UNIVERSIDADE NOVE DE JULHO (UNINOVE)

THIAGO MARQUES SALOMÃO

O MODELO DAS TRÊS LINHAS: UM SISTEMA EFICIENTE DE CONFORMIDADE PARA EMPRESAS

SÃO PAULO/SP

2025

THIAGO MARQUES SALOMÃO

O MODELO DAS TRÊS LINHAS: UM SISTEMA EFICIENTE DE CONFORMIDADE PARA EMPRESAS

Dissertação apresentada ao programa de pós-graduação *stricto sensu* em Direito da Universidade Nove de Julho (Uninove), como requisito parcial para a obtenção do título de Mestre em Direito.
Orientação: Professor Doutor Marcelo Costenaro Cavali.

SÃO PAULO/SP

2025

Salomão, Thiago Marques.
O modelo das três linhas: um sistema eficiente de conformidade para empresas. / Thiago Marques Salomão. 2025.
106 f.

Dissertação (Mestrado)- Universidade Nove de Julho - UNINOVE, São Paulo, 2025.
Orientador (a): Prof. Dr. Marcelo Costenaro Cavali.

1. Gestão de riscos. 2. Governança corporativa. 3. Compliance. 4. Modelo das três linhas. 5. Empresa.
I. Cavali, Marcelo Costenaro. II. Título

CDU 34

THIAGO MARQUES SALOMÃO

O MODELO DAS TRÊS LINHAS: UM SISTEMA EFICIENTE DE CONFORMIDADE PARA EMPRESAS

Dissertação apresentada ao Programa de Pós-Graduação Stricto Sensu em Direito da Universidade Nove de Julho como parte das exigências para a obtenção do título de Mestre em Direito.

São Paulo, 15 de dezembro de 2025.

BANCA EXAMINADORA

Marcelo Costenaro Cavali

Assinado de forma digital por Marcelo Costenaro Cavali
Dados: 2025.12.16 09:44:25 -03'00'

Prof. Dr. Marcelo Costenaro Cavali
Orientador
UNINOVE

Prof. Dr. Walter Godoy dos Santos Júnior
Examinador Interno
UNINOVE

Prof. Dr. Rodrigo de Grandis
Examinador Externo
FGV

AGRADECIMENTOS

A materialização desta pesquisa transcende o esforço individual; é fruto da colaboração, do afeto e do suporte de muitos que se fizeram presentes, direta ou indiretamente, ao longo desta jornada acadêmica.

Elevo meu pensamento a Deus, a quem sou grato pela força espiritual que sustentou minha serenidade e resiliência frente aos obstáculos, iluminando a trajetória até este momento.

Aos meus pais, ofereço este trabalho como tributo ao alicerce moral e afetivo que me proporcionaram. A confiança que sempre depositaram em mim foi o primeiro e mais importante incentivo à minha constituição intelectual.

À minha esposa, entrego gratidão perene pela paciência e companheirismo. Sua compreensão foi o sustentáculo que me permitiu o afinco necessário aos estudos; sua presença, o refúgio seguro nas incertezas.

À minha filha, inspiração maior e renovação do meu propósito de vida. Sua alegria dá sentido a todo esforço e reforça meu compromisso em construir um futuro digno e virtuoso.

Ao meu orientador, Professor Doutor Marcelo Costenaro Cavali, agradeço pela condução exemplar. O rigor acadêmico, somado à generosidade no meu acolhimento, no compartilhamento do saber e no incentivo à autonomia, foram determinantes para a qualidade desta investigação.

Aos colegas de pesquisa, agradeço o partilhar das angústias e das conquistas. A troca de saberes e a solidariedade mútua tornaram o árduo percurso acadêmico uma experiência de crescimento coletivo.

À Universidade Nove de Julho (UNINOVE), pelo suporte institucional e pelo ambiente propício à excelência acadêmica.

A todos que contribuíram para que este ciclo se encerrasse com êxito, registro meu sincero reconhecimento.

RESUMO

Compliance é um tema que atualmente está crescendo dentro das empresas e que deve ser visualizado por todas as áreas. A implantação do programa requer uma estrutura bem definida e a participação e apoio da alta direção. As primeiras providências permeiam o conhecimento dos objetivos, metas, princípios e visão da empresa. Trata-se de requisito primordial conhecer bem o negócio e entender a área de atuação. O foco de um programa de *compliance* também deve ser na prevenção e na melhoria contínua de processos. A importância da cultura de *compliance* contribui significativamente no processo de implementação e manutenção de um programa de *compliance* efetivo e eficiente, além de ajudar as empresas a minimizarem situações de desvio de conduta e reduzir o impacto dos eventuais problemas de *compliance*. Uma estrutura de *compliance* engloba vários componentes que contribuem na prevenção, detecção e resposta no Modelo das Três Linhas. Os responsáveis pelos processos de negócios formam a primeira linha; as funções de *compliance* e de gestão de riscos centralizada compõem a segunda linha; e a auditoria interna representa a terceira linha. Cada uma delas desempenha uma função importante na estrutura e governança de *compliance*. O Modelo das Três Linhas ajuda as empresas a promoverem a agilidade de *compliance*, identificar riscos emergentes e esclarecer os pontos fortes e fracos do programa.

Palavras chaves: Gestão de Riscos. Governança Corporativa. *Compliance*. Modelo das Três Linhas. Empresa.

ABSTRACT

Compliance is a topic that is currently growing within companies and that must be viewed by all areas. Implementation of the program requires a well-defined structure and the participation and support of senior management. The first steps involve understanding the company's objectives, goals, principles and vision. It is a fundamental requirement to know the business well and understand the area of operation. The focus of a compliance program is also on prevention and continuous improvement of processes. The importance of compliance culture contributes significantly to the process of implementing and maintaining an effective and efficient compliance program, in addition to helping companies minimize situations of misconduct and reduce the impact of potential compliance problems. A compliance framework encompasses several components that contribute to prevention, detection and response in the Three Lines Model. Those responsible for business processes form the front line; compliance and centralized risk management functions make up the second line of responsibility; and internal auditing represents the third line of reasoning. Each of them plays an important role in the structure and governance of compliance. The Three Lines Model helps companies promote compliance agility, identify emerging risks, and clarify the strengths and weaknesses of the program.

***Keywords**: Risk Management. Corporate Governance. Compliance. Three Lines Model. Company.*

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados.

B3 – Brasil, Bolsa, Balcão.

BC – Banco Central.

BIRD – Banco Internacional para Reconstrução e Desenvolvimento.

CADE – Conselho Administrativo de Defesa Econômica.

CAE – Chefe da Auditoria Interna.

CFATF – *Caribbean Financial Action Task Force*.

CCM – *Continuous Control Monitoring*.

CGU – Controladoria Geral da União.

CVM – Comissão de Valores Mobiliários.

DPA – *Deferred Prosecution Agreements*.

DPO – *Data Protection Officer*.

DOJ – *Department of Justice*.

ECIIA – *European Confederation of Institutes of Internal Auditing*.

EUA – Estados Unidos da América.

FATF – *Financial Action Task Force*.

FCPA – *Foreign Corrupt Protection Act*.

FDIC – *Federal Deposit Insurance Corporation*.

FEPA – *Foreign Extortion Prevention Act*.

FERMA – *Federation of Risk and Insurance Management Associations*.

FMI – Fundo Monetário Internacional.

GAFI – Grupo de Ação Financeira.

GDPR – Regulamento Geral de Proteção de Dados da União Europeia.

IBGC – Instituto Brasileiro de Governança Corporativa.

IA – Inteligência Artificial.

IIA – *The Institute of Internal Auditors*.

IPEA – Instituto de Pesquisa Econômica Aplicada.

ISO – *International Organization for Standardization*.

L1 – Primeira Linha.

L2 – Segunda Linha.

L3 – Terceira Linha.

LGPD – Lei Geral de Proteção de Dados.

M3L – Modelo das Três Linhas.

NPA – *Non-Prosecution Agreements.*

OCDE – Organização para a Cooperação e o Desenvolvimento Econômico.

OECE – Organização Europeia de Cooperação Econômica.

ONU – Organização das Nações Unidas.

RICO – *Racketeer Influenced and Corrupt Organizations Act*.

SBDC – Sistema Brasileiro de Defesa da Concorrência.

SEC – *Securities and Exchange Commission*.

SFO – *Serious Fraud Office*.

SOx – *Sarbanes-Oxley Act*.

SUSEP – Superintendência de Seguros Privados.

TCC – Termos de Compromisso de Cessação.

TCU – Tribunal de Contas da União.

TOC – Transnational Criminal Organizations.

UIFs – Unidades de Inteligência Financeira.

UKBA – *United Kingdom Bribery Act*.

VUCA – *Volatile, Uncertain, Complex, Ambiguous*.

SUMÁRIO

INTRODUÇÃO

A crescente complexidade do ambiente de negócios contemporâneo, marcada pela globalização e pela rápida evolução tecnológica, impõe às empresas desafios cada vez maiores relativos à gestão de riscos e à conformidade legal. Neste cenário, a adoção de mecanismos robustos de governança corporativa e *compliance* deixou de ser uma simples vantagem competitiva, para se tornar uma necessidade para sustentabilidade e reputação das sociedades.

O Modelo das Três Linhas, reconhecido e recomendado internacionalmente pelo *The Institute of Internal Auditors (IIA)*, desponta como uma resposta eficaz a essa demanda, fornecendo uma estrutura clara para a organização da gestão de riscos e do controle, ao estabelecer responsabilidades e promover uma sólida cultura de *compliance*. Ao permitir que as empresas gerenciem melhor seus riscos, aprimorem a governança e garantam a conformidade com regulamentações e melhores práticas, esse modelo se revela fundamental na busca por eficiência e integridade corporativa.

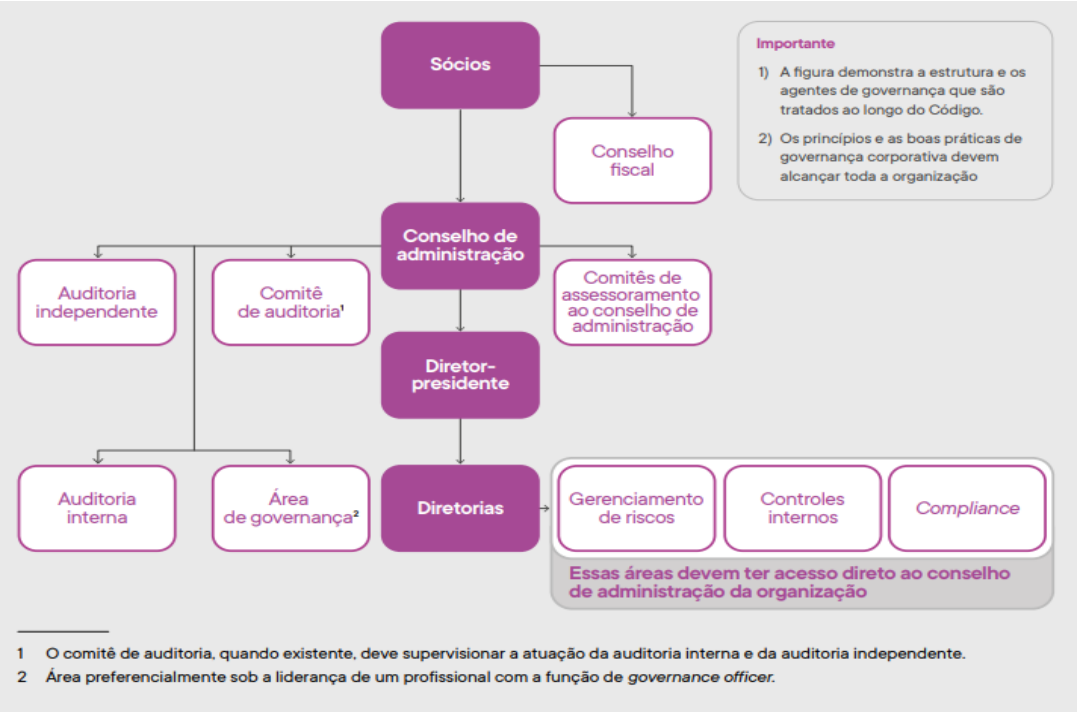
Governança Corporativa, Gestão de Riscos e *Compliance*

É cediço que a má conduta empresarial gera danos significativos à esfera negocial como um todo, pois a prática de infrações (em especial, corrupção e propina) tem como consectário legal a imposição de graves penalidades, gerando prejuízos financeiros, estruturais e reputacionais aos envolvidos. Desse modo, a governança corporativa, a gestão de riscos e o *compliance* surgiram como forma de reação às más condutas empresariais, com vistas a minimizar os riscos daí advindos e solidificar o alicerce para a perenidade e a criação de valor.

A base histórica que “preparou o solo” para o surgimento desses institutos se deu na primeira metade do século XX, marcada pela Primeira Guerra Mundial (com a ascensão dos Estados Unidos como a nova potência econômica e industrial), pela Segunda Guerra Mundial e ainda por profundas crises financeiras, enfraquecimento das moedas e pelo declínio do comércio entre os países. Só mais tarde, já na segunda metade do século XX, em meio a diversos casos de corrupção (dentre os quais se destaca o episódio que ficou conhecido como “Escândalo de *Watergate*”), é que as sementes outrora plantadas finalmente germinaram, nascendo assim a governança

corporativa, a gestão de riscos e o *compliance*, os quais foram sendo paulatinamente incorporados ao espectro empresarial.

Apesar da semelhança e complementaridade entre os institutos, eles possuem conceitos e objetivos diferentes. A governança estabelece a estrutura e diretrizes para a tomada de decisões e gestão da empresa, visando criação de valor e alinhamento com interesses das partes envolvidas. A gestão de riscos, por sua vez, concentra-se na identificação, avaliação e mitigação de riscos potenciais que podem impactar a organização. Já o *compliance* busca uma cultura de conformidade com as leis, os regulamentos e as normas internas, garantindo que a empresa opere em consonância com parâmetros legais e éticos, através de suas três vertentes: prevenção, detecção e resposta. A ilustração abaixo foi extraída do Código das Melhores Práticas de Governança Corporativa, do Instituto Brasileiro de Governança Corporativa (IBGC)[1], e traz a representação gráfica dos referidos institutos dentro do organograma empresarial:



Denota-se, pois, haver uma inter-relação crítica e inseparável entre esses três conceitos. Um programa de *compliance* robusto não é um fim em si mesmo, mas uma ferramenta essencial de governança e de gestão de riscos.

[1] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/24640/2023_C%c3%b3digo%20das%20Melhores%20Pr%c3%a1ticas%20de%20Governan%c3%a7a%20Corporativa_6a%20Edi%c3%a7%c3%a3o.pdf. Acesso em 17 mai. 2025.

Justificativa do Modelo das Três Linhas como Objeto Central

Com a governança corporativa, a gestão de riscos e o *compliance* alçados a setores estratégicos no ramo empresarial, vários formatos foram experimentados até que se chegasse ao atual conceito do Modelo das Três Linhas. Essa estrutura fornece um método simples e eficaz para melhorar a comunicação e o esclarecimento dos papéis e responsabilidades essenciais no gerenciamento de riscos e controles.

Este trabalho analisará em profundidade a aplicação e evolução desse modelo, explorando suas origens, críticas e sua atualização mais recente. O foco é demonstrar como essa estrutura se consolidou como um referencial para a construção de um programa de *compliance* eficiente, capaz de não apenas proteger a organização, mas também de contribuir para a criação de valor.

Logo, a pesquisa se justifica pela relevância do tema, pois o Direito Empresarial desempenha papel de destaque na regulamentação das atividades econômicas, e a crescente influência da globalização e da era digital está transformando, de modo cada vez mais rápido e profundo, o ambiente organizacional. Assim, compreender as implicações jurídicas e sociais dessas mudanças é crucial para o desenvolvimento das atividades empresariais, garantindo um ambiente de negócios ético e equitativo.

O trabalho também atende à necessidade de atualização do conhecimento jurídico, destacando a importância do *compliance* no contexto globalizado e digital. Além disso, oferece subsídios para a elaboração de estratégias empresariais que levem em consideração os desafios legais e sociais enfrentados pelas organizações, com vistas a torná-las mais eficientes, ao mesmo tempo em que reduzem os riscos.

A importância do Modelo das Três Linhas se dá na medida em que estrutura a gestão de riscos e a conformidade legal de forma clara e eficaz, estabelecendo responsabilidades e promovendo sólida cultura de *compliance*. Trata-se de um modelo reconhecido e recomendado internacionalmente pelo IIA, o qual permite que as empresas gerenciem melhor seus riscos, aprimorem a governança e garantam a conformidade com regulamentações e melhores práticas.

Portanto, ao integrar a teoria com a prática, este trabalho busca não apenas oferecer uma análise crítica do Modelo das Três Linhas, mas também contribuir para o avanço do campo do Direito Empresarial. Os *insights* valiosos que emergem desta pesquisa destinam-se a acadêmicos, profissionais do direito e também a empresários, fomentando discussão relevante e informada sobre a governança e a conformidade

legal no Brasil. Por fim, vale destacar que o estudo se posiciona como uma ferramenta de reflexão e aprimoramento, apta a auxiliar na construção de um ambiente de negócios mais ético e resiliente.

Problema, Hipóteses e Objetivos da Pesquisa

Apesar da ampla aceitação e da fundamentação teórica que o modelo oferece, sua efetividade prática ainda suscita importantes questionamentos. A presente pesquisa busca investigar se os programas de integridade são, de fato, efetivos naquilo que se propõem — combater fraudes e crises nas companhias — ou se, em alguns casos, constituem apenas "roteiros de fachada", desprovidos de aplicação substancial. Adicionalmente, examina-se se o Modelo das Três Linhas é uma solução ideal e universal, aplicável indistintamente a qualquer empresa, ou se, pelo contrário, necessita de adaptações e de um nível de customização conforme o porte, o setor de atuação e o nível de maturidade da companhia. A superação de tais indagações é crucial para aprimorar a implementação de práticas de compliance e garantir que elas gerem valor real para as organizações.

As questões ora levantadas evidenciam que discutir *compliance* é compreender a natureza e a dinâmica das más condutas nas relações organizacionais, de tal sorte que a conduta em conformidade com a regra (*compliance*) ou em desconformidade com ela (fraude, propina, corrupção) possuem várias causas e podem ser igualmente influenciadas pelas circunstâncias.

Com relação às hipóteses, considerando os problemas ora elencados, pode-se sustentar que, apenas quando bem estruturados e implementados, os programas de integridade se mostrariam efetivos no combate a fraudes e crises nas empresas, pois, neste caso, permitiriam prevenir, detectar e corrigir atos ilícitos, promovendo uma cultura de transparência e ética. No entanto, revela-se fundamental que o programa não seja apenas uma fachada, devendo ser parte integrante da gestão da empresa e contar com o apoio da alta direção (*tone at the top*) para que seja realmente eficaz. Pode-se ainda sustentar que o Modelo das Três Linhas não seria ideal para toda e qualquer empresa em igual medida, precisando ser adaptado ao tamanho, setor de atuação e nível de maturidade da organização para garantir sua eficácia.

Nesse sentido, o objetivo geral deste estudo é analisar a efetividade do *compliance* na redução de fraudes e riscos nas companhias, bem como avaliar a

relação custo-benefício da implementação de programas de integridade, haja vista as dificuldades de sua efetivação, em contraponto aos benefícios proporcionados.

Para tanto, a pesquisa se desdobra em objetivos específicos, que incluem: expor os conceitos de governança corporativa e de gestão de riscos, analisando os pontos que devem ser considerados para que eles sejam utilizados como ferramentas capazes de atrair investidores; investigar a importância do *compliance* para empresas em um ambiente globalizado e digitalizado; avaliar os desafios jurídicos e sociais enfrentados pelas organizações em suas relações internas e externas; propor recomendações para lidar com as demandas legais e sociais resultantes desse complexo cenário; e contribuir para a compreensão das implicações da globalização e da era digital no seio empresarial, visando à promoção de práticas mais éticas e eficazes nesse setor.

Metodologia e Estrutura do Trabalho

A presente pesquisa utilizará o método hipotético-dedutivo no exame acurado de balizada doutrina, da legislação e jurisprudência pertinentes, bem assim de dados estatísticos extraídos de fontes oficiais, traduzindo-se, pois, em um trabalho de caráter qualitativo. Vale mencionar que o caráter qualitativo se dará em função da revisão bibliográfica, a qual requer o cruzamento de todas as pesquisas que forem realizadas acerca da temática em questão.

A pesquisa de caráter qualitativo possui peculiar relevância em estudos que tenham foco no social, pois há perceptível aumento nas condicionantes acerca do que está sendo observado. Para compreender o tema proposto, o trabalho se pautará, em um primeiro momento, no delineamento da pesquisa, referente a seu planejamento, com vistas a abordar a sua dimensão mais ampla.

Nesse sentido, tal abordagem permite que se analise dados obtidos por meio de levantamento bibliográfico, sem que se tenha a necessidade de desenvolver uma profunda análise a respeito de cada um desses dados. Em relação a essa coleta de dados, será realizada uma pesquisa bibliográfica e documental, e posteriormente será efetivada uma triagem, na qual serão separados apenas o material que realmente contribua para a elaboração da pesquisa. Esse tipo de investigação busca trazer uma contribuição teórica à resolução de problemas técnicos, transformando o saber em saber-fazer, por isso as pesquisas bibliográficas e documentais.

A metodologia adotada nesta pesquisa, trata-se de uma revisão de literatura com base em livros, artigos científicos e revistas pertinentes à área escolhida para o trabalho, cuja finalidade será trazer padrões distintos que possam servir de exemplo e serem trabalhados nos *stakeholders*[2] jurídicos. Os artigos e revistas incluem *cases* (lições aprendidas) que fomentem as necessárias e relevantes ações das ferramentas do *compliance*, todas respaldadas nas literaturas dos livros científicos, para trazer um conceito histórico ao tema abordado.

As fontes de pesquisa serão criteriosamente selecionadas, abrangendo livros, artigos científicos, revistas e relatórios de instituições de referência. Para a revisão bibliográfica, serão utilizadas bases de dados como SciELO, JSTOR, *Google Scholar* e *Web of Science*. Na busca, serão empregados termos-chave em português e inglês, como: "Modelo das Três Linhas", "*The Three Lines Model*", "programas de integridade", "*compliance* corporativo", "gestão de riscos", "governança corporativa", "fraude empresarial" e "*due diligence*". Adicionalmente, serão consultadas plataformas de jurisprudência do Supremo Tribunal Federal (STF), do Superior Tribunal de Justiça (STJ) e de outros tribunais relevantes, além de portais de legislação, do Sistema de Bibliotecas Integradas e de órgãos reguladores como a Controladoria-Geral da União (CGU) e o Tribunal de Contas da União (TCU). Essa combinação de fontes teóricas, legais e práticas visa a garantir um exame acurado e completo do tema.

[2] Termo cunhado pelo filósofo *Robert Edward Freeman*, em 1983, podendo ser definido como “grupos e indivíduos que, de uma forma ou de outra, apresentam algum nível de interesse nos projetos, atividades e resultados de uma determinada organização”. Em uma tradução direta, seria algo parecido com todas as partes interessadas de uma empresa.

CAPÍTULO 1 – FUNDAMENTOS TEÓRICOS DE *COMPLIANCE*

1.1 – Evolução Histórica

É certo que o *compliance* surgiu como forma de reação às más condutas empresariais, com vistas a minimizar os riscos daí advindos. Nessa senda, a primeira metade do século XX foi marcada por diversos acontecimentos que criaram as condições necessárias para o surgimento do *compliance* – fato que efetivamente veio a ocorrer apenas na segunda metade daquele século.

Dentre os marcos históricos[3], merece destaque a ascensão dos Estados Unidos (berço do sistema de *compliance*) como nova potência financeira e industrial, em consequência da Primeira Guerra Mundial, quando o país funcionou como uma espécie de celeiro, abastecendo os países europeus. Nesse mesmo período, os Estados Unidos experimentaram um forte crescimento econômico, advindo da compra e venda de ações na bolsa de valores, em que empresas e cidadãos investiam alto na compra de títulos, almejando retornos financeiros.

Porém, com o fim da Primeira Guerra Mundial, a Europa retomou sua produção alimentícia e industrial e os países se fecharam em seus mercados internos, para se fortalecerem e amenizarem os efeitos negativos da guerra. Para conter a “Grande Depressão” e evitar o colapso do sistema, tornou-se essencial recuperar a economia e restaurar a confiança no mercado de capitais. Nesse intento, entre 1933 e 1939, os Estados Unidos implementaram o *New Deal*[4] que, na seara financeira, impôs medidas drásticas como o fechamento temporário de bancos (para avaliação e reestruturação) e a regulação do mercado de valores mobiliários.

Na sequência, foi promulgada a Lei de Valores Mobiliários (*Securities Act* - 1933), cujo propósito foi aumentar a confiança no mercado de capitais, por meio da exigência de divulgação uniforme de informações sobre ofertas de títulos públicos (as empresas deveriam informar ao público sobre seus negócios, títulos que estavam

[3] Os fatos históricos mencionados neste capítulo foram extraídos das obras de Marcos Assi (Gestão de *compliance* e seus desafios: como implementar controles internos, superar dificuldades e manter a eficiência nos negócios. São Paulo. Saint Paul Editora, 2013. p.19-29) e Vanessa Alessi Manzi (Compliance no Brasil: consolidação e perspectivas. São Paulo. Saint Paul Editora, 2013. p.27-34).

[4] De acordo com Boris Fausto, tratou-se de intervenção estatal em meio à crise, consistente em um conjunto de reformas e programas governamentais nos mais variados setores (como agricultura, finanças, indústria e segurança social), com o objetivo de combater o desemprego, auxiliar os desempregados, reativar a economia e regulamentar o âmbito financeiro.

vendendo e os riscos envolvidos no investimento, colocando em primeiro plano os interesses dos investidores). Ainda em 1933, foi criada a *Federal Deposit Insurance Corporation* (FDIC - agência independente do governo dos Estados Unidos), cuja principal função era fornecer seguro de depósito para os depositantes de bancos comerciais e caixas de poupança, protegendo-os em caso de falência bancária.

