integridade como um processo sistêmico, dotado de recursos adequados e capaz de integrar diferentes áreas da companhia para melhor antecipar e lidar com as consequências inesperadas de riscos já conhecidos e daqueles que possam surgir em novos cenários.

O sistema de integridade é particularmente útil no tema relacionado às organizações criminosas. Diferentemente de ilícitos isolados, organizações criminosas operam por meio de redes informais, relações pessoais e mecanismos sofisticados de ocultação, que desafiam modelos tradicionais de controle. Nesse cenário, **o enfrentamento ao risco de infiltração criminosa exige interlocução contínua e coordenação efetiva entre diferentes áreas da companhia**. A gestão desse risco não deve ser atribuída a uma unidade isolada: áreas operacionais, especialmente aquelas envolvidas em contratações, pagamentos, gestão de ativos, logística e relacionamento com terceiros, precisam estar formalmente integradas ao sistema de prevenção, detecção, monitoramento e controles, com responsabilidades claramente definidas.

À alta administração compete estabelecer diretrizes estratégicas, aprovar políticas internas, prover recursos adequados e supervisionar sua eficácia, demonstrando ativamente seu compromisso e engajamento pela integridade institucional. As áreas responsáveis por *compliance*, integridade ou prevenção de ilícitos devem atuar com autonomia funcional, acesso direto às instâncias decisórias superiores e recursos compatíveis com o nível de exposição ao risco.

Como boa prática de fortalecimento da governança e de aumento de confiabilidade dos processos, recomenda-se que as empresas avaliem a adesão a programas de certificação e a auditorias periódicas promovidas tanto por estruturas internas, quanto por associações setoriais e entidades reconhecidas. Esses mecanismos voluntários promovem a convergência aos padrões mínimos de integridade e gestão de riscos, introduzem rotinas de verificação independente, favorecem a comparabilidade entre pares e reduzem assimetrias de informação com clientes, fornecedores, investidores e autoridades. Empresas engajadas nessas iniciativas tendem a possuir controles internos mais robustos, maior transparência e menor propensão a práticas ilícitas.

No Brasil, destacam-se as seguintes iniciativas empreendidas pela Controladoria-Geral da União (CGU) voltadas ao fortalecimento da integridade empresarial:

Pacto Brasil pela Integridade Empresarial

Consiste em um compromisso público voluntário que incentiva a adoção de medidas de prevenção à corrupção e boas práticas de governança, oferecendo, entre outros benefícios, uma ferramenta de autoavaliação que permite às empresas diagnosticar o grau de maturidade de seus programas de integridade.

Empresa Pró-Ética

Programa de reconhecimento de empresas que demonstram comprometimento com a implementação efetiva de programas de integridade, a partir de um processo estruturado de avaliação alinhado às melhores práticas nacionais e internacionais.

A participação nessas iniciativas pode contribuir para o aprimoramento contínuo dos mecanismos de controle, para o alinhamento a padrões reconhecidos e para o fortalecimento da capacidade da entidade de prevenir, identificar e responder aos riscos associados à atuação de organizações criminosas.

Destaca-se que, para além da instituição de políticas e normativos internos, a estruturação dos programas de integridade deve considerar a cultura, o ambiente de negócios e os riscos a que a entidade esteja submetida, não se limitando ao mero cumprimento regulatório, mas ao estabelecimento de uma estrutura de defesa compatível com a sofisticação de organizações criminosas.

Com o objetivo de aumentar a proteção da empresa à ação de organizações criminosas, ganham destaque os instrumentos de definição de padrões de conduta, prevenção à lavagem de dinheiro, gestão de conflitos de interesse, comunicação e apuração de irregularidades e, notadamente, a gestão dos riscos associados ao relacionamento com terceiros.

Nesse âmbito, incluem-se práticas como conheça o seu cliente (*know your client*), conheça o seu parceiro ou fornecedor (*know your partner*), bem como os terceiros que estes integrem em sua base de atendimento, conheça o seu funcionário (*know your employee*) e, quando aplicável, outras relações relevantes, como investidores e parceiros financeiros. Esses instrumentos devem ser cuidadosamente elaborados, formalmente aprovados, amplamente disseminados e incorporados não apenas às rotinas decisórias e operacionais da empresa, mas também aos sistemas de pagamento, de modo a evitar a saída de recursos sem a devida análise. O mesmo se aplica às avaliações periódicas de efetividade e eficácia.

Isso porque o simples atendimento a requisitos formais não assegura, por si só, a integridade do processo. Procedimentos como a exigência de múltiplas cotações, por exemplo, podem ser cumpridos por empresas distintas que, na prática, integram a mesma estrutura criminosa, produzindo apenas uma aparência de regularidade. Há, portanto, uma necessidade de adoção de uma abordagem que consiga ir para além da verificação simplesmente formal.

A atuação formal do *compliance* encontra limites estruturais diante das dinâmicas próprias das organizações criminosas, que se orientam por relações de confiança pessoal, coação, dependência econômica e adaptação e alteração constante dos instrumentos de gestão e de controles existentes.

Essas estruturas exploram, com frequência, a ausência de níveis e limites de aprovação claramente definidos, a falta de segregação de funções, a tolerância a exceções procedimentais, a insuficiência de controles cruzados e, em muitos casos, a própria falta de experiência da área de *Compliance* na formulação de respostas efetivas, inclusive diante dos riscos de criação de animosidades no entorno de suas operações.

Situações de "urgência operacional", por exemplo, podem tornar-se justificativa recorrente para autorizações fora do fluxo normal, criando atalhos que facilitam a inserção de pagamentos ilícitos em processos legítimos. Do mesmo modo, a permanência prolongada de um funcionário em atividades sensíveis, como o cadastro de fornecedores e clientes ou a validação de instituições financeiras, pode favorecer o estabelecimento de vínculos indevidos, comprometendo a independência necessária à detecção de irregularidades e facilitando a inclusão de empresas de fachada nos sistemas internos.

Por essa razão, a estrutura de governança deve incorporar mecanismos complementares de controle, como a segregação efetiva de funções sensíveis, a rotação periódica em cargos críticos, o estabelecimento de cenários de risco, o monitoramento e a análise periódica, o reforço do controle sobre decisões discricionárias, a realização de auditorias independentes, a automatização de controles, o cruzamento de dados e o monitoramento de padrões atípicos de comportamento institucional. Em áreas financeiras, por exemplo, a concentração de cadastro de fornecedores, aprovação e execução de pagamentos em um único agente amplia significativamente o risco de instrumentalização dos sistemas internos por redes criminosas.

Também é essencial a existência de canais seguros, internos ou externos (independentes), para a comunicação de indícios de irregularidade, acompanhados de procedimentos estruturados, transparentes e devidamente definidos para apuração, escalonamento decisório e adoção de medidas de prevenção, detecção e correção, cujo fortalecimento conjunto se recomenda. A proteção contra retaliações a comunicantes de boa-fé e testemunhas constitui elemento necessário para romper dinâmicas de silêncio e medo frequentemente exploradas por organizações criminosas.

Assim, quando um colaborador identifica que determinado fornecedor continua sendo reiteradamente contratado apesar de praticar preços incompatíveis com os de mercado, a possibilidade de reportar a situação sem exposição pessoal pode ser decisiva para interromper ciclos de favorecimento ilícito.

Por fim, a efetividade da governança e do *compliance* no enfrentamento às organizações criminosas depende da consolidação de uma cultura institucional estruturada e orientada à integridade, que reconheça os níveis e limites dos controles formais e trate a vigilância organizacional como parte da rotina de negócios. A integração entre áreas, a capacitação contínua e a adoção consistente de mecanismos estruturais de prevenção e controle constituem condições para aumentar a resistência institucional à infiltração criminosa.

3.2. Políticas e Procedimentos Mínimos

Para viabilizar a implementação prática e proporcional do programa de integridade, recomenda-se que as companhias adotem um conjunto mínimo de políticas e procedimentos, alinhados ao porte, à complexidade operacional e ao nível de exposição setorial e geográfica. Esse padrão mínimo deverá assegurar, ao menos:

Diretrizes claras de *due diligence* de terceiros com identificação de beneficiário final;

Triagem em listas públicas e privadas, Pessoas Expostas Politicamente (PEPs) e sanções;

Controles financeiros com segregação de funções e validações de titularidade bancária;

Gestão formal de contratações e exceções com registro de justificativas e alçadas;

Procedimentos de monitoramento contínuo baseados em gatilhos objetivos de risco; e

Canais de reporte com proteção efetiva contra retaliação.

Como complemento à implementação interna, incentiva-se a adoção de mecanismos voluntários de auditoria regular e certificação setorial, capazes de validar a aplicação prática de políticas, testar controles em processos críticos e atestar conformidade com padrões reconhecidos. Essa verificação independente aumenta a credibilidade externa, oferece blindagem institucional adicional e amplia a capacidade de detecção de lacunas, especialmente em ambientes com cadeias longas de fornecedores e múltiplos terceiros.

Em empresas de menor porte ou com exposição limitada, esses controles podem ser menores, priorizando a documentação mínima, a dupla verificação em cadastros e pagamentos e a rastreabilidade das decisões; enquanto nos contextos de maior exposição, exige-se diligência reforçada para terceiros críticos, integração com *bureaus* e bases públicas e privadas, automação de alertas e auditorias independentes.

Para orientar a aplicação dos procedimentos, é útil adotar um *checklist* operacional em linguagem simples e incorporado às rotinas. Assim, antes da homologação de um terceiro, deverá estar minimamente documentado:

- O cadastro completo com validação de CNPJ;
- Classificação Nacional de Atividades Econômicas (CNAE);
- Endereço e representantes;
- A identificação e qualificação do beneficiário final;
- A verificação de capacidade operacional compatível com o objeto contratual; e
- A triagem reputacional e em listas de sanções e a confirmação da titularidade da conta bancária indicada para pagamento.

Antes da contratação, recomenda-se verificar comparabilidade de cotações e aderência aos preços de mercado e formalizar cláusulas de integridade. Antes do primeiro pagamento e de quaisquer alterações cadastrais, deverão ocorrer validações técnicas com segregação entre quem solicita, analisa e aprova, além do registro de eventuais exceções com justificativa e aprovação por instância competente.

A avaliação de cenários de risco pode ser apoiada por um roteiro de perguntas orientadoras que facilite a identificação de sinais de alerta sem depender exclusivamente de especialistas. Em situações de fornecedor recém-constituído ou com estrutura mínima, convém confirmar se a capacidade declarada é verossímil frente ao escopo; se há histórico operacional comprovável e se existem vínculos societários, endereços ou procuradores compartilhados com outros participantes do processo.

Na ocorrência de concentração atípica de contratos em curto espaço de tempo ou de preços fora do mercado, é pertinente avaliar o racional econômico, a presença de intermediários sem função clara e a existência de rotas logísticas ou de execução que se afastem do padrão habitual. Por fim, pressões por urgência e pedidos de exceção devem ser analisados com cautela. Igualmente, em caso de solicitações de troca de conta bancária, devem ser apuradas a titularidade, a documentação comprobatória e a proximidade temporal com pagamentos relevantes.

Em empresas menores ou com cadeia de fornecedores mais estável, a combinação de *due diligence* básica com verificação de beneficiário final, triagem em listas de sanções, dupla checagem de cadastros e contas bancárias e registro formal de exceções tende a ser suficiente como ponto de partida.

Em empresas médias ou com exposição moderada, recomenda-se evoluir para um mapa consolidado de riscos de terceiros, critérios de diligência reforçada por criticidade, gatilhos para reavaliação (mudança societária, alteração de objeto ou de conta, picos de faturamento sem explicação operacional), auditorias por amostragem, entre outros.

