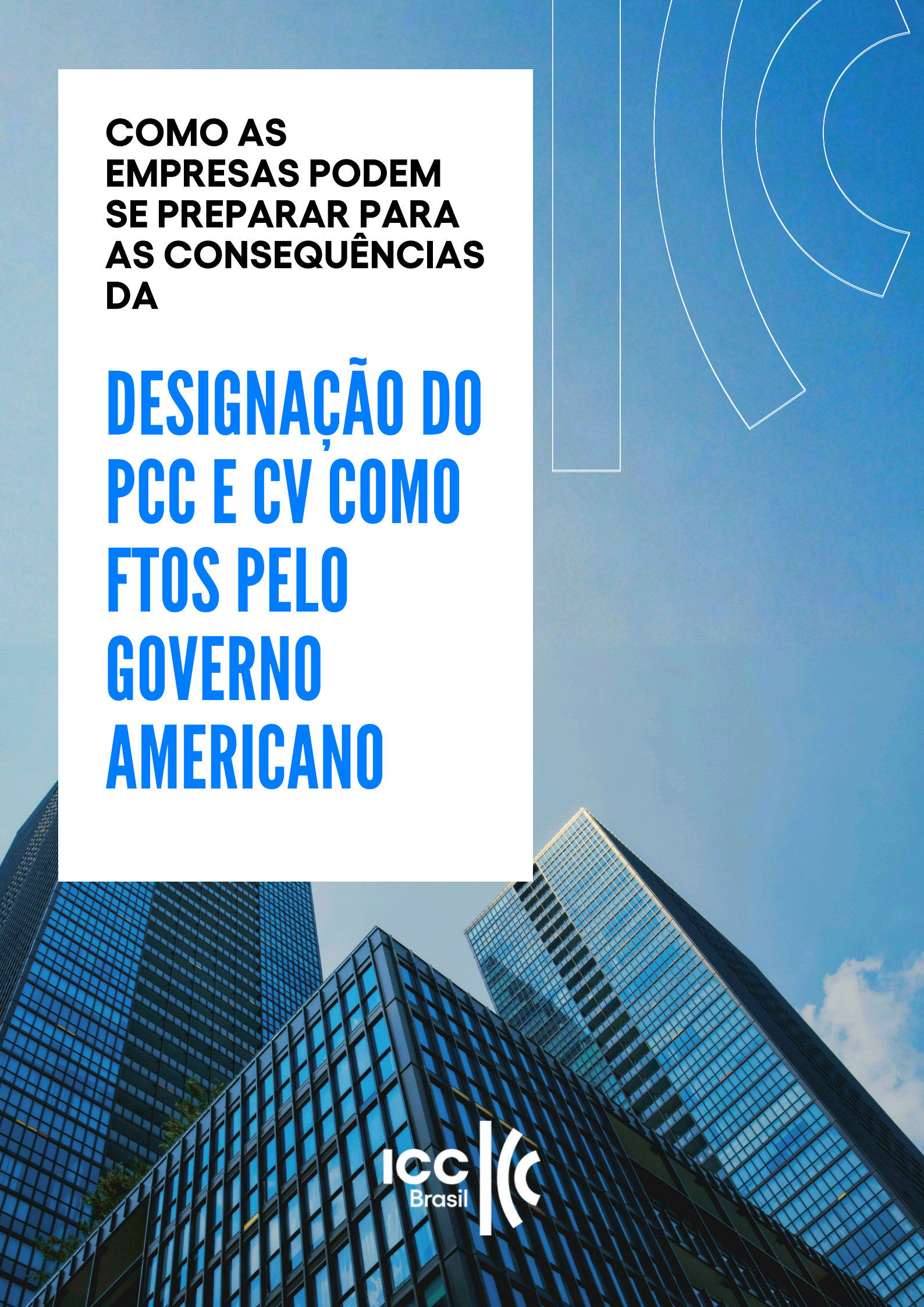
COMO AS EMPRESAS PODEM SE PREPARAR PARA AS CONSEQUÊNCIAS DA

# DESIGNAÇÃO DO PCC E CV COMO FTOS PELO GOVERNO AMERICANO



**Sobre a ICC (International Chamber of Commerce) e a ICC Brasil**
Como representante institucional de mais de 45 milhões de empresas em mais de 170 países, a Câmara de Comércio Internacional (ICC) atua como a principal voz da economia real em organizações multilaterais como a Organização das Nações Unidas e a Organização Mundial do Comércio, entre outras, contribuindo para as tomadas de decisão globais.