Já em 1934, foi criada a agência reguladora *U.S. Securities and Exchange Commission* (SEC - equivalente à Comissão de Valores Mobiliários brasileira), a qual passou a regular o mercado de ações, com vistas a prevenir fraudes e manipulação.

Na prática, o *New Deal* representou um rompimento com os princípios do liberalismo clássico, marcando o surgimento da política econômica conhecida como *Welfare State*[5], inspirada nos ensinamentos do economista britânico John Maynard Keynes. Nessa esteira, em 1940, foram criadas as leis *Investment Advisers Act* (trazia princípios e restrições específicas) e *Investment Company Act* (estatuto primário que regulava os fundos), quando os Estados Unidos passaram a exigir que profissionais e empresas que oferecessem consultoria em investimentos tivessem registro na SEC.

Outro fato histórico digno de nota, dada a contribuição essencial ao surgimento do *compliance*, foi a Segunda Guerra Mundial (1939-1945). Afora as consequências nefastas próprias das guerras (estima-se cerca de 80 milhões de mortos – ou seja, aproximadamente 3% da população mundial em 1940), esse período foi marcado por acentuada desvalorização das moedas e declínio do comércio entre países.

Dessa vez, a busca pela reestabilização do sistema monetário internacional se deu por meio da Conferência de *Bretton Woods*[6], realizada em 1944. Nesse mesmo ano, foi criado o Banco Internacional para Reconstrução e Desenvolvimento (BIRD), para financiar projetos de reconstrução na Europa e de desenvolvimento em países emergentes. Em 1945, foi fundada a Organização das Nações Unidas (ONU) e criado o Fundo Monetário Internacional (FMI), para monitorar as taxas de câmbio, fornecer assistência financeira a países em dificuldades e promover cooperação monetária internacional. Por fim, definiu-se o sistema de taxas de câmbio fixas entre as moedas, designando-se o dólar americano como moeda de referência, lastreado em ouro.

---

[5] Boris Fausto o conceitua como sistema que busca garantir o bem-estar social dos cidadãos (incluindo saúde, educação, habitação e seguridade social), por meio da intervenção estatal, com o objetivo de reduzir desigualdades e promover um padrão de vida digno para todos.

[6] Segundo Carlos Cozendey, o objetivo primordial da conferência foi criar um sistema que promovesse a estabilidade, cooperação e o desenvolvimento econômico global (por meio da regulação do sistema monetário e financeiro mundial, com vistas a evitar a instabilidade econômica da década de 1930), bem como ajudar a reconstruir a Europa (então devastada por duas guerras).

Após a Segunda Guerra Mundial, os Estados Unidos experimentaram um novo ciclo de crescimento econômico, movido por inúmeros fatores, como o início da Guerra Fria, a implementação do Plano *Marshall*, a corrida armamentista e espacial, a rápida retomada do desenvolvimento industrial e tecnológico, sustentada por um expressivo aumento demográfico e, por consequência, pelo aumento do consumo.

Assim, com as condições propícias, a partir da década de 1960, o *compliance* finalmente se desenvolveu, alçando posição semelhante à auditoria interna dentro do ramo empresarial. Segundo Carvalho[7], o instituto surgiu nos Estados Unidos, por estratégia das próprias corporações, consolidando-se pela conjugação de interesses do meio empresarial com interesses das autoridades públicas, quando as empresas organizaram políticas de conformidade às normas antitrustes. Vale ressaltar que um fator decisivo desse desenvolvimento foi a exigência da SEC para a contratação de *compliance officers*[8], os quais, de acordo com Bragato[9], eram encarregados de criar procedimentos internos de controle, realizar o treinamento de pessoal, bem como monitorar e supervisionar atividades suspeitas.

Entretanto, com os gastos elevados[10], os Estados Unidos começaram a imprimir dinheiro, sem que o dólar americano, no entanto, tivesse o devido lastro em ouro, conforme fora pactuado na Conferência de *Bretton Woods*. A consequência foi o aumento vertiginoso da inflação, na década de 1970. Nesse período, também surgia outro grave problema: a entrada de dinheiro sujo na economia – cuja prática dava suporte para o crescimento de máfias, grupos terroristas e narcotraficantes.

Além disso, a década de 1970, foi marcada por vários episódios de corrupção e subornos internacionais, praticados por empresas multinacionais norte-americanas, como a *Exxon*, a *Northrop*, a *Gulf Oil*, a *Mobil Oil* e a *Lockheed Aircraft Corporation*[11].

---

[7] CARVALHO, Victor Aguiar de. **Corrupção Empresarial e Administração Pública. Diagnóstico e Estratégias de Enfrentamento**. Belo Horizonte: Fórum, 2022.

[8] Profissionais responsáveis por garantir que a organização opere conforme as leis, regulamentos e as políticas internas aplicáveis, ou seja, são "guardiões" da conformidade da empresa.

[9] BRAGATO, Adelita Aparecida Podadera Bechelani. **O compliance no Brasil:** a empresa entre a ética e o lucro. 2017. Dissertação (Mestrado em Direito) – Universidade Nove de Julho, São Paulo, 2017.

[10] À época, os Estados Unidos mantinham a política econômica do *Welfare State* (que prevalecia desde o *New Deal*), implementaram a expansão armamentista e espacial e ainda passaram a financiar guerras externas (a exemplo da Guerra da Coréia – 1950 a 1953 – e do Vietnã – 1955 a 1975), fatores que cobraram um alto preço da economia norte-americana.

[11] Segundo Spalding, em 1971, o Congresso forneceu à Lockheed Corporation (grande fabricante de aeronaves civis e militares) garantia de empréstimo federal de US$ 250 milhões para evitar a falência. Logo depois, reguladores descobriram que a Lockheed havia subornado vários governos estrangeiros para obter contratos. Em 1976, após investigação do Senado americano, a Lockheed revelou subornos da ordem de US$ 22 milhões de dólares a oficiais estrangeiros de diversos países, particularmente Holanda, Japão e Itália, o que gerou escândalos embaraçosos tanto para esses países quanto para os

Em 1972, ocorreu o caso de maior repercussão, que ficou conhecido como 'Escândalo de *Watergate*'[12]. Diante desta conjuntura, a credibilidade do mercado norte-americano mais uma vez precisava ser restaurada, com providências globais forjadas para combater a corrupção no ambiente empresarial.

Neste intento, Richard Nixon implementou uma série de medidas, dentre as quais se destacam: 1) a aprovação, em 1970, da *Racketeer Influenced and Corrupt Organizations Act* (RICO – Lei de Organizações Influentes e Corruptas – que previa penas de até 20 anos de prisão, multas e confisco de qualquer propriedade, negócio ou dinheiro oriundos destes atos); 2) a declaração de "guerra às drogas", durante uma coletiva de imprensa, em 1971, expandindo a presença de agências federais de controle de entorpecentes pelo país, com adoção de ações drásticas[13]; e 3) imposição de providências econômicas conhecidas por '*Choque Nixon*', em 1971, suspendendo a conversibilidade do dólar em ouro, o que implicou o fim do sistema de *Bretton Woods* (abrindo caminho para um regime de taxas de câmbio flutuantes) e congelou preços e salários (visando combater a inflação e a pressão sobre o dólar).

Outrossim, em um esforço internacional para fazer frente aos graves casos de corrupção, os bancos centrais dos países membros do G-10 criaram, em 1974, na Suíça, o Comitê de Basileia para Supervisão Bancária[14]. Com isso, o sistema financeiro foi fortalecido, pois passou a adotar maior conceituação sistemática de suas atividades, aplicar padrões de boas práticas financeiras e utilizar procedimentos de prudência em sua atuação.

Ainda como parte das medidas anticorrupção, em 1977, os Estados Unidos promulgaram a primeira legislação específica para lidar com o tema, intitulada *Foreign*

Estados Unidos. (SPALDING, Andrew Brady. The Irony of International Business Law: U.S. Progressivism, China's New Laissez Faire, and Their Impact in the Developing World (March 25, 2011). **UCLA Law Review**, Vol. 59, 2011. p. 19. Disponível em SSRN: http://dx.doi.org/10.2139/ssrn.1795563 ou https://ssrn.com/abstract=1795563. Acesso em: 03 mai. 2025).

[12] Tratou-se de um escândalo de espionagem, ocorrido em 1972, contra o comitê nacional do partido Democrata (partido rival ao do então presidente Nixon – Republicanos), em que houve uma tentativa de grampear seus telefones, no complexo *Watergate*, em Washington. As investigações revelaram o conhecimento do presidente Nixon sobre as operações ilegais, bem como suas tentativas de atrapalhar as investigações, culminando com sua renúncia da presidência, em 1974.

[13] Essa política de "guerra às drogas", anos depois, iria refletir nos países-membros da ONU no combate à lavagem de dinheiro, repercutindo de modo especial nas políticas de *compliance*.

[14] Criado em 1974, pelo Grupo dos Dez (G10 - organização internacional que reúne onze economias desenvolvidas), o Comitê de Supervisão Bancária da Basileia era composto por autoridades de supervisão bancária e bancos centrais da Alemanha, Bélgica, Canadá, Estados Unidos, França, Itália, Holanda, Japão, Reino Unido, Suécia e Suíça. Atualmente, o Comitê é composto por 45 membros de 28 jurisdições, incluindo bancos centrais e autoridades de supervisão bancária, além de oito observadores de outros organismos internacionais. (Informações disponíveis em: https://www.bcb.gov.br/estabilidadefinanceira/recomendacoesbasileia. Acesso em 22 fev. 2025).

Corrupt Protection Act (FCPA). De acordo com Hess[15], a referida lei deu novo impulso à organização de sistemas de *compliance*, desta vez com o escopo anticorrupção. Além de proibir e punir a prática de subornos a oficiais e a funcionários públicos estrangeiros por cidadãos e empresas norte-americanas para obter ou manter negócios, o FCPA também passou a exigir a organização de controles e registros de contabilidade internos, visando manter a transparência das operações e evitar que os malabarismos contábeis escondessem pagamentos a agentes corruptos[16]. Sistemas de gestão semelhantes aos modernos programa de *compliance* foram estruturados em razão do dever de conformidade a tais novos comandos de contabilidade.

O FCPA reforçou o poder do Departamento de Justiça (DOJ) e da SEC dos Estados Unidos, para processarem pessoas jurídicas de capital aberto, de qualquer nacionalidade, registradas na SEC e que tivessem ações nas bolsas de valores norte-americanas. Desse modo, o DOJ e a SEC passaram a dispor de autoridade legal e instrumentos para investigar e punir a corrupção transnacional. A referida lei conferiu responsabilidades de fiscalização e execução legal (*enforcement*) ao DOJ e à SEC, dividindo a competência da seguinte forma: cabe DOJ agir em casos de violações das disposições antissuborno e contábeis praticadas por qualquer pessoa ou entidade, aplicando penas criminais; já a SEC possui competência cível, agindo igualmente em casos de violações de disposições antissuborno e contábeis praticadas por empresas listadas em bolsas dos EUA (emissores), mas aplicando sanções de natureza civil.

Ademais, a lei ainda introduziu o *The 10 Hallmarks of an Effective Compliance Program*[17], que serviu de base para o modelo da *U.S. Sentencing Guidelines*[18].

---

[15] HESS, David. Ethical infrastructures and evidence-based corporate compliance and ethics programs: policy implications from the empirical evidence. **New York University Journal of Law & Business**, v.12, n. 2, p. 325, 2016. Disponível em: https://www.nyujlb.org/12-2. Acesso em 03 mai. 2025.

[16] Por conta dos escândalos precedentes de abrangência internacional, anos depois o FCPA se tornou fonte de inspiração para a criação de convenções internacionais para o combate à corrupção.

[17] Em tradução livre, significa 10 características de um programa de *compliance* eficaz. Tratam-se de princípios que visam a garantir que um programa de conformidade seja bem-sucedido, ajudando a organização a evitar riscos legais e financeiros, a fortalecer a sua reputação e a promover uma cultura de ética e integridade, podendo ser assim sintetizados: 1. Comunicação e Treinamento; 2. Código de Conduta e Políticas de *Compliance*; 3. Supervisão e Autonomia; 4. Avaliação de Riscos; 5. Canais de Denúncia; 6. Monitoramento e Investigação; 7. Responsabilidade; 8. Incentivos e Penalidades; 9. Diligência Prévia; e 10. Adaptação e Melhoria Contínua.

[18] Em tradução livre, significa diretrizes federais de sentenças dos Estados Unidos. Trata-se de um conjunto de regras e políticas criadas pela Comissão de Sentenças dos Estados Unidos (*U.S. Sentencing Commission*), para fornecer uma base uniforme para a determinação de sentenças em casos criminais federais. Elas visam reduzir a disparidade nas sentenças e garantir que indivíduos condenados por crimes semelhantes recebam punições comparáveis, levando em conta tanto a gravidade do crime quanto o histórico criminal do infrator. Tais diretrizes são usadas pelos juízes como guia, mas não são vinculativas, permitindo que eles se desviem delas em casos específicos, mormente quando a sua aplicação se mostre excessivamente dura ou injusta.

Assim, com a promulgação do FCPA, o *compliance* passou a ganhar peso geopolítico, especialmente após o lançamento de programa de *disclosure*[19] pela SEC, no qual oferecia anistia para empresas que assumissem pagamentos indevidos a funcionários públicos no exterior, desde que (dentre outras exigências) as companhias se comprometessem a adotar medidas internas de *compliance*.

Já na década de 1980, os Estados Unidos iniciaram uma ofensiva contra a lavagem de capitais, tornando-a crime federal. De acordo com Mendroni[20], a ação ganhou força internacional na convenção da ONU de 1988, em Viena, estruturando medidas abrangentes contra o tráfico internacional de drogas, incluindo métodos contra a lavagem de dinheiro. Já em 1989, na reunião do G7, em Paris, foi criado o Grupo de Ação Financeira Internacional (GAFI), organismo intergovernamental cujo objetivo era desenvolver e promover políticas para combater lavagem de dinheiro e financiamento do terrorismo. Outro fator decisivo para a expansão do enfrentamento à lavagem de capitais foi o documento produzido em 1988 pelo Comitê de Supervisão Bancária da Basileia, intitulado “Prevenção da Utilização Criminosa do Sistema Bancário para Fins de Branqueamento de Capitais”, que trouxe diretrizes ao sistema financeiro internacional para impedir e prevenir a utilização de instituições financeiras nos atos de lavagem de dinheiro.

Todas essas ações contribuíram para o desenvolvimento do *compliance*, pois exigia das empresas (e mais tarde de instituições financeiras) adoção de mecanismos de integridade, com vistas à prevenção da novel prática criminosa.

Apesar da guerra declarada à lavagem de dinheiro, a década seguinte (1990) foi marcada pela expansão desse delito, que passou a adotar diferentes formatos, exigindo alterações nas leis internas dos países que se comprometiam a combatê-la. De igual modo, o *compliance* também se expandiu, influenciando gradualmente outros setores além do financeiro, haja vista necessidades comerciais e de competitividade.

O período foi marcado por diversos esforços internacionais no enfrentamento à lavagem de dinheiro (com o consequente fortalecimento dos sistemas de *compliance*), dentre os quais se destacam: 1) a publicação pelo GAFI (Grupo de Ação Financeira

[19] Na ocasião, centenas de companhias (entre elas as 100 maiores do mundo) confessaram ter pago propinas. A partir daí, os Estados Unidos pressionaram os países membros da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) para que também adotassem procedimentos similares, com vistas a coibir o pagamento de propinas em transações comerciais internacionais.
[20] MENDRONI, Marcelo Batlouni. **Lavagem de dinheiro:** prevenção e repressão. 6. ed. São Paulo: Atlas, 2021.

Internacional), em 1990, de uma lista com 40 recomendações sobre o tema[21]; 2) a criação do CFATF (*Caribbean Financial Action Task Force*), para atuar nos paraísos fiscais do Caribe; 3) a exigência do Conselho da Europa para que seus signatários criminalizassem a prática da lavagem de capitais, inclusive com a imposição de embargos e confisco, a partir de 1993; 4) a criação pelas unidades de inteligência financeira de vários países do *Egmont Group of Financial Intelligence Units*[22], em 1995, em Bruxelas; 5) a realização pela OCDE, em 1997, em Paris, da Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, na qual os países signatários se comprometeram adotar medidas anticorrupção, inclusive de *self compliance* pelas empresas; 6) a elaboração pelo Comitê de Basileia do *Core Principles for Effective Banking Supervision*[23], em 1997, apontando princípios universais no fortalecimento do sistema financeiro - esta foi a primeira vez que o termo *compliance* fora citado de forma expressa pela entidade.

Dos anos 2000 em diante, as políticas de integridade passaram a ter a sua conotação atual. Esse período foi caracterizado por vários escândalos de corrupção internacional, bem como pela grave crise financeira dos anos de 2007 e 2008, fatos que colocaram novamente os Estados Unidos em destaque mundial[24].

O acontecimento considerado ponto de inflexão para o *compliance* nos tempos modernos foram os ataques terroristas ao *World Trade Center*, em Nova York, no dia 11 de setembro de 2001. Como reação imediata ao atentado, os Estados Unidos aprovaram o *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (*USA Patriot Act*)[25].

---

[21] Conforme atualizado em junho de 2025. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Feburary%202025%20FATF%20Recommendations.pdf. Acesso em: 5 out. 2025.

[22] Trata-se de organização internacional essencial no combate aos crimes financeiros e ao terrorismo, que atua como um fórum de cooperação e intercâmbio de informações entre as UIFs (Unidades de Inteligência Financeira), promovendo a segurança do sistema financeiro e a proteção da sociedade.

[23] BANCO DE COMPENSAÇÕES INTERNACIONAIS. Comitê de Supervisão Bancária da Basileia. **Sound management of risks related to money laundering and financing of terrorism**. Basel: Bank for International Settlements, July 2020. Disponível em: https://www.bis.org/bcbs/publ/d573.pdf. Acesso em: 22 fev. 2025.

[24] Os 10 maiores casos de corrupção dos Estados Unidos, nos últimos vinte e cinco anos, foram listados pela Revista Forbes. Disponível em: https://forbes.com.br/sem-categoria/2015/09/10-maiores-fraudes-da-historia-recente-dos-estados-unidos/#foto1. Acesso em 15 mai. 2025.

[25] Lei federal dos Estados Unidos, aprovada em 2001, para aprimorar medidas de segurança nacional e combate ao terrorismo, após os ataques de 11 de setembro. Em suma, a lei ampliou os poderes de vigilância e investigação das agências de segurança, permitindo, por exemplo, grampo telefônico, monitoramento de e-mails e acesso a dados de clientes de instituições financeiras, ainda que sem uma ordem judicial em determinadas situações. No sistema bancário, impôs uma série de restrições e medidas de segurança para combater a lavagem de dinheiro.

Outrossim, em 2002, foi também promulgada a *Sarbanes-Oxley Act* (SOx), após a qual os programas de integridade passaram a ser obrigatórios (*mandatory compliance*), ostentando um caráter mais rigoroso e punitivo.

Segundo Carneiro e Santos Júnior[26], a SOx foi editada após vários escândalos financeiros envolvendo empresas como Enron e WorldCom (que tinham práticas contábeis fraudulentas e inflavam artificialmente seus resultados), com o objetivo de estabilizar o mercado e recuperar sua credibilidade, evitando o esvaziamento dos investimentos financeiros e a fuga de investidores causada pela aparente insegurança a respeito da governança adequada das empresas. A SOx fixou regras mais severas para práticas de auditoria e governança corporativa, alcançando pessoas jurídicas americanas ou que possuam valores mobiliários inscritos no mercado de capital dos Estados Unidos. Isso aumentou a transparência, a responsabilidade e a integridade nas práticas contábeis de auditorias internas e externas. Além disso, a lei exigia que diretores executivos e financeiros certificassem a precisão das demonstrações financeiras, assumindo responsabilidade pessoal pela veracidade das informações.

Outra lei norte-americana relevante foi a *Dodd-Frank Wall Street Reform and Consumer Protection Act*, promulgada no ano de 2010, como resposta à grave crise financeira de 2008[27]. Conforme lição de Carneiro e Santos Júnior[28], a referida norma passou a regular o mercado de ações e bancário dos Estados Unidos, modificando atos normativos do mercado aberto norte-americano e afetando agências reguladoras financeiras federais, bem como a indústria de serviços financeiros do país, com vistas a evitar riscos à economia e assegurar a efetiva proteção dos consumidores. A lei teve ainda o mérito de propagar a prática de delações acerca de condutas ilegais, pois possibilitou aos denunciantes (*whistleblowers*) receberem recompensas entre 10 a 30% do montante das sanções impostas e exigidas dos infratores.

Superada a noção histórica do *compliance*, é possível passar à análise dos conceitos e definições que alguns autores trazem sobre o instituto.

---

[26] CARNEIRO, Claudio; SANTOS JUNIOR, Milton de Castro. **Compliance e Boa Governança**. Curitiba: Juruá, 2018, p. 40.

[27] Tratou-se de grave crise financeira, originada no mercado imobiliário dos EUA, impulsionada por empréstimos hipotecários de alto risco (*subprime*). O *default* massivo de hipotecas acarretou perdas enormes para os bancos, levando à falência do banco Lehman Brothers, em setembro de 2008, bem como ao colapso das bolsas mundiais. A crise gerou recessão global, queda na produção, aumento do desemprego e instabilidade econômica.

[28] CARNEIRO; SANTOS JUNIOR, ref. 26, p. 41.

1.2 – Conceito

Afinal, o que é *compliance*? Etimologicamente, a expressão tem raízes no latim *complere*, que transmite a ideia de preencher totalmente, tornar algo completo, ou de um objetivo que é atingido por completo. O termo foi primeiro utilizado pelos norte-americanos, derivando do verbo *to comply* – significa cumprir, estar em conformidade, executar ou responder a um comando, seja de cunho normativo ou não.

Sob tal enfoque, Blok[29] defende que o referido verbo requer um complemento. A autora questiona com o que exatamente as instituições devem estar em conformidade. E ela mesmo responde: com o dever de cumprir e fazer cumprir regulamentos internos e externos impostos às atividades da instituição.

Já para Carvalho[30], essa conotação traduz mero anglicismo, pois a língua portuguesa dispõe de verbos e substantivos que podem ser empregados em idênticas situações, sem qualquer perda de conteúdo semântico, a exemplo da palavra "conformidade". Assim, ele sugere que o melhor uso do vocábulo se refere ao que seria em verdade um programa, sistema ou política de *compliance*.

Nesse sentido, o conceito de *compliance* transcende a simples obediência às normas. Conforme Carneiro e Santos Júnior[31], os chamados programas de integridade expressam a ideia de *compliance* e consistem em políticas e procedimentos destinados a prevenir, detectar e corrigir violações de leis, regulamentos e políticas da empresa, desenvolvendo, desse modo, uma verdadeira cultura de ética, honestidade e de prevenção de atividades ilícitas.

Para Marcos Assi[32], o *compliance* se caracteriza como um sistema de controle interno que permite esclarecer e proporcionar maior segurança contábil e jurídica, prevenindo a empresa da execução de operações ilegais, o que é feito a partir de uma perspectiva de controle de comportamento organizacional. Logo, o objetivo central do programa de integridade é mitigar riscos dos negócios desenvolvidos, pela adoção de um sistema de controle interno, atento às normas que a empresa deve observar.

---

[29] BLOK, Marcella. **Compliance e governança corporativa**. 4. ed. *[S.l.]*: Freitas Bastos, 2023. *E-book*.
[30] CARVALHO, ref. 7, p. 215.
[31] CARNEIRO; SANTOS JUNIOR, ref. 26, p. 56.
[32] ASSI, Marcos. **Governança, riscos e compliance:** mudando a conduta nos negócios. São Paulo: Saint Paul Editora, 2017. *E-book*. ISBN 9788580041279. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788580041279. Acesso em 26 set. 2024.

E é sob esta perspectiva que a legislação pátria trata o tema, por meio do Decreto n.º 11.129/2022[33], que regulamenta a Lei n.º 12.846/2013. De igual maneira e sob o mesmo ângulo, o Instituto Brasileiro de Governança Corporativa (IBGC)[34] também conceitua o vocábulo.

Em uma acepção ampla, o termo pode ser compreendido como prevenção de riscos de responsabilidade empresarial, em face do descumprimento de regulações legais[35]. Sob esse prisma, os mecanismos de *compliance* são cruciais na prevenção e detecção de atos lesivos, incluindo consequências para conveniência da persecução penal, bem como para mitigar eventuais sanções a serem aplicadas.

No ponto, Marcella Blok[36] destaca que, para um programa de *compliance* ser eficaz, a alta administração precisa estar comprometida e enraizar essa mentalidade na cultura da empresa. A autora enfatiza que a responsabilidade não é exclusiva de um departamento, mas sim de todos os funcionários. Além disso, afirma que, embora um programa de *compliance* não garanta que a empresa esteja imune a crises, ele contribui significativamente para o aprimoramento dos controles internos e para uma gestão de riscos mais eficiente.

A partir dessa visão mais abrangente do sistema de integridade, denota-se que o instituto se aplica aos mais variados ramos empresariais, os quais estão expostos a diversos riscos regulatórios, próprios às respectivas atividades. Desse modo, nessas políticas de governança empresarial, criam-se regulamentações jurídicas específicas,

---

[33] Art. 56. Para fins do disposto neste Decreto, programa de integridade consiste, no âmbito de uma pessoa jurídica, no 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:
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.
Parágrafo único. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e os riscos atuais das atividades de cada pessoa jurídica, a qual, por sua vez, deve garantir o constante aprimoramento e a adaptação do referido programa, visando garantir sua efetividade.