Em empresas grandes, reguladas ou multinacionais, além das medidas anteriores, cabem integração com análises relacionais, revisões periódicas de parâmetros e testes de estresse[8] em fornecedores críticos.

Considerando a limitação de recursos, a definição e a aplicação dos controles devem ser orientadas por materialidade e impacto no negócio, priorizando processos e terceiros cujo risco potencial possa comprometer a continuidade operacional, os resultados, a conformidade regulatória e a reputação da companhia. Para assegurar efetividade e melhoria contínua, recomenda-se instituir métricas periódicas de avaliação da execução e do desempenho dos controles, permitindo mensurar seu grau de maturidade, identificar lacunas e retroalimentar o processo decisório, com a recalibração dos níveis de diligência e o direcionamento de investimentos para os pontos de maior relevância e retorno em mitigação de risco.

8 Os testes de estresse em *compliance* consistem na simulação de cenários adversos extremos, como crises, fraudes ou falhas sistêmicas, com o objetivo de avaliar a resiliência dos controles internos, a capacidade de resposta da empresa e a efetividade dos mecanismos de prevenção, detecção e remediação, contribuindo para o fortalecimento da conformidade regulatória.

3.3. Proposições de Gestão de Riscos

A gestão de riscos tem por finalidade identificar, avaliar, tratar, monitorar e mitigar os riscos aos quais a instituição esteja exposta, considerando a natureza de suas atividades, seus produtos e serviços, o perfil de seus clientes, as operações realizadas e as áreas geográficas de atuação. A título de referência, vale dizer que a abordagem baseada na identificação de riscos já vem sendo aplicada de forma consolidada no contexto de prevenção da prática de corrupção, de lavagem de dinheiro e de financiamento ao terrorismo. Esse histórico e conhecimento podem servir de ponto de partida e até de inspiração para a construção de um modelo que trata especificamente dos riscos associados ao crime organizado.

Os controles implementados devem ser proporcionais aos riscos identificados. A metodologia de riscos deverá ser previamente definida e frequentemente revisada. Isto porque, o apetite de risco de uma companhia varia com frequência ao longo do tempo, porquanto relacionados à estratégia organizacional e objetivos de negócios.

No processo de identificação de riscos, deverão ser considerados, no mínimo, **os riscos relacionados aos clientes, aos produtos e serviços, às áreas geográficas e aos aspectos operacionais**.

Quanto aos **clientes**, devem ser avaliados fatores como:

- A condição de PEP;
- A residência ou sede em jurisdições classificadas como de maior risco;
- A existência de estruturas societárias complexas; e
- O exercício de atividades econômicas intensivas em numerário.

Em relação aos **produtos e serviços**, deverão ser observadas:

- Operações em espécie;
- Operações internacionais;
- Produtos que possibilitem anonimato ou rápida movimentação de recursos; e
- Canais de atendimento não presenciais.
- No tocante ao **risco geográfico**, deverão ser considerados países ou regiões com deficiências em seus regimes de PLD/FT e localidades associadas ao crime organizado.
- No âmbito **operacional**, devem ser avaliadas fragilidades de processos internos, a terceirização de atividades críticas e a dependência excessiva de sistemas automatizados sem adequada validação humana.

Como mencionado, os riscos identificados devem ser avaliados com base em critérios objetivos e pré-estabelecidos, levando em conta, ao menos, a probabilidade de ocorrência e o impacto potencial, inclusive sob os aspectos financeiro, regulatório, reputacional e, também, penal. A partir dessa avaliação, os riscos deverão ser classificados, sendo imprescindível a formalização e a documentação dessa classificação.

Para o tratamento e a mitigação dos riscos classificados, deverão ser estabelecidas medidas compatíveis com o nível de exposição identificado, que poderão incluir, conforme o caso, a limitação ou a recusa de determinadas operações, o monitoramento contínuo e automatizado de transações, a revisão periódica de cadastros, a realização de treinamentos específicos para as áreas mais expostas e a implementação de outros mecanismos de controle adicionais.

O sistema de gestão de riscos deverá ser acompanhado por indicadores que permitam avaliar sua efetividade e tempestividade. Nesse contexto, poderão ser utilizados

KPIs, como o percentual de cadastros atualizados, o tempo médio de análise de alertas e o volume de treinamentos realizados, KRI, como o aumento atípico de operações em espécie, o crescimento do número de clientes classificados como de alto risco e a reincidência de alertas relacionados ao mesmo cliente, bem como KCI, que permitem aferir se os mecanismos de controle estão funcionando adequadamente, isto é, a eficácia dos controles internos. Como exemplos de KCI, podem ser mencionados o percentual de contratos auditados, o número de revisões de *compliance* realizadas e o tempo médio de investigação de denúncias.

Ferramentas de IA podem apoiar a gestão de riscos ao automatizar a coleta e a integração de dados internos e externos, produzir indicadores preditivos e aprimorar a priorização de riscos conforme cenários definidos pela empresa. O uso de algoritmos para análise de risco setorial, geográfico e comportamental favorece a atualização dinâmica da matriz de riscos e a qualificação de KRI, desde que respaldado por governança robusta, com definição clara de objetivos e limites de uso, critérios de qualidade e de atualidade dos dados, validação e testes periódicos e monitoramento de modelos e mecanismos que permitam compreender, auditar e contestar resultados quando necessário.

Como mencionado, a matriz de riscos e as políticas de gestão de riscos deverão ser revisadas, no mínimo, anualmente e sempre que houver alterações relevantes no modelo de negócios, a introdução de novos produtos ou serviços, a realização de operações de fusões e aquisições ou outras reorganizações societárias relevantes, mudanças normativas aplicáveis ou a ocorrência de eventos relevantes, tais como fraudes, sanções ou comunicações de operações suspeitas aos órgãos competentes.

Por fim, pode ser citada a importância da governança da gestão de riscos de PLD/FT, que deverá assegurar a definição clara de responsabilidades das diferentes áreas da companhia, como alta administração, área responsável por PLD/FT ou *compliance* e áreas operacionais.

Em relação a parceiros, financiadores e garantidores, recomenda-se:

- Identificar e validar o beneficiário final e a estrutura completa de controle do investidor ou garantidor;
- Validar a origem dos recursos;
- Mapear todos os veículos da transação para avaliar inexistência de estruturas de circularidade de recursos entre financiador e tomador (mesmo grupo econômico);
- Mapear as estruturas de uso de crédito, garantias e securitização com lastro artificial ou com geração recorrente de caixa, que podem gerar juros e amortizações como "renda limpa"; e
- Validar o racional estratégico e a coerência do *valuation*.

3.4. Proposições em *Due Diligence* de Terceiros

A *due diligence* de terceiros constitui um dos instrumentos centrais para a gestão de riscos, tendo como objetivo conhecer e auxiliar na prevenção de associação das empresas com organizações criminosas.

Para a condução de processos de *due diligence* de terceiros de forma eficaz e consistente, é essencial compreender os mecanismos pelos quais organizações criminosas se infiltram na economia formal. Em muitos casos, essa infiltração está associada à necessidade de reintroduzir recursos ilícitos no sistema econômico, conferindo-lhes aparência de legalidade. Esse processo ocorre, em regra, por meio da lavagem de dinheiro, estruturada em três etapas interdependentes: i) a colocação dos recursos no sistema econômico; ii) a ocultação de sua origem por meio de múltiplas transações; e, por fim, iii) sua integração em atividades aparentemente legítimas.

Nesse contexto, todos os terceiros que mantenham qualquer relação comercial ou operacional com a instituição, incluindo clientes, fornecedores, instituições financeiras, prestadores de serviços, parceiros comerciais, representantes, intermediários e consultores, devem ser submetidos a procedimentos de *due diligence* (conhecidos como *know you partner*, *know your client*, etc.), cuja intensidade deve variar conforme o grau de risco associado.

O objetivo é identificar a estrutura e o melhor conhecimento sobre o terceiro, determinar quem exerce controle efetivo sobre suas atividades, identificar o beneficiário econômico da relação (beneficiário final) e verificar se a atividade contratada possui finalidade econômica legítima. Entre as verificações a serem feitas, incluem-se as o histórico reputacional, vínculos com PEPs e exposição geográfica a organizações criminosas.

Tais verificações devem incluir também os próprios funcionários e colaboradores da empresa (*Know Your Employee*), para evitar riscos relacionados a cooptação de profissionais em áreas sensíveis, como logística, financeiro e jurídico, seja por incentivos financeiros, seja por coação em territórios sob influência de organizações criminosas.

A literatura e os casos analisados por órgãos de inteligência financeira evidenciam padrões recorrentes, como empresas recém-constituídas, sem estrutura operacional e com movimentação de elevados volumes de recursos sem lastro econômico. Diante disso, a *due diligence* de terceiros deve compreender, no mínimo, a identificação cadastral completa do terceiro, sua estrutura societária, a definição do beneficiário final da relação, eventual exposição política, histórico reputacional e a presença em listas restritivas[9]. O local em que o terceiro opera também deve ser avaliado. Operações em regiões de conflito armado, narcotráfico ou de fronteira podem constituir um risco relevante.

Recomenda-se, adicionalmente, a realização de cruzamento estruturado de informações empresariais, incluindo dados cadastrais, histórico societário, vínculos entre sócios e administradores, endereços e procuradores, com bases internas e externas. A utilização de *bureaus* especializados, bem como de bases públicas e privadas, pode fortalecer a capacidade de identificar incongruências societárias, estruturas de fachada, relações indiretas entre terceiros e beneficiários finais ocultos, funcionando como instrumento essencial para detecção de *red flags* e mitigação de riscos de infiltração criminosa.

Também deve ser analisada a compatibilidade entre o serviço prestado, o valor contratado, as evidências da relação de negócios e a capacidade operacional do terceiro. A constituição recente de uma empresa que passa a receber contratos de alto valor sem dispor de estrutura compatível para executá-los, é indício relevante de risco, ainda que toda a documentação formal esteja regular. Outro sinal de alerta é a solicitação para que os pagamentos relativos à contraprestação dos serviços sejam realizados em contas bancárias de titularidade diversa da do terceiro contratado.

9 O tratamento de dados pessoais de terceiros e colaboradores deverá observar a legislação de proteção de dados, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), sendo realizado de forma lícita, proporcional e limitada às finalidades de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

A coleta de dados deverá restringir-se ao mínimo necessário para a identificação, verificação e avaliação de risco, observando o princípio do *need-to-know*. O tratamento deverá estar amparado em base legal adequada, notadamente o cumprimento de obrigação legal ou regulatória e o exercício regular de direitos. Os dados deverão ser armazenados de forma segura, com retenção limitada aos prazos legais aplicáveis, e descartados de modo seguro e rastreável após o atingimento de sua finalidade.

O encarregado pelo Tratamento de Dados Pessoais (DPO) deverá ser envolvido na definição e supervisão dos procedimentos, inclusive quanto à avaliação de riscos, à definição de bases legais e à resposta a incidentes.

O compartilhamento de dados deverá ocorrer exclusivamente nos limites legais e para as finalidades de PLD/FT, assegurada a confidencialidade das informações e a transparência aos titulares, observadas as exceções legais aplicáveis.

Desse modo, os principais sinais de alerta aos quais as empresas devem ficar atentas em fornecedores, clientes e demais parceiros de negócios, podem ser organizados da seguinte forma:

Estrutura societária

- Mudanças frequentes de sócios ou diretores sem justificativa;
- Presença de sócios com capacidade financeira incompatível com o faturamento da empresa, a exemplo de beneficiários de programas sociais de distribuição de renda[10];
- Sócios sem experiência profissional na área de atividade da empresa;
- Dificuldade em identificar beneficiários finais;
- Empresas recém-constituídas;
- Concentração de múltiplos CNPJ em um mesmo endereço; e
- Empresas sem website ou presença digital.