No Brasil, a ICC atua com a missão de trazer o setor privado para o centro da agenda de inserção internacional, integridade e sustentabilidade, atuando junto a governos locais e organismos internacionais na construção de políticas públicas voltadas para o desenvolvimento econômico, social e a melhoria do ambiente de negócios. A instituição possui uma visão multissetorial com 200 associados entre empresas multinacionais, bancos, consultorias e escritórios de advocacia. Conta com oito comissões temáticas nas quais desenvolve projetos e endereça assuntos de alta relevância para o setor empresarial brasileiro nas frentes de *advocacy* e da formulação de melhores práticas.

ICC Brasil
Rua Surubim 504, 12° andar. Brooklin, São Paulo - SP
CEP 04571-050
Tel: +55 11 3040-8832 / 8835
iccbrasil@iccbrasil.org

**Favor citar como:**
ICC Brasil (2026), "**Como as empresas podem se preparar para as consequências da designação do PCC e CV como FTOs pelo Governo Americano**"

# Prefácio

O presente memorando analisa o recente reposicionamento da política externa norte-americana em relação a organizações criminosas latino-americanas, designadas como Foreign Terrorist Organizations (FTO), nos termos da Section 219 do Immigration and Nationality Act, e como Specially Designated Global Terrorists (SDGT), nos termos da Executive Order 13224.

**Em maio de 2026, os Estados Unidos anunciaram a designação do Comando Vermelho (CV) e do Primeiro Comando da Capital (PCC) como SDGTs, e a designação de ambos como FTOs tornou-se efetiva em 5 de junho de 2026.**

**Essa mudança altera o ambiente de risco para empresas no Brasil, inclusive aquelas com programas robustos de compliance.** A designação modifica e amplia a natureza jurídica da exposição corporativa relacionada a contrapartes, razão pela qual merece atenção prioritária de acionistas, órgãos de governança e estruturas de controle.

Organizações criminosas como o PCC e o CV expandem suas atividades ilícitas por meio de estratégias destinadas a contornar mecanismos de fiscalização e de aplicação da lei. **Isso pode envolver o uso de estruturas empresariais aparentemente lícitas, a tomada gradual do controle de negócios estabelecidos ou a utilização de pessoas interpostas para assumir a titularidade efetiva de ativos e operações.**

Na prática, esses grupos podem se inserir em cadeias de valor empresariais que, à primeira vista, parecem regulares. A questão central para as empresas é, portanto, demonstrar que essa exposição foi identificada, avaliada e tratada de forma adequada no novo quadro regulatório.

Operações com terceiros, intermediários ou cadeias de suprimento expostas a essas organizações deixam de configurar risco predominantemente reputacional ou de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT) clássico. **Passam a configurar risco penal corporativo sob a legislação extraterritorial dos Estados Unidos, com gatilhos jurisdicionais que vão além da liquidação em dólar e abrangem, entre outros vetores, o uso do sistema financeiro americano, a presença de cidadãos ou residentes americanos na cadeia decisória e a utilização de tecnologia originária dos Estados Unidos.**

**Dessa forma, a resposta adequada deve ser proporcional e baseada em risco.** Não se exige controle perfeito, mas sim um processo razoável, documentado, testado e revisado em ciclos regulares. Este documento orientador apresenta um referencial inicial prático e não vinculante destinado a auxiliar empresas de diferentes portes e setores, reguladas ou não, na identificação de possíveis áreas de risco e no fortalecimento de controles internos. Sua aplicação deve ser adaptada ao contexto de negócios, ao setor de atuação, ao perfil de risco e ao grau de maturidade em governança e compliance de cada organização.