[34] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, ref. 1.
"Com vistas a materializar o princípio da integridade, o *compliance* é a busca permanente de coerência entre aquilo que se espera de uma organização – respeito a regras, propósito, valores e princípios que constituem sua identidade – e o que ela, de fato, pratica no dia a dia.
O programa de *compliance* de uma organização deve abranger um conjunto de mecanismos e procedimentos, políticas, diretrizes, código de conduta, canal de denúncias e demais instrumentos com o objetivo de prevenir, detectar e sanar desvios de conduta, fraudes, atos de corrupção, lavagem de dinheiro, atos ilícitos praticados contra a administração pública, dentre outras questões. Além disso, deve alinhar a atuação de todos na organização com os princípios, valores e propósito dela e promover uma cultura de integridade".

[35] BACIGALUPO, Enrique. **Compliance y Derecho Penal**. Pamplona, Thomson Reuters, 2011, p. 22.

[36] BLOK, ref. 29.

não prosperando a ideia de que exista apenas um único modelo considerado correto para ser adotado como padrão em sistemas de conformidade. Logo, tem-se que os programas de *compliance* devem ser formatados de acordo com a realidade de cada organização, considerando o tamanho, o setor e o nível de maturidade da companhia.

Em geral, a doutrina[37] também conceitua *compliance* segundo uma análise de suas dimensões ou vertentes, a saber: prevenção, detecção e resposta. Sob tal ótica, a prevenção visa evitar a prática de atos ilícitos, como corrupção, propina, fraudes e outros desvios. Aqui, inclui-se a definição de princípios e valores, criação de códigos de conduta, implementação de controles internos, comunicação e treinamento dos colaboradores. Já a detecção busca identificar possíveis irregularidades ou atos de descumprimento, mediante a estruturação de canais de denúncia, monitoramento de processos, realização de auditorias e avaliação de riscos. Por fim, a resposta objetiva reparar irregularidades detectadas, adotar medidas disciplinares, implementar ações corretivas e garantir a aplicação de sanções adequadas, promovendo uma melhoria contínua do programa de integridade.

Porém, na glosa de Carvalho[38], as funções de um programa de *compliance* eficaz podem ser melhor compreendidas ao se expandir a dimensão de "resposta", para incluir a autodenúncia e o contínuo aprimoramento. Nesse sentido, o autor argumenta que um programa de *compliance* ideal possui cinco dimensões principais, que abrangem as três atividades de autorregulação que o Poder Público deseja estimular, somadas a essas duas características adicionais. A quarta dimensão (autodenúncia) é vista como uma resposta específica esperada das empresas: a comunicação de condutas indevidas às autoridades públicas. Já a quinta dimensão (contínuo aprimoramento) é essencial para que os programas de integridade evoluam constantemente, adaptando-se a novas situações e descobertas, com vistas a manter sua eficácia na prevenção e detecção de corrupção.

A partir deste ponto de vista, Carneiro e Santos Júnior[39] destacam a importância de as corporações adotarem uma posição de precaução, elaborando códigos de conduta mais rígidos e nomeando um *compliance officer* para monitorar, assessorar, prevenir e avaliar os riscos legais inerentes à gestão. Dessa forma, o desenvolvimento

[37] ZENKNER, Marcelo. **Integridade governamental e empresarial:** um espectro da repressão e da prevenção à corrupção no Brasil e em Portugal. Belo Horizonte: Fórum, 2019. p. 372-373.
[38] CARVALHO, ref. 7, p. 216.
[39] CARNEIRO; SANTOS JUNIOR, ref. 26, p. 64.

desses programas se dá para coibir práticas de corrupção contra a empresa e crimes que possam ocorrer em favor da empresa, ocultando os interesses de sócios, diretores, consumidores, funcionários e até interesses sociais[40].

Finalmente, para completar a compreensão do assunto, vale destacar os sete elementos mínimos que devem estar presentes em um programa de *compliance*, nos termos elaborados pela CGU, em 2024, e extraídos de seu guia intitulado “Programa de Integridade: Diretrizes para Empresas Privadas”[41].

Vale destacar que esses sete elementos ou pilares encontram respaldo na legislação, mais precisamente no art. 57, do Decreto n.º 11.129/2022[42]. Vejamo-los.

---

[40] VIOL, Dalila Martins. **Programas de Integridade e Combate à Corrupção:** aspectos teóricos e empíricos da multiplicação do compliance anticorrupção no Brasil. São Paulo: Almedina Brasil, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556273815.

[41] CONTROLADORIA GERAL DA UNIÃO (CGU). **Programa de Integridade:** Diretrizes para Empresas Privadas (vol. II). Brasília: CGU, 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/10/cgu-publica-novo-guia-de-diretrizes-para-empresas-privadas/GuiaDiretrizes_v14out1.pdf. Acesso em: Acesso em 23 mar. 2025.

[42] “Art. 57. Para fins do disposto no inciso VIII do caput do art. 7º da Lei nº 12.846, de 2013, o programa de integridade será avaliado, quanto a sua existência e aplicação, de acordo com os seguintes parâmetros:

I - comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa, bem como pela destinação de recursos adequados;

II - padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente do cargo ou da função exercida;

IV - treinamentos e ações de comunicação periódicos sobre o programa de integridade;

V - gestão adequada de riscos, incluindo sua análise e reavaliação periódica, para a realização de adaptações necessárias ao programa de integridade e a alocação eficiente de recursos;

VIII - procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, como pagamento de tributos, sujeição a fiscalizações ou obtenção de autorizações, licenças, permissões e certidões;

IX - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e pela fiscalização de seu cumprimento;

X - canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e mecanismos destinados ao tratamento das denúncias e à proteção de denunciantes de boa-fé”.

O primeiro elemento versa sobre o comprometimento e apoio da alta direção da empresa, o qual deve ser demonstrado por ações concretas e contínuas. Assim, os líderes devem ser modelos de comportamento ético e ter conhecimento sobre integridade empresarial, anticorrupção, governança corporativa e critérios ASG, com treinamentos periódicos para atualização. Outrossim, é desejável que a aplicação do programa de integridade seja incluída como critério na avaliação de desempenho e na remuneração variável dos líderes, de forma que irregularidades ou omissões não sejam recompensadas. A alta direção deve ainda destinar recursos financeiros e humanos adequados e proporcionais ao porte e aos riscos da empresa, para implementar e manter o programa de integridade. Também se mostra relevante manifestar apoio por meio de mensagens internas, redes sociais, reuniões e outras formas de comunicação. Por fim, os líderes devem assegurar que as irregularidades sejam investigadas e sancionadas, independentemente do cargo do infrator.

O segundo elemento aduz à existência de instância interna, responsável pela política de *compliance*, dotada de autonomia, independência, imparcialidade, recursos materiais, humanos e financeiros para seu pleno funcionamento, inclusive com acesso direto, quando necessário, ao alto escalão da companhia. Essa instância pode ser um departamento específico ou uma pessoa designada, dependendo do porte e da natureza da empresa. Dentre as principais atribuições, destacam-se: realizar análise de riscos para integridade; elaborar, atualizar e garantir a aplicação das políticas de integridade; disseminar a cultura de integridade por meio da comunicação e do treinamento; tratar e investigar denúncias de irregularidades; monitorar o programa de integridade e desenvolver indicadores e metas de desempenho; e reportar à alta direção sobre o andamento e aplicação do programa.

Já o terceiro pilar diz respeito à gestão de riscos para a integridade, de acordo com o qual a empresa deve conhecer seus processos e sua estrutura organizacional, identificar sua área de atuação e principais parceiros de negócio, bem como seu nível de interação com o setor público (nacional ou estrangeiro), avaliando os riscos para o cometimento dos atos lesivos previstos na Lei n.º 12.846/2013. Nesse intuito, as empresas devem adotar metodologias de avaliação de riscos que sejam adequadas a sua realidade, classificando os riscos por probabilidade e impacto, priorizando os mais relevantes e definindo medidas mitigatórias. Devem ainda adotar ações para reduzir a probabilidade e o impacto dos riscos identificados, bem como registrar todo o processo de gestão de riscos para garantir transparência e rastreabilidade.

O quarto elemento trata da estruturação de regras e instrumentos, a partir da elaboração ou atualização do código de ética ou de conduta e as regras, políticas e procedimentos de prevenção de irregularidades. Engloba ainda o desenvolvimento de mecanismos de detecção ou reportes de irregularidades (alertas; canais de denúncia; mecanismos de proteção ao denunciante), a definição de medidas disciplinares para casos de violação e medidas de remediação e a elaboração do plano de comunicação e treinamento com estratégias específicas para os diversos públicos da empresa.

O quinto componente se refere à existência de uma política anticorrupção, isto é, procedimentos que vedem de forma expressa e clara a concessão de vantagens indevidas (econômicas ou não) a agentes públicos, incluindo subornos e fraudes em licitações e contratos administrativos. Para tanto, a política deve ser operacional, com regras e fluxos de trabalho definidos e controles proporcionais aos riscos identificados. Deve ainda ser monitorada regularmente para garantir sua efetividade e adaptação às mudanças no ambiente regulatório e nos riscos da empresa. Nota-se, portanto, que a política anticorrupção visa prevenir, detectar e remediar atos ilícitos, fraudes e outras irregularidades contra a administração pública.

O sexto pilar versa sobre ações de treinamento e comunicação, as quais devem ser direcionadas aos funcionários da empresa, abordando conteúdos de integridade que constam no código de ética. Nesse intento, os treinamentos devem ser realizados regularmente, adaptando-se o conteúdo aos riscos e públicos específicos, com foco nos colaboradores que ocupam funções de maior risco. A comunicação também é importante e compreende a divulgação do código de ética, políticas, procedimentos e canais de denúncia, com vistas a incentivar comportamentos éticos, respeito aos direitos humanos, diversidade e práticas ambientais sustentáveis, refletindo as ações e valores das lideranças, bem como promovendo confiança e credibilidade.

O sétimo e último elemento trata da existência de um canal de denúncias, o qual deve ser estruturado de forma acessível, confiável e transparente, garantindo a proteção do denunciante quanto à confidencialidade das informações e ao anonimato, para evitar retaliações. Nesse sentido, o canal deve estar acessível em português, principalmente em empresas multinacionais, ser de fácil acesso para públicos interno e externo e estar, de preferência, na página institucional da empresa. O canal deve ainda possibilitar o acompanhamento da denúncia realizada. Por fim, é recomendável a divulgação periódica de informações gerais sobre denúncias recebidas, apurações e sanções aplicadas, mas sem expor indivíduos ou processos sensíveis.

Denota-se, assim, que a política de *compliance* compreende um processo contínuo, em que todos os envolvidos (de funcionários até o alto escalão) devem se comprometer com a cultura organizacional, englobando a identificação de exigências (éticas, administrativas e legais), a análise e a mitigação dos riscos de inconformidade, bem como a adoção de medidas preventivas e corretivas necessárias.

Salienta-se ainda que os programas de *compliance* não podem ser genéricos, mas sim construídos com base nas necessidades e particularidades de cada empresa. Em princípio, o instituto é aplicável a todos os tipos societários, embora sua estrutura e grau de formalização variem conforme a complexidade e o porte da organização. Originalmente difundido em grandes corporações, o conceito vem sendo aos poucos incorporado por sociedades limitadas, cooperativas, associações civis, fundações e até micro e pequenas empresas, em virtude de pressões regulatórias e da crescente demanda social por integridade e transparência nas relações empresariais.

No ponto, Assi[43] afirma não haver modelos padronizados, pois cada empresa precisa identificar, organizar e implementar a gestão de *compliance* e de controles internos que melhor se adeque a suas necessidades, facilitando o gerenciamento do negócio de acordo com seu apetite por riscos. Logo, o *compliance* não constitui uma exclusividade das grandes instituições financeiras, mas representa um conjunto de procedimentos e mecanismos de controle passíveis de adaptação à realidade de qualquer organização, seja qual for seu porte ou forma jurídica. Essa visão é corroborada por Treviño e Nelson[44], que afirmam que programas de conformidade eficazes dependem menos da forma societária e mais do comprometimento da alta administração com padrões éticos e de governança.

No cenário nacional, a Lei n.º 12.846/2013 reforça a aplicabilidade universal do *compliance*, ao prever que pessoas jurídicas de direito privado, “independentemente da forma de organização ou modelo societário”, podem ser responsabilizadas por atos lesivos contra a administração pública. Assim, o *compliance* deve ser compreendido como instrumento transversal de gestão e integridade, aplicável a qualquer entidade que exerça atividade econômica ou social, pública ou privada, exigindo adaptações proporcionais à sua estrutura de governança e aos riscos inerentes à sua operação.

[43] ASSI, ref. 32, p. 45.
[44] TREVIÑO, Linda K.; NELSON, Katherine A. **Managing Business Ethics:** Straight Talk About How to Do It Right. 8. ed. Hoboken: John Wiley & Sons, 2021.

Sob essa ótica, o sistema de conformidade atua como ferramenta de integração dos fundamentos da governança corporativa e da gestão de riscos, criando uma verdadeira cultura de integridade no ambiente empresarial – a qual, embora inclua, não se limita à mera observância de normas legais e regulamentos ou à adoção de um simples código de ética dou de conduta pela empresa.

A temática do imbricamento entre governança corporativa, gestão de riscos e sistemas de *compliance* é deveras rica, motivo porque será melhor aprofundada e devidamente analisada no subcapítulo adiante, conforme detalhado a seguir.

1.3 – Relação com Governança Corporativa e Gestão de Riscos

Conforme bem delineado por Blok[45], o termo "governança corporativa" surgiu em 1980, em razão de eventos ocorridos nos Estados Unidos e na Europa, ainda na década de 1970. Nessa época, houve um elevado crescimento da abertura de capital, dos fundos de investimentos e ainda da valorização dos acionistas. No entanto, em conjunto com esses avanços, as empresas de capital aberto começaram a enfrentar um intenso colapso corporativo em decorrência da falta de transparência e gestão no ambiente das companhias, resultando na insatisfação dos acionistas, que viram seus interesses prejudicados em detrimento dos interesses dos empresários.

De acordo com a autora, a governança corporativa surgiu na seara empresarial em decorrência de três aspectos distintos, a saber: 1) relações fracassadas entre os acionistas e as corporações; 2) conselhos colegiados ineficazes quanto à proteção dos interesses dos acionistas; e 3) atuação da diretoria da empresa em desacordo com as vontades dos acionistas, dos controladores ou ainda dos sócios minoritários.

Sobre o significado do vocábulo, Almeida[46] ensina que não há conceito sintético de governança corporativa que forneça os elementos necessários para compreendê-la, pois o termo versa sobre assunto de grande amplitude, de modo que os inúmeros conceitos acadêmicos e práticos disponíveis não são coesos, mas complementares entre si. Apesar das divergências conceituais, o autor aduz haver pontos comuns: governança corporativa se relaciona com o modo como as companhias são geridas e como as decisões de gestão são tomadas.

---

[45] BLOK, ref. 29.
[46] ALMEIDA, Luiz Eduardo de. Governança Corporativa. *In*: ALVIM, T. et al (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024.

Partindo dessa premissa e sem a pretensão de trazer um conceito hermético, pode-se dizer que a governança corporativa consiste em um conjunto de práticas que orientam a gestão da empresa, definindo a forma como ela será dirigida, monitorada e incentivada, envolvendo relação entre sócios, conselho de administração, diretoria, órgãos de fiscalização e acionistas. Com isso, busca-se garantir atuação transparente, ética e responsável, visando otimização dos resultados, movimentação da economia, produção de riquezas, manutenção de empregos e proteção às partes interessadas.

Nesse trilhar, o Código das Melhores Práticas de Governança Corporativa, do IBGC[47], atualizou sua definição de governança corporativa. Segundo o documento, a governança expandiu seu foco da otimização de valor econômico exclusivamente aos sócios para o de geração de valor compartilhado entre os sócios e as demais partes interessadas. Além disso, atualmente abarca não apenas empresas de capital aberto, mas também as médias e pequenas empresas, empresas familiares, estatais e entidades do terceiro setor. Essa perspectiva reconhece a interdependência entre as empresas e as realidades econômica, social e ambiental em que elas estão inseridas.

Analisando tais conceitos, infere-se que governança corporativa e sistemas de integridade estão intimamente relacionados, sendo relevante mencionar que a função de *compliance* deve ser dotada de autonomia na estrutura organizacional, tendo em vista os fatores de riscos a ele inerentes.

Porém, essa autonomia - a depender do porte da empresa - não impede que a execução da função de *compliance* seja delegada a setores que possuam outros encargos. Na verdade, conforme leciona Almeida[48], o importante é que a alocação da função de *compliance* em outras áreas não gere conflitos de interesses, pois isso sim afetaria a autonomia do sistema de integridade. Sobre o tema, a própria CGU[49], em

---

[47] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, ref. 1.
"Governança corporativa é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente".

[48] ALMEIDA, ref. 46.

[49] CONTROLADORIA GERAL DA UNIÃO (CGU), ref. 41.
"Obviamente, podem ser contratados terceiros para auxiliar em determinadas atividades, como operacionalização de canais de denúncia, desenvolvimento de treinamentos ou apoio na realização de análise de riscos. De todo modo, os serviços prestados por esses terceiros devem ser supervisionados pelo responsável pela instância interna.
Assim, ainda que seja considerada a possibilidade de terceirizar parte das funções relacionadas ao Programa de Integridade – por questões de otimização de recursos, especialização ou qualquer outra razão –, recomenda-se que a empresa mantenha em sua estrutura interna uma instância responsável pelo Programa de Integridade, que seja adequada à sua realidade e que esteja atenta para promover

seu guia intitulado “Programa de Integridade: Diretrizes para Empresas Privadas (vol. II)”, já validou a terceirização da função de *compliance* por pequenas companhias, com enxuto quadro de funcionários.

Nesse passo, as boas práticas que integram a governança corporativa estão embasadas em princípios, sendo várias as propostas inerentes a eles, as quais são previamente estabelecidas pela OCDE, pelo IBGC, pela SOx, dente outros. No Brasil, a principal referência sobre o tema está elencada no Código das Melhores Práticas de Governança Coorporativa, do IBGC[50], segundo o qual a governança corporativa é agora composta por 5 princípios, sendo eles: integridade, transparência, equidade, responsabilização (*accountability*) e sustentabilidade – (este último não constava da 5ª edição, de 2015, na qual eram elencados apenas quatro princípios).

Ainda sob o escólio de Almeida[51], tem-se que os princípios de governança corporativa surgiram como resposta a diversos escândalos. Eles buscam promover boas práticas para que as empresas cumpram sua função social, contribuindo para o desenvolvimento econômico e regional, a geração de empregos e o uso racional dos recursos naturais. Além disso, a governança visa gerar valor e resultados positivos para os sócios e acionistas (*shareholders*), ao mesmo tempo em que oferece os incentivos necessários para todas as partes interessadas (*stakeholders*).

Vale aqui uma breve incursão sobre esses princípios, com fulcro no referido documento elaborado pelo IBGC, eis que eles se aplicam a qualquer organização, independentemente de porte, natureza jurídica ou estrutura de capital, formando o alicerce sobre o qual se desenvolve a boa governança.

Quanto à integridade, a organização deve praticar e promover o contínuo aperfeiçoamento de uma cultura de ética em suas operações, evitando decisões sob influência de conflitos de interesses, mantendo a coerência entre discurso e ação, preservando a lealdade à empresa e o cuidado com partes interessadas, sociedade em geral e o meio ambiente.

Já a transparência consiste na disponibilização para as partes interessadas de informações verdadeiras, de modo tempestivo, coerente, claro e relevante, sejam elas positivas ou negativas, e não apenas aquelas impostas por disposições legais. Tais

---

uma cultura organizacional que não apenas minimize os riscos de prática de irregularidades, mas que contribua para o desenvolvimento sustentável da empresa e da sociedade na qual ela está inserida”.

[50] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, ref. 1.

[51] ALMEIDA, ref. 46, p. 15.

informações não se restringem ao desempenho econômico-financeiro, abarcando os fatores ambiental, social e de governança, o que favorece o desenvolvimento dos negócios e estimula um ambiente de confiança para o relacionamento de todas as partes interessadas.

A equidade, por sua vez, refere-se à obrigação da empresa de tratar todos os acionistas e demais *stakeholders* de forma justa, considerando seus direitos, deveres, necessidades, interesses e expectativas, como indivíduos ou coletivamente, motivada pelo senso de justiça, respeito, diversidade, inclusão, pluralismo e igualdade de direitos e oportunidades.

A responsabilização (*accountability*), traduz a ideia de que a empresa deve desempenhar suas funções com diligência, independência, visando à geração de valor sustentável no longo prazo, assumindo a responsabilidade pelas consequências de seus atos e omissões. Além disso, prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, cientes de que suas decisões podem não apenas responsabilizá-los individualmente, como impactar a organização, suas partes interessadas e o meio ambiente.

Por fim, a sustentabilidade (novo princípio incorporado) zela pela viabilidade econômico-financeira da organização, objetivando reduzir externalidades negativas de seus negócios e operações, e aumentar as positivas, tendo em vista, no modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, natural, reputacional) no curto, médio e longo prazos. Nessa perspectiva, compreender que as organizações atuam em uma relação de interdependência com os ecossistemas social, econômico e ambiental, fortalece seu protagonismo e suas responsabilidades perante a sociedade.

Posto isto, tem-se que o programa de *compliance* se caracteriza como um dos principais pilares de apoio à governança corporativa e sua aplicação demonstra o comprometimento da organização em firmar seu negócio com bases sólidas, éticas e sustentáveis, contribuindo para aumentar seu valor e assegurar sua continuidade e conformidade legal. Portanto, é por intermédio do desenvolvimento adequado e da perfeita integração entre os pilares e princípios já citados que as melhores práticas são adotadas nas empresas em conformidade com a governança corporativa.

A abordagem do tema também está intimamente relacionada com a gestão de riscos. Nessa análise, mostra-se relevante traçar uma prévia definição daquilo que se entende por “riscos”, o qual pode ser assim delineado: efeitos internos e externos que

causam incerteza ou imprevisibilidade para os processos de gestão e que, caso não sejam geridos da maneira correta, podem trazer prejuízos.

Segundo Assi[52], os riscos são condições de variáveis com potencial necessário para causar dano ao patrimônio (tangível ou intangível) das sociedades. Já de acordo com a norma ISO (*International Organization for Standardization* – padrão internacional para a gestão de riscos corporativos)[53] atualmente em vigor sobre o assunto, são estes definidos como “efeito das incertezas nos objetivos”.

A partir desse prévio entendimento, pode-se dizer, de modo simples e direto, que a gestão de riscos é um processo contínuo e sistemático que visa analisar, identificar, avaliar, tratar e monitorar riscos, para garantir que a empresa alcance seus objetivos de forma razoavelmente segura. Nos termos da norma ISO[54], a gestão de riscos pode ser definida como “atividades coordenadas para dirigir e controlar uma organização em relação ao risco”. O gerenciamento de riscos também está previsto no Código das Melhores Práticas de Governança Coorporativa, do IBGC[55].

Trata-se, pois, de atividade essencial na identificação de eventos potenciais que possam afetar os objetivos da organização, com análise da probabilidade e do impacto desses eventos, bem como tomada de medidas para mitigar ou evitar esses riscos. Conforme detalhado por Fernandes, Figueiroa e Neves[56], nota-se que a gestão de riscos é um processo composto por cinco etapas, nas quais a empresa decidirá como agir diante de um risco detectado.

No ensinamento dos referidos autores, a primeira etapa para a promoção do gerenciamento de riscos consiste na realização de uma auto análise pela sociedade, evidenciando seus valores, sua missão e seus objetivos, para que possa identificar sua postura no mercado onde está inserida e estipular a natureza e a magnitude dos riscos que está disposta a assumir.

---

[52] ASSI, ref. 32.

[53] ISO. **31000:2018(en)**. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en. Acesso em 13 fev. 2025.

[54] ISO, ref. 53.

[55] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, ref. 1, p. 63.
“O gerenciamento de riscos se dá por meio de processos estruturados que auxiliem a identificação, o controle e a mitigação dos fatores de risco relacionados ao negócio. A gestão de riscos contribui para a continuidade e geração de valor da organização. Essa atividade é responsabilidade de todos os agentes de governança e deve ter como base a conformidade com princípios, políticas, normas, regulamentos e leis aplicáveis. A gestão de riscos está suportada por três linhas de atuação. A primeira corresponde aos gestores de cada linha de negócio; a segunda, às funções de gestão de riscos, controles internos e compliance; e a terceira, à auditoria interna”.

[56] FERNANDES, Nelson Ricardo; FIGUEIROA, Caio; e NEVES, Edmo. Gestão de Riscos. *In*: ALVIM, T. et al (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024. p. 21-36.

Em seguida, passa-se a identificar e listar todos os riscos potenciais que podem afetar a empresa, em termos financeiros, operacionais, de segurança, de imagem ou de conformidade legal. Os métodos para realizar o levantamento de riscos são os mais diversificados, incluindo entrevistas com áreas operacionais da organização, análise de relatórios de auditorias e de processos judiciais, entre outros. O importante aqui é que seja feita uma detalhada e específica descrição de todos os riscos identificados e considerados sensíveis para a sociedade, uma vez que as demais etapas do processo dependerão desse cenário de risco previamente estipulado.

O terceiro passo consiste em uma avaliação quali-quantitativa da probabilidade de ocorrência dos riscos identificados e do potencial impacto na sociedade. Pelo vetor quantitativo, realiza-se uma avaliação simplesmente financeira dos riscos, mediante utilização de ferramentas estatísticas. Já o vetor qualitativo leva em conta a percepção humana (mensurada em tabelas de riscos) sobre o cenário de risco quantitativamente traçado, traduzindo não uma mera probabilidade, mas sim uma possibilidade real de um risco ocorrer (ou não).