Operações financeiras

- Uso excessivo de dinheiro em espécie;
- Transferências internacionais sem justificativa econômica;
- Fluxos financeiros complexos ou circulares;
- Inconsistências contábeis; e
- Inconsistência entre valores cobrados e os praticados no mercado.

Atividade operacional

- Falta de infraestrutura física compatível com o tamanho declarado (poucos empregados, instalações precárias, ausência de estoque);
- Sede da empresa localizada em endereço predominantemente residencial;
- Volume de negócios incompatível com a estrutura operacional;
- Contratação de empresas sem histórico para contratos relevantes; e
- Atividade declarada da empresa (CNAE) incompatível com atividades praticadas.

10 Informações relevantes podem ser obtidas no Portal da Transparência da Controladoria-Geral da União, que dispõe de dados sobre relacionamento de empresas com o Poder Público e o recebimento de programas sociais por parte de pessoas físicas.

Relacionamentos comerciais

- Contratos com fornecedores ou clientes sem histórico verificável ou ligados a pessoas investigadas;
- Relacionamentos intermediados por terceiros sem justificativa;
- Relutância em fornecer documentação e informações durante a *due diligence*; e
- Transações atípicas para o padrão do setor.

Comportamento organizacional ou má reputação

- Ausência de programa de integridade e de práticas estruturadas de governança;
- Resistência ao aceite de cláusulas contratuais que impliquem na adoção de mecanismos de prevenção de ilícitos;
- Resistência ao fornecimento de documentos que permitam esclarecer a situação da empresa;
- Indícios de fragilidade de controles internos ou dos registros contábeis apresentados;
- Urgência incomum para fechar o negócio.
- Inclusão em listas de sanções (como CEIS, CEPIM e CNEP ou as internacionais, OFAC, União Europeia, Banco Mundial, Banco Interamericano de Desenvolvimento); e
- Mídias negativas ou existência de múltiplos processos judiciais.

Indicadores adicionais

- Atuação em setores vulneráveis (comércio e serviços intensivos em numerário, combustíveis, comércio exterior, transporte e logística, construção e infraestrutura, segurança privada, mercado imobiliário);
- Empresas detidas por *offshores*; e
- Risco financeiro elevado decorrente de autuações por órgãos de fiscalização ou processos judiciais.

Com base nesses elementos, o terceiro deve ser classificado conforme seu nível de risco. Para terceiros classificados como de maior risco, devem ser adotadas medidas reforçadas de *due diligence*, tais como:

- A solicitação de documentação complementar;
- A realização de entrevistas e visitas *in loco* para validação;
- A verificação aprofundada da estrutura societária;
- A aprovação por instância hierárquica superior e inclusão de cláusulas contratuais específicas de integridade; e
- O monitoramento contínuo da relação.

Cabe destacar que é relevante a empresa possuir um mapa de riscos consolidado e integrado de seus terceiros para a respectiva gestão.

Tais medidas de reforço da *due diligence* são especialmente relevantes pois, além dos impactos reputacionais e financeiros, a não identificação ou o tratamento inadequado de sinais de alerta pode expor a empresa e seus administradores a riscos legais e financeiros relevantes. Em determinadas circunstâncias, gestores e responsáveis por controles internos podem ser responsabilizados quando, dispondo de elementos suficientes para identificar irregularidades, deixam de adotar medidas adequadas dentro de sua esfera de atuação.

Apesar de sua relevância, os processos tradicionais de *due diligence* apresentam limitações estruturais diante das estratégias das organizações criminosas. A existência de registros empresariais válidos, certidões negativas e contratos regulares não impede que estruturas criminosas utilizem empresas formalmente constituídas para ocultar a origem ilícita dos recursos. Por essa razão, a *due diligence* deve ser compreendida como instrumento de mitigação, e não de eliminação do risco. Mesmo quando conduzida adequadamente, subsistem riscos residuais associados à capacidade adaptativa das organizações criminosas e à assimetria entre controles formais e redes informais. Um fornecedor inicialmente considerado de baixo risco, por exemplo, pode passar a ser utilizado por grupo criminoso ao longo do tempo, sem alteração imediata de seus dados cadastrais.

Para lidar com esses riscos, a gestão de terceiros deve incorporar mecanismos de monitoramento contínuo e planos de ação, incluindo a atualização periódica das análises, monitoramento de alterações relevantes em CNPJ e cadastros, mudanças de controle societário, capital social ou objeto social, verificação de transações atípicas, reavaliação de contratos sensíveis e a integração das informações de risco aos processos decisórios da instituição.

A efetividade das atividades de *due diligence* também depende de sua integração com a estrutura de governança e *compliance*. As informações obtidas na avaliação de riscos de terceiros devem orientar decisões de contratação,

pagamento e renovação contratual, evitando que a análise se reduza a uma etapa meramente formal desvinculada da realidade operacional. Quando um terceiro passa a concentrar contratos relevantes sem justificativa econômica clara, a reavaliação de sua situação deve ser imediata.

Por fim, a política de *due diligence* deve reconhecer expressamente seus próprios limites e prever respostas objetivas para situações em que, apesar do cumprimento formal dos procedimentos, surjam indícios de vínculos ilícitos. A adoção de uma abordagem baseada em risco, aliada ao monitoramento contínuo e à atuação coordenada entre áreas, especialmente com as áreas e os colaboradores contratantes, é condição essencial para reduzir a probabilidade de instrumentalização da instituição por estruturas vinculadas às organizações criminosas.

Uma vez decidida a continuidade do engajamento com o terceiro, os contratos deverão conter cláusulas específicas voltadas à prevenção e ao combate às organizações criminosas e à lavagem de dinheiro, como instrumento de mitigação de riscos e de proteção da integridade das relações comerciais. Deverá ser prevista a possibilidade de rescisão ou suspensão contratual na hipótese de identificação de *red flags* de envolvimento da contraparte com organizações criminosas ou outras atividades ilícitas.

Os contratos deverão estabelecer, ainda, a obrigação de comunicação imediata de qualquer alteração de controle societário, de beneficiário final ou das contas utilizadas para a execução contratual, bem como vedar a subcontratação ou a cessão sem prévia anuência da contraparte.

Sempre que aplicável, deverão ser previstas condições precedentes à eficácia contratual, incluindo a comprovação de licenças e autorizações, a contratação e a manutenção de seguros adequados e a demonstração de capacidade técnica, operacional e financeira compatível com o objeto contratado. Ademais, os contratos deverão contemplar cláusulas específicas de anticorrupção e de prevenção à lavagem de dinheiro, prevendo compromissos de conformidade legal, de cooperação e a aplicação de sanções contratuais em caso de descumprimento, sem prejuízo das demais responsabilidades cabíveis.

3.5. Proposições em Mecanismos de Monitoramento

Modelos tradicionais de monitoramento, baseados em regras fixas, parâmetros estáticos e controles predominantemente *ex post* apresentam limitações diante da crescente sofisticação dos esquemas ilícitos.

Fontes públicas indicam que estruturas criminosas se organizam por meio de:

- Empresas de fachada (*shell companies*);
- Contratos simulados ou sem proporcionalidade econômica;
- Fracionamento e circularidade de pagamentos (*smurfing*);
- Atuação em setores intensivos em numerário ou com elevada terceirização;
- Cadeias de fornecimento longas e opacas; e
- Intermediários com baixa transparência quanto ao beneficiário final.

Essas práticas se dissimulam em operações aparentemente regulares, dificultando a identificação por controles estritamente transacionais.

Os modelos clássicos enfrentam desafios recorrentes. Dependem de parâmetros estáticos, rapidamente superados pela evolução dos esquemas ilícitos, e geram excesso de falsos positivos, com fadiga operacional e perda de foco analítico. Persistem fragmentação de informações e dispersão de responsabilidades entre áreas como finanças, compras, logística, comercial e jurídico. Soma-se a isso a dificuldade para capturar riscos não financeiros, como:

- Pressões externas;
- Influência territorial;
- Comportamentos atípicos;
- Padrões relacionais suspeitos; e
- Foco em transações isoladas em detrimento da identificação de padrões sistêmicos.

Nesse cenário, tornam-se necessárias abordagens mais integradas e baseadas em risco, com reconhecimento explícito das limitações dos controles tradicionais.

A evolução da lavagem de dinheiro e da infiltração das organizações criminosas reforça a necessidade de que empresas da economia real, mesmo quando não obrigadas por lei, adotem mecanismos proporcionais de prevenção e detecção, em consonância com o princípio da abordagem baseada em risco.

A estruturação de um sistema objetivo e proporcional parte da identificação de vulnerabilidades, com mapeamento de processos e atividades mais suscetíveis a abuso ou infiltração. Exemplos incluem:

- Compras e contratação de terceiros críticos;
- Logística e transporte;
- Gestão de numerário;
- Subcontratação e mão de obra local;
- Canais indiretos;
- Revendas e franquias;
- Comissionamento e incentivos;
- Doações, patrocínios e apoios institucionais; e
- Obras, expansões e serviços prestados em campo.

A partir desse diagnóstico, a empresa deve definir cenários de risco e tipologias de comportamento para orientar a gestão contínua, com revisões periódicas para incorporar mudanças nos padrões de atuação criminosa.

Um pilar essencial consiste em assegurar rastreabilidade do que foi feito, por quem e por qual motivação, por meio de documentação mínima e padronizada relativa a contratos, aditivos, medições, pagamentos e aprovações, além do registro claro das justificativas para exceções ou decisões fora do fluxo usual. Recomenda-se padronizar, de forma consistente, os campos e registros mínimos necessários à rastreabilidade, incluindo:

- Contrato ou contrato-base, aditivo ou justificativa operacional, quando aplicável;
- Fornecedor, CNPJ e, quando pertinente, identificação do beneficiário final;
- Conta bancária ou dados bancários de destino;
- Centro de custo ou projeto vinculado;
- Motivo da contratação ou motivação da decisão;
- Quem solicitou e quem aprovou; e
- Eventuais exceções e respectivas justificativas.

É importante que nos registros também constem a presença de eventuais intermediários (corretores, representantes comerciais, entre outros) que participaram da negociação. Deve-se evitar aprovações verbais ou informais, registrar decisões em canais oficiais e documentar integralmente as exceções com registro, justificativa e supervisão apropriada.

Empresas com grau de internacionalização devem avaliar exposição a sanções internacionais, especialmente quando houver fatores de conexão com jurisdições específicas, como

- Participação de *US persons*;
- Pagamentos em dólar;
- Uso de tecnologias ou serviços de origem norte-americana; e
- Inserção em cadeias de fornecimento globais.

Nesses casos, recomenda-se adotar controles proporcionais alinhados a referências reconhecidas, como o OFAC e seu *framework* para programas de sanções, bem como orientações públicas de risco. Situações devem ser encaminhadas para a área de *compliance* quando houver, por exemplo, fornecedor recém-criado (ex: inferior a 24 meses), estrutura societária incomum ou ausência de beneficiário final claramente identificado.

A eficácia do monitoramento depende de fluxo claro para tratar sinais de alerta. Um processo mínimo deve contemplar a definição de cenários de riscos, bem como as etapas de detecção, qualificação, registro, decisão e remediação.

Além disso, é essencial estabelecer responsabilidades e critérios de escalonamento proporcionais ao risco identificado, em alinhamento com *framework*s de governança de risco de crimes financeiros, como os princípios do Wolfsberg Group.