# 1 Arcabouço Legal e Natureza dos Riscos

Na legislação brasileira, o PCC e o CV não são classificados como organizações terroristas. A Lei Antiterrorismo exige elementos específicos para esse enquadramento, como motivação ligada à xenofobia, discriminação ou preconceito de raça, cor, etnia ou religião, além da finalidade de provocar terror social ou generalizado.

Essa classificação no Brasil não reduz a exposição das empresas à legislação dos Estados Unidos. Os marcos jurídicos norte-americanos são aplicados independentemente da qualificação adotada pela jurisdição em que os fatos ocorreram. A classificação como SDGT permite impor **sanções financeiras e restrições a pessoas ou entidades que mantenham vínculos com as organizações designadas.** Já a designação como FTO **amplia as consequências legais, inclusive quanto ao apoio material, ao financiamento e à cooperação com esses grupos.**

Assim, se uma empresa tem presença, operações financeiras, transações sujeitas à jurisdição americana ou outro ponto de conexão relevante com os EUA, as regras americanas podem ser aplicáveis.

A designação como FTO aciona o **regime penal de apoio material ao terrorismo.** Esse conceito é interpretado de forma ampla e vai além do financiamento direto. Pode abranger pontos que necessitam atenção, como:

- relações comerciais e intermediação;
- empresas de fachada e interpostas pessoas;
- operadores logísticos e transporte;
- estruturas imobiliárias e cessão de espaço;
- negócios em espécie e meios de pagamento;
- prestação de bens, serviços, tecnologia, consultoria ou outras formas de suporte, inclusive por meio de terceiros ou de cadeias de fornecimento.

O regime **não exige vínculo com um ato terrorista específico nem intenção de promover terrorismo**, desde que esteja presente o conhecimento exigido pela norma.

Entre as consequências práticas estão:

- bloqueio e obrigação de comunicação de ativos ou fundos vinculados a essas organizações;
- aplicação de sanções a pessoas físicas e jurídicas que mantenham relações financeiras ou comerciais com os grupos;
- restrições a transações com pessoas ou entidades listadas;
- risco de confisco civil de ativos, independentemente de condenação penal;
- litígios perante tribunais americanos;
- punições mais severas para casos de apoio material, financiamento ou colaboração com as facções; e
- reflexos nas obrigações de divulgação ao mercado de transações com pessoas ou entidades bloqueadas para companhias abertas nos EUA.

Empresas sem sede nos EUA também podem ser alcançadas. As **sanções primárias se aplicam quando há jurisdição americana**, inclusive pelo uso do sistema financeiro dos EUA, por correspondentes bancários americanos, por operações em dólares que passem pelo sistema financeiro americano ou por participação de pessoas sujeitas à jurisdição americana. Já as **sanções secundárias podem atingir empresas não americanas**, mesmo sem operações diretas nos EUA, caso mantenham negócios relevantes com partes sancionadas.

O risco aumenta quando as operações ordinárias continuam apesar dos sinais de alerta. **Estar a uma ou duas etapas de distância de um ator de alto risco não é, por si só, suficiente para afastar a exposição.**