Logo depois, com base na avaliação, a quarta etapa consiste em adotar as medidas necessárias para o tratamento dos riscos, que podem envolver a eliminação (o risco aqui é simplesmente evitado), a mitigação (nesse caso, a empresa assume o risco, mas limita seu alcance e/ou efeito), a transferência (que ocorre por meio da contratação de seguros, da mutualização, do oferecimento de garantias, entre outros), ou a aceitação dos riscos (quando a organização aceita os riscos e não adota qualquer providência), a depender de sua natureza e da capacidade da companhia.

O quinto e último passo da gestão de riscos diz respeito ao monitoramento periódico, pois, tratando-se de um processo contínuo, é necessário verificar os riscos ao longo do tempo, visando garantir que as medidas de tratamento sejam eficazes, bem como identificar novos riscos que possam surgir.

Por esse ângulo, observa-se que a gestão de riscos deve ser estabelecida nas mais diversas áreas da organização – financeira, jurídica, planejamento, conselho administrativo, gestão de *compliance*, entre outras – dada a sua multiplicidade.

Nesse sentido, fica evidente que gestão de riscos e *compliance* são conceitos interligados, pois ambos auxiliam na prevenção de ameaças à estrutura legal e aos ativos da sociedade. Ademais, os riscos de *compliance* são categorizados como riscos não financeiros (englobam riscos reputacionais, legais, de segurança de informações, e éticos, os quais não se refletem diretamente na saúde financeira da empresa, mas

podem ter consequências significativas em outros aspectos) e operacionais (referem-se à execução de atividades como segurança de dados, cumprimento de normas internas e externas, e gestão de processos), de tal sorte que é a partir da identificação desses riscos que programas efetivos de integridade são desenvolvidos.

Ainda na lição de Fernandes, Figueiroa e Neves[57], para que a governança corporativa seja aplicada, as boas práticas incorporadas e, consequentemente, os objetivos sejam alcançados, é imprescindível que se envolva a gestão de riscos e os programas de integridade. Na visão dos autores, a gestão de riscos e a de *compliance* estão intrinsecamente conectadas, sendo elementos centrais para a governança corporativa. Esta, por sua vez, traduz um conceito mais amplo, abrangendo as duas áreas. Desse modo, a implementação eficaz da gestão de riscos e de *compliance* é fundamental para a construção de um sólido modelo de governança. As duas atividades não são concorrentes, mas complementares e convergentes, permitindo a criação de um modelo robusto e eficaz de governança de riscos.

Embora complementares, os institutos não se confundem. Enquanto a gestão de riscos configura uma prática que busca prevenir os erros dentro da organização, com um olhar de prognóstico e foco na identificação, avaliação e mitigação de riscos, o *compliance* garante a conformidade com leis, regulamentos e normas internas.

Para encerrar a temática, cumpre destacar os benefícios de se incorporar a gestão de riscos na estrutura empresarial. Em primeiro lugar, o mecanismo ajuda a prevenir ou, pelo menos, minimizar as perdas causadas por eventos adversos. Além disso, ao identificar e analisar os riscos, a alta administração passa a ter informações mais precisas para tomada de decisões estratégicas e operacionais. Outrossim, uma gestão de riscos eficaz também revela que a sociedade está preparada para lidar com incertezas, aumentando a confiança de acionistas, investidores, clientes e de outras partes interessadas. Ademais, ao mitigar ou evitar riscos, a organização pode otimizar seus processos e recursos, aumentando a eficiência e a produtividade. Por fim, pode-se ainda destacar que a gestão de riscos contribui para que a companhia cumpra as leis e regulamentos em vigor, evitando multas e outras sanções.

1.4 – Modelos Internacionais de Integridade e Prevenção (FCPA, UKBA, OCDE)

[57] FERNANDES, ref. 56.

Conforme já mencionado alhures, o *Foreign Corrupt Protection Act* (FCPA) foi promulgado pelo Congresso Nacional dos Estados Unidos, em 1977, sendo a primeira norma a tratar sobre corrupção. O relatório de justificativa[58] acerca da necessidade da legislação revela que centenas de companhias admitiram ter feito pagamentos ilegais a políticos, partidos e agentes estrangeiros.

Na visão de Bertoccelli[59], num contexto marcado por grandes escândalos de corrupção, os Estados Unidos – maior potência econômica mundial – tinham que garantir a confiança e o bom funcionamento dos mercados, não só em seu território, mas em escala global. Para tanto, o país precisava estruturar regras e punir aqueles que não as cumprissem. Isso porque as maiores empresas (sejam americanas ou estrangeiras) estavam listadas em seu mercado de capitais e, portanto, o modo como elas conduziam seus negócios poderia impactar diretamente o valor da companhia e o interesse de seus acionistas.

Nesse mote, o FCPA foi responsável por ampliar e aprimorar os sistemas de integridade até então vigentes. Como estratégia, a norma traz duas frentes distintas de enfrentamento: de um lado, proíbe a prática de subornos a oficiais e a funcionários públicos estrangeiros por cidadãos e empresas norte-americanas, seja para obter ou para manter negócios; por outro, exige das companhias a organização de controles e registros de contabilidade internos, visando a maior transparência das operações.

Sobre o tema, discorre Blok[60] que a lei proíbe, de forma rigorosa, o pagamento de subornos, tanto de forma direta quanto por intermediários, a representantes de governos estrangeiros. O objetivo aqui é evitar que empresas obtenham vantagens comerciais indevidas ao influenciar as ações de funcionários públicos. Além disso, a lei estende a proibição a empresas listadas na bolsa de valores dos EUA, tornando crime qualquer pagamento não registrado de forma clara e precisa.

Quanto à fiscalização, lecionam Alencar e Varella[61] que o FCPA, de igual modo, estabeleceu uma arquitetura dual, reforçando os poderes do DOJ e da SEC para

---

[58] Disponível no sítio eletrônico do Departamento de Justiça norte-americano: https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/houseprt-95-640.pdf. Acesso em: 18 abr. 2025.

[59] BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: ALVIM, Tiago Cripa *et al* (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024.

[60] BLOK, ref. 29.

[61] ALENCAR, C. H. R.; VARELLA, M. D. Combate globalizado à corrupção: da gênese do modelo norte-americano à sua implementação internacional. **Revista de Direito Internacional Econômico e Tributário – RDIET**, Brasília, v. 16, n. 2, p. 184–226, jul./dez. 2021. Disponível em: https://portalrevistas.ucb.br/index.php/rdiet/article/view/13486. Acesso em: 12 out. 2025.

processarem pessoas jurídicas de capital aberto (qualquer que seja a nacionalidade) registradas na SEC e que tivessem ações nas bolsas de valores norte-americanas. Assim, o DOJ fiscaliza o cumprimento da lei, por meio da aplicação penal e civil dos dispositivos antissuborno, ao passo que a SEC fica responsável por sua coordenação e por apurar as infrações contábeis, aplicando penas de caráter civil e administrativo.

A respeito das contribuições efetivadas pelo FCPA em prol da ampliação do campo de atuação do DOJ e da SEC, vale o aprofundamento da temática. Nesse sentido, há que se considerar que a jurisdição do FCPA é notoriamente ampla, vigendo o princípio da extraterritorialidade[62]. Assim, as autoridades podem aplicar a referida lei a emissores de títulos nos EUA (*issuers*), a empresas e pessoas americanas (*domestic concerns*) e, desde as emendas de 1998 (introduzidas em resposta à Convenção Antissuborno da OCDE), também a estrangeiros que cometam qualquer ato em prol do suborno em território norte-americano[63].

O FCPA representou uma ampliação significativa do escopo de atuação do DOJ, sobretudo em razão da interpretação extensiva conferida à cláusula *to obtain or retain business* (obter ou reter negócios), que passou a abranger qualquer vantagem indevida capaz de assegurar competitividade ou lucratividade empresarial, ainda que de forma indireta. Inicialmente, poderia parecer que a lei se limitaria a pagamentos feitos para garantir contratos governamentais diretos. Contudo, o precedente judicial no caso *United States v. Kay*[64] confirmou que a proibição se estende amplamente a pagamentos feitos para obter propósitos de negócios impróprios que não envolvem

[62] A aplicação extraterritorial do FCPA pela SEC e DOJ (alcançando empresas estrangeiras com laços mínimos com o território ou mercado de capitais dos EUA) serviu como um poderoso mecanismo para exportar o padrão de *compliance* e fiscalização americanos. Dessa forma, os EUA impuseram e disseminaram seu paradigma regulatório a nível global, influenciando o arcabouço legal de muitos países, incluindo a Lei Anticorrupção brasileira (Lei 12.846/2013).
Todavia, a aplicação agressiva e extraterritorial do FCPA pelo DOJ e SEC é objeto de uma forte corrente crítica na doutrina jurídica, que a qualifica como "imperialismo legal" ou "neocolonialismo jurídico". Segundo Coelho e Heringer, essa crítica sustenta que a aplicação expansiva do estatuto representa uma intromissão nos assuntos internos e na soberania de outras nações (Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2004/1285. Acesso em: 12 out. 2025).
De la Torre, por sua vez, ensina que ao processar e penalizar empresas estrangeiras por condutas que ocorreram inteiramente fora do território americano, o DOJ e a SEC estariam aplicando uma definição estritamente americana de corrupção em mercados globais (Disponível em: http://scholarship.law.cornell.edu/cilj/vol49/iss2/5. Acesso em: 12 out. 2025).
[63] DEPARTMENT OF JUSTICE (DOJ). **Foreign Corrupt Practices Act. [S.l.]:** DOJ, 1977. Disponível em: https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act. Acesso em: 10 out. 2025.
[64] UNITED STATES v. KAY. **Court of Appeals for the Fifth Circuit (5th Cir.)**, 359 F.3d 738, 2004. Disponível em: https://caselaw.findlaw.com/court/us-5th-circuit/1119030.html. Acesso em: 10 out. 2025.

diretamente a obtenção de um novo contrato, como a redução de impostos ou taxas alfandegárias, pois mantêm a rentabilidade e a posição de mercado da empresa.

Este entendimento jurisprudencial validou a visão do Congresso de aplicar o FCPA de maneira extensiva, garantindo que o DOJ pudesse perseguir uma gama muito mais ampla de atividades corruptas que afetam a concorrência internacional, e não apenas o suborno na aquisição de grandes projetos.

O FCPA também trouxe contribuições de ordem processual ao DOJ, sendo a mais significativa a que institucionalizou o uso de veículos de resolução alternativa: os *Deferred Prosecution Agreements* (DPAs) e os *Non-Prosecution Agreements* (NPAs). Por meio dos DPAs, o DOJ apresenta acusações criminais, mas pode suspender a persecução judicial, sob a condição de que a empresa cumpra os termos definidos no acordo (multas, cooperação, reformas de *compliance*). Já com os NPAs, nenhuma acusação é formalmente apresentada, desde que a empresa cumpra as sanções e reformas estipuladas pelo DOJ.

Consoante Koheler[65], historicamente, o DOJ tinha apenas duas opções ao investigar organizações empresariais: acusar a entidade criminalmente ou declinar a acusação. No entanto, a partir de 2004, o DOJ passou a utilizar esses contratos de resolução - que se tornaram a forma dominante de resolver o escrutínio corporativo sob o FCPA. A utilização generalizada desses mecanismos processuais, embora não estivesse explicitamente prevista no estatuto do FCPA, transformou o DOJ de um mero litigante para um regulador *de facto* de *compliance* global, com o poder de impor multas bilionárias e exigir mudanças estruturais na governança corporativa. Tal conduta, porém, tem sido alvo de intensa crítica acadêmica[66].

---

[65] KOEHLER, M. The FCPA, Deferred Prosecution Agreements, and Non-Prosecution Agreements. **U.C. Davis Law Review**, Davis, v. 49, n. 2, 2015.

[66] Segundo Martins, a centralidade dos DPAs e NPAs na aplicação do FCPA é objeto de intensa crítica acadêmica, frequentemente referida como a "cultura do acordo". A resolução por meio desses contratos oferece eficiências econômicas para as empresas ao evitar longos e custosos litígios, mas a prática tem implicações negativas para o *rule of law* internacional (Disponível em: https://revistas.usp.br/rdda/article/view/185311/174582. Acesso em 12 out. 2025).
De acordo com Yockey, os críticos argumentam que o processo de resolução permite que empresas evitem a admissão pública de culpa e o escrutínio judicial completo, comprometendo a transparência. Além disso, a exigência do DOJ de "cooperação plena" como pré-requisito para resoluções favoráveis gera um dilema ético fundamental. A cooperação corporativa frequentemente significa que a empresa deve identificar e disciplinar os indivíduos responsáveis pelo alegado suborno. Esta dinâmica pode levar a uma quebra de confiança entre a administração, os funcionários e os advogados internos, criando uma cultura de desconfiança e aversão a riscos excessiva. O FCPA, por meio da política de DPAs, estabeleceu uma tensão inerente: o incentivo à cooperação, crucial para a política de *enforcement* do DOJ, pode acabar prejudicando a capacidade da empresa de construir uma cultura de integridade duradoura e baseada em comunicação aberta (Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029241. Acesso em: 12 out. 2025).

A contribuição mais recente do Congresso Nacional americano para o mandato criminal do DOJ foi a promulgação do *Foreign Extortion Prevention Act* (FEPA) em 2023[67]. Enquanto o FCPA foca na criminalização do lado da *oferta* de suborno (a empresa ou indivíduo que paga), o FEPA preenche a lacuna histórica ao criminalizar o lado da *demanda*, proibindo explicitamente que funcionários estrangeiros exijam, busquem, recebam ou aceitem qualquer coisa de valor de emissores dos EUA (*domestic concerns*) ou qualquer pessoa em território americano.

Dessa forma, o FEPA expandiu o poder do DOJ para processar os agentes corruptos diretamente, isto é, sem depender da vontade ou capacidade de governos estrangeiros. Isso reforça o DOJ como o executor primário contra a corrupção transnacional, permitindo-lhe avançar em casos de extorsão onde o oficial estrangeiro é o instigador. O FEPA compartilha a ampla jurisdição do FCPA, aplicando-se a qualquer pessoa que atue em nome de um governo ou organização internacional.

Já em relação ao mandato da SEC, a principal contribuição estrutural do FCPA foi a introdução da exigência de controles internos e registros precisos. Com isso, a SEC (antes uma agência meramente reguladora de valores mobiliários) se firmou como instituição crucial no combate à corrupção transnacional. A partir das inovações colmatadas pela FCPA, a SEC pôde fiscalizar e punir falhas de governança e de transparência corporativa, mesmo quando a prova do suborno (*quid pro quo*) era difícil de obter, expandindo exponencialmente seu alcance de *enforcement*[68]. Dentre as sanções aplicáveis pela SEC, incluem-se multas civis substanciais, restituição de lucros ilícitos (*disgorgement*) e juros de pré-julgamento. O escopo destas disposições é vasto, cobrindo não apenas a alta administração, mas também oficiais, diretores, funcionários, acionistas e terceirizados (consultores e parceiros de *joint venture*).

Outra norma de peso, que estabeleceu uma sinergia regulatória fundamental para a SEC, foi a lei *Sarbanes-Oxley* (SOX), de 2002. O SOX foi uma resposta a escândalos de fraude financeira, exigindo maior transparência e supervisão e, embora

[67] CONGRESS (United States). *S. 4548* – **Foreign Extortion Prevention Technical Corrections Act**. Projeto de lei — 118th Congress, 2023-2024. Disponível em: https://www.congress.gov/bill/118th-congress/senate-bill/4548/text. Acesso em: 12 out. 2025.

[68] O estatuto impõe a todos os emissores listados nos EUA a obrigação de manter livros e registros que reflitam com precisão as transações. Esta exigência garante que fundos ilícitos, frequentemente disfarçados como despesas legítimas (como honorários de consultoria ou vendas), sejam rastreáveis, fornecendo à SEC o poder de investigar e sancionar falhas de *due diligence* relacionadas a terceiros, que são os principais veículos para subornos. SECURITIES AND EXCHANGE COMMISSION (SEC). *Foreign Corrupt Practices Act (FCPA)*. [S.l.]: SEC, [s.d.]. Disponível em: https://www.sec.gov/enforcement/foreign-corrupt-practices-act. Acesso em: 18 abr. 2025.

não seja uma lei anticorrupção, ele complementa o FCPA. Na prática, o SOX impôs requisitos de certificação para CEOs e CFOs sobre precisão de relatórios financeiros, exigindo que a administração e auditores externos avaliem a eficácia dos sistemas de controle interno. Segundo Christensen, Maffett e Rauter[69], tais exigências forçaram as empresas a incorporarem o *compliance* antissuborno do FCPA diretamente em seu regime de divulgação financeira e de controles de TI. Esta integração aumentou a probabilidade de detecção de transações questionáveis por auditores, fortalecendo a SEC em sua função de vigilância.

O ponto de maior poder do FCPA em relação ao SOX é a ausência de um limite de materialidade. Enquanto o SOX foca em controles destinados a prevenir distorções financeiras *materiais*, as cláusulas contábeis do FCPA não exigem que o registro incorreto seja materialmente relevante para as demonstrações financeiras. Assim, qualquer falha de controle que oculte um pagamento impróprio (ainda que de pequeno valor) constitui uma violação do FCPA processável pela SEC. Esta distinção confere à SEC autoridade ampla para garantir a integridade em todos os níveis transacionais, indo além da prevenção da fraude de grande escala.

A natureza dual da aplicação do FCPA, envolvendo o DOJ e a SEC, levou à necessidade de padronizar as interpretações e as políticas. O produto deste esforço interinstitucional foi o *A Resource Guide to the U.S. Foreign Corrupt Practices Act*[70], documento que detalha os marcos de um programa de *compliance* eficaz que as empresas devem implementar, para mitigar o risco de corrupção e obter crédito junto às agências em caso de investigação.

Entre os critérios avaliativos usados pelas autoridades norte-americanas para prevenir infrações ao FCPA (práticas de suborno de agentes públicos estrangeiros) e demonstrar boa-fé e mitigação de culpa (*good faith compliance efforts*) em eventuais investigações conduzidas pelo DOJ ou SEC, encontram-se: 1) a avaliação de risco (*risk assessment* - voltada à identificação de áreas e operações mais suscetíveis à ocorrência de práticas corruptas); 2) o treinamento (*training and communication* - com

[69] CHRISTENSEN, H. B.; MAFFETT, M. G.; RAUTER, T. *Policeman for the World: U.S. Enforcement of Foreign Corruption Regulation and Corporate Investment Policies*. SSRN Electronic Journal, 2021. DOI: 10.2139/ssrn.3349272. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349272. Acesso em: 12 out. 2025.

[70] DEPARTMENT OF JUSTICE (DOJ); SECURITIES AND EXCHANGE COMMISSION (SEC). **A Resource Guide to the U.S. Foreign Corrupt Practices Act**. 2. ed. Washington, D.C.: DOJ/SEC, 2020. Disponível em: https://www.justice.gov/criminal-fraud/file/1292051/download. Acesso em: 10 out. 2025.

o propósito de difundir padrões éticos e procedimentos de integridade, mediante a educação contínua de funcionários e parceiros sobre as políticas anticorrupção da empresa, códigos de conduta e canais de denúncia); e 3) a devida diligência de terceiros (*third-party due diligence* - consiste em investigar e verificar a idoneidade de quem atua em nome da empresa antes de contratar ou renovar vínculos comerciais, incluindo a análise de antecedentes, verificação da necessidade comercial do terceiro e monitoramento contínuo de cláusulas contratuais de integridade).

Além disso, as agências também enfatizam a necessidade de *tone at the top*, aplicando incentivos positivos (promoções, recompensas) e medidas disciplinares justas (do conselho à base) para reforçar uma cultura de ética. Assim, as agências esperam que as organizações realizem diligência baseada em risco para entender a reputação, qualificações e associações dos parceiros, garantindo que a compensação seja razoável e não seja usada para pagamentos corruptos.

Embora o Guia seja uma orientação informal e não vinculante, ele se tornou a referência padrão para corporações, profissionais de *compliance* e advogados em todo o mundo. O seu valor institucional reside na codificação da interpretação das agências sobre temas complexos, como a definição ampla de funcionário estrangeiro, a aplicação da responsabilidade sucessória em fusões e aquisições e ainda os marcos de um programa de *compliance* corporativo eficaz. Tais orientações garantem uma previsibilidade e transparência desejáveis no ambiente regulatório transnacional.

Cabe ainda destacar algumas outras peculiaridades relativas aos dispositivos legais do FCPA[71], a saber: 1) não se aplica a atos de corrupção de funcionários públicos nacionais, mas apenas de funcionários públicos estrangeiros; 2) versa apenas sobre atos lesivos referentes à corrupção; 3) as penalidades cíveis e criminais são aplicadas tanto a pessoas físicas, quanto jurídicas; 4) a responsabilização não é objetiva, sendo, portanto, necessário provar o dolo; 5) as penalidades criminais, em caso de violação antissuborno, sujeitam as sociedades a multa de até US$ 2 milhões, enquanto os indivíduos estão sujeitos a multa de até US$ 250.000, bem como prisão de até cinco anos; 6) as penalidades criminais, em caso de violação contábil e de registros, impõem às entidades empresariais multas de até US$ 25 milhões, ao passo que aos indivíduos a multa imposta é de até US$ 5 milhões e pena de prisão de até 20 anos; 7) as penalidades civis, na hipótese de violação antissuborno, sujeitam as

[71] Disponível no sítio eletrônico do *U.S. Securities and Exchange Commission*: https://www.sec.gov/enforcement/foreign-corrupt-practices-act. Acesso em: 18 abr. 2025.

empresas e os indivíduos a multa civil de até US$ 16.000; 8) já as penalidades civis, em caso de violações contábeis e de registros, variam – a SEC oferece a opção de penalizar empresas e pessoas físicas na faixa de US$ 75.000 a US$ 725.000 e de US$ 7.500 a US$ 150.000, respectivamente, ou penalizar com base no "valor bruto do ganho pecuniário" (o que, na prática, é ilimitado); 9) é possível aplicar outras penalidades, como declaração de inidoneidade e monitoramento; 10) as organizações ganham créditos se tiverem programas de integridade eficiente, conforme modelo da *U.S. Sentencing Guidelines*; e 11) há créditos também por reporte voluntário e cooperação.

Uma vez feita esta análise pormenorizada do FCPA, mostra-se relevante tratar da suspensão temporária de sua aplicação nos Estados Unidos, instituída pela Ordem Executiva nº 14209, de 10 de fevereiro de 2025[72].

Essa suspensão significou uma reorientação estratégica da política de combate à corrupção transnacional. Ordenada para um período de 180 dias, a medida instruiu o Procurador-Geral a cessar a abertura de novas investigações e revisar as ações existentes. A motivação central articulada pela Administração foi a necessidade de reverter a aplicação "excessivamente expansiva e imprevisível" do FCPA. Segundo o governo, a norma prejudicava a competitividade econômica e a segurança nacional dos EUA, alegando interferência nas prerrogativas presidenciais de política externa. Durante a suspensão, a incerteza regulatória foi elevada, muito embora o FCPA tenha permanecido válido e outras autoridades, em especial a SEC, mantiveram capacidade de fiscalização civil, mitigando o risco de um vácuo completo no *enforcement*.

O período de revisão culminou na emissão de novas diretrizes pelo DOJ, em junho de 2025, sinalizando o fim da suspensão e a adoção de um novo paradigma de *enforcement* alinhado à doutrina *America First*. De acordo com Parker *et al*.[73], as orientações subsequentes focaram na aplicação seletiva e estratégica, priorizando esquemas de suborno substanciais envolvendo *Transnational Criminal Organizations* (TCOs) e atos que minem diretamente os interesses de segurança nacional ou as

[72] THE WHITE HOUSE. **Fact Sheet:** President Donald J. Trump Restores American Competitiveness and Security in FCPA Enforcement. 10 fev. 2025. Disponível em: https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-restores-american-competitiveness-and-security-in-fcpa-enforcement/. Acesso em: 12 out. 2025.

[73] PARKER, K. A.; SLOANE, E. G. H.; CESTARO, C.; HOLTMEIER, J.; STARK, E. L.; WINGERT, M. G. *Department of Justice Announces FCPA Guidelines*. WilmerHale – Client Alert, 10 jun. 2025. Disponível em: https://www.wilmerhale.com/en/insights/client-alerts/20250610-department-of-justice-announces-fcpa-guidelines. Acesso em: 12 out. 2025.

vantagens competitivas dos EUA em setores críticos. Essa reorientação implicou a preterição de casos de baixo valor ou cortesias rotineiras e a centralização do controle político na abertura de investigações, visando monetização eficiente do *enforcement*.

As perspectivas de longo prazo indicam que o *compliance* corporativo global deve evoluir para incorporar uma avaliação de risco geopolítico estratégico, mormente para empresas estrangeiras cujas atividades concorrentes podem ser consideradas prejudiciais aos interesses americanos. Segundo Baker McKenzie[74], embora o novo filtro do DOJ possa reduzir a pressão sobre as infrações menores, o risco de responsabilização permanece, sobretudo devido ao estatuto de limitações de cinco anos e à possibilidade de reversão da política por futuras administrações, exigindo cautela contínua e programas de integridade robustos.

Em síntese, além de ser a primeira lei no combate à corrupção, o FCPA sem dúvida é a norma mais importante sobre o tema, razão por que serviu de modelo para legislações anticorrupção de diversos outros países e como fonte de inspiração para a criação de convenções internacionais acerca da matéria. Trata-se de um verdadeiro catalisador para a expansão dos poderes regulatórios e de fiscalização do DOJ e da SEC, moldando a política de *enforcement* corporativo nos Estados Unidos, bem como exportando um modelo de *compliance* para o restante do mundo.