Para apoiar o desenho e a calibragem de alertas, a empresa pode recorrer a bibliotecas oficiais de *red flags*, como as advisories do FinCEN, úteis para padrões associados a *trade-based money laundering*. Entre pontos de atenção destacam-se:

- Mudanças frequentes de conta bancária;
- Valores incompatíveis com o mercado;
- Existência de intermediários sem função clara;
- Pressão por exceções;
- Divergências entre o contratado e o executado; e
- Presença recorrente de terceiros não cadastrados no local de operação.

Com a adoção de estruturas societárias mais sofisticadas e operações aparentemente legítimas pelas organizações criminosas, cresce a necessidade de uso de ferramentas de inteligência, integração de dados e análise preditiva na mitigação desses riscos. O foco na transação suspeita permanece relevante, mas não é suficiente. Torna-se necessário observar relações, padrões e conexões indiretas, em linha com recomendações sobre transparência do beneficiário final. Isso inclui:

- Mapear sócios, administradores, procuradores, intermediários e representantes;
- Identificar endereços, contas bancárias, telefones e vínculos compartilhados;
- Cruzar dados de fornecedores, subfornecedores e prestadores de serviço; e
- Aplicar técnicas de *network analytics* para revelar redes ocultas.

A utilização de ferramentas de Inteligência Artificial (IA) pode fortalecer o monitoramento contínuo ao ampliar a capacidade de identificar padrões atípicos e correlações não evidentes em tempo hábil, priorizando alertas por materialidade e risco. Modelos supervisionados e não supervisionados podem apoiar a detecção de anomalias em pagamentos, preços e custos praticados, assim como rotas logísticas, cadastros e alterações societárias, enquanto técnicas de análise de redes ajudam a revelar conexões indiretas entre terceiros.

Adicionalmente, a IA, quando apoiada por um sistema de gravação e retenção das mensagens trocadas por meio de ferramentas de comunicação corporativas (ex.: e-mail e ligações telefônicas) pode contribuir para identificação de anomalias na interação com contrapartes.

A adoção de IA e o monitoramento das ferramentas de comunicação corporativas devem observar princípios de proporcionalidade, rastreabilidade e revisão periódica de performance, preservando a supervisão humana e os controles de qualidade de dados, de modo a evitar vieses, reduzir falsos positivos/negativos e assegurar aderência à legislação (ex.: LGPD) e às políticas internas de segurança da informação.

Para ampliar a robustez das análises, recomenda-se, ainda, integrar às rotinas de monitoramento informações provenientes de:

- *Bureaus* externos;
- Bases públicas e privadas;
- Cadastros empresariais;
- Registros mercantis; e
- Fontes abertas verificáveis.

O cruzamento sistemático desses dados com os registros internos permite:

- Identificar inconsistências societárias;
- Alterações atípicas de controle;
- Vínculos indiretos entre terceiros; e
- Padrões incompatíveis com a atividade declarada, contribuindo para a detecção rápida e prévia de sinais de alerta.

Para elevar a qualidade analítica, companhias mais maduras instituem **estruturas integradas e células multidisciplinares**, com participação das áreas de vendas, compras, finanças/tesouraria, operações, segurança corporativa, jurídico e *compliance*.

Tecnologias analíticas e automação de alertas apoiam priorização por risco, detecção de *outliers* e identificação de padrões complexos, desde que observem requisitos mínimos de maturidade, como explicabilidade, rastreabilidade e revisões periódicas, de modo a evitar vieses e perda de acurácia. A automação deve complementar, e não substituir, o julgamento humano, especialmente em decisões sensíveis.

Em complemento, a *due diligence* deve ultrapassar o *onboarding* e ser acionada sempre que surgirem gatilhos que indiquem mudança de risco, como:

- Alterações na estrutura societária;
- Mudanças incomuns em rotas logísticas;
- Picos de faturamento sem explicação operacional;
- Aditivos sucessivos sem racional econômico;
- Trocas frequentes de contas bancárias;
- Pressão por exceções fora do fluxo; e
- Incidentes de segurança ou denúncias locais.

Simulações e testes de estresse permitem avaliar a capacidade de resposta diante de cenários realistas, como:

- Tentativas de infiltração em fornecedores críticos;
- Coação de equipes locais;
- Fraude logística;
- Captura de processos de contratação; ou
- Vazamento interno de informações sensíveis, fortalecendo a preparação antes da materialização do risco.

Mesmo programas robustos enfrentam limitações, como:

- Custos de implementação e manutenção;
- Qualidade e disponibilidade de dados;
- Riscos de opacidade algorítmica;
- Necessidade de equipes capacitadas;
- Assimetrias de informação e restrições de privacidade; e
- Expectativas regulatórias diversas e, por vezes, assimétricas para empresas não obrigadas.

Por isso, esse conjunto de medidas deve ser compreendido como processo evolutivo e integrado à governança, e não como garantia absoluta contra riscos ilícitos.

3.6. Proposições em Treinamentos e Cultura Organizacional

A capacidade de uma empresa de identificar e reagir rapidamente a tentativas de infiltração das organizações criminosas em suas operações depende da robustez dos controles formais e da qualidade da cultura organizacional. Em muitos casos, comportamentos cotidianos, percepções das equipes e o ambiente interno determinam se um risco será percebido no início ou se permanecerá invisível até ganhar escala.

Os primeiros sinais raramente se apresentam como transações suspeitas. Costumam surgir de forma sutil, por meio de padrões comportamentais, pressões informais e pequenas mudanças que, quando normalizadas, evoluem para riscos estruturais. Entre exemplos recorrentes estão:

- Aceitação de práticas informais no dia a dia;
- Pressões para flexibilizar controles;
- Uso de intermediários sem justificativa operacional clara; e
- Silêncio organizacional diante de desconfortos éticos ou operacionais.

Quando esses sinais não são reconhecidos e discutidos, passam a compor a rotina, criando um ambiente em que o risco se instala com facilidade e no qual controles formais, por si só, perdem capacidade de reação.

Treinamentos convencionais, embora necessários, têm limitações. Com frequência:

- Adotam conteúdo excessivamente normativo e distante da prática;
- Apresentam baixa retenção quando longos e esporádicos;
- Deixam de enfrentar dilemas reais, em que a resposta depende de julgamento e contexto; e
- Reforçam a percepção de que o risco é atribuição exclusiva da área de *compliance*.

Como resultado, equipes podem cumprir trilhas formais e ainda assim não reconhecer sinais fracos no cotidiano operacional. Empresas mais maduras demonstram que cultura eficaz depende de intencionalidade, debate estruturado e ambientes psicologicamente seguros.

A implementação dessas iniciativas demanda equilíbrio com as rotinas e prioridades do negócio. Capacitações e ações de engajamento, quando excessivas ou desconectadas da prática, podem gerar sobrecarga ou perda de efetividade. Nesse contexto, é importante que a companhia acompanhe a absorção do conhecimento pelas equipes treinadas, de forma a avaliar a efetividade das ações e orientar eventuais ajustes. Por isso, recomenda-se uma abordagem gradual, proporcional ao risco e integrada aos processos existentes, com apoio da liderança e foco em soluções simples e aplicáveis ao dia a dia.

Outro eixo é o foco em sinais fracos e comportamentais. Riscos relevantes tendem a começar com:

- Alterações de padrão;
- Pressões informais;
- Mudanças repentinas; e
- Condutas atípicas.

Capacitar equipes para perceber e reportar essas variações aumenta a capacidade preventiva e antecipa respostas.

A liderança engajada é decisiva. Quando líderes reforçam a importância de controles, transparência e registro, reduzem ambiguidades e estabelecem expectativas claras. A presença consistente da liderança desloca o tema de uma obrigação burocrática para uma prioridade de gestão.

Também é essencial assegurar espaços seguros para diálogo e questionamento. Ambientes em que colaboradores podem relatar dúvidas e preocupações sem receio reduzem zonas de silêncio e ampliam a detecção precoce. A cultura se consolida quando ética, gestão de riscos e tomada de decisão se conectam a rotinas concretas. Nessa lógica, *compliance* deixa de ser apenas um conjunto de regras e passa a orientar escolhas diárias. Uma cultura sólida funciona como sensor coletivo, capaz de perceber riscos antes que cheguem aos sistemas.

Mesmo sem medidas sofisticadas, algumas ações já elevam a percepção e a capacidade de resposta.

Capacitações específicas devem ser realizadas com lideranças locais e as áreas mais expostas, como:

- Compras;
- Logística;
- Obras e serviços;
- Área comercial e canais;
- Financeiro e tesouraria;
- Segurança patrimonial;
- Jurídico; e
- *Compliance*.

O conteúdo deve cobrir:

- Tipologias relevantes ao negócio;
- Sinais de alerta ao longo dos processos;
- Aplicação da política de exceções;
- Requisitos mínimos de registro; e
- Critérios para escalonamento.

A comunicação interna precisa traduzir conceitos para a realidade operacional, com dilemas recorrentes, como "urgência", "fornecedor indicado" e "mudança de conta bancária". Narrativas simples e adaptadas ao contexto da companhia ajudam a demonstrar como desvios começam. A cultura não se sustenta se houver receio de relatar. Por isso, a liderança deve reafirmar o *tone from the top*, os canais internos devem assegurar proteção efetiva ao reportante e a empresa deve oferecer devolutivas sobre encaminhamentos. Sem proteção, não há engajamento. Sem engajamento, não há cultura.

Para manter a cultura ativa, práticas de aprendizagem contínua podem substituir treinamentos extensos.

O *microlearning*, com módulos curtos distribuídos ao longo do ano, tende a aumentar a retenção e a aplicação imediata do conteúdo, especialmente quando complementado por comunicados internos breves, objetivos, frequentes e adaptados aos diferentes públicos, reforçando mensagens-chave e expectativas de conduta. Treinamentos baseados em cenários, com simulações e *role-plays*, permitem que equipes pratiquem respostas a situações como:

- Pressão para contratar fornecedores e colaboradores "indicados";
- Urgências fora do fluxo;
- Interferência externa indevida; e
- Tentativas de obtenção de dados sensíveis.

Esses exercícios, aliados a comunicações direcionadas e recorrentes, reforçam o aprendizado, testam o tempo de escalonamento, a qualidade do registro, e a aderência aos fluxos definidos, contribuindo, assim, para a consolidação da cultura no dia a dia operacional.

A lógica de *speak-up by design* reforça que a cultura deve facilitar e normalizar relatos, dúvidas e pedidos de ajuda. Isso pode ser apoiado por mecanismos de esclarecimento rápido, campanhas internas e devolutivas consistentes, além de proteção objetiva contra retaliação. Relatar não deve ser exceção, mas comportamento esperado e incentivado.

A integração com a *due diligence* da cadeia também é relevante, para que colaboradores compreendam que condutas internas afetam diretamente a integridade de fornecedores, parceiros e intermediários.

Por fim, indicadores de cultura, como KPI e KRI, permitem acompanhar volume e qualidade de relatos, reincidência por área, concentração de exceções, taxa de *waivers* e percentual de terceiros críticos capacitados. Esses indicadores ajudam a medir a maturidade, identificar pontos cegos e priorizar ações.

Esse conjunto de práticas importa porque a cultura atua como linha de defesa viva:

- Reduz zonas de cegueira;
- Antecipa percepção de risco;
- Fortalece equipes locais;
- Evita normalização de desvios;
- Melhora a qualidade do monitoramento; e
- Eleva a resiliência em ambientes vulneráveis.

A cultura não elimina o risco, especialmente em contextos de coerção, informalidade territorial ou assimetrias de poder, mas permite perceber mais cedo, reagir com mais rapidez e tratar os riscos com consistência, reduzindo a probabilidade de conversão em danos estruturais. O monitoramento deve ser entendido como processo imperfeito e evolutivo, integrado à governança, e não como garantia absoluta contra riscos ilícitos.