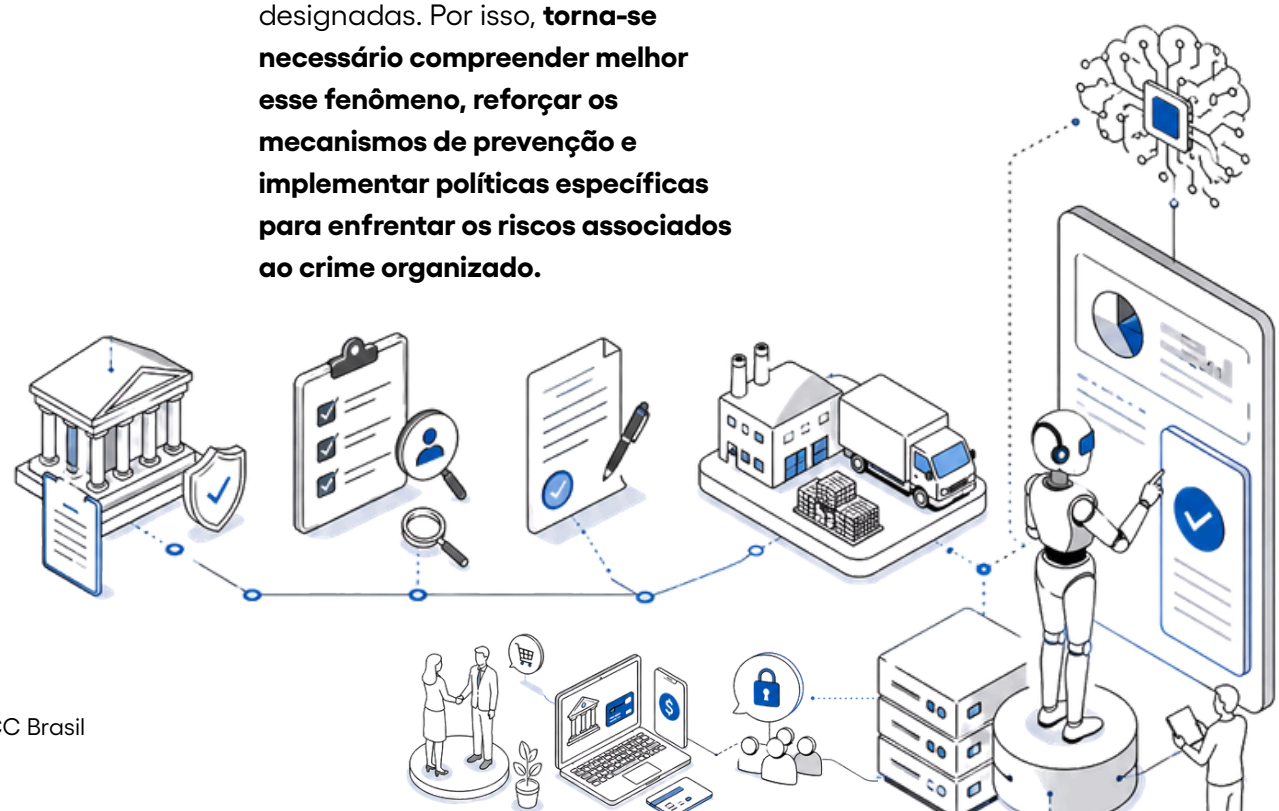
# 2 Recomendações Práticas para Empresas

Ao se tornar mais ousado e profissionalizado, o crime organizado deixou de se limitar à ocultação de recursos e passou a buscar infiltração em negócios formais. Estruturas societárias, veículos de investimento e empresas regulares podem ser utilizados como mecanismos de integração econômica. Como essas estratégias muitas vezes se apoiam em históricos empresariais aparentemente legítimos, sua detecção torna-se mais complexa.

Nesse contexto, elos da cadeia de valor de empresas podem estar diretamente ou indiretamente vinculados a organizações designadas. Por isso, **torna-se necessário compreender melhor esse fenômeno, reforçar os mecanismos de prevenção e implementar políticas específicas para enfrentar os riscos associados ao crime organizado.**

Diante desse novo cenário regulatório, as empresas devem **adotar uma resposta documentada e baseada em risco.** O objetivo não é demonstrar controle absoluto sobre todas as camadas do negócio, mas **evidenciar que os riscos foram identificados, avaliados e tratados de forma proporcional e tempestiva.**

As medidas a seguir devem ser consideradas para fortalecer a governança, a diligência sobre terceiros e clientes, os mecanismos de reporte, a segurança dos colaboradores e o uso de tecnologia na gestão de riscos.



## 2.1 Governança, Escalada e Responsabilidade dos Dirigentes

**A robustez da estrutura de governança constitui a primeira linha de controle da defesa corporativa.** A captura da alta liderança por interesses associados a estruturas criminosas raramente ocorre de forma explícita. Manifesta-se por meio de padrões mais sutis, que se aproveitam de fragilidades, como a aceitação de membros sem processo formal de seleção ou por indicação de terceiros; a concentração de decisões em comitês informais; a opacidade nos processos decisórios, com aprovações sem racional registrado; a ausência de registro dos debates que embasaram as decisões; e o uso de canais não institucionais para comunicações relevantes.