Nesse sentido, já na história mais recente, no ano de 2010, outra norma surgiu no cenário internacional, tornando-se também um modelo de grande influência no comércio global. Trata-se do *United Kingdom Bribery Act* (UKBA)[75], lei anticorrupção promulgada pelo Parlamento britânico, nitidamente inspirada na lei norte-americana, sendo, no entanto, mais rígida que ela em vários panoramas.

Um aspecto notável do UKBA é que o órgão responsável por sua aplicação – o *Serious Fraud Office* (SFO – agência governamental especializada na investigação e processo de crimes financeiros graves e complexos, incluindo corrupção e fraude) – opera tanto no Reino Unido quanto na Nova Zelândia, com o objetivo de proteger a integridade dos sistemas financeiros e a segurança pública. Vale ainda mencionar que a aplicação do UKBA também é extraterritorial, nos mesmos moldes do FCPA.

---

[74] BAKER MCKENZIE. **United States: Why compliance still matters**. InsightPlus – Baker McKenzie, 13 fev. 2025. Disponível em: https://insightplus.bakermckenzie.com/bm/investigations-compliance-ethics/united-states-why-compliance-still-matters. Acesso em: 12 out. 2025.

[75] UNITED KINGDOM. **Bribery Act 2010**. London: The Stationery Office, 2010. Disponível em: https://www.legislation.gov.uk/ukpga/2010/23/contents. Acesso em: 05 mai. 2025.

Aliás, um comparativo entre essas duas normas (FCPA e UKBA) revela haver semelhanças e divergências interessantes. Conforme apontamentos de Blok[76], de modo análogo ao que ocorre com o FCPA, que se limita à repressão de atos de corrupção, o UKBA tem por escopo exclusivo o combate ao suborno, compreendido como espécie do gênero "corrupção". Tal legislação não contempla normas de *compliance* que ultrapassem o âmbito de disposições antissuborno ou anticorrupção. Diferentemente da legislação brasileira — que, por meio do Decreto n.º 11.129/2022 (e anteriormente do Decreto n.º 8.420/2015), estabelece parâmetros objetivos para a implementação de programas de integridade e sua exigência em contratações com a Administração Pública, conforme previsto na Lei n.º 12.846/2013 —, tanto o FCPA quanto o UKBA não disciplinam de modo expresso os requisitos para um sistema de integridade corporativa efetivo.

No que se refere à responsabilização, o UKBA prescinde da comprovação do intuito de corromper por parte de agente público estrangeiro ou de qualquer outro indivíduo, seja no setor público ou privado, bastando a mera consumação do ato, ainda que de forma culposa. Dessa forma, a responsabilidade atribuída é de natureza objetiva – diferentemente do FCPA, que exige a prova do dolo. O rol de possíveis sujeitos passivos é amplo, abrangendo empregados, terceiros intermediários, agentes e até subsidiárias, desde que a conduta tenha como propósito a obtenção ou manutenção de vantagem indevida na condução das atividades empresariais.

A pessoa jurídica, por sua vez, apenas poderá afastar a responsabilidade penal caso comprove a existência de mecanismos efetivos de prevenção à corrupção — o que implica possuir área específica e programa de integridade implementado, com treinamentos periódicos, mitigação de riscos, canais de denúncia (*hotlines*), códigos de conduta e outras medidas de controle interno. Embora o ordenamento britânico não imponha de maneira obrigatória a criação de uma estrutura independente de *compliance* nem a operacionalização de um programa formalmente certificado (diversamente do que ocorre na legislação anticorrupção brasileira), a adoção de tais instrumentos pode reduzir substancialmente ou até eliminar a aplicação de sanções de natureza administrativa, civil ou penal a pessoas físicas e jurídicas.

[76] BLOK, ref. 29.

De acordo com os ensinamentos de Muliterno e Palazzi[77], apesar dos paralelos comuns entre essas duas legislações, elas possuem diferenças relevantes. No ponto, destaca-se que o UKBA estabelece um crime geral de suborno, que abrange tanto o ato de oferecer quanto o de receber vantagens indevidas, sem distinguir entre as práticas ocorridas no setor público e as verificadas no âmbito privado (*commercial bribery*). Dessa maneira, a legislação britânica criminaliza condutas voltadas a induzir, recompensar ou influenciar agentes públicos e particulares a desempenhar suas funções ou atividades de modo indevido (*improper performance*), independentemente da efetiva obtenção de resultado ilícito.

Importa ainda salientar que o UKBA não diferencia as partes envolvidas no ato corrupto, punindo tanto quem oferece ou promete, quanto quem solicita ou recebe a vantagem indevida[78]. Logo, qualquer transação que envolva promessa, pagamento ou recebimento de suborno entre particulares ou agentes públicos, com o propósito de alcançar benefícios indevidos, é suscetível de sanção penal de até dez anos de prisão e/ou multa.

Em consonância com os princípios da Convenção das Nações Unidas contra a Corrupção, o UKBA incrimina a concessão e a aceitação de vantagens que violem os deveres de confiança, lealdade e boa-fé, inerentes às relações entre indivíduos e as entidades públicas ou privadas que representam.

Por outro lado, ainda que o UKBA não contenha disposições relativas à manutenção de livros e registros contábeis (*books and records*) ou a violações de controles internos — obrigações expressamente previstas no FCPA e no SOX —, a existência de mecanismos internos de controle e de um compromisso institucional autêntico com o combate à corrupção pode ser considerada circunstância atenuante na análise de responsabilidade corporativa. Tais elementos demonstram a adoção de boas práticas de governança e *compliance*, podendo reduzir sanções ou contribuir para a exclusão de penalidades impostas a pessoas jurídicas.

Em relação aos crimes, a norma britânica elenca cinco infrações principais, sendo elas: 1) suborno ativo – oferecer ou dar suborno a outrem (pune-se a vantagem

---

[77] MULITERNO, Paulo Tiago Sulino; e PALAZZI, Leonardo. Corrupção Privada e *Compliance*. *In*: CARNEIRO, Cláudia; e DELLOSO, Ana Ayres (coord.). **Compliance Aplicado ao Direito**. ISBN: 978-65-00-27380-9. ICTS protiviti, 2021. p. 456-496.

[78] Ressalte-se que esta disparidade entre o UKBA e o FCPA apenas foi suprida com o advento da FEPA (em 2024), que passou a criminalizar o lado da *demanda*, proibindo que funcionários estrangeiros exijam, busquem, recebam ou aceitem qualquer coisa de valor de emissores dos EUA ou qualquer pessoa em território americano.

oferecida para que o destinatário faça algo impróprio no exercício de suas funções); 2) suborno passivo – aceitar ou solicitar suborno (pune-se a vantagem recebida para executar funções impropriamente); 3) suborno de um funcionário público estrangeiro (a pena é aplicada em virtude da vantagem destinada a influenciar funcionário público a ajudar seu negócio de qualquer forma); 4) consentimento ou conivência de diretor ou alto funcionário da organização em suborno por uma empresa; e 5) falha da sociedade em impedir suborno em seu nome por pessoas associadas (as duas últimas punem o delito de ser conivente e/ou não impedir).

Acerca da aplicação da lei britânica, cabe mencionar o Guia do Ministério da Justiça do Reino Unido, publicado em 2011 (*Guidance* UKBA)[79], que estabelece seis princípios a serem observados pela empresa em seu sistema de *compliance*, com vistas a prevenir atos de corrupção e com foco em procedimentos ativos e eficazes (não bastando a mera existência de um programa de fachada).

O documento aduz que tais princípios não são prescritivos, mas projetados para serem flexíveis, permitindo sua adequação à enorme gama de circunstâncias em que as organizações comerciais se encontram.

O primeiro princípio versa sobre “procedimentos proporcionais”, de acordo com o qual os procedimentos de uma organização comercial para prevenir o suborno por pessoas associadas a ela são proporcionais aos riscos de suborno que enfrenta e à natureza, escala e complexidade das atividades da organização comercial. Eles também são claros, práticos, acessíveis, efetivamente implementados e aplicados.

O segundo trata do “compromisso da alta gestão” (conselho de diretores, proprietários ou qualquer outro órgão ou pessoa equivalente), a qual deve estar comprometida em prevenir o suborno por pessoas associadas a ela. Eles promovem uma cultura dentro da organização na qual o suborno nunca é aceitável.

O terceiro princípio traz a “avaliação de riscos”, devendo a sociedade avaliar a natureza e extensão de sua exposição a potenciais riscos externos e internos de suborno, em seu nome por pessoas associadas a ela. A avaliação deve ser periódica, informada e documentada.

[79] UNITED KINGDOM. **Bribery Act 2010:** Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing. London: Ministry of Justice, 2011. Disponível em: https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf. Acesso em: 05 mai. 2025.

Já o quarto princípio fala acerca da “diligência prévia”, pela qual a organização deve adotar abordagem proporcional e baseada em riscos, em relação às pessoas que desempenham ou desempenharão serviços para ou em nome da organização, a fim de mitigar os riscos de suborno identificados.

O quinto princípio versa sobre “comunicação (incluindo treinamento)”, segundo o qual a organização deve buscar garantir que suas políticas e procedimentos de prevenção ao suborno sejam incorporados e compreendidos em todos da empresa, por meio de comunicação interna e externa, incluindo treinamento, de modo que seja proporcional aos riscos que enfrenta.

O sexto e derradeiro princípio trata do “monitoramento e revisão”, em que a empresa monitora e revisa os procedimentos projetados para prevenir o suborno por pessoas associadas a ela e faz melhorias quando necessário.

Em suma, o UKBA representa um marco normativo de significativa relevância no aperfeiçoamento das práticas globais de integridade corporativa. Ao adotar uma abordagem abrangente, que criminaliza tanto o oferecimento quanto o recebimento de vantagens indevidas — independentemente do setor em que ocorram —, o UKBA estabelece um padrão normativo de alta exigência ética, influenciando políticas públicas e estratégias empresariais além das fronteiras do Reino Unido. Sua ênfase na responsabilidade corporativa objetiva e na implementação de mecanismos internos de prevenção ao suborno impulsionou a consolidação de programas de *compliance* baseados em avaliação de riscos, diligência de terceiros e monitoramento contínuo, que hoje compõem o cerne das boas práticas internacionais de governança.

Nesse contexto, além de reforçar o compromisso global com a integridade e transparência, a legislação britânica também atua como vetor de harmonização regulatória, promovendo a convergência de sistemas jurídicos distintos em torno de um modelo preventivo de enfrentamento à corrupção.

Passando agora à análise do último grande modelo internacional de integridade e prevenção, vamos tratar da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE). Para tanto, faz-se mister traçar um breve histórico da instituição.

Após duas Guerras Mundiais, os países da Europa estavam devastados, tendo em vista os efeitos nefastos dos embates. Visando estabilizar as economias europeias e evitar o avanço do comunismo, foi posto em prática o Plano *Marshall*, o qual, na essência, foi um pacote de ajuda financeira e material concedido pelos EUA aos países europeus para reparar suas infraestruturas, indústrias e economias. Nesse

intento, foi criada a Organização Europeia de Cooperação Econômica (OECE), em 1948, com o objetivo de administrar o Plano *Marshall*.

A OECE foi substituída pela OCDE, em 1961, após a assinatura de uma convenção, em dezembro de 1960. Esta convenção criou uma nova organização com uma abrangência maior, incluindo os Estados Unidos e o Canadá. A criação da OCDE teve o objetivo de promover padrões internacionais nas áreas econômica, financeira, comercial, social e de meio ambiente, além de desenvolver o bem-estar econômico e social dos seus membros.

A OCDE também tem o fim de promover a integridade pública e a prevenção da corrupção, por meio de recomendações e guias. A Instituição estabelece ainda princípios para gestão da integridade pública, incluindo a transparência, participação de partes interessadas e mecanismos de fiscalização. As recomendações da OCDE são referências para os países no desenvolvimento de políticas anticorrupção, tanto em nível nacional quanto internacional.

Vale lembrar que a OCDE contribuiu significativamente na criação e expansão dos sistemas de integridade, em especial na década de 1970, quando centenas de companhias (entre elas as 100 maiores do mundo) confessaram ter pago propinas. A partir daí, os Estados Unidos pressionaram os países membros da Organização para que também adotassem procedimentos similares ao do FPCA, com vistas a coibir o pagamento de propinas em transações comerciais internacionais.

Outro marco importante da contribuição da OCDE para o desenvolvimento das políticas de *compliance* se deu com a realização, em Paris, no ano de 1997 (com vigor a partir de 1999), da Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais[80], em que os países membros e Argentina, Brasil, Bulgária, Chile e República Eslovaca, comprometeram-se a adotar medidas anticorrupção, inclusive de *self compliance* pelas empresas.

[80] Embora o Brasil não seja um país membro da OCDE, tem participado como observador em algumas atividades da Organização, bem como tem se comprometido a seguir suas recomendações. O Brasil promulgou a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais por meio do Decreto n.º 3.678/2000. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3678.htm. Acesso em 10 mai. 2025.

Mais recentemente, em 2022, a Organização lançou o "Manual de Integridade Pública da OCDE"[81], que elenca princípios, estratégias e ferramentas para promover a integridade pública e combater a corrupção.

O guia destaca a importância do compromisso político, da atribuição clara de responsabilidades, do desenvolvimento de estratégias baseadas em evidências e da implementação de altos padrões de conduta no setor público. Promove a colaboração entre governos, empresas, sociedade civil e indivíduos, bem como a liderança ética e sistemas de contratação baseados no mérito. O manual também aborda a capacitação contínua, a abertura organizacional, a gestão de riscos, a prestação de contas e a supervisão externa. Além disso, o documento enfatiza a transparência, a participação das partes interessadas na formulação de políticas públicas e a prevenção da captura de políticas por interesses privados. Ademais, o guia mostra a relevância de estruturas legais robustas, recursos adequados e uma cultura de integridade para garantir a eficiência e confiança nas instituições públicas.

Com isso, a Organização estabelece diretrizes e recomendações internacionais sobre integridade pública, fornecendo subsídios aos países para desenvolverem suas próprias políticas e sistemas de *compliance*, com vistas ao combate à corrupção e à fraude, e à melhoria da boa governança. Além disso, a OCDE realiza avaliações de integridade pública em países membros, identificando pontos fortes e fracos em seus sistemas e emitindo recomendações para evolução. A Organização fornece ainda ferramentas e recursos, como o Kit de Ferramentas de Integridade Pública, para apoiar a implementação de medidas de integridade e gestão de riscos de integridade. Ademais, a Instituição enfatiza a importância de promover uma cultura de integridade no setor público, incentivando a ética, a transparência e a responsabilização, atuando em parceria com governos, organizações internacionais e sociedade civil. Por fim, a OCDE também se preocupa com a integridade no setor empresarial, incentivando as empresas a adotarem práticas éticas e a combater a corrupção e a fraude.

Desse modo, observa-se que a OCDE desempenha um papel fundamental no desenvolvimento e fortalecimento de sistemas de integridade pública, promovendo boas práticas e oferecendo suporte técnico aos países.

[81] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Manual de Integridade Pública da OCDE**. Paris: OECD Publishing, 2022. Disponível em: https://doi.org/10.1787/db62f5a7-pt. Acesso em 10 mai. 2025.

CAPÍTULO 2 – O MODELO DAS TRÊS LINHAS NO ORDENAMENTO JURÍDICO BRASILEIRO

A consolidação do Modelo das Três Linhas no ordenamento jurídico brasileiro traduz um marco evolutivo na formação da cultura de integridade e responsabilidade corporativa. Aperfeiçoado pelo IIA[82], em 2020, o modelo visa delimitar de forma clara as atribuições entre gestores operacionais (primeira linha), funções de controle e conformidade (segunda linha) e auditoria independente (terceira linha), assegurando a eficácia dos mecanismos internos de governança, controle de riscos e *compliance*.

No Brasil, a incorporação dos fundamentos desse modelo ocorreu de forma gradual, por meio de diversos diplomas legais e regulatórios que introduziram a exigência de estruturas de integridade, prevenção à corrupção e governança responsável. A partir da década de 2010, o país passou a adotar uma série de instrumentos normativos que reforçaram a integração entre os setores público e privado na promoção da ética corporativa, entre eles a Lei Anticorrupção (Lei n.º 12.846/2013), a Lei de Defesa da Concorrência (Lei n.º 12.529/2011), a Lei das Estatais (Lei n.º 13.303/2016), o Decreto n.º 11.129/2022, a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) e a Nova Lei de Licitações (Lei n.º 14.133/2021).

Essas normas, embora distintas em seus objetos, convergem em um mesmo eixo principiológico: a necessidade de promover transparência, *accountability* e prevenção de riscos institucionais. Sob essa ótica, o Modelo das Três Linhas não constitui apenas uma estrutura de controle interno, mas um paradigma de governança que passou a influenciar a formulação e a aplicação das políticas públicas de integridade no país.

O presente capítulo tem como objetivo examinar de que forma o Modelo das Três Linhas foi incorporado ao ordenamento jurídico brasileiro, analisando suas manifestações nas principais legislações de integridade e governança. Ao longo do texto, serão exploradas as bases legais que institucionalizam o *compliance* no Brasil, suas interfaces com o direito concorrencial, anticorrupção e de proteção de dados, bem como os desafios que persistem na aplicação efetiva desses instrumentos.

[82] THE INSTITUTE OF INTERNAL AUDITORS. **The IIA's Three Lines Model:** updated guidance. Lake Mary, FL: The Institute of Internal Auditors, 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Acesso em: 20 jun. 2025.

2.1 – Política de *Compliance* no Combate a Ilícitos Concorrenciais (Lei n.º 12.529/2011)

A Lei nº 12.529/2011, que estruturou o Sistema Brasileiro de Defesa da Concorrência (SBDC)[83], inaugurou um marco de modernização na política antitruste nacional, substituindo o modelo anterior da Lei nº 8.884/1994 e criando um sistema integrado de prevenção e repressão a infrações à ordem econômica. O Conselho Administrativo de Defesa Econômica (CADE) passou a exercer papel central como órgão de controle, instrução e julgamento de condutas anticoncorrenciais, dotado de autonomia técnica e decisória.

Embora a Lei nº 12.529/2011 não mencione expressamente o termo *compliance*, seu conteúdo e a atuação institucional do CADE impulsionaram a formação de uma cultura de conformidade concorrencial. O artigo 36 da referida lei define as infrações à ordem econômica como atos que tenham por objeto ou possam produzir os efeitos de limitar, falsear ou de qualquer forma prejudicar a livre concorrência ou a livre iniciativa. Nesse contexto, a observância a padrões éticos e preventivos se tornou componente essencial da política de defesa da concorrência.

O CADE, com vistas a promover práticas corporativas preventivas, publicou em 2016 o Guia de Programas de *Compliance* Concorrencial[84], documento técnico que sistematiza as diretrizes de implementação de programas internos de conformidade. O guia estabelece que os programas devem: 1) ser apoiados pela alta administração; 2) identificar e monitorar riscos concorrenciais; 3) promover treinamentos periódicos; e 4) prever mecanismos de denúncia e resposta disciplinar.

Esses quatro pilares coincidem com os fundamentos do Modelo das Três Linhas. Nesse sentido, tem-se que a primeira linha é representada por gestores operacionais e colaboradores, responsáveis pela execução das atividades comerciais em conformidade com as normas concorrenciais. Já a segunda linha é constituída pelas áreas de controle, *compliance* e assessoramento jurídico, incumbidas de orientar e supervisionar as práticas de mercado. Por fim, a terceira e última linha é

---

[83] BRASIL. **Lei nº 12.529, de 30 de novembro de 2011**. Estrutura o Sistema Brasileiro de Defesa da Concorrência. Diário Oficial da União, Brasília, DF, 1 dez. 2011.

[84] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia de programas de compliance concorrencial.** Brasília, DF: CADE, 2016. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-compliance-versao-oficial.pdf. Acesso em: 15 out. 2025.

materializada pela auditoria interna ou por revisões independentes, que avaliam a adequação e a efetividade do sistema de conformidade.

Essa estrutura reflete uma transição paradigmática: o *compliance* deixa de ser um instrumento de defesa reativa e passa a ser um mecanismo de governança preventiva, alinhado às recomendações internacionais da OCDE. De acordo com sua cartilha *The Good Practice Guidance on Internal Controls, Ethics and Compliance*[85], as corporações devem adotar controles internos capazes de prevenir, detectar e remediar infrações à legislação de concorrência e corrupção.

A obra de Misale[86] faz uma análise dos Termos de Compromisso de Cessação (TCCs) do CADE, celebrados sob a antiga Lei nº 8.884/94. O resultado dessa análise aponta que desde então já vinham sendo exigidos programas de *compliance* (ou compromisso de implementação) como condição do termo, sugerindo que esses mecanismos têm valor mitigador. Assim, nos julgamentos administrativos do CADE, programas de *compliance* concorrencial têm sido reconhecidos como circunstância atenuante na fixação de penalidades[87]. Essa tendência foi inclusive expressamente prevista no Guia de Programas de *Compliance* Concorrencial do CADE, que autoriza a consideração de mecanismos de prevenção e controle na dosimetria das multas[88].

O incentivo à autorregulação também dialoga com a política de leniência prevista na própria Lei nº 12.529/2011, cujo art. 86 institui o acordo de leniência como instrumento de colaboração empresarial para elucidação de infrações à ordem econômica. A existência de um programa de *compliance* efetivo é vista, na prática, como fator que facilita a detecção precoce de condutas ilícitas, além de reforçar o compromisso institucional da empresa com a ética e a transparência.

---

[85] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OECD). **Governments' Assessments of Corporate Anti-Corruption Compliance**. Paris: OECD, 2025. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/governments-assessments-of-corporate-anti-corruption-compliance_6100e758/e798903c-en.pdf. Acesso em: 10 mai. 2025.

MISALE, Guilherme Teno Castilho. **Programas de compliance à luz do ordenamento concorrencial brasileiro:** instrumentos de conformidade para a política anticartel. 2019. 190 f. Dissertação (Mestrado em Direito) — Faculdade de Direito, Universidade de São Paulo, São Paulo, 2019.

[87] Em uma análise crítica, tem-se que a maioria dos casos acessíveis não apresenta votos unânimes ou claras fundamentações que digam "redução da multa em razão do *compliance*". Em muitos casos, observa-se que o *compliance* figura como compromisso dentro de TCCs, cooperação ou exigência de cláusulas de conduta futura – mais como contrapartida que como atenuante autônomo. Ademais, a efetiva redução ou atenuação exige que o programa seja robusto, eficaz, e devidamente demonstrado nos autos, sendo que o ônus da prova recai sobre o representado (conforme o Guia do CADE).

[88] CADE, ref. 84.

Desse modo, pode-se concluir que o direito concorrencial brasileiro passou a integrar, mesmo que de forma implícita, os princípios estruturais do Modelo das Três Linhas, em especial quanto à atribuição de responsabilidades internas, à segregação de funções e à necessidade de auditoria independente. O resultado é um sistema mais equilibrado entre repressão estatal e prevenção corporativa, que fortalece a cultura de integridade empresarial e aproxima o Brasil dos padrões internacionais de governança concorrencial.

A incorporação do *compliance* concorrencial pelo CADE, portanto, não se limita a uma inovação administrativa: trata-se de uma manifestação normativa e institucional da primeira dimensão do Modelo das Três Linhas, no qual o Estado estimula as empresas a desenvolverem estruturas internas autônomas de controle, reduzindo a assimetria informacional e aumentando a eficiência regulatória.

2.2 – Lei Anticorrupção (Lei n.º 12.846/2013) e os Programas de Integridade

A promulgação da Lei n.º 12.846/2013 (Lei Anticorrupção Empresarial)[89], representou uma evolução da responsabilização corporativa no Brasil. Inspirada em legislações estrangeiras como o FCPA e o UKBA, a norma introduziu o regime de responsabilidade objetiva das pessoas jurídicas por atos de corrupção praticados contra a administração pública, nacional ou estrangeira.

Segundo Aguiar[90], antes da entrada em vigor da Lei Anticorrupção, havia no sistema jurídico brasileiro lacunas quanto à imputação de responsabilidade direta a empresas. A repressão a condutas ilícitas de natureza corporativa se limitava a sanções administrativas e civis dispersas, sem um marco normativo coeso voltado à integridade institucional. A Lei Anticorrupção, ao inovar nesse aspecto, não apenas instituiu novo modelo de responsabilização, como também promoveu a incorporação do *compliance* como instrumento de governança e de mitigação de riscos legais.

O art. 7º, inciso VIII, da Lei n.º 12.846/2013, estabelece expressamente que a existência de programa de integridade efetivo constitui fator relevante na dosimetria

[89] BRASIL. **Lei n.º 12.846, de 1º de agosto de 2013.** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. *Diário Oficial da União: seção 1*, Brasília, DF, 2 ago. 2013.
[90] AGUIAR, André Amaral de. **Responsabilidade objetiva na Lei Anticorrupção e compliance:** construção do conceito de culpabilidade de empresa na busca de uma política pública eficiente. São Paulo: Editora Dialética, 2022.

das penalidades aplicáveis às empresas condenadas. Trata-se de um reconhecimento normativo da importância do *compliance* como meio de prevenção e autorregulação, que permite à empresa demonstrar diligência e boa-fé na condução dos negócios.

Essa disposição concretiza, no plano legal, os fundamentos do Modelo das Três Linhas. A primeira linha, formada pelos gestores e colaboradores, deve atuar com integridade e aderência às normas; a segunda linha, composta pelas funções de controle e *compliance*, é responsável pela gestão de riscos, pela implementação de políticas anticorrupção e pela disseminação da cultura ética; e a terceira linha, representada pela auditoria interna ou externa, exerce função de supervisão e avaliação independente sobre a efetividade do sistema[91].