4 Proposições em Gestão de Incidentes e Tomada de Decisão

4.1. Proposições em Identificação, Registro e Preservação de Informações

A gestão eficaz dos riscos associados às organizações criminosas exige um ciclo contínuo de:

01 Identificação;

02 Registro;

03 Decisão;

04 Qualificação;

05 Detecção;

06 Remediação;

07 Monitoramento dos indícios.

Para que o ciclo funcione, a empresa precisa de mecanismos estruturais e consistentes para identificar sinais relevantes, aplicar critérios objetivos de avaliação, manter registros íntegros e preservar evidências, com incorporação sistemática de aprendizados ao longo do tempo.

Nesse contexto, recomenda-se a criação e manutenção de um arquivo organizado de *red flags* que consolide sinais de alerta identificados nos processos internos, com padronização de análises, orientação de decisões e fortalecimento da memória institucional. Para cada *red flag*, deve-se indicar o processo de origem, o nível de severidade e a conduta esperada. Exemplos incluem:

- Beneficiário final não identificado;
- Alterações societárias sem justificativa;
- Operações incompatíveis com a capacidade declarada;
- Uso atípico de rotas logísticas;
- Solicitações de urgência sem documentação adequada;
- Pagamentos fracionados ou por exceção;
- Abordagens indevidas a colaboradores em funções críticas; e
- Interações com regiões ou setores reconhecidamente sensíveis.

Para captação e tratamento consistentes, é necessário estabelecer um fluxo estruturado de integração entre *compliance*, jurídico, recursos humanos, operações e demais áreas pertinentes, com responsabilidades definidas e compartilhamento ordenado de informações, a fim de evitar análises fragmentadas e perda de contexto.

A qualificação das informações também é determinante. Aquelas que são verificáveis, como documentos, dados de sistemas e evidências materiais, permitem análise imediata e, quando necessário, escalonamento célere. Já os relatos preliminares, ainda sem comprovação, demandam checagem de plausibilidade, solicitação de evidências adicionais e classificação provisória. Por fim, percepções subjetivas e sinais fracos devem ser registrados de forma sintética e direcionados a monitoramento ampliado, pois podem antecipar riscos, sobretudo quando analisados em conjunto com outros indícios.

A robustez do processo depende, ainda, da preservação adequada de registros e evidências para assegurar integridade, validade e utilidade futura. Recomenda-se:

- O armazenamento seguro e rastreável de registros;
- A vedação de qualquer manipulação que comprometa sua confiabilidade;
- A restrição de acesso às pessoas diretamente envolvidas;
- O registro, sempre que possível, da cadeia de custódia; e
- A adoção de prazos de retenção compatíveis com a complexidade de casos relacionados às organizações criminosas;

Esses cuidados fortalecem a capacidade interna de prevenção e resposta e protegem a companhia em eventual necessidade de comprovação perante autoridades ou auditorias externas, ao assegurar decisões ancoradas em evidências robustas e devidamente documentadas.

4.2. Proposições em Avaliação Interna e Escalonamento

Como parte da gestão de incidentes e da tomada de decisão, uma vez concluídos a identificação, o registro e a preservação das informações relacionadas ao caso, a instituição deve definir como avaliar e escalonar o assunto internamente. Como já indicado, as organizações criminosas geram exposições distintas conforme o setor, a localização, o porte e as características operacionais de cada empresa. Assim, a avaliação e o escalonamento podem seguir boas práticas, mas precisam ser ajustados à realidade de cada empresa.

A avaliação de questões de *compliance* e governança, bem como a definição do momento adequado para escalonamento, constituem ponto sensível da governança corporativa. Em situações relacionadas às organizações criminosas, essa sensibilidade aumenta, pois **a infiltração tende a ocorrer de forma gradual, fragmentada e informal, explorando assimetrias de informação, pressões territoriais, dependência econômica e lacunas operacionais**. Em regra, a empresa não se depara, no início, com evidências conclusivas ou fatos plenamente comprovados.

Organizações criminosas exploram deliberadamente zonas cinzentas da tomada de decisão empresarial, nas quais sinais isolados são tratados como insuficientes ou meramente operacionais. Essa dinâmica retarda respostas institucionais e permite a consolidação do risco ao longo do tempo. Redes criminosas também se beneficiam da hesitação diante de informações incompletas, utilizando empresas formalmente regulares para acessar contratos, fluxos financeiros e cadeias logísticas legítimas.

Sem escalonamento tempestivo, as relações se consolidam, criam dependência operacional e ampliam o risco de uso da infraestrutura logística para atividades ilícitas.

No sistema financeiro e em meios de pagamento, por exemplo, investigações públicas têm mostrado o uso de empresas formalmente ativas para movimentações incompatíveis com sua atividade econômica declarada. Alertas iniciais sobre fracionamento de transações, vínculos societários pouco transparentes ou movimentações atípicas por vezes permanecem em monitoramento passivo, retardando decisões internas mais restritivas e permitindo o uso continuado dessas estruturas para lavagem de recursos.

Também se observam situações de infiltração em processos de contratação, nas quais empresas distintas participam de cotações ou concorrências, atendem formalmente aos requisitos e, ainda assim, mantêm vínculos indiretos entre sócios, representantes ou endereços.

Quando analisados isoladamente, esses elementos não provocam escalonamento, favorecendo a aparência de regularidade e a permanência prolongada de estruturas vinculadas às organizações criminosas nos sistemas corporativos. Um *modus operandi* antes interpretado como "apenas fraude ou conluio" pode, em determinados contextos, representar porta de entrada para redes criminosas.

Em regiões sob influência territorial de grupos criminosos, relatos informais de colaboradores sobre pressões externas ou "indicações" de fornecedores costumam ser desconsiderados por falta de evidência documental. No entanto, a coação é parte frequente do método de atuação e, por sua natureza, tende a não deixar registros formais que possam ser apresentados. Sinais classificados como subjetivos podem constituir vetores relevantes de captura silenciosa de operações.

Diante desse cenário, a avaliação interna não deve se apoiar em lógica binária de confirmação ou descarte. Trata-se de exercício contínuo de gestão de risco, com adoção de medidas proporcionais à exposição identificada, ainda que em ambiente de incerteza. Experiências documentadas por Unidades de Inteligência Financeira e por autoridades europeias reforçam a utilidade de distinguir, no processo decisório, **fatos verificáveis, indícios objetivos** e **hipóteses analíticas**.

Fatos consistem em elementos de comprovação direta, tais como documentos, registros de sistemas, dados transacionais e evidências materiais.

Já os **indícios** correspondem a informações consistentes ainda não plenamente confirmadas, como relatos reiterados, padrões atípicos ou alertas de monitoramento.

E **hipóteses** são interpretações construídas a partir desses elementos, que orientam diligências adicionais e medidas de contenção.

Essa distinção reduz o risco de paralisia decisória e evita respostas precipitadas. Porém, a suficiência de informações para fins de prevenção e mitigação não deve ser confundida com o padrão probatório exigido para responsabilização penal ou administrativa. No âmbito da governança corporativa, a questão central é se os elementos disponíveis justificam medidas razoáveis para reduzir exposição, preservar evidências e impedir a continuidade de potenciais práticas ilícitas.

A priorização e o escalonamento devem considerar, de forma integrada, dois eixos: **severidade potencial** e **urgência**.

A **severidade** envolve magnitude de impactos legais, regulatórios, financeiros, reputacionais e operacionais, com atenção especial à segurança de pessoas e ativos.

Já a **urgência** decorre do tempo disponível para agir antes que o risco se agrave, seja pela dissipação de informações relevantes, seja pela continuidade de pagamentos, execução de contratos sensíveis ou exposição de equipes em campo.

Situações que indiquem possível acesso das organizações criminosas a processos críticos, como logística, transporte, segurança, gestão de ativos, cadastro de fornecedores e tecnologia da informação, exigem atenção reforçada, mesmo quando os valores inicialmente envolvidos não sejam expressivos.

O escalonamento deve ser compreendido como mecanismo de proteção institucional, e não como reconhecimento automático de irregularidade. Ao submeter situações sensíveis à análise de instâncias superiores ou comitês multidisciplinares, a empresa amplia a qualidade do julgamento, reduz vieses individuais e assegura decisões orientadas por múltiplas perspectivas, em linha com boas práticas de governança e gestão de riscos.

A ausência de critérios claros tende a favorecer dois desvios recorrentes, identificados em investigações públicas: (i) inação prolongada diante de riscos relevantes sob o argumento de falta de evidência; e (ii) adoção de medidas abruptas e desproporcionais, com impactos operacionais e efeitos colaterais significativos. Protocolos internos, ainda que flexíveis, conferem previsibilidade, consistência e rastreabilidade às decisões.

Determinadas situações justificam escalonamento imediato, independentemente do estágio da apuração. Entre elas estão:

- Indícios de coação;
- Extorsão ou ameaça a colaboradores;
- Sinais de infiltração em processos críticos, tentativas de ocultação ou destruição de informações;
- Pressões explícitas para contratações ou pagamentos fora do fluxo regular;
- Alterações suspeitas de beneficiário bancário; e
- Exposições relevantes a crimes transnacionais, como contrabando e tráfico.

Nesses casos, a proteção de pessoas, a preservação de evidências e a contenção do risco devem prevalecer sobre considerações estritamente operacionais.

Ademais, medidas iniciais devem, sempre que possível, priorizar respostas cautelares e reversíveis, tais como:

- Suspensão temporária de pagamentos;
- Ampliação de diligências;
- Restrição de acessos a sistemas e instalações; e
- Revisão de rotas ou fornecedores críticos.

A governança do processo decisório requer clareza de papéis e responsabilidades. A avaliação técnica deve ser conduzida por áreas qualificadas, com autonomia e acesso às informações relevantes. Decisões com impacto material significativo devem envolver a alta administração, conforme a estrutura de governança da companhia.

A documentação das decisões, com registro dos elementos considerados, das alternativas avaliadas e das justificativas adotadas, constitui prática essencial para auditoria, aprendizado institucional e eventual interação com autoridades.

Por fim, a experiência internacional demonstra que decisões sobre interrupção, substituição ou continuidade de relações comerciais potencialmente expostas a organizações criminosas envolvem *trade-offs* complexos entre segurança, impacto financeiro, responsabilidade social e reputação. Reconhecer previamente esses limites, estabelecer critérios claros de escalonamento e pactuar expectativas no nível da liderança reduz improvisações sob pressão e fortalece a resiliência institucional.

Assim, avaliação interna e escalonamento devem ser compreendidos como instrumentos centrais para antecipar riscos, reagir de forma proporcional e preservar integridade, pessoas e operações em ambientes complexos, nos quais a atuação das organizações criminosas desafia continuamente os controles formais.

4.3. Proposições em Canais Internos de Reporte

É importante destacar que, na identificação de possíveis fornecedores com vínculos com organizações criminosas, a efetividade dos canais internos de reporte depende de diretrizes estruturadas capazes de mitigar a subutilização dos canais, o receio de retaliação e as fragilidades de confidencialidade. Essas diretrizes não se limitam à criação formal de um canal de denúncias, mas abrangem sua governança, operacionalização e integração ao sistema de integridade corporativa, para funcionar, na prática, como instrumento de prevenção, detecção e resposta. Sua concepção deve, portanto, estar alinhada a parâmetros de **confiança, acessibilidade** e **proteção ao denunciante**.

O acesso de terceiros ao canal de denúncias, por outro lado, constitui um dos principais obstáculos à efetividade do processo global de denúncia, apuração e remediação. Em cadeias produtivas complexas, parceiros comerciais frequentemente não estão plenamente integrados à cultura de integridade da empresa, o que dificulta a disseminação, compreensão e confiança nos mecanismos de reporte. O problema tende a se agravar quando fornecedores e prestadores de serviços desconhecem a existência do canal de denúncias, enfrentam mecanismos excessivamente complexos para a realização dos relatos ou temem consequências comerciais decorrentes de um relato, reduzindo significativamente a probabilidade de que irregularidades sejam comunicadas de forma tempestiva.