No mais, no exercício da atividade, **o sistema de governança deve ser capaz de demonstrar**:

- quando o risco foi identificado;
- quem foi informado;
- como a questão foi escalada;
- quais análises foram realizadas;
- quais medidas foram adotadas;
- por que determinada decisão foi tomada.

**A ausência desses fatores pode sustentar alegações de cegueira deliberada.** O conhecimento pode ser inferido das circunstâncias, especialmente quando havia sinais de alerta que a empresa deveria ter identificado.

## 2.2 Risco de Terceiros, Cadeia de Fornecimento e Clientes

A exposição a um FTO exige **análises aprofundadas e recorrentes** sobre como terceiros e clientes operam. Fornecedores, prestadores logísticos, intermediários, subcontratados e clientes **podem representar risco mesmo após triagens convencionais de compliance.**

A diligência deve considerar:

- estrutura societária e beneficiários finais;
- atuação em áreas de influência criminosa;
- uso de **subcontratados e intermediários**;
- rotas, instalações e regiões de maior risco;
- histórico operacional e conduta empresarial;
- volume, forma e frequência das **transações**;
- sinais de **pagamentos de proteção ou taxas de acesso**.

Os contratos devem prever obrigações claras de compliance, direitos de auditoria e dever de replicar padrões equivalentes nos níveis subsequentes da cadeia. Embora nem sempre seja viável monitorar cada subcontratado, a empresa deve exigir que seus contratados gerenciem esse risco de forma documentada.

A base de clientes deve ser avaliada com rigor semelhante ao aplicado aos fornecedores. Pagamentos em espécie, transações atípicas, estruturas incompatíveis com a capacidade econômica do cliente ou comportamentos fora do padrão devem acionar uma análise complementar.

Pagamentos de proteção e taxas de acesso a rotas não podem ser tratados como custos operacionais ordinários. A terceirização de transporte ou de operações locais não afasta a exposição quando a empresa transfere conscientemente o risco a terceiros.

## 2.3 Controles Internos, Canais de Reporte, Gestão de Crises e Segurança

A solidez do programa depende de controles internos desenhados para **reduzir a probabilidade de que pagamentos indevidos, contratações suspeitas ou desvios operacionais sejam executados sem detecção tempestiva.** Destacam-se:

- Plano de alçadas;
- Interfaces sistêmicas e segregação de funções;
- Revisão de lançamentos manuais;
- Gestão de acessos a sistemas críticos.

E, quando os controles preventivos não forem suficientes para evitar o contato com a situação de risco, os colaboradores e gestores locais devem saber que pagamentos indevidos, situações de coerção, taxas de acesso a rotas ou relações com agentes vinculados a organizações criminosas precisam ser imediatamente escalados.

Os canais de reporte devem permitir:

1. Recebimento seguro de relatos
2. Proteção de colaboradores
3. Preservação de evidências
4. Análise rápida da exposição
5. Definição de medidas de resposta
6. Eventual coordenação com autoridades

A resposta a casos envolvendo organizações criminosas é mais complexa do que em investigações tradicionais de corrupção. A interrupção abrupta de pagamentos ou contratos pode gerar ameaças, violência ou paralisação operacional. Por isso, **a resposta jurídica deve ser integrada à gestão de crise.**

**A proteção dos colaboradores é parte essencial da resposta corporativa.** Empresas que atuam em áreas remotas ou fronteiriças devem reforçar protocolos para funções mais expostas, segurança física de instalações, mapeamento de rotas críticas e mecanismos de coordenação com autoridades, quando pertinente.