Com a regulamentação inicial promovida pelo antigo Decreto n.º 8.420/2015, e posteriormente aprimorada pelo Decreto n.º 11.129/2022[92], o programa de integridade deixou de ser mera expectativa de conduta para se tornar critério formal de avaliação administrativa. No ponto, vale destacar que o art. 56, inc. II, do novo decreto passou a prever de modo expresso a cultura de integridade no ambiente organizacional. Já o art. 57, do novel diploma elenca cinco dimensões de integridade corporativa, a saber: comprometimento da alta direção; padrões de conduta e código de ética; análise de riscos; comunicação e treinamento; e, por fim, transparência e medidas disciplinares.

Esses parâmetros conferem densidade jurídica ao conceito de *compliance*, integrando-o às práticas de governança e controle interno. Conforme observa Alencar e Varella[93], a institucionalização normativa do *compliance* representa a transição do discurso ético para o campo jurídico vinculante, em que a empresa é chamada a demonstrar não apenas intenções, mas resultados verificáveis de integridade.

Todavia, como se pode notar, o ordenamento jurídico pátrio trata o tema do *compliance* de forma concisa, limitando-se a elencar técnicas e instrumentos clássicos sem detalhar o funcionamento ou a aplicabilidade prática de cada um deles. Essa abordagem reducionista evidencia a necessidade de reflexão sobre os desafios da efetividade real dos programas de integridade, para além de uma mera formalidade

[91] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.
[92] BRASIL. **Decreto nº 11.129, de 11 de julho de 2022.** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e altera o Decreto nº 8.420, de 18 de março de 2015. *Diário Oficial da União: seção 1*, Brasília, DF, 12 jul. 2022.
[93] ALENCAR; VARELLA, ref. 61.

normativa, buscando compreender elementos culturais, comportamentais e métricos que sustentam sua implementação genuína.

Nesse sentido, segundo o professor Carvalho[94], um primeiro caminho para a efetividade do *compliance* estaria na formação de uma cultura organizacional baseada em valores éticos. Programas voltados à consolidação de princípios morais (*values-based*), mostram-se mais eficazes na prevenção de condutas ilícitas do que aqueles que se restringem à imposição de regras e sanções (*compliance-based*). A construção de uma cultura ética fortalece o compromisso individual dos colaboradores com a integridade, criando suporte necessário para o uso eficiente das ferramentas técnicas de conformidade. Assim, o equilíbrio entre valores e obediência normativa constitui a base de um sistema de integridade sustentável.

A segunda via ilustrada pelo professor, chamada *compliance* comportamental, propõe integração de conhecimentos das ciências comportamentais aos programas de conformidade. Essa perspectiva reconhece que, em regra, os indivíduos tendem a agir de forma honesta, de modo que políticas excessivamente punitivas podem gerar custos desnecessários e comprometer produtividade. Logo, o foco deve ser o estímulo de fatores psicológicos e culturais que favoreçam a adesão voluntária às normas.

Por fim, Carvalho destaca a importância de métricas confiáveis capazes de mensurar a efetividade dos programas. A ausência de indicadores objetivos prejudica tanto o controle público quanto a gestão privada, comprometendo a legitimidade e a credibilidade das políticas de integridade. Assim, a adoção de métricas robustas e imparciais é indispensável para distinguir programas efetivos de iniciativas simbólicas.

Desse modo, verifica-se que as reflexões trazidas por Carvalho ampliam a compreensão jurídica do *compliance* ao evidenciar que sua efetividade não depende só da existência formal de mecanismos de controle, mas da capacidade institucional de internalizar valores éticos, compreender determinantes comportamentais e aferir, de forma objetiva, os resultados obtidos. Essa abordagem multidimensional reforça o vínculo entre cultura organizacional e responsabilidade corporativa, aproximando o discurso da integridade da esfera de governança e do dever jurídico de prevenção.

É precisamente nesse ponto que o debate retorna ao campo normativo, pois a responsabilização objetiva introduzida pela Lei nº 12.846/2013 desloca o foco da conduta individual para a estrutura organizacional, reforçando a importância da

[94] CARVALHO, ref. 7.

segunda linha. No ponto, destaca-se que a negligência na estruturação e supervisão de controles internos pode ser considerada omissão corporativa relevante, sujeitando a pessoa jurídica a sanções severas, como multas de até 20% do faturamento bruto anual e publicação extraordinária da decisão condenatória.

Além disso, o art. 16, da Lei Anticorrupção instituiu o acordo de leniência, instrumento que permite à empresa colaboradora obter redução de penalidades mediante confissão e cooperação efetiva com as investigações. Este benefício está condicionado à demonstração de boa-fé e efetividade do programa de integridade, reconhecendo credibilidade negocial e valor probatório ao *compliance*.

Na prática, portanto, o sistema de integridade previsto na Lei nº 12.846/2013 pressupõe a atuação articulada das três linhas. A alta administração, como primeira linha, é responsável por dar o exemplo e fomentar a cultura ética (*tone at the top*); a área de *compliance*, como segunda linha, executa e monitora políticas e controles; e a auditoria, como terceira linha, verifica a conformidade e emite relatórios de melhoria contínua. Tal disposição institucional confere maior resiliência corporativa e contribui para a prevenção de riscos reputacionais e regulatórios.

Vale ainda destacar que a lei não impõe um modelo único de programa de integridade, mas, ao contrário, determina que sua estrutura seja proporcional ao porte, à complexidade e natureza das operações da empresa. Essa orientação, reproduzida no art. 57, §§ 1º e 2º, do Decreto n.º 11.129/2022[95], está alinhada às recomendações da CGU[96], segundo as quais a efetividade do *compliance* deve ser mensurada pela capacidade do programa de identificar, mitigar e responder a riscos específicos, e não apenas pela existência formal de códigos e políticas.

---

[95] Art. 57.
(...)
§ 1º Na avaliação dos parâmetros de que trata o caput, serão considerados o porte e as especificidades da pessoa jurídica, por meio de aspectos como:
I - a quantidade de funcionários, empregados e colaboradores;
II - o faturamento, levando ainda em consideração o fato de ser qualificada como microempresa ou empresa de pequeno porte;
III - a estrutura de governança corporativa e a complexidade de unidades internas, tais como departamentos, diretorias ou setores, ou da estruturação de grupo econômico;
IV - a utilização de agentes intermediários, como consultores ou representantes comerciais;
V - o setor do mercado em que atua;
VI - os países em que atua, direta ou indiretamente;
VII - o grau de interação com o setor público e a importância de contratações, investimentos e subsídios públicos, autorizações, licenças e permissões governamentais em suas operações; e
VIII - a quantidade e a localização das pessoas jurídicas que integram o grupo econômico.
§ 2º A efetividade do programa de integridade em relação ao ato lesivo objeto de apuração será considerada para fins da avaliação de que trata o caput.

[96] CONTROLADORIA GERAL DA UNIÃO (CGU), ref. 41.

Em síntese, a Lei Anticorrupção e seus regulamentos estabeleceram as bases jurídicas para a consolidação do Modelo das Três Linhas no setor privado brasileiro, vinculando o *compliance* à responsabilidade corporativa e à mitigação de sanções. Ao deslocar o enfoque do controle *ex post* (punitivo) para o controle *ex ante* (preventivo), o ordenamento jurídico brasileiro deu um passo decisivo rumo à consolidação de uma governança ética e sustentável.

2.3 – Decreto n.º 11.129/2022: Critérios Avaliativos da Efetividade do *Compliance*

O Decreto n.º 11.129/2022[97], em substituição ao antigo Decreto n.º 8.420/2015, aperfeiçoou a regulamentação da Lei n.º 12.846/2013, introduzindo um conjunto mais detalhado e objetivo de critérios para a avaliação da efetividade dos programas de integridade. Essa atualização normativa corrigiu lacunas e ambiguidades presentes no decreto anterior, aproximando o modelo brasileiro das práticas internacionais consolidadas no âmbito do *compliance* corporativo.

Em termos estruturais, o novo decreto reafirma a centralidade dos princípios de proporcionalidade, efetividade e verificabilidade, estabelecendo que o programa de integridade deve ser adequado ao porte, à estrutura, à complexidade e à natureza das atividades da pessoa jurídica. Tal disposição rompe com a visão meramente formal do *compliance* e introduz a noção de maturidade organizacional, reconhecendo que a efetividade não decorre da existência de documentos, mas da operacionalização de práticas integradas de controle e governança.

Nesse sentido, o art. 57, do novel decreto lista cinco eixos fundamentais, que orientam a avaliação dos programas de integridade, a saber: 1) comprometimento e apoio da alta direção (*tone at the top*); 2) padrões de conduta, código de ética e políticas de integridade; 3) análise e monitoramento contínuo de riscos; 4) ações de comunicação e de treinamento, bem como canais de denúncia; e 5) transparência, remediação e medidas disciplinares.

Esses eixos correspondem, em essência, à arquitetura do Modelo das Três Linhas[98]. A primeira linha está contemplada no compromisso da alta administração e dos gestores operacionais, que devem internalizar a cultura de integridade e adotar condutas exemplares. A segunda linha, composta pelas áreas de *compliance* e de

[97] BRASIL, ref. 92.
[98] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

controle interno, é responsável pela implementação das políticas, gestão dos riscos e disseminação dos valores éticos. Por fim, a terceira linha é constituída por instâncias de auditoria interna e de revisão independente, encarregadas de avaliar a efetividade dos controles e recomendar melhorias contínuas.

2.3.1. Da formalidade à mensuração de resultados

Dentre os principais avanços do Decreto n.º 11.129/2022, destaca-se a ênfase na mensuração empírica da efetividade dos programas de integridade. Ao elaborar o novo Manual de Avaliação de Programas de Integridade[99], a CGU passou a adotar indicadores qualitativos e quantitativos que medem o grau de aderência das empresas às boas práticas de *compliance*. Essa metodologia rompe com a lógica declaratória do decreto anterior e inaugura uma abordagem baseada em evidências, que exige documentação comprobatória, auditorias regulares e monitoramento contínuo.

Tal mudança aproxima o sistema brasileiro das diretrizes do DOJ e da SEC, que desde 2019 publicam o *Evaluation of Corporate Compliance Programs*[100], documento utilizado como referência global para medir a efetividade de estruturas de *compliance*. Nesse passo, o decreto brasileiro adota concepção semelhante ao considerar a efetividade como o grau em que o programa é capaz de prevenir, detectar e remediar atos lesivos.

Essa perspectiva funcional é igualmente compatível com o Modelo das Três Linhas, pois reconhece que a integridade corporativa é produto de um processo de interação contínua entre as três instâncias de defesa — gestão, controle e auditoria — e não uma estrutura estática ou meramente documental.

2.3.2. Proporcionalidade e análise de riscos

Outro ponto inovador do decreto é o realce na proporcionalidade do programa ao perfil de risco da organização. A norma aduz que a política de conformidade deve ser dimensionada conforme a natureza e complexidade das atividades desenvolvidas, a interação com o setor público e o grau de exposição a riscos de integridade.

---

[99] CONTROLADORIA-GERAL DA UNIÃO (CGU). **Plano de Integridade da Controladoria-Geral da União 2023–2025**. Brasília, DF: CGU, 2023. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/93464/1/Plano_Integridade_CGU_2023_2025.pdf. Acesso em: 1 nov. 2025.

[100] DEPARTMENT OF JUSTICE (DOJ). Criminal Division. **Evaluation of Corporate Compliance Programs**. Washington, D.C.: U.S. Department of Justice, 2024. Disponível em: https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=. Acesso em: 1 nov. 2025.

Esse enfoque é coerente com o conceito de *risk-based compliance*, que se tornou padrão internacional de governança e gestão de integridade. O *risk-based approach* implica que as empresas concentrem recursos de *compliance* nas áreas mais suscetíveis a ilícitos, evitando tanto a insuficiência quanto o excesso de controles. Desde 2010, a OCDE[101] já havia destacado que a proporcionalidade é elemento essencial da efetividade de programas de integridade, devendo as medidas adotadas ser ajustadas à natureza e à magnitude dos riscos enfrentados.

Sob a ótica do Modelo das Três Linhas, a proporcionalidade reforça o papel da segunda linha (*compliance* e gestão de riscos), que atua como elo intermediário entre a operação e a auditoria, transformando informações em planos de mitigação e resposta. Essa dimensão é crucial para que o *compliance* não se torne um mecanismo burocrático, mas um instrumento estratégico de tomada de decisão.

2.3.3. Governança, transparência e *accountability*

O Decreto n.º 11.129/2022 também enfatiza a importância da transparência e da governança corporativa como elementos constitutivos da integridade. Seu art. 57, nos incisos VI, VII, IX e X[102], determina que os programas devem incluir mecanismos de transparência e remediação, reforçando o dever de comunicação e a obrigação de corrigir irregularidades identificadas pelos controles internos.

Essa diretriz está alinhada à doutrina contemporânea de governança, que entende a transparência como instrumento de *accountability* horizontal, isto é, a responsabilização entre os diferentes níveis hierárquicos dentro da própria empresa, consoante escólio de Martins *et al*[103]. Nesse sentido, a governança corporativa eficaz

---

[101] OECD, ref. 85.

[102] "Art. 57. Para fins do disposto no inciso VIII do caput do art. 7º da Lei nº 12.846, de 2013, o programa de integridade será avaliado, quanto a sua existência e aplicação, de acordo com os seguintes parâmetros:
VI - registros contábeis que reflitam de forma completa e precisa as transações da pessoa jurídica;
VII - controles internos que assegurem a pronta elaboração e a confiabilidade de relatórios e demonstrações financeiras da pessoa jurídica;
IX - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e pela fiscalização de seu cumprimento;
X - canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e mecanismos destinados ao tratamento das denúncias e à proteção de denunciantes de boa-fé".

[103] MARTINS, Simone; TEIXEIRA, Marco Antonio Carvalho; PINEDA NEBOT, Carmen; PEÑA LÓPEZ, María Alejandra. **Transparência, accountability e governança pública**. Brasília, DF: Escola Nacional de Administração Pública (ENAP), 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4161/4/Transparencia.pdf. Acesso em: 2 nov. 2025.

requer a articulação de fluxos de informação e de responsabilização que permitam o monitoramento cruzado entre as linhas dentro do Modelo das Três Linhas.

A aplicação dessa lógica no contexto do decreto evidencia uma compreensão sistêmica do *compliance*, que ultrapassa o campo jurídico e se insere na esfera da gestão ética e organizacional. Assim, o *compliance* deixa de ser mero conjunto de normas internas, tornando-se uma ferramenta de governança e gestão de riscos integrados, capaz de fortalecer a confiança institucional e a reputação corporativa.

2.3.4. Integração com padrões internacionais de efetividade

A convergência do Decreto n.º 11.129/2022 com padrões internacionais é perceptível não apenas na linguagem, mas também na estrutura dos critérios de avaliação. O documento reflete as recomendações dos já mencionados *The Good Practice Guidance*, do UKBA (2011), e *Evaluation of Corporate Compliance Programs*.

Tais referências compartilham uma matriz comum: necessidade de demonstrar, de forma verificável, a autonomia funcional do *compliance*, a independência da auditoria e o comprometimento da alta administração. No caso brasileiro, o decreto salienta que a avaliação da efetividade não deve se restringir à forma, mas incluir a análise do engajamento real da alta direção, a autonomia dos responsáveis pelo programa e a implementação prática das políticas de integridade.

Essa abordagem confere densidade operacional ao Modelo das Três Linhas, pois traduz em parâmetros normativos o que antes era apenas uma diretriz de boas práticas. Vale frisar que a incorporação legislativa do conceito de autonomia funcional é particularmente relevante, uma vez que garante a independência da segunda e da terceira linhas em relação às pressões da gestão executiva.

Conforme Zaganelli[104], em termos comparativos, observa-se que o Decreto n.º 11.129/2022 é um dos regulamentos mais completos da América Latina em termos de integridade corporativa. Um estudo realizado pela OCDE[105] aponta que o Brasil vem desenvolvendo instrumentos de conformidade no setor público e de governança,

[104] ZAGANELLI, Margareth Vetis. Corrupção empresarial e compliance: um estudo comparado no Brasil e Argentina. **Humanidade & Tecnologia**, Curitiba, v. 57, p. 14–27, abr./jun. 2025. Disponível em: https://revistas.icesp.br/index.php/FINOM_Humanidade_Tecnologia/article/download/6235/3828. Acesso em: 2 nov. 2025.

[105] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Fortalecendo a Integridade Pública no Brasil:** Consolidando as Políticas de Integridade no Poder Executivo Federal. Paris: OECD Publishing, 2021. Disponível em: https://www.oecd.org/content/dam/oecd/pt/publications/reports/2021/12/strengthening-public-integrity-in-brazil_e7d2d27b/5414ae92-pt.pdf. Acesso em: 2 nov. 2025.

revelando maturidade crescente. Assim, a estrutura do decreto aproxima o Brasil de países desenvolvidos, que já adotam sistemas robustos de *compliance*, como os Estados Unidos, Reino Unido e França, reforçando o papel brasileiro como referência regional em regulação de integridade e combate à corrupção.

2.3.5. Síntese crítica

A análise do Decreto n.º 11.129/2022 permite afirmar que o Brasil alcançou um patamar normativo avançado na institucionalização da integridade corporativa. No entanto, de acordo com Oliveira[106], a efetividade prática do modelo depende de dois fatores essenciais: (i) a internalização da cultura de integridade pelas lideranças organizacionais; e (ii) a capacitação técnica das áreas de *compliance* e auditoria. Sem esses elementos, o decreto corre o risco de reproduzir um "*compliance* de fachada", no qual a estrutura formal existe, mas o compromisso ético é superficial.

Logo, o grande desafio reside em transformar a regulação em governança viva, em que as Três Linhas atuem de forma coordenada, integrando o controle jurídico, a gestão operacional e a auditoria independente. Essa visão integrada representa a maturidade do *compliance* no ordenamento brasileiro e a consolidação de um modelo que articula prevenção, transparência e responsabilidade corporativa.

2.4 – Lei das Estatais (Lei nº 13.303/2016): Exigência de Programa de Integridade

Para compreender o tema, há que se recordar que a Lei nº 13.303/2016[107] foi promulgada em um contexto de intensa crise de confiança nas instituições públicas e privadas brasileiras, decorrente de sucessivos escândalos de corrupção e má gestão envolvendo empresas estatais de grande porte, como a Petrobras e a Eletrobras. Inspirada em modelos de governança da OCDE, a norma estabeleceu marco jurídico inovador ao impor padrões de integridade, transparência e de controle interno às empresas públicas e sociedades de economia mista.

---

[106] OLIVEIRA, E. Compliance, Cultura de Integridade e Aliança para Boas Práticas. **Francis Yearbook of Legal Sciences & Human Rights**, Curitiba: Author's Edition, v. 1, n. 1, 2024. ISBN 978-65-00-97652-6. Disponível em: https://dialnet.unirioja.es/descarga/articulo/9571676.pdf. Acesso em: 2 nov. 2025.

[107] BRASIL. **Lei nº 13.303, de 30 de junho de 2016.** Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. *Diário Oficial da União*: seção 1, Brasília, DF, 1 jul. 2016.

O art. 9º da referida lei[108] determina que essas entidades devem adotar regras de estruturas de governança, de gestão de riscos e de controle interno, mecanismos de auditoria e programas de integridade e de conformidade. Tal disposição consolidou a obrigatoriedade do *compliance* como instrumento legal de governança pública, vinculando sua implementação a deveres de diligência dos administradores e à responsabilização de conselhos de administração e fiscal.

Na essência, a Lei nº 13.303/2016 internaliza o Modelo das Três Linhas, ao estruturar a gestão pública empresarial em três níveis funcionais interdependentes: primeira linha (L1: composta pela gestão operacional – diretores, superintendentes e gestores das unidades de negócio –, responsável pela condução das atividades e aderência às políticas de controles internos); segunda linha (L2: formada por funções de controle e conformidade, como unidades de *compliance*, corregedorias e comitês de riscos, cuja função é supervisionar, orientar e garantir a efetividade dos controles implementados); e terceira linha (L3: exercida pela auditoria interna e pelos conselhos fiscais, incumbidos de realizar avaliações independentes e emitir recomendações à alta administração e ao conselho de administração)[109].

Essa estrutura reflete o reconhecimento de que a governança das estatais não pode ser apenas formal, mas deve assegurar independência e coordenação entre as três linhas, para que cada uma faça seu papel sem interferência indevida das demais.

2.4.1. Governança e *accountability* nas empresas estatais

A Lei nº 13.303/2016 também reforçou os princípios de governança corporativa, transparência e *accountability*, introduzindo dispositivos que vinculam a nomeação e a atuação de administradores e conselheiros à observância de padrões éticos e de integridade. Nesse intuito, o art. 17 da referida norma[110] exige que os administradores

[108] Art. 9º A empresa pública e a sociedade de economia mista adotarão regras de estruturas e práticas de gestão de riscos e controle interno que abranjam:
I - ação dos administradores e empregados, por meio da implementação cotidiana de práticas de controle interno;
II - área responsável pela verificação de cumprimento de obrigações e de gestão de riscos;
III - auditoria interna e Comitê de Auditoria Estatutário".

[109] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

[110] "Art. 17. Os membros do Conselho de Administração e os indicados para os cargos de diretor, inclusive presidente, diretor-geral e diretor-presidente, serão escolhidos entre cidadãos de reputação ilibada e de notório conhecimento, devendo ser atendidos, alternativamente, um dos requisitos das alíneas "a", "b" e "c" do inciso I e, cumulativamente, os requisitos dos incisos II e III:
§ 2º É vedada a indicação, para o Conselho de Administração e para a diretoria:

de estatais tenham reputação ilibada, experiência profissional e ausência de conflito de interesses, prevenindo práticas de captura política e corporativa.

Essas exigências são complementadas pelas regras do art. 9º, que determinam a instituição de políticas de gestão de riscos e controles internos, visando à mitigação de desvios e ao fortalecimento da confiança pública. Em consonância com o Modelo das Três Linhas, a norma reforça o papel das instâncias de supervisão interna e externa como barreiras sucessivas de proteção contra a ineficiência, o abuso de poder e o uso indevido de recursos públicos.

Segundo Fontes Filho[111], a lei rompeu com a tradição patrimonialista do setor público nacional, ao impor uma lógica de governança baseada em responsabilidades claras, métricas de desempenho e supervisão independente. Tal ruptura foi essencial para alinhar as práticas de gestão das empresas estatais aos padrões internacionais de integridade recomendados pela OCDE – no *Guidelines on Corporate Governance of State-Owned Enterprises* (2015)[112] – que prevê a separação entre funções de gestão, controle e auditoria como elemento fundamental para a eficiência institucional.

2.4.2. A independência da auditoria e dos conselhos fiscais

Outro ponto de destaque da Lei nº 13.303/2016 é o fortalecimento da auditoria interna e dos conselhos fiscais, que passam a desempenhar papel estratégico na terceira linha. A norma estabelece que todas as empresas estatais deverão dispor de auditoria interna própria ou compartilhada, responsável por avaliar a adequação e a eficácia dos controles internos, da gestão de riscos e da governança. Ela determina ainda que resultados de auditorias internas sejam encaminhados diretamente ao

---

V - de pessoa que tenha ou possa ter qualquer forma de conflito de interesse com a pessoa político-administrativa controladora da empresa pública ou da sociedade de economia mista ou com a própria empresa ou sociedade".

[111] FONTES-FILHO, Joaquim Rubens. A governança corporativa em empresas estatais brasileiras frente à Lei de Responsabilidade das Estatais (Lei nº 13.303/2016). **Revista do Serviço Público**, Brasília, v. 69, edição especial "Repensando o Estado Brasileiro", p. 181-209, dez. 2018. Disponível em: https://repositorio.enap.gov.br/jspui/bitstream/1/5373/1/A%20governança%20corporativa%20em%20empresas%20estatais%20brasileiras%20frente%20à%20Lei%20de%20Responsabilidade%20das%20Estatais%20(Lei%20nº%2013.303-2016).pdf. Acesso em: 2 nov. 2025.

[112] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Guidelines on Corporate Governance of State-Owned Enterprises:** 2015 Edition. Paris: OECD Publishing, 2015. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/11/oecd-guidelines-on-corporate-governance-of-state-owned-enterprises-2015-edition_g1g5a749/9789264244160-en.pdf. Acesso em: 2 nov. 2025. DOI: 10.1787/9789264244160-en.

conselho de administração e ao conselho fiscal, criando um canal institucionalizado de supervisão cruzada (*cross accountability*).

Essa dinâmica fortalece a transparência horizontal dentro das estatais e assegura que falhas de controle ou irregularidades sejam comunicadas a instâncias capazes de adotar as medidas corretivas necessárias.

Na perspectiva do Modelo das Três Linhas, essa independência operacional se mostra essencial para evitar a captura das áreas de auditoria e *compliance* pelos interesses da gestão. Logo, a efetividade do sistema de integridade depende da capacidade de as segundas e terceiras linhas funcionarem como barreiras autônomas à pressão política e econômica, atuando como garantidoras da *accountability* pública.

2.4.3. O programa de integridade como instrumento de governança

O programa de integridade nas empresas estatais deve ser compreendido não apenas como um requisito formal, mas como instrumento de governança estratégica. Nesse sentido, o Decreto nº 8.945/2016[113], que regulamenta a Lei das Estatais no âmbito da União, reforça tal concepção ao exigir que os programas promovam a ética, a integridade, a prevenção e detecção de desvios, bem como o monitoramento e o aperfeiçoamento contínuo e a responsabilização de agentes e gestores.

Essa abordagem insere o *compliance* estatal dentro de uma lógica sistêmica de gestão pública responsável, integrando controles preventivos, auditorias corretivas e políticas de transparência. O Modelo das Três Linhas, neste contexto, oferece a arquitetura conceitual que permite organizar as funções de controle (*compliance*, gestão de riscos, auditoria, corregedoria e ouvidoria) de forma coordenada e eficiente.