Por isso, é essencial divulgar amplamente os canais de denúncia com linguagem clara e acessível, garantindo que possam ser utilizados por empregados, administradores, prestadores de serviços e demais terceiros da cadeia de fornecimento. Também é necessário estabelecer procedimentos internos transparentes para recebimento, triagem, investigação e encerramento de relatos, de modo a fortalecer a credibilidade do mecanismo e incentivar seu uso responsável.

Já o receio de retaliação é um dos principais fatores inibidores quando a denúncia envolve suspeitas de infiltração de organizações criminosas em fornecedores estratégicos ou parcerias relevantes. Nesses casos, a percepção de risco pessoal, patrimonial, profissional ou reputacional pode reduzir a disposição para relatar condutas ilícitas ou indícios de irregularidade, comprometendo a finalidade preventiva do canal.

Diante disso, recomenda-se adotar políticas explícitas de não retaliação, acompanhadas de mecanismos de monitoramento e responsabilização capazes de identificar e sancionar práticas retaliatórias, inclusive indiretas ou veladas. A proteção ao denunciante deve ser tratada como elemento central da mitigação de riscos, pois viabiliza fluxo contínuo de informações relevantes para a gestão da integridade corporativa.

Considerando o grau de criticidade associado a relatos sobre possível envolvimento de organizações criminosas, a preservação da identidade do reportante é requisito essencial para sustentar legitimidade e confiança no canal.

Em consonância com a norma ISO 37002, recomenda-se adotar ferramentas que permitam o anonimato e assegurem tratamento sigiloso dos casos, com restrição de acesso aos profissionais responsáveis pela apuração e asseguração da observância aos princípios da necessidade, da finalidade e da proporcionalidade.

A gestão adequada da confidencialidade também requer critérios claros para compartilhamento interno e externo das informações reportadas, especialmente quando houver necessidade de comunicação com autoridades. Esse compartilhamento deve ser responsável e conduzido de forma a proteger a identidade do reportante e a integridade das apurações, evitando exposições que comprometam a segurança dos envolvidos e a eficácia das medidas adotadas.

Por fim, o fortalecimento dos canais de denúncia não constitui medida meramente procedimental, mas estratégia de mitigação de riscos relacionada à exposição da empresa a vínculos indiretos com organizações criminosas, tendo impactos sobre responsabilidade jurídica, governança e sustentabilidade institucional.

4.4. Proposições em Reporte a Autoridades Competentes

No âmbito da mitigação de riscos decorrentes da atuação das organizações criminosas nas relações empresariais, o reporte às autoridades competentes pode constituir uma medida relevante e necessária a ser adotada pela empresa, conforme a natureza e a gravidade da situação identificada.

Diferentemente dos mecanismos internos, a comunicação externa envolve o compartilhamento de informações com órgãos estatais, como autoridades policiais, Ministério Público, agências reguladoras e órgãos de controle, com potenciais efeitos jurídicos, reputacionais e operacionais. Nesse sentido, o reporte externo pode gerar incertezas quanto ao momento, à extensão e à forma mais adequada de comunicação, especialmente quando os fatos ainda estão em fase inicial de apuração interna.

A legislação brasileira incentiva a cooperação entre o setor privado e o poder público, cabendo às empresas avaliar a forma e o momento mais apropriados para eventual comunicação às autoridades. Essa decisão deve considerar, entre outros elementos, a robustez dos indícios disponíveis, o risco de continuidade da prática ilícita, a existência de ameaça à integridade física de colaboradores, o eventual envolvimento de agentes públicos e a incidência de obrigações regulatórias específicas.

Nesse cenário, a Lei Anticorrupção e o respectivo Decreto Regulamentador, ao valorizarem programas de integridade efetivos, reforçam a importância da atuação diligente, estruturada e de boa-fé. Assim, a avaliação cuidadosa das informações disponíveis e das circunstâncias do caso contribui para que eventual comunicação às autoridades seja realizada de forma responsável e tempestiva.

A omissão diante de indícios consistentes de envolvimento de fornecedores ou clientes com organizações criminosas pode ser interpretada como falha de diligência e de gestão de riscos, especialmente quando a empresa mantém relações comerciais potencialmente contaminadas por práticas ilícitas. Nesses casos, o reporte externo pode se revelar necessário como instrumento de mitigação de riscos sistêmicos e de demonstração de comprometimento institucional com a legalidade, preservando a boa-fé objetiva.

A condução cuidadosa do processo de comunicação contribui para preservar a credibilidade e a imagem institucional, sem prejuízo da cooperação com as autoridades competentes. A decisão sobre a comunicação, ou não, às autoridades também deve levar em consideração eventuais repercussões reputacionais que demandam atenção quanto à forma, canais e estratégias de comunicação institucional, considerando a sensibilidade e a relevância das informações.

Diante disso, recomenda-se avaliação individualizada de cada caso. Devem ser considerados, entre outros fatores, a natureza e a consistência dos indícios, o grau de envolvimento de contrapartes e colaboradores internos, os riscos de continuidade da operação comercial, a possibilidade de ocultação ou destruição de provas e os potenciais desdobramentos de investigações em curso. Essa avaliação pode ser conduzida por instâncias internas qualificadas, a exemplo das áreas jurídica e de *compliance*, de modo a assegurar decisões coerentes com a estratégia de integridade da empresa. A adoção de protocolos internos para reporte externo, com definição de responsabilidades e a adoção de fluxos decisórios estruturados, com o devido assessoramento jurídico, reduz arbitrariedades e confere previsibilidade ao processo decisório.

A comunicação externa pode ser necessária para interromper práticas ilícitas de maior gravidade, mitigar riscos sistêmicos ou colaborar com investigações de interesse público. Ainda assim, a decisão sobre a comunicação, ou não, às autoridades deve levar em conta critérios relacionados à sensibilidade do tema, principalmente para que, nos casos em que a comunicação vier a ocorrer, isso seja feito de forma adequada e proporcional. Em regra, o reporte tende a ser mais recomendável quando houver indícios consistentes de prática ilícita, risco concreto de reiteração, possibilidade de destruição de provas ou potencial impacto relevante sobre terceiros, o mercado ou a administração pública.

Nessa perspectiva, a cooperação responsável com as autoridades, quando alinhada a um programa de integridade efetivo, contribui para reduzir a exposição a riscos jurídicos e reputacionais associados à influência das organizações criminosas nas relações comerciais.

Canal Fala.BR e reporte a autoridades

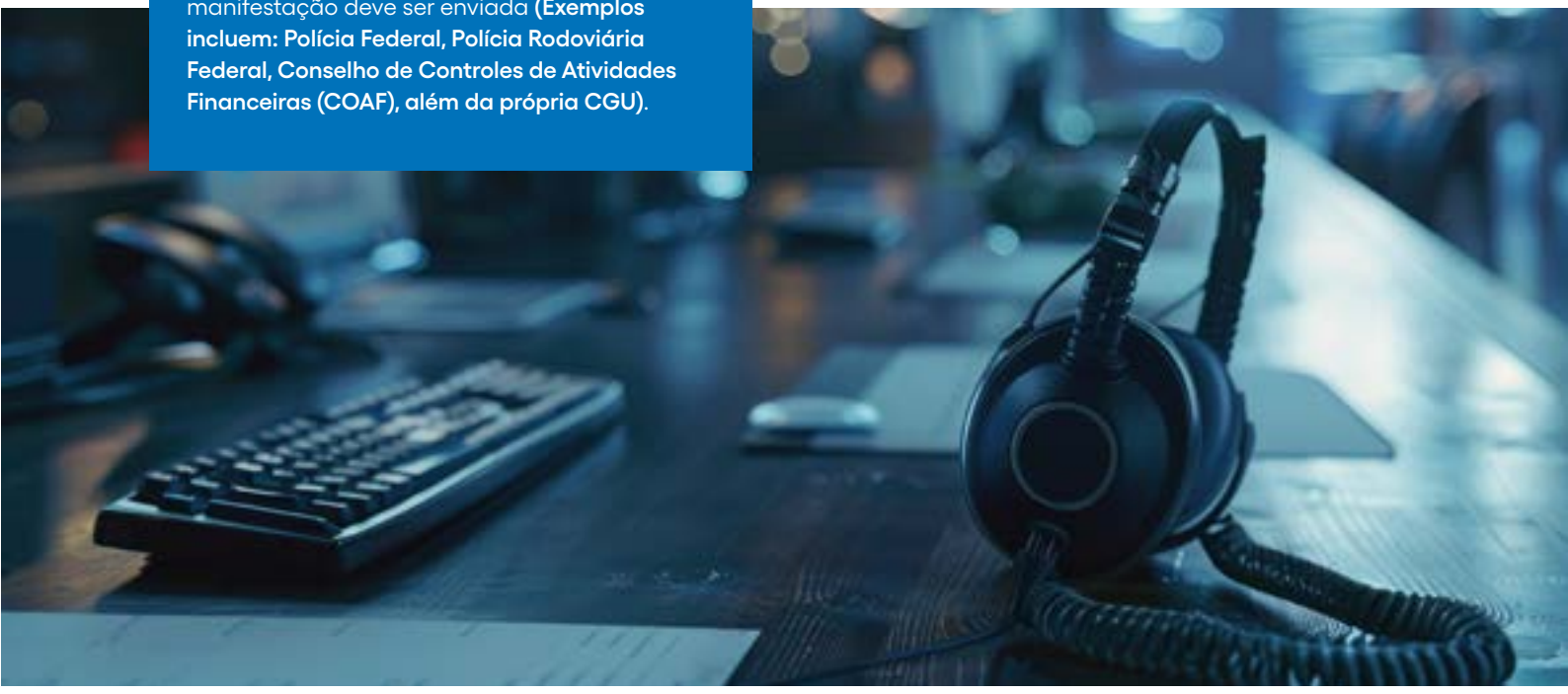
Um dos canais que empresas e colaboradores podem se valer para o reporte de situações relacionadas a possíveis irregularidades ou indícios de atuação de organizações criminosas é aquele disponibilizado pela CGU.

O **Fala.BR** (falabr.cgu.gov.br) é a plataforma oficial para recebimento e tratamento de denúncias, inclusive de forma anônima, com mecanismos destinados à proteção da identidade do denunciante. As manifestações podem ser realizadas por pessoas físicas ou jurídicas, com possibilidade de acompanhamento por meio da conta Gov.br, além do envio de informações detalhadas e anexos que auxiliem a apuração.

O sistema adota medidas de proteção como sigilo da identidade (quando informada), restrição de acesso aos dados e possibilidade de registro anônimo. As denúncias são avaliadas quanto à sua consistência e podem ser encaminhadas aos órgãos competentes para apuração. Não é necessário apresentar provas, mas o fornecimento de informações completas contribui para a efetividade da análise. Ao fazer a denúncia, é possível selecionar para qual órgão ou entidade a manifestação deve ser enviada **(Exemplos incluem: Polícia Federal, Polícia Rodoviária Federal, Conselho de Controles de Atividades Financeiras (COAF), além da própria CGU)**.

Não se pode perder de vista, ainda, a existência de situações em que a atuação de organizações criminosas represente risco à integridade física de colaboradores, seja por meio de ameaças, seja pelo cometimento de atividades criminosas nas dependências da empresa ou com utilização de seus recursos. Nessas hipóteses, torna-se essencial a existência de protocolo específico para avaliação dos riscos e comunicação segura às autoridades policiais.