Pagamentos de proteção que se consolidam como parte do modelo de negócios geram risco jurídico elevado. Uma posição defensável exige **ação imediata, redução documentada da exposição e plano estruturado de encerramento, com salvaguardas aos colaboradores envolvidos.**

## 2.4 Tecnologia e Alocação de Recursos

A tecnologia pode **fortalecer a gestão de riscos ao aprimorar o uso de dados internos e externos.** Ferramentas de inteligência artificial podem apoiar a identificação de alterações societárias, beneficiários finais de risco, vínculos com partes sancionadas, exposição geográfica, padrões atípicos de pagamento e conexões entre empresas aparentemente não relacionadas.

A IA também pode automatizar alertas e permitir o monitoramento contínuo, indo além da due diligence realizada apenas no onboarding ou em ciclos periódicos. Isso permite uma reação mais rápida diante de mudanças relevantes no perfil de risco de fornecedores, clientes ou intermediários.

A IA não substitui o julgamento humano. Seu papel é ajudar a priorizar investigações, direcionar diligências reforçadas e alocar recursos de forma mais eficiente.

A metodologia adotada deve ser documentada e compatível com o perfil de risco da organização.

Em cadeias extensas, a empresa **não precisa demonstrar controle absoluto sobre todas as camadas do negócio.** Deve, no entanto, ser capaz de explicar por que determinadas áreas receberam controles mais robustos, por que certos fornecedores ou clientes foram submetidos a diligência reforçada e por que determinada transação foi aprovada.

A resposta esperada é prática, proporcional e documentada. A empresa deve estar em condições de demonstrar que suas **escolhas foram baseadas em critérios claros e em uma avaliação realista dos riscos.**

# 3 Considerações finais

A designação do PCC e do CV como organizações terroristas estrangeiras exige que as **empresas reavaliem a forma como identificam, gerenciam e documentam sua exposição ao crime organizado.**

O tema deve ser tratado como **risco estratégico**, e não como uma rotina de compliance. Embora os arcabouços tradicionais permaneçam relevantes, podem não ser suficientes diante da sofisticação das organizações criminosas e da amplitude dos regimes de sanções e de apoio material. Uma resposta defensável exige **compreensão prática da operação, diligência proporcional ao risco, canais de reporte efetivos, preservação de evidências, envolvimento da alta administração e integração da segurança ao planejamento de compliance.**

Não se exige controle perfeito sobre todas as camadas da operação, mas a empresa deve demonstrar que adotou um processo razoável, documentado e baseado em risco. A prioridade é construir um **modelo de resposta viável às condições reais do negócio e robusto o suficiente para resistir a escrutínios futuros**, inclusive por meio de cooperação estruturada com autoridades, quando pertinente.

O setor privado brasileiro, especialmente o segmento financeiro, parte de uma base relevante de maturidade em compliance e gestão de riscos. Ainda assim, a nova exposição exige a atualização dos controles internos.

Este documento oferece referências iniciais para a compreensão e mitigação dos riscos associados ao novo cenário regulatório, em diálogo com instrumentos já disponíveis, como o **Guia para Empresas sobre Gestão de Riscos Associados a Organizações Criminosas**, publicado pela **ICC Brasil** em colaboração com a **Controladoria-Geral da União (CGU)**. Não substitui assessoramento jurídico ou regulatório especializado. As decisões empresariais devem priorizar a proteção de pessoas, de ativos, da integridade e da conformidade legal, especialmente em contextos de elevado risco ou de informações incompletas.

**Este documento foi elaborado por representantes da equipe executiva da ICC Brasil e Chantal Pillet, vice-chair da Comissão de Integridade e Responsabilidade Corporativa.**

**Representantes da Equipe Executiva da ICC Brasil:**

Gabriella Dorlhiac, Diretora Executiva

Paula Costim, Head de Policy

Guilherme Rabel, Analista Junior de Policy

Pedro Godoi, Estagiário de Policy

**Conheça a liderança da Comissão de Integridade e Responsabilidade Corporativa da ICC Brasil:**

Chair: José Alexandre Buaiz, Sócio de Pinheiro Neto Advogados

Vice-chair: Ana Paula Carracedo, Chief Compliance Officer na Aegea

Vice-chair: Chantal Pillet, Diretora na Kroll Associates

Vice-chair: Karina Martins, Regional Compliance Officer para a América do Sul na Schneider Electric



**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