2.4.4. Desafios de implementação e maturidade institucional

Apesar do rigor técnico e avanço normativo retratados na Lei das Estatais, sua efetividade enfrenta obstáculos estruturais e culturais: a relutância à consolidação de áreas de *compliance* autônomas, falta de capacitação técnica e a interferência política na gestão das estatais comprometem a efetividade do Modelo das Três Linhas.

[113] BRASIL. **Decreto nº 8.945, de 27 de dezembro de 2016**. Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias. *Diário Oficial da União*: seção 1, Brasília, DF, 28 dez. 2016.

Segundo levantamento feito pelo Instituto de Pesquisa Econômica Aplicada (IPEA)[114], as empresas estatais ainda estão em estágio inicial da implementação de programas de integridade formalizados e estruturados sob a coordenação de uma área responsável. Os dados revelam descompasso entre norma e prática, indicando que a maturidade institucional do sistema de integridade público está em construção.

Para superar tais desafios, é necessário que o *compliance* nas estatais seja incorporado à cultura organizacional, e não tratado como imposição formal. Não por outra razão, a Portaria CGU nº 226/2025[115] passou a exigir que os programas de integridade sejam genuinamente implantados e aperfeiçoados, demonstrando que a simples existência de códigos e normativos não garantiu a integridade ao longo dos anos. A capacitação de lideranças, o fortalecimento dos conselhos e a proteção da independência técnica das áreas de controle são condições indispensáveis para a plena efetividade do Modelo das Três Linhas no setor público.

Em síntese, os dados estatísticos inferidos do relatório e da atuação da CGU, como a necessidade de monitorar a efetividade e não apenas a conformidade formal, mostram o comprometimento sistêmico do Modelo das Três Linhas. A L1 (Gestão) está fragilizada e politicamente direcionada; a L2 (*Compliance*) atua formalmente e sem autonomia efetiva; e a L3 (Auditoria Interna) é sobrecarregada ao ter que auditar falhas crônicas de gestão e controle que deveriam ter sido prevenidas, limitando sua capacidade de agregar valor estratégico.

Logo, observa-se que a lacuna reside na diferença entre a adesão normativa (o que a Lei 13.303/2016 exige) e a funcionalidade operacional (o que a CGU realmente encontra, como "*compliance* de fachada" e a insuficiência documental nos programas de integridade). A efetividade da Lei das Estatais exige uma transformação cultural profunda – que a esfera pública empresarial, ainda marcada por vícios políticos e estruturais, resiste a incorporar. Portanto, o principal desafio da Lei nº 13.303/2016

[114] BOLETIM DE ANÁLISE POLÍTICO-INSTITUCIONAL: Avaliação de Integridade nas Estatais pela CGU. Rio de Janeiro: **Ipea**, n. 15, Jul.-Dez. 2018. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/boletim_analise_politico/180905_bapi_15_cap08.pdf. Acesso em: 4 nov. 2025.

[115] CONTROLADORIA-GERAL DA UNIÃO (CGU). **Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025**. Estabelece diretrizes para implementação e monitoramento de programas de integridade no âmbito da Administração Pública Federal direta, autárquica e fundacional. Brasília, DF: CGU, 2025. Disponível em: https://www.gov.br/ana/pt-br/acesso-a-informacao/integridade/normativos/arquivos/portaria-normativa-se_cgu-no-226-de-9-de-setembro-de-2025.pdf. Acesso em: 4 nov. 2025.

não é o texto legal, mas a persistência de uma cultura que desvincula o ato de gerir da responsabilidade técnica e do *accountability* genuíno.

2.5 – Governança Corporativa e *Compliance* na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD)[116] trouxe um novo paradigma regulatório para o Brasil, ao estabelecer regras gerais sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais no setor público e privado. De acordo com Doneda[117], a LGPD foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[118] e tutela os direitos fundamentais de privacidade e de autodeterminação informativa, criando obrigações organizacionais de governança e integridade informacional, com impactos diretos sobre a estrutura e as funções do *compliance* corporativo.

Diversamente de outras legislações, a LGPD tem natureza transversal, pois se aplica a todos os agentes de tratamento (públicos e privados), exigindo que cada um deles desenvolva um sistema interno de gestão de dados que assegure licitude, transparência e responsabilidade pelo tratamento. Esse sistema, por sua própria estrutura, reflete a lógica do Modelo das Três Linhas, ao determinar a integração entre gestores operacionais (primeira linha), funções de controle e conformidade (segunda linha) e auditorias e revisões independentes (terceira linha)[119].

2.5.1. O artigo 50 da LGPD e as regras de boas práticas e governança

O art. 50, da LGPD[120] previu expressamente o *compliance* como ferramenta de governança no contexto da proteção de dados. O dispositivo estimula os agentes de

---

[116] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.
[117] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.
[118] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – RGPD). **Jornal Oficial da União Europeia**, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 6 nov. 2025.
[119] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.
[120] "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os

tratamento a adotarem regras de boas práticas e de governança que estabeleçam condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, padrões técnicos e obrigações específicas para os diversos envolvidos no tratamento.

Esta previsão legal confere densidade jurídica ao *compliance* digital (conjunto de protocolos, políticas e práticas de segurança que uma organização adota para proteger dados e informações no ambiente virtual), ao reconhecer que a proteção de dados não se limita à observância formal da lei, mas requer a criação de estruturas institucionais de governança e controle. Assim, a norma do art. 50 transfaz a LGPD em um instrumento que articula as três linhas da integridade informacional.

Verifica-se, pois, que a primeira linha (gestores e operadores) atua para adotar práticas seguras, respeitando as bases legais do tratamento. Já a segunda linha (encarregado de dados, *compliance* e jurídico) visa monitorar e orientar a observância às normas. E a terceira linha (auditorias internas ou externas) opera na verificação independente da conformidade, identificando vulnerabilidades e propondo melhorias.

Nesse passo, ao regulamentar o art. 50, da LGPD, por seu *Guia Orientativo*[121], a Autoridade Nacional de Proteção de Dados (ANPD) reforçou a necessidade de que as empresas implementem mecanismos de auditoria, relatórios de impacto e políticas de revisão periódica, firmando o conceito de *data compliance*[122] como uma dimensão autônoma da integridade corporativa. De acordo com Tepedino, Frazão e Olívia[123], o programa de *compliance* de dados pessoais compreende a estruturação de políticas e procedimentos organizacionais voltados à conformidade com a lei de proteção de dados, à gestão de riscos e à responsabilidade corporativa no ciclo de vida dos dados.

---

procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais".

[121] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 6 nov. 2025.

[122] Refere-se à conformidade de dados, ou seja, a prática de gerenciar e utilizar dados em consonância com leis, regulamentos e padrões do setor, para garantir a segurança e a privacidade das informações. Envolve implementação de políticas e procedimentos para coletar, armazenar, processar e compartilhar dados de forma responsável e ética, protegendo-os contra acesso não autorizado e uso indevido.

[123] TEPEDINO, Gustavo; FRAZÃO, Ana de Oliveira; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 3. ed., rev., atual. e ampl. São Paulo: Thomson Reuters Revista dos Tribunais, 2023.

2.5.2. O papel do encarregado de dados (DPO) na segunda linha

Tal qual previsto na legislação europeia (GDPR), a LGPD introduziu a figura do encarregado pelo tratamento de dados pessoais (*Data Protection Officer* - DPO). O tema vem tratado nos artigos 5º, inc. VIII, 23, inc. III, e 41, da lei brasileira[124]. Esse profissional funciona como ponto de contato entre o controlador, os titulares e a ANPD, de modo que sua função abrange tanto atividades de orientação e supervisão quanto de coordenação do sistema de conformidade interna.

Dada a relevância desse agente, a ANPD lançou, em 2024, Guia Orientativo[125] para regulamentar sua atuação. Na prática, o DPO opera na segunda linha, dentro do Modelo das Três Linhas: supervisiona gestores operacionais (primeira linha), promove o treinamento e o alinhamento das práticas de tratamento e se reporta à alta administração e à autoridade reguladora.

Logo, denota-se que a independência técnica do encarregado é essencial para a efetividade da governança de dados, devendo dispor de autonomia funcional e ausência de conflito de interesses para exercer seu papel de forma plena. Essa diretriz, replicada pela ANPD em pareceres e orientações normativas, reforça o caráter de controle autônomo típico da segunda linha.

---

[124] "Art. 5º Para os fins desta Lei, considera-se:
(...)
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD".
"Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
(...)
III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei".
"Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados".

[125] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo - Atuação do encarregado pelo tratamento de dados pessoais**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf. Acesso em: 6 nov. 2025.

O DPO, portanto, constitui o elo entre o *compliance* digital e o *compliance* corporativo, integrando as políticas de privacidade aos sistemas mais amplos de integridade empresarial. Sua atuação deve estar articulada às demais instâncias de controle, como auditoria interna, segurança da informação e governança corporativa, consolidando uma abordagem transversal da conformidade.

2.5.3. Auditorias e *accountability* informacional

A terceira linha, no contexto da LGPD, manifesta-se pelas auditorias internas e externas de conformidade digital. Tais auditorias visam avaliar a eficácia das políticas de privacidade, a robustez dos mecanismos de segurança da informação e o grau de aderência das práticas organizacionais às normas de proteção de dados.

O art. 50, da LGPD recomenda expressamente a existência de mecanismos internos e externos de supervisão e auditoria para verificar o cumprimento de normas. Esse comando normativo consolida a ideia de que a conformidade em matéria de dados pessoais depende de avaliações independentes e periódicas, que constituem a essência da terceira linha.

Ademais, a LGPD trouxe o conceito de relatório de impacto à proteção de dados pessoais, no art. 5º, inc. XVII. Tal relatório, elaborado pelo controlador, deve descrever os processos de tratamento de dados pessoais que podem gerar riscos a liberdades civis e a direitos fundamentais e demonstrar as medidas, salvaguardas e mecanismos de mitigação de risco adotados. Trata-se de instrumento que operacionaliza o princípio da *accountability*, traduzindo o dever de prestar contas verificáveis e auditáveis.

Nessa perspectiva, destaca Reis[126] que a proteção de dados pessoais passa a integrar o núcleo do *compliance* moderno, estruturado não apenas no cumprimento de normas, mas na demonstração ativa de conformidade. Assim, a LGPD inaugura uma nova geração de *compliance*, em que o foco se desloca da obediência formal para a capacidade de gestão responsável e transparente das informações.

2.5.4. Cultura de privacidade e integração com o Modelo das Três Linhas

[126] REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho**, São Paulo, v. 214, p. 323-340, nov./dez. 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/ewp-m/documents/brazil/pt/pdf/other/rdt-214-a-cultura-de-compliance-em-materia.pdf?utm_source. Acesso em: 6 nov. 2025.

A efetividade do *compliance digital* depende, sobretudo, da internalização da cultura de privacidade na organização. Essa cultura deve permear o Modelo das Três Linhas: na primeira linha, os colaboradores precisam compreender a relevância ética e jurídica da proteção de dados; já na segunda linha, o DPO e a área de *compliance* devem promover políticas contínuas de capacitação e atualização; na terceira linha, a auditoria deve garantir que o ciclo de revisão e melhoria dos controles seja constante.

Dessa forma, a LGPD não apenas cria obrigações jurídicas, mas reformula a concepção de governança, passando a informação a ser concebida como um ativo estratégico e a proteção de dados como expressão contemporânea da integridade corporativa. Ao exigir transparência, prestação de contas e revisões independentes, a LGPD consolida a dimensão informacional do Modelo das Três Linhas, projetando o *compliance* como eixo central da confiança digital e institucional.

2.6 – Nova Lei de Licitações (Lei nº 14.133/2021): Exigências e Incentivos à Integridade

A Lei nº 14.133/2021[127] representa a mais ampla reforma do regime jurídico das contratações públicas desde a promulgação da Lei nº 8.666/1993. Em um cenário pós-*Lava Jato*, no qual a corrupção sistêmica evidenciou as fragilidades dos mecanismos de controle público, o legislador optou por incorporar, de forma explícita, princípios e estruturas de *compliance* e governança corporativa ao novo modelo de contratações.

No ponto, a maior inovação está no art. 25, §4º, da Nova Lei de Licitações, que prevê a obrigatoriedade de programas de integridade para as empresas vencedoras de licitações de grande vulto, conforme parâmetros definidos em regulamento. Obras, serviços e fornecimentos de grande vulto são aqueles cujo valor estimado supera R$ 200.000.000,00 (duzentos milhões de reais), conforme art. 6º, inc. XXII. Nesses casos, as empresas contratadas deverão implementar, no prazo de seis meses, programa de *compliance* compatível com o objeto, a complexidade e os riscos da contratação.

Esta previsão normativa consolida a integração entre o Direito Administrativo e os programas de conformidade, incorporando formalmente o Modelo das Três Linhas à gestão de contratações públicas. De modo inédito, a integridade deixa de ser apenas

[127] BRASIL. **Lei nº 14.133, de 1º de abril de 2021**. Lei de Licitações e Contratos Administrativos. *Diário Oficial da União*, Brasília, DF, 1 abr. 2021.

um valor ético desejável e passa a constituir condição jurídica de execução contratual, vinculando diretamente a conformidade à eficiência administrativa e à probidade.

2.6.1. A integridade como requisito jurídico das contratações

A nova exigência legal dos programas de integridade consagra o princípio da prevenção de riscos de corrupção como eixo central da governança contratual. Tal determinação está em harmonia com o art. 7º, inc. VIII, da Lei nº 12.846/2013, que já previa a existência de programa de integridade efetivo como fator a ser considerado na dosimetria das penas aplicáveis a empresas condenadas. A Lei nº 14.133/2021, no entanto, vai além desse mero benefício legal e cria uma obrigação para contratar, reforçando a ideia de que a integridade é um dever de cuidado institucional imposto ao setor privado quando este interage com o poder público.

A imposição de programas de integridade também representa um mecanismo de seleção adversa positiva, pois favorece a participação de organizações melhor estruturadas, dotadas de controles internos e mecanismos de prevenção. Segundo o guia “Programa de Integridade: Diretrizes para Empresas Privadas (vol. II)”[128], a exigência de *compliance* em contratações de grande vulto visa a reduzir assimetrias de informação e a prevenir riscos de fraude e conluio entre empresas.

Dessa forma, a lei fortalece o Modelo das Três Linhas[129], na medida em que: a primeira linha exige que gestores e operadores atuem em conformidade com padrões éticos e legais; a segunda linha supervisiona e orienta a execução contratual, incluindo as áreas de *compliance* das empresas contratadas e os órgãos de controle interno dos entes públicos; e a terceira linha repassa às auditorias e tribunais de contas a função de avaliar, de forma independente, a integridade e eficiência das contratações.

2.6.2. Incentivos e sanções vinculadas ao *compliance*

A Nova Lei de Licitações também introduziu incentivos e sanções relacionados à existência e efetividade de programas de integridade. Em seu art. 156, §1º, inc. V, a lei aduz que a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades poderá ser considerada atenuante na aplicação de sanções administrativas, desde que comprovada sua efetividade.

[128] CONTROLADORIA GERAL DA UNIÃO (CGU), ref. 41.
[129] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

Por outro lado, a inexistência de controles internos poderá ser considerada agravante na dosimetria da penalidade.

Esse mecanismo reproduz a lógica da Lei Anticorrupção, segundo a qual o *compliance* é fator de mitigação de responsabilidade. Entretanto, a Lei nº 14.133/2021 amplia o alcance dessa lógica para o âmbito contratual e administrativo, de modo que a integridade passa a ser também critério de avaliação de desempenho e continuidade das relações contratuais. Em perspectiva sistêmica, tal correlação entre integridade e incentivos revela a adoção de um modelo de regulação responsiva, em que o Estado alterna estratégias de controle com mecanismos de apoio ao cumprimento voluntário.

Os programas de *compliance* e integridade operam, portanto, como tecnologias de governança, pois introduzem mecanismos estruturados de controle, transparência, monitoramento e responsabilização. Segundo Oliveira[130], isso permite ao Estado e ao contratado convergirem para uma lógica de confiança recíproca, fator que pode até mesmo contribuir para a redução dos custos de supervisão.

2.6.3. Governança pública e o Modelo das Três Linhas na execução contratual

A Lei nº 14.133/2021 insere o *compliance* no centro da governança pública, ao reconhecer que a integridade é elemento crucial da eficiência e da economicidade na execução de contratos. O art. 11, parágrafo único, da lei estipula que as contratações observem os princípios da governança, transparência e responsabilização. O art. 169, por sua vez, reforça que os entes públicos devem implementar mecanismos de controle interno e auditoria voltados à gestão contratual, trazendo expressamente na legislação as três linhas.

Essas previsões normativas se articulam diretamente com o Modelo das Três Linhas. Nesse sentido, tem-se que, na primeira linha, o gestor do contrato atua como responsável direto pela execução e pela conformidade das atividades contratadas. Na segunda linha, as unidades de controle interno, corregedorias e áreas de *compliance* supervisionam os riscos de integridade, fornecendo orientação técnica e verificando a aderência às políticas públicas. Por fim, na terceira linha, as auditorias internas e

[130] OLIVEIRA, Nildete dos Passos. **Governança pública:** um estudo sobre os mecanismos de controle interno e transparência pública no Brasil. 2017. Dissertação (Mestrado em Administração Pública) – Universidade de Brasília, Brasília, 2017. Disponível em: https://repositorio.unb.br/bitstream/10482/31508/1/2017_NildetedosPassosOliveira.pdf. Acesso em: 8 nov. 2025.

externas (incluindo os tribunais de contas) realizam avaliações independentes sobre a legalidade, a economicidade e a efetividade dos contratos.

O TCU, em seu *Referencial Básico de Governança Organizacional*[131], insere o Modelo das Três Linhas como estrutura de boas práticas aplicável ao setor público brasileiro e recomenda sua adoção por órgãos de controle e unidades executoras de políticas públicas. Assim, a Nova Lei de Licitações institucionaliza o modelo como infraestrutura de governança pública, promovendo a coordenação entre gestores, controles internos e auditorias independentes.

2.6.4. *Compliance* e inovação regulatória nas contratações públicas

É evidente que a Lei nº 14.133/2021 modernizou a regulação contratual, ao prever a conformidade como vetor de inovação e sustentabilidade. Nessa trilha, o Relatório de Gestão (2024), da CGU[132], revela que a exigência de programas de *compliance* em licitações de grande vulto impulsiona o desenvolvimento de soluções tecnológicas voltadas à gestão de riscos, como plataformas de integridade, *due diligence* automatizada e monitoramento contínuo de contratos.

Tal perspectiva se alinha à tendência global de governança regulatória baseada em dados (*data-driven governance*), em que os mecanismos de controle se apoiam em tecnologia, análise preditiva e transparência digital para reduzir o espaço de discricionariedade e de corrupção, consoante se denota do escólio de Bitencourt[133]. Assim, conforme "Manual de Integridade Pública da OCDE"[134], o *compliance* passa a ser entendido não apenas como mecanismo de defesa jurídica, mas como instrumento de inovação institucional, capaz de aprimorar a eficiência, a legitimidade, bem como a previsibilidade das contratações públicas.

O desafio, contudo, permanece na implementação efetiva dessas estruturas, especialmente nos níveis subnacionais, onde a capacitação técnica e a cultura de

---

[131] TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial básico de governança organizacional: *3ª edição.*** Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2020. Disponível em: https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf. Acesso em: 7 nov. 2025.

[132] CONTROLADORIA-GERAL DA UNIÃO (CGU). **Relatório de Gestão – 2024**. Brasília, DF: CGU, 2024. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/auditorias/arquivos/2024/RelatorioGestao2024.pdf. Acesso em: 8 nov. 2025.

[133] BITENCOURT, C. M. A inteligência artificial nos órgãos constitucionais de controle de contas públicas: tornar transparente suas funções e resultados. **Revista Interdisciplinar de Controle e Gestão Pública**, 2023. Disponível em: https://www.scielo.br/j/rinc/a/WJgdHhvqpvyr7XnHhMN39Wz/?lang=pt. Acesso em: 8 nov. 2025.

[134] OCDE, ref. 81.

integridade ainda são limitadas. A plena consolidação do Modelo das Três Linhas na administração pública nacional exigirá não apenas normas, mas lideranças éticas, cultura organizacional e compromisso político com a transparência e a eficiência.

CAPÍTULO 3 – MODELO DAS TRÊS LINHAS: ESTRUTURA, EFETIVIDADE E PERSPECTIVAS DE APERFEIÇOAMENTO NO CONTEXTO BRASILEIRO

Encerrada a análise teórica e normativa sobre os fundamentos do *compliance* e dos sistemas de integridade corporativa abordados nos capítulos anteriores, impõe-se o aprofundamento da discussão acerca dos instrumentos de governança que sustentam a efetividade desses mecanismos no âmbito organizacional.

Nesse intuito, surge o Modelo das Três Linhas (M3L), concebido como estrutura de referência internacional que fornece um método simples e eficaz para melhorar a comunicação e o esclarecimento dos papéis e responsabilidades no gerenciamento de riscos, controles internos e auditoria. A adoção desse modelo tem assegurado a coerência e eficácia dos programas de *compliance*, ao definir fronteiras funcionais claras entre as áreas operacionais, de controle e de avaliação independente.

Assim, o presente capítulo tem por objetivo examinar a estrutura, a aplicação e a efetividade do M3L, que evoluiu de uma lógica puramente defensiva para uma abordagem que visa a criação de valor. O estudo se debruça nos pilares do modelo original de 2013 e na subsequente atualização de 2020, explorando as mudanças conceituais e suas implicações.

O tópico ainda examina criticamente os debates sobre sua eficácia, os desafios práticos de implementação, as limitações culturais e oportunidades de aprimoramento normativo e institucional. Por fim, detalha-se a recepção e aplicação do modelo no ordenamento jurídico e nas instituições brasileiras, destacando a sua relevância para o campo da pesquisa jurídica e do Direito Administrativo.

3.1 – Origem e Evolução do Modelo das Três Linhas

Segundo Chambers[135], embora seja comum a crença de que o IIA tenha criado o modelo das Três Linhas de Defesa, sua formulação original é objeto de controvérsia. O IIA não foi o responsável por desenvolver o sistema, mas, em 2013, divulgou uma declaração de posicionamento que o endossava, destacando especialmente o papel

[135] INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. **O The IIA redesenhará as Linhas de Defesa?** São Paulo: IIA Brasil, [s.d.]. Disponível em: https://iiabrasil.org.br/noticia/o-the-iia-redesenhara-as-linhas-de-defesa. Acesso em: 11 nov. 2025.
Richard F. Chambers atuou, de 2009 a 2021, como presidente e CEO do Instituto de Auditores Internos (IIA), a associação profissional global e órgão normatizador para auditores internos.

essencial da auditoria interna como terceira linha, responsável por fornecer avaliações independentes dentro das organizações.

O documento intitulado “As Três Linhas de Defesa”[136] foi formalmente publicado pelo IIA, em 2013, com o objetivo de fornecer um arcabouço abrangente para a gestão de riscos e o controle interno dentro de uma organização. A premissa central do modelo era a clara separação e a atribuição de papéis e responsabilidades para evitar lacunas na cobertura de riscos e a desnecessária duplicação de esforços. Ele se baseava na ideia de que três grupos distintos e complementares eram essenciais para a gestão eficaz de riscos e o controle.

A Primeira Linha de Defesa era composta pela gestão operacional e pelos procedimentos de rotina. Essa linha era responsável por gerenciar e possuir os riscos no dia a dia. Incluía os gerentes e os funcionários da linha de frente que, por meio do desenvolvimento e implementação de políticas e procedimentos internos, buscavam mitigar riscos e garantir que as atividades estivessem em conformidade com as metas e os objetivos organizacionais. A primeira linha, portanto, era a proprietária dos riscos e a responsável direta por controlá-los.

A Segunda Linha de Defesa era formada por funções de apoio, monitoramento e supervisão. Ela incluía departamentos como o de gestão de riscos, *compliance*, segurança, controle financeiro e o jurídico. O papel dessa linha era ajudar a primeira linha a gerenciar riscos de forma mais eficaz, fornecendo diretrizes, ferramentas e metodologias. As funções da segunda linha, apesar de fazerem parte da gestão, tinham a responsabilidade de monitorar a eficácia dos controles e de desafiar as ações da primeira linha, reportando-se à alta gestão.

A Terceira Linha de Defesa era formada pela auditoria interna. Seu principal papel era assegurar uma avaliação independente e objetiva à alta administração e aos órgãos de governança (conselho de administração, comitê de auditoria) sobre a eficácia da governança, da gestão de riscos e dos controles internos, incluindo os controles da primeira e segunda linhas. Assim, a auditoria interna atuava de forma independente da gestão e se reportava diretamente ao órgão de governança, garantindo sua objetividade. Diferentemente das outras linhas, a terceira linha não era

[136] THE INSTITUTE OF INTERNAL AUDITORS. **As três linhas de defesa no gerenciamento eficaz de riscos e controles**. Altamonte Springs, FL: The Institute of Internal Auditors, 2013. Declaração de posicionamento. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/as-trs-linhas-d-ippf-00000010-28082019095801.pdf. Acesso em: 11 nov. 2025.

responsável por gerenciar riscos ou implementar controles, mas sim por avaliá-los e oferecer recomendações para melhoria.

Apesar da ampla adoção, o modelo clássico foi alvo de críticas contundentes. A principal delas era a sua própria terminologia. O foco exclusivo em "defesa" levava a uma percepção reativa e passiva da gestão de riscos, priorizando a proteção do valor existente em detrimento da criação de novo valor. A metáfora de uma série de barreiras passivas sugeria que a falha de uma linha seria contida pela próxima, mas não incentivava a colaboração ou a proatividade na identificação de oportunidades de risco. A abordagem puramente defensiva, portanto, podia inibir a inovação e o crescimento, que muitas vezes exigem a tomada de riscos calculados.