Embora também se apliquem as ponderações anteriormente expostas quanto ao momento e à forma do reporte, situações de urgência podem exigir comunicação imediata ao Estado. Por essa razão, recomenda-se que a empresa tenha previamente mapeados os canais disponíveis para denúncia e reporte de crimes na localidade. A esse respeito, vale mencionar outros canais de denúncia de abrangência nacional mantidos pelo poder público. Destacam-se o **Disque-Denúncia (181)**, amplamente utilizado para o recebimento de informações sobre crimes em geral, especialmente no âmbito local e de forma anônima; o **Comunica PF**, canal da Polícia Federal destinado ao recebimento de informações sobre crimes federais; o **Disque 100**, voltado ao registro de violações de direitos humanos; e o **Ligue 180**, canal especializado no atendimento e encaminhamento de casos de violência contra a mulher.



4.5. Proposições em Medidas de Proteção, Continuidade das Operações e de Gestão de Crises

A mitigação de impactos e a preservação da continuidade dos negócios diante de riscos associados às organizações criminosas exigem abordagem integrada, proporcional e orientada por evidências.

A proteção de pessoas e de ativos essenciais deve constituir o primeiro eixo de qualquer resposta. Protocolos de segurança devem orientar a atuação de colaboradores expostos a regiões, rotas ou contrapartes de maior risco, com diretrizes para conduta segura e, quando necessário, atuação sigilosa, a fim de reduzir vulnerabilidades e riscos de retaliação. Conforme a gravidade, pode-se adotar, por exemplo, afastamento temporário de colaboradores ameaçados ou envolvidos em situações sensíveis.

A continuidade das operações, com preservação da integridade, requer que o funcionamento do negócio não implique flexibilização de padrões éticos ou critérios de conformidade. Em ambientes com presença de grupos criminosos, por exemplo, recomenda-se mapear e acionar rotas alternativas de fornecimento e logística, ainda que isso imponha replanejamento e custos adicionais. Da mesma forma, terceiros associados a sinais consistentes de irregularidade devem ser substituídos de forma temporária ou definitiva com base em critérios objetivos de severidade e materialidade, mesmo quando houver impacto operacional relevante. Já em relação a processos críticos, planos de contingência devem prever níveis mínimos de serviço, operação degradada e rotas paralelas previamente testadas. Assim, a revisão periódica de riscos geográficos, setoriais e comportamentais deve integrar o planejamento para que vulnerabilidades emergentes não sejam tratadas apenas de forma reativa.

Nesse mesmo sentido, o processo de gestão de crises deve estar estruturado com o conhecimento dos cenários relacionados aos riscos de terceiros, de modo a garantir respostas eficazes acompanhadas de comunicação interna e externa criteriosa, objetiva, coordenada e consistente.

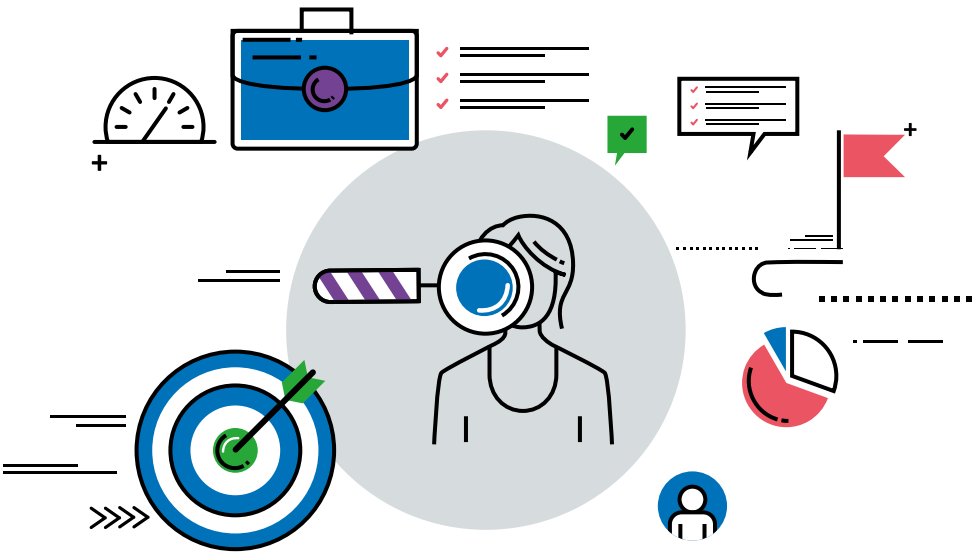
Também é importante que informações sensíveis não circulem de maneira informal, a fim de evitar distorções, alarme indevido ou exposição de colaboradores e ativos. Internamente, equipes de linha de frente devem receber orientações objetivas e direcionadas sobre conduta, canais de reporte e procedimentos em caso de agravamento. Externamente, clientes, parceiros e demais partes interessadas devem ser informados de forma factual e proporcional, com preservação de sigilo quando exigido por lei ou pela integridade da apuração, sob orientação jurídica. Comunicados precipitados ou contraditórios prejudicam decisões e corroem a confiança, de modo que disciplina comunicacional integra a própria resposta.

No planejamento de cenários e no reconhecimento de limites operacionais, é necessário admitir que, mesmo com protocolos robustos, a capacidade de intervenção da empresa é limitada em territórios sob influência de grupos criminosos. Informações podem ser incompletas ou baseadas em percepções locais, e decisões envolvem escolhas difíceis entre segurança, impacto financeiro e reputação. O papel da empresa não é substituir o Estado, mas atuar com responsabilidade dentro de sua esfera de controle, com apoio de especialistas externos e coordenação com autoridades competentes quando necessário. Definições de limite de perda, gatilhos de escalonamento e critérios para suspensão, redução ou realocação de operações devem ser pactuados previamente e revisados à luz de lições aprendidas.

Em suma, a avaliação de efeitos indiretos e colaterais deve ser contínua e multidisciplinar. A desmobilização de fornecedores locais pode produzir impactos socioeconômicos em comunidades vulneráveis. A substituição de rotas ou contrapartes pode aumentar a exposição de equipes em campo. Dependências não mapeadas na cadeia de suprimentos podem emergir após intervenções. Além disso, tanto ação quanto inação podem gerar efeitos reputacionais relevantes. Por isso, decisões devem incorporar perspectivas de diferentes áreas, como *compliance*, operações, segurança e compras, com revisões periódicas de impacto e medidas de mitigação social e operacional quando aplicáveis.

Por fim, postura preventiva e cultura organizacional são tão relevantes quanto controles técnicos. A companhia deve sustentar ambiente em que reportes precoces sejam valorizados, temores de retaliação sejam reduzidos e transparência seja reforçada por lideranças exemplares. Também é necessário explicitar que decisões difíceis em favor da integridade contam com apoio efetivo da alta administração, para que o princípio de "continuar operando com ética" prevaleça diante de pressões de prazo, custo e mercado. Nesse contexto, é igualmente importante considerar que métricas de desempenho baseadas exclusivamente em volume de produção ou de análise podem desestimular a atenção a indícios de fraude e reduzir a adesão da equipe a práticas de reporte de irregularidades ou situações suspeitas.

Cultura preventiva, aprendizado pós-incidente, atualização da biblioteca de *red flags* e melhoria contínua de fluxos elevam a resiliência empresarial e protegem pessoas, ativos e reputação, preservando a continuidade sem renúncia a princípios.



5 Proposições Finais

Este Guia oferece referências iniciais para reflexão empresarial quanto à melhor compreensão e à mitigação dos riscos associados à atuação das organizações criminosas nas relações empresariais e comerciais, reconhecendo a complexidade e a natureza assimétrica desse fenômeno. Tais riscos extrapolam perdas financeiras diretas, alcançando dimensões reputacionais e, em determinados contextos, a segurança de pessoas e ativos. O Guia não substitui aconselhamento jurídico ou regulatório, fundamentais para esse tipo de tema. As decisões empresariais devem priorizar a proteção de pessoas, ativos, integridade e conformidade legal, especialmente em contextos de risco elevado ou incerteza informacional.

As proposições apresentadas partem do reconhecimento de que não existem soluções únicas ou definitivas. A efetividade das medidas de prevenção, gerenciamento e resposta depende da capacidade das organizações em adotar abordagens proporcionais ao seu perfil de risco, de integrar governança, *compliance*, operações e cultura organizacional e de revisar continuamente seus mecanismos diante do avanço e refinamento constante das organizações criminosas. Controles formais revelam seus limites quando não contam com o compromisso da alta administração, com a cooperação entre áreas e com um ambiente institucional que favoreça e priorize a identificação e o tratamento tempestivo de sinais de alerta.

Nesse contexto, destaca-se a relevância da adoção de uma governança robusta de gestão de riscos de terceiros que estabeleça e exija a documentação necessária, a fundamentação e a rastreabilidade das decisões, o fortalecimento do mapeamento de contrapartes e operações de maior risco, a promoção da confiança nos canais internos de reporte, a proteção de colaboradores e a adoção de medidas de mitigação proporcionais aos riscos identificados. A gestão de incidentes e a tomada de decisão

devem ser compreendidas como processos voltados a lidar com imprevisibilidades e equilibrar segurança e integridade com a continuidade das operações. Esse conjunto de desafios demanda compromisso contínuo dos órgãos de governança, da alta administração, investimento em capacitação e ferramentas de monitoramento, integração entre áreas e aprendizado institucional.

Este documento foi elaborado no âmbito da Comissão de Integridade e Responsabilidade Corporativa da ICC Brasil, capítulo nacional da ICC, organização que representa institucionalmente mais de 45 milhões de empresas em mais de 130 países. A ICC Brasil reúne seus membros em oito comissões temáticas e busca contribuir para a formulação de políticas públicas voltadas ao desenvolvimento socioeconômico do país, por meio de interlocução contínua entre os setores público e privado.

A Comissão de Integridade e Responsabilidade Corporativa tem por missão fortalecer a cultura de ética e integridade nas organizações, bem como contribuir para o aprimoramento contínuo do ambiente regulatório nacional. Sua atuação é orientada ao enfrentamento da corrupção e à promoção da ética e da integridade como referências fundamentais de reputação, confiança e competitividade.

A elaboração deste Guia contou com a colaboração da Secretaria de Integridade Privada da Controladoria-Geral da União (CGU), que possui a competência de atuação em três vertentes: fomento, regulamentação e avaliação de programas de integridade; responsabilização de pessoas jurídicas pela prática de ilícitos; e celebração de acordos de leniência com pessoas jurídicas que estejam comprometidas com a remediação de atos lesivos praticados, com o aperfeiçoamento de suas medidas de integridade e que auxiliem a Administração Pública na investigação de ilícitos e recuperação de valores desviados.

Checklist

1. Governança e *Compliance*

- ☐ A alta administração estabeleceu diretrizes estratégicas, aprovou políticas internas e supervisiona a sua implementação em relação a riscos de organizações criminosas.
- ☐ As áreas responsáveis por *compliance*, integridade ou prevenção de ilícitos atuam com autonomia funcional, acesso direto às instâncias decisórias superiores e possuem recursos compatíveis com o nível de exposição ao risco.
- ☐ A gestão do risco de infiltração criminosa não está atribuída a uma unidade isolada: áreas operacionais (contratações, pagamentos, gestão de ativos, logística e relacionamento com terceiros) estão formalmente integradas ao sistema de prevenção, com responsabilidades claramente definidas.
- ☐ A empresa possui interlocução contínua e coordenação efetiva entre diferentes áreas da companhia para enfrentamento do risco de infiltração criminosa.
- ☐ Existe um processo estruturado e abrangente de avaliação de riscos, com definição de instrumentos de gestão, controles internos e mecanismos eficazes de monitoramento ao longo da cadeia de valor.

---

2. *Due diligence* de Terceiros

- ☐ Todos os terceiros que mantêm relação comercial ou operacional com a empresa (clientes, fornecedores, prestadores de serviços, parceiros comerciais, representantes, intermediários e consultores) são submetidos a procedimentos de *due diligence*.
- ☐ A *due diligence* compreende, no mínimo: identificação cadastral completa, estrutura societária, definição do beneficiário final, eventual exposição política, histórico reputacional e presença em listas restritivas.
- ☐ É avaliado o local em que o terceiro opera, especialmente em regiões de conflito armado, narcotráfico ou de fronteira.
- ☐ Há mecanismos de monitoramento contínuo, incluindo atualização periódica das análises, monitoramento de alterações em CNPJs e cadastros, mudanças de controle societário, capital social ou objeto social.
- ☐ Pagamentos fracionados, valores incompatíveis com o mercado ou alterações repentinas de beneficiários bancários são tratados como sinais de alerta.
- ☐ As informações obtidas na avaliação de terceiros orientam decisões de contratação, pagamento e renovação contratual, evitando que a análise se reduza a uma etapa meramente formal.

- ☐ A política de *due diligence* reconhece expressamente seus próprios limites e prevê respostas para situações em que surjam indícios de vínculos ilícitos, mesmo após cumprimento formal dos procedimentos.
- ☐ São mapeados sócios, administradores, procuradores, intermediários e representantes, bem como identificados endereços, contas bancárias, telefones e vínculos compartilhados.
- ☐ São cruzados dados de fornecedores, subfornecedores e prestadores de serviço, com aplicação de técnicas de *network analytics* para revelar redes ocultas.

---

3. Rastreabilidade e Documentação

- ☐ A empresa assegura rastreabilidade do que foi feito, por quem e por qual motivação, por meio de documentação mínima e padronizada relativa a contratos, aditivos, medições, pagamentos e aprovações.
- ☐ São padronizados campos críticos como: CNPJ ou identificação do beneficiário final, conta bancária de destino, centro de custo, contrato-base, motivo da contratação e responsável pela aprovação.
- ☐ Constam de forma consistente nos registros: contrato, aditivo ou justificativa operacional, fornecedor e CNPJ, dados bancários de destino, centro de custo ou projeto vinculado, quem solicitou, quem aprovou, motivação da decisão e eventuais exceções.
- ☐ A empresa evita aprovações verbais ou informais, registra decisões em canais oficiais e documenta integralmente as exceções.
- ☐ Existem regras claras para exceções, com registro, justificativa e supervisão apropriada.

---

4. *Red flags* e Sinais de Alerta

- ☐ A empresa criou e mantém uma biblioteca de *red flags* que consolida sinais de alerta identificados nos processos internos.
- ☐ Para cada *red flag*, a biblioteca indica o processo de origem, o nível de severidade e a conduta esperada.
- ☐ São monitorados, entre outros, os seguintes sinais: beneficiário final não identificado, alterações societárias sem justificativa, operações incompatíveis com a capacidade declarada, uso atípico de rotas logísticas, solicitações urgentes sem documentação adequada, pagamentos fracionados, abordagens indevidas a colaboradores em funções críticas e interações com regiões ou setores reconhecidamente sensíveis.
- ☐ A empresa possui atenção a sinais como: mudanças frequentes de conta bancária, valores incompatíveis com o mercado, intermediários sem função clara, pressão por exceções, divergências entre o contratado e o executado e presença recorrente de terceiros não cadastrados no local de operação.
- ☐ Existe um fluxo claro para tratar sinais de alerta, contemplando as etapas de detectar, qualificar, registrar, decidir e remediar, com responsáveis definidos e critérios de escalonamento proporcionais ao risco identificado.

5. Gestão de Incidentes e Tomada de Decisão

- ☐ Existe um ciclo contínuo de detecção, registro e preservação de evidências, com incorporação sistemática de aprendizados ao longo do tempo.
- ☐ Existe fluxo estruturado de integração entre as áreas de *compliance*, jurídico, recursos humanos, operações e demais áreas pertinentes, com responsabilidades definidas e compartilhamento ordenado de informações.
- ☐ As informações são qualificadas, distinguindo-se informações verificáveis (documentos, dados de sistemas), relatos preliminares (que demandam checagem de plausibilidade) e percepções subjetivas (registradas para monitoramento ampliado).
- ☐ Os registros e evidências são armazenados de forma segura e rastreável, com restrição de acesso, registro da cadeia de custódia e prazos de retenção compatíveis com a complexidade dos casos.
- ☐ A avaliação interna e o escalonamento distinguem fatos verificáveis, indícios objetivos e hipóteses analíticas, reduzindo o risco de paralisia decisória e evitando respostas precipitadas.
- ☐ A priorização e o escalonamento consideram de forma integrada severidade potencial (impactos legais, regulatórios, financeiros, reputacionais e operacionais) e urgência (tempo disponível para agir antes que o risco se agrave).
- ☐ Há escalonamento imediato para situações como: indícios de coação, extorsão ou ameaça a colaboradores; sinais de infiltração em processos críticos; tentativas de ocultação ou destruição de informações; pressões explícitas para contratações ou pagamentos fora do fluxo regular; alterações suspeitas de beneficiário bancário; e exposições relevantes a crimes transnacionais.
- ☐ Medidas iniciais priorizam respostas cautelares e reversíveis, como suspensão temporária de pagamentos, ampliação de diligências, restrição de acessos a sistemas e instalações e revisão de rotas ou fornecedores críticos.
- ☐ As decisões são documentadas, com registro dos elementos considerados, alternativas avaliadas e justificativas adotadas.

---

6. Canais Internos de Reporte

- ☐ A empresa possui canais de denúncia amplamente divulgados, com linguagem clara e acessível, que podem ser utilizados por empregados, administradores, prestadores de serviços e demais terceiros da cadeia de fornecimento.
- ☐ Foram estabelecidos procedimentos internos transparentes para recebimento, triagem, investigação e encerramento de relatos.
- ☐ Foram adotadas políticas explícitas de não retaliação, acompanhadas de mecanismos de monitoramento e responsabilização para identificar e sancionar práticas retaliatórias, inclusive indiretas ou veladas.
- ☐ A identidade do reportante é preservada sempre que tecnicamente possível, com ferramentas que permitam anonimato ou, ao menos, tratamento sigiloso, com restrição de acesso aos profissionais responsáveis pela apuração.
- ☐ Existem critérios claros para compartilhamento interno e externo das informações reportadas, especialmente quando houver necessidade de comunicação com autoridades.
- ☐ A empresa oferece devolutivas sobre encaminhamentos das denúncias recebidas.

7. Reporte a Autoridades Competentes

- ☐ O reporte a autoridades competentes deve ser efetuado mediante avaliação jurídica criteriosa e alinhada à estratégia de integridade da empresa.
- ☐ O reporte externo observa critérios de necessidade, adequação e proporcionalidade, evitando exposições indevidas que comprometam a segurança jurídica da empresa ou de seus colaboradores.
- ☐ A empresa assegura que haja apuração interna mínima e lastro informacional suficiente antes de realizar o reporte, evitando comunicações precipitadas.

---

8. Treinamentos e Cultura Organizacional

- ☐ Áreas mais expostas recebem capacitações específicas: compras, logística, obras e serviços, área comercial e canais, financeiro e tesouraria, segurança patrimonial, jurídico, *compliance* e lideranças locais.
- ☐ O conteúdo dos treinamentos cobre tipologias relevantes ao negócio, sinais de alerta ao longo dos processos, aplicação da política de exceções, requisitos mínimos de registro e critérios para escalonamento.
- ☐ A comunicação interna traduz conceitos para a realidade operacional, com dilemas recorrentes como "urgência", "fornecedor indicado" e "mudança de conta bancária".
- ☐ São utilizadas práticas de *microlearning*, com módulos curtos distribuídos ao longo do ano, para aumentar retenção e aplicação imediata.
- ☐ São realizados treinamentos baseados em cenários, com simulações e *role-plays*, incluindo situações como pressão para contratar fornecedor "indicado", urgências fora do fluxo, interferência externa indevida e tentativas de obtenção de dados sensíveis.
- ☐ A liderança reforça consistentemente a importância de controles, transparência e registro (*tone from the top*).
- ☐ São assegurados espaços seguros para diálogo e questionamento, reduzindo zonas de silêncio e ampliando detecção precoce.
- ☐ A empresa adota a lógica de *speak-up by design*, normalizando relatos, dúvidas e pedidos de ajuda como comportamento esperado.

9. Indicadores de Cultura e Monitoramento

- ☐ São acompanhados indicadores de cultura (KPIs e KRIs), como volume e qualidade de relatos, reincidência por área, concentração de exceções, taxa de *waivers* e percentual de terceiros críticos capacitados.
- ☐ Esses indicadores são utilizados para medir maturidade, identificar pontos cegos e priorizar ações.
- ☐ O monitoramento é compreendido como processo imperfeito e evolutivo, integrado à governança, e não como garantia absoluta contra riscos ilícitos.

---

10. Medidas de Proteção e Continuidade das Operações

- ☐ Protocolos de segurança orientam a atuação de colaboradores expostos a regiões, rotas ou contrapartes de maior risco, com diretrizes para conduta discreta e, quando necessário, atuação sigilosa.
- ☐ Conforme a gravidade, é previsto afastamento temporário de colaboradores ameaçados ou envolvidos em situações sensíveis.
- ☐ A empresa mapeia e aciona rotas alternativas de fornecimento e logística em ambientes com presença de grupos criminosos.
- ☐ Terceiros associados a sinais consistentes de irregularidade são substituídos de forma temporária ou definitiva, com base em critérios objetivos de severidade e materialidade.
- ☐ Para processos críticos, existem planos de contingência prevendo níveis mínimos de serviço, operação degradada e rotas paralelas previamente testadas.
- ☐ A revisão periódica de riscos geográficos, setoriais e comportamentais integra o planejamento.
- ☐ A comunicação interna e externa é conduzida de forma criteriosa, coordenada e consistente, evitando a circulação informal de informações sensíveis.
- ☐ Estão definidos limites de perda, gatilhos de escalonamento e critérios para suspensão, redução ou realocação de operações, revisados à luz de lições aprendidas.
- ☐ A avaliação de efeitos indiretos e colaterais é contínua e multidisciplinar, incorporando perspectivas de *compliance*, operações, segurança e compras.

11. Sanções Internacionais (para empresas com grau de internacionalização)

- ☐ A empresa avalia sua exposição a sanções internacionais, participação de *US persons*, pagamentos em dólar, uso de tecnologias ou serviços de origem norte-americana e cadeias de fornecimento globais.
- ☐ São adotados controles proporcionais alinhados a referências reconhecidas, como o OFAC e seu *framework* para programas de sanções, bem como orientações públicas de risco.

---

12. Revisão Contínua e Aprendizado Institucional

- ☐ As estratégias de prevenção, detecção e resposta são revisadas de forma contínua, à medida que novos padrões de atuação e vulnerabilidades se tornam evidentes.
- ☐ A empresa promove cultura preventiva, aprendizado pós-incidente, atualização da biblioteca de *red flags* e melhoria contínua de fluxos.
- ☐ A efetividade das medidas depende da integração de governança, *compliance*, operações e cultura organizacional, com revisão contínua dos mecanismos diante da adaptação constante das organizações criminosas.

Comitê Brasileiro da Câmara de Comércio Internacional (ICC Brasil)
Rua Surubim, 504 – 12° andar
Brooklin – São Paulo – SP – CEP 04571-050, Brasil
www.iccbrasil.org