Além disso, a estrutura rígida e hierárquica do modelo tendia a fomentar uma mentalidade de "silos" dentro da organização, em que as funções operavam de forma isolada, com pouca comunicação. Essa falta de coordenação e colaboração resultava em uma duplicidade de esforços, com a segunda e a terceira linhas realizando testes sobre os mesmos controles, o que gerava a "fadiga de auditoria" na primeira linha e desviava o foco de suas atividades de negócio.

Problema ainda mais grave era a relação potencialmente adversarial entre as linhas. Dada a rigidez do sistema, a primeira linha podia passar a ver a segunda e a terceira linhas como entidades fiscalizadoras, que apenas estariam preocupadas em apontar seus erros, diminuindo, pois, a viabilidade da formação de parcerias entre as linhas. Nesse ponto, a auditoria interna, em particular, era frequentemente percebida como uma função combativa, reacionária e retrospectiva, minando o potencial de uma abordagem mais colaborativa e construtiva.

Ademais, em certas situações, o fortalecimento excessivo da segunda linha acarretava o descuido da primeira linha de suas responsabilidades no gerenciamento de riscos, acreditando que a função havia sido assumida pelas áreas de apoio.

Em resposta às críticas e visando acompanhar a evolução do gerenciamento de riscos e da governança, o IIA iniciou um processo de revisão que culminou na publicação do "Modelo das Três Linhas", em 2020[137]. O objetivo da atualização era claro: refletir as mudanças no cenário corporativo e aprofundar o entendimento sobre as funções de controle, preservando a abordagem direta e clara do modelo original.

[137] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

O projeto de revisão envolveu um grupo de trabalho global e incorporou os pareceres de especialistas e partes interessadas do mundo todo, garantindo uma abordagem abrangente e consensual acerca do tema[138].

A alteração mais notável foi a remoção da palavra "defesa" do nome do modelo. Mais do que uma simples mudança semântica, a revisão representou uma profunda transição de um paradigma reativo para um proativo e estratégico. A nova proposta enfatiza menos a "proteção passiva" e mais a "colaboração, integração e contribuição estratégica para a governança". A gestão de riscos passa a ser vista não apenas como uma forma de proteger a organização de perdas, mas como um meio de "ajudar as organizações a identificar estruturas e processos que facilitem uma forte governança e gerenciamento de riscos" e, consequentemente, que ajudem a atingir os objetivos e criar valor. Essa mudança de paradigma abordou diretamente a crítica central ao modelo anterior, ao reconhecer que a gestão de riscos tem tanto um aspecto ofensivo (tomar riscos para criar valor) quanto um defensivo (proteger o valor).

O novo modelo delineia as funções e responsabilidades da gestão executiva, da auditoria interna e, de forma mais proeminente, do corpo administrativo (conselho e comitês). A principal alteração é o posicionamento do órgão de governança acima das linhas. A responsabilidade para definir o apetite a riscos da organização e para supervisionar a eficácia do modelo é explicitamente atribuída ao conselho, fator que fortalece a governança e a responsabilização, garantindo que o gerenciamento de riscos esteja alinhado com a estratégia geral da companhia.

Conforme Chambers[139], o novo M3L introduz uma transformação significativa ao ser estruturado sobre seis princípios fundamentais. O primeiro estabelece que a governança organizacional depende da existência de estruturas e processos que assegurem responsabilidade, ação efetiva e avaliação contínua. O segundo enfatiza que o corpo administrativo deve garantir a aplicação dessas estruturas e processos, proporcionando uma governança sólida e eficiente.

O terceiro princípio define que a gestão, responsável pelo alcance dos objetivos institucionais, atua por meio das funções da primeira e da segunda linha: a primeira,

[138] INSTITUTO DOS AUDITORES INTERNOS DO BRASIL, ref. 135.
[139] INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. *Novo modelo das Três Linhas do IIA oferece evolução tempestiva de uma ferramenta confiável.* São Paulo: IIA Brasil, 25 ago. 2020. Disponível em: https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-oferece-evolucao-tempestiva-de-uma-ferramenta-confiavel. Acesso em: 11 nov. 2025.

mais próxima da entrega de produtos e serviços e das atividades de suporte; e a segunda, dedicada ao apoio no gerenciamento de riscos.

O quarto princípio atribui à auditoria interna, enquanto terceira linha, a função de realizar avaliações e consultorias independentes e imparciais sobre a adequação e a eficácia da governança e da gestão de riscos. Essa atuação se baseia na aplicação sistemática e disciplinada de metodologias, competências técnicas e conhecimentos especializados, podendo incluir a consideração de análises realizadas por avaliadores internos e externos.

O quinto princípio reforça que a independência da auditoria interna em relação às funções gerenciais é indispensável para garantir sua objetividade, autoridade e credibilidade. No entanto, a independência não implica isolamento, devendo haver interação regular entre auditoria interna e gestão. Por fim, o sexto princípio reconhece que todas as funções envolvidas — quando atuam de forma coordenada e alinhada aos interesses estratégicos das partes interessadas — contribuem para a criação, preservação e fortalecimento do valor organizacional.

Desse modo, as funções da primeira e segunda linhas foram tornadas mais fluidas. O novo modelo sugere que as organizações podem "misturar" (*blending*) as responsabilidades da primeira e da segunda linha, aumentando a comunicação e a colaboração. A segunda linha é agora concebida como uma fonte de "expertise, apoio, monitoramento e desafio" para a primeira, e não como uma entidade separada e hierarquicamente superior.

A auditoria interna, por sua vez, deixa de ser vista somente como a "última barreira de controle" e passa a ser uma parceira estratégica na criação de valor e no fortalecimento do sistema como um todo. Seu papel evolui de uma visão puramente retrospectiva para uma abordagem mais proativa, fornecendo aconselhamento e antecipando riscos emergentes para o conselho.

A evolução do modelo demonstra uma compreensão sofisticada do tema, na medida em que a conformidade e a gestão de riscos são vistas não como obrigações burocráticas, mas como componentes essenciais para a resiliência e competitividade organizacional. Um sistema eficiente, nesse contexto, não se limita a prevenir perdas, mas também otimiza a capacidade da empresa de alcançar seus objetivos e gerar resultados sustentáveis. A tabela abaixo sintetiza as principais diferenças entre as duas versões do modelo, destacando a evolução de sua filosofia:

Aspecto	Modelo Clássico (2013)	Novo Modelo (IIA 2020)
Terminologia	"Três Linhas de Defesa"	"Modelo das Três Linhas"
Filosofia Central	Reativa e defensiva, focada na proteção de valor	Proativa e estratégica, focada na criação e na proteção de valor
Relacionamento entre Linhas	Rígido e segregado (mentalidade de silos)	Colaborativo e integrado (*blending* das funções)
Papel da Governança	Implícito e limitado à supervisão geral	Explícito e central, com responsabilidade de definir riscos e supervisionar
Foco Principal	Gerenciamento de riscos e controles como barreiras de proteção	Gerenciamento de riscos como facilitador para atingir objetivos

Tabela 1: Comparativo: Modelo das Três Linhas de Defesa Clássico (2013) vs. Modelo das Três Linhas (IIA 2020)

3.2 – Estrutura Funcional do Novo Modelo

A estrutura de governança, risco e controle de uma organização complexa exige uma alocação clara de responsabilidades que evite lacunas e redundâncias. O M3L surge como um arcabouço conceitual fundamental, redefinindo as funções e o relacionamento entre os órgãos responsáveis pela gestão de riscos e pelo provimento de asseguramento. Este modelo, em sua concepção revisada, posiciona o conselho e a administração superior no topo, como elementos de governança, e estrutura a gestão e o asseguramento em três camadas funcionais distintas e interconectadas.

A funcionalidade do M3L reside na sua capacidade de segregar deveres, garantindo que a tomada de risco (primeira linha) seja balanceada pelo monitoramento especializado (segunda linha) e sujeita à avaliação independente (terceira linha). Essa separação não implica isolamento, mas sim uma parceria coesa destinada a criar e proteger o valor organizacional de forma sustentável.

3.2.1. Primeira linha: gestores operacionais e áreas de negócio

A primeira linha constitui o pilar operacional do M3L. Ela engloba os gestores e colaboradores, os quais possuem a responsabilidade primária pela execução das atividades, pela entrega dos produtos e serviços e pela consecução dos objetivos organizacionais. Sua essência reside na propriedade do risco.

Assim, as equipes de primeira linha são responsáveis por identificar, avaliar, controlar e mitigar proativamente os riscos inerentes a suas operações diárias. Essas tarefas se manifestam das seguintes formas: i) implementação de controles (desenho e operação de controles internos básicos, geralmente preventivos e detectivos, em nível transacional e processual); ii) decisão e risco (tomada de decisões operacionais que, por natureza, envolvem a assunção de riscos - os gestores operacionais são os principais *risk owners*, pois suas ações determinam a exposição imediata da organização); e iii) conformidade operacional (assegurar que os procedimentos sejam executados em conformidade com as leis, regulamentos internos e as políticas definidas pela segunda linha).

A eficácia desta linha é importante, pois atua como primeiro filtro de contenção. Uma primeira linha fraca eleva o risco residual, sobrecarregando as demais linhas e, em última análise, o capital da organização. Logo, o sucesso da estrutura depende da internalização da cultura de risco e controle pelos gestores de negócio, transformando a gestão de riscos de uma função de *staff* para uma competência de *linha*. Em outras palavras, significa mudar a responsabilidade primária pela gestão de riscos de uma equipe de apoio especializada para gerentes e colaboradores, que estão diretamente envolvidos nas operações diárias da organização.

3.3.2. Segunda linha: funções de controle, *compliance* e gestão de riscos

A segunda linha é composta por funções especializadas que dão suporte, expertise e monitoramento sobre a gestão de riscos realizada pela primeira linha. Seu mister é estabelecer e fiscalizar a estrutura de controle e risco de forma independente das áreas operacionais, consubstanciando elo vital entre a execução e a governança.

As funções típicas da segunda linha incluem: i) gestão de riscos (com aplicação de metodologias, apetite a risco e limites predefinidos, consolidando o perfil de risco e se reportando à administração); ii) *compliance* (fixação de políticas e procedimentos que assegurem a observância de requisitos legais, regulatórios e éticos, monitorando

transações para detecção de não conformidade); e iii) controle financeiro e segurança da informação (funções que estabelecem parâmetros técnicos e políticas de controle que a primeira linha deve seguir, como, por exemplo, planos de continuidade de negócios e política de acesso a dados).

A segunda linha não assume a propriedade do risco (que permanece na primeira linha), mas sim a responsabilidade por seu monitoramento. Ela funciona como um *challenge function*, desafiando criticamente as suposições de risco das áreas de negócio, fornecendo treinamento e desenvolvendo ferramentas e relatórios que permitem à administração avaliar a adequação do sistema de controle interno.

A proximidade com a primeira linha confere à segunda linha a capacidade de ser um agente de mudança, promovendo a melhoria contínua dos controles antes que falhas se materializem, garantindo assim que o apetite a risco definido pelo conselho seja efetivamente traduzido em limites operacionais.

3.2.3. Terceira linha: auditoria interna e avaliação independente

A terceira linha é exercida pela auditoria interna e outras funções de avaliação independente, como avaliações externas de qualidade. Sua característica definidora é a independência total das duas primeiras linhas e, principalmente, da gestão. A sua subordinação funcional deve ser direta ao conselho de administração ou ao comitê de auditoria.

O principal mandato da terceira linha é fornecer asseguramento objetivo e *insights* sobre a eficácia dos processos de governança, gestão de riscos e controles internos. A auditoria interna não se limita a verificar a conformidade processual, mas avalia também: i) o desenho e operação do M3L (analisa se o modelo está realmente bem desenhado e se as responsabilidades das primeira e segunda linhas estão sendo executadas de forma eficaz e eficiente); ii) a aptidão e confiança dos controles (emite pareceres sobre a adequação dos controles, a precisão dos relatórios de risco e o cumprimento do apetite a risco); e iii) melhoria da governança (indica recomendações que visam aprimorar a estrutura de governança, a cultura de risco e o desempenho organizacional de forma ampla).

A independência permite à auditoria interna oferecer uma perspectiva não enviesada e holística. Ao contrário da segunda linha, que participa do estabelecimento do sistema, a terceira linha o avalia *a posteriori*, garantindo que as duas primeiras linhas não se tornem complacentes ou autossuficientes. Essa avaliação independente

é o mecanismo final para garantir que as informações reportadas à administração superior e ao conselho são confiáveis e que a organização está, de fato, caminhando em direção aos seus objetivos com riscos gerenciados.

Conforme já mencionado, o sucesso do M3L não está na rigidez da separação, mas sim na qualidade da comunicação e coordenação entre as linhas. Nesse sentido, uma estrutura funcional coesa exige que: i) a primeira linha reporte os riscos e as falhas de controle à segunda linha; ii) a segunda linha forneça suporte metodológico, defina políticas e monitore a conformidade da primeira linha; e iii) a terceira linha avalie a eficácia das duas primeiras linhas e reporte o asseguramento ao conselho.

Logo, essa sinergia entre as linhas é o fator diferencial que garante uma gestão contínua (primeira linha), sistemática (segunda linha) e sujeita a uma validação crítica e independente (terceira linha), formando um ciclo virtuoso que eleva a maturidade de governança da organização.

3.3 – Vantagens e Aplicabilidade do Modelo em Ambientes Corporativos Complexos

A gestão organizacional contemporânea é desafiada pela aceleração da mudança, incerteza e volatilidade, características inerentes ao que se convencionou chamar de ambientes VUCA (*Volatile, Uncertain, Complex, Ambiguous*). Em cenários assim, o risco emerge não apenas como uma ameaça a ser mitigada, mas como um elemento intrínseco à estratégia e à criação de valor[140]. O M3L, após sua revisão de 2020, oferece um arcabouço de governança que se demonstra particularmente apto a enfrentar a atual complexidade corporativa, promovendo resiliência, alinhamento estratégico e otimização de recursos.

A aplicabilidade do M3L em grandes corporações e conglomerados complexos reside na capacidade de prover uma estrutura hierárquica e funcional para tratamento de riscos, garantindo a sinergia necessária entre o conselho, a administração e as funções de gestão e asseguramento.

[140] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise Risk Management – Integrating with Strategy and Performance**. New York: COSO, 2017.

Em um contexto em que a estratégia e o risco são indissociáveis, o M3L atua como catalisador para alinhar os objetivos, conferindo clareza de responsabilidade (*accountability*) em todos os níveis da organização.

A principal vantagem estrutural do M3L é a distinção clara entre a *gestão* do risco e o *asseguramento* do risco. A alocação da propriedade do risco na primeira linha (gestores e áreas de negócio) garante que o risco seja tratado na origem, onde o conhecimento operacional é mais agudo. Esta abordagem evita que a gestão de riscos se torne uma função isolada, transformando-a em uma competência de linha.

A segunda linha, ao monitorar e desafiar as práticas da primeira linha, garante que o apetite a risco definido pelo conselho seja respeitado, servindo como uma ponte essencial entre a estratégia e a execução. Como apontam Kaplan e Norton[141], o ajuste de objetivos é vital para a execução da estratégia e o M3L traduz esse alinhamento ao definir quem assume, quem monitora e quem avalia o risco assumido.

A estrutura é finalizada com a terceira linha (auditoria interna), que fornece ao conselho uma salvaguarda objetiva e independente. Tal independência é crítica para a transparência do processo decisório, pois a auditoria interna deve se manter livre de quaisquer condições que possam comprometer sua capacidade de exercer o trabalho com a mentalidade imparcial[142]. Em ambientes complexos, essa separação funcional garante que a alta administração receba relatórios fidedignos sobre a exposição ao risco, sem vieses operacionais ou de monitoramento.

A complexidade corporativa frequentemente resulta na proliferação de funções de controle (qualidade, segurança, riscos, *compliance*, fraude), as quais, sem a devida coordenação, podem gerar redundância ou conflitos. O M3L oferece uma taxonomia para harmonizar essas funções.

Ao delimitar a natureza do asseguramento, o modelo facilita a otimização de recursos. A segunda linha faz o monitoramento *contínuo* de políticas e procedimentos (asseguramento *in process*), liberando a terceira linha para focar na avaliação *periódica e estratégica* da eficácia dos processos de governança e gestão de riscos em sua totalidade. Essa coordenação evita que a auditoria interna (terceira linha) duplique as atividades de monitoramento da segunda linha, permitindo um foco maior em riscos emergentes e transversais que afetam a organização como um todo.

---

[141] KAPLAN, Robert S.; NORTON, David P. **Mapas estratégicos:** convertendo ativos intangíveis em resultados tangíveis. Rio de Janeiro: Elsevier Campus, 2004.
[142] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

A aplicabilidade do M3L se torna evidente na gestão de riscos que perpassam múltiplas unidades de negócio, como o risco cibernético, o risco de ESG (Ambiental, Social e Governança) e o risco de terceiros (cadeia de suprimentos).

Em corporações que dependem criticamente da tecnologia, o risco cibernético é universal e o M3L permite uma resposta estruturada, a saber: i) Primeira Linha (desenvolvedores e gestores de TI são responsáveis pela implementação diária de controles de acesso e segurança nos sistemas); ii) Segunda Linha (a função de segurança da informação define as políticas – tal como *patch management*[143], testes de invasão e planos de continuidade – e monitora a conformidade dessas políticas nas diversas unidades de negócio); e iii) Terceira Linha (a auditoria interna avalia, de forma independente, a maturidade da gestão de riscos cibernéticos da organização e a adequação dos controles, reportando as vulnerabilidades estratégicas ao conselho).

Similarmente, no contexto de ESG, a segunda linha (função de sustentabilidade e *compliance*) pode definir as métricas e políticas (como a redução de carbono e a diversidade) que a primeira linha deve executar, enquanto a terceira linha verifica a confiabilidade dos dados e relatórios de sustentabilidade divulgados publicamente.

A complexidade exige agilidade e adaptabilidade, características que só se sustentam em uma cultura de risco forte. O M3L, ao incutir a responsabilidade pela gestão de riscos na primeira linha, integra o gerenciamento de riscos ao desempenho operacional. Ao invés de ser visto como obstáculo, o controle passa a ser percebido como um facilitador do desempenho.

Essa internalização cultural eleva a resiliência corporativa, pois a identificação e a mitigação de riscos ocorrem em tempo real e de forma distribuída. Assim, o modelo se transforma em um mecanismo que não apenas protege a empresa contra perdas, mas que, ao gerenciar a incerteza de forma proativa, permite à organização ousar e buscar oportunidades alinhadas com seu apetite a risco.

Portanto, a aplicabilidade do M3L em ambientes corporativos complexos é inquestionável. Suas vantagens residem na clareza de *accountability*[144], na eficiência do asseguramento coordenado e na capacidade de adaptação a riscos emergentes e transversais[145]. Ao formalizar as funções de gestão e asseguramento, o M3L fornece

[143] Processo de identificar, testar e aplicar atualizações de software e firmware para corrigir bugs, fechar vulnerabilidades de segurança e melhorar o desempenho e a funcionalidade dos sistemas de TI.
[144] KAPLAN; NORTON, ref. 141.
[145] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ref. 140.

a base para uma governança robusta, garantindo que o conselho e a administração superior operem fundamentados em informações transparentes e bem avaliadas, impulsionando a resiliência e a criação de valor sustentável.

3.4 – Desafios e Limitações da Aplicação do Modelo no Brasil

A estrutura conceitual do M3L representa o padrão internacional ideal para a gestão integrada de governança, risco e controle. Entretanto, sua transposição e implementação em ambientes corporativos no Brasil enfrentam desafios singulares que decorrem da especificidade regulatória, maturidade de governança de mercado e ainda de fatores culturais históricos. A simples adoção formal do modelo, sem uma adaptação contextual e um compromisso cultural genuíno, pode resultar em ineficácia ou na criação de estruturas meramente protocolares, contrariando o objetivo de resiliência e criação de valor[146].

A seguir, serão detalhados os principais obstáculos à aplicação plena e efetiva do M3L no cenário empresarial brasileiro, divididos em barreiras práticas, riscos culturais e a imprescindível função da liderança.

3.4.1. Dificuldades práticas na implementação nas empresas brasileiras

A materialização do M3L exige investimento em recursos, treinamento e uma reengenharia organizacional que nem sempre é viável, especialmente considerando o vasto contingente de pequenas e médias empresas que compõem o empresariado nacional, ou mesmo para sociedades familiares com estruturas de governança ainda incipientes. Conforme já fora mencionado alhures, o M3L não é ideal para toda e qualquer empresa em igual medida, mas necessita ser adaptado ao tamanho, ao setor de atuação e ao nível de maturidade da organização para garantir sua eficácia.

Uma das dificuldades práticas mais significativas é a alocação de recursos humanos e financeiros para estruturar uma segunda linha robusta e especializada. Em muitas organizações brasileiras, a função de *compliance* ou gestão de riscos (segunda linha) é frequentemente acumulada por profissionais que já desempenham funções na primeira linha (como gestores operacionais ou jurídicos). Tal sobreposição

[146] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ref. 140.

viola o princípio básico da segregação de deveres central ao M3L, comprometendo a independência da função de monitoramento.

A auditoria interna (terceira linha) também sofre com escassez de profissionais que tenham conhecimento técnico especializado necessário para auditar riscos emergentes, como segurança cibernética, *machine learning* ou riscos climáticos. A carência de orçamento para contratar ou treinar auditores internos especializados obriga as organizações a dependerem de terceiros, o que, embora válido, pode reduzir o conhecimento institucional e a capacidade de avaliação contínua interna.

Outrossim, apesar de as responsabilidades de cada serem claras (L1 assume o risco, L2 monitora o risco e L3 avalia a gestão do risco), na prática brasileira, essa delimitação é frequentemente nebulosa.

Muitas vezes, a L1 resiste em aceitar a propriedade do risco, transferindo a responsabilidade por falhas de controle para a L2. Inversamente, a L2 pode exceder sua função de monitoramento e acabar executando tarefas de controle que caberiam à L1, tornando-se de fato um coproprietário do risco. Nesse sentido, o IBGC[147] enfatiza que a eficácia do M3L depende de uma matriz de responsabilidade (RACI)[148], a qual deve ser meticulosamente definida e comunicada, fator que representa um desafio cultural e burocrático em organizações com histórico de ambiguidade funcional.

3.4.2. Programas de fachada e influência da cultura organizacional

A implementação do M3L no Brasil muitas vezes é motivada por pressões regulatórias (Lei Anticorrupção) ou de mercado (anseios de investidores estrangeiros), mas não por um desejo genuíno de mudança cultural. Esse cenário abre espaço para os chamados "programas de fachada" ou *compliance theater*.

O risco de criar um programa de fachada é inerente a qualquer iniciativa de governança imposta externamente. Nesses casos, a empresa implementa a estrutura do M3L apenas no papel, com políticas, procedimentos e organogramas definidos, mas sem o endosso ou o investimento cultural necessário. Não por outro motivo, o

[147] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC), ref. 1.
[148] Ferramenta de gestão de projetos que define e formaliza os papéis e responsabilidades de cada membro da equipe em relação a uma tarefa. A sigla significa: Responsável (quem executa), Aprovador (quem tem a palavra final), Consultado (quem fornece informações/conselhos) e Informado (quem é notificado do progresso). A ferramenta ajuda a evitar confusões, sobreposição de funções e a garantir que todos saibam o que precisam fazer, melhorando a comunicação e a eficiência do projeto

Decreto n.º 11.129/2022, em seu artigo 56, inciso II passou a prever expressamente a internalização da cultura de *compliance* na organização[149].

A L2, neste contexto, passa a existir apenas para satisfazer requisitos de *due diligence* ou auditoria externa, e não para exercer sua função crítica de *challenge function* (função de desafio). Por sua vez, a L3 (auditoria interna) pode ser sutilmente coagida a suavizar achados ou a priorizar auditorias que validem a estrutura, em detrimento de uma avaliação verdadeiramente independente dos riscos mais críticos. Assim, o M3L se torna um mero artefato de *marketing* de governança, enquanto as práticas operacionais e as decisões de risco continuam sendo guiadas por processos informais, atalhos ou pelo histórico cultural.

A cultura organizacional brasileira, em muitos setores, historicamente valoriza a hierarquia estrita e, por vezes, a informalidade nas relações interpessoais e de negócio. Esses traços culturais representam uma barreira direta à essência do M3L, quais sejam: independência da L2 (a cultura hierárquica dificulta que a segunda linha desafie abertamente as decisões de risco tomadas por gestores seniores da primeira linha); e comunicação de riscos (a aversão a reportar más notícias e falhas de controle internamente pode levar à supressão de informações na primeira linha, privando as linhas subsequentes dos dados essenciais para o monitoramento efetivo).

Conforme a estrutura do COSO sobre Gestão de Riscos Corporativos[150], a cultura deve ser o alicerce sobre o qual o sistema de controle é construído. No Brasil, frequentemente, o M3L é forçado sobre uma cultura que o rejeita, resultando em uma dissociação entre o que é prescrito e o que é praticado.

3.4.3 Papel da alta administração (*tone at the top*) na efetividade do *compliance*

Nenhum modelo de governança prospera sem o apoio irrestrito de sua alta administração e do conselho. O *tone at the top* ("tom vindo de cima") é o fator de sucesso mais crítico para que o M3L vá além da fachada e se torne efetivo.

---

[149] "Art. 56. Para fins do disposto neste Decreto, programa de integridade consiste, no âmbito de uma pessoa jurídica, no 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:
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".

[150] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ref. 140.

A efetividade do *compliance* e da gestão de riscos, em especial no contexto da Lei Anticorrupção brasileira, depende sobretudo da liderança. Se a alta administração não demonstra, por meio de ações concretas e alocação de recursos, que valoriza a ética e a conformidade acima dos resultados imediatos, as Três Linhas perdem sua credibilidade perante os demais colaboradores da empresa.

Assim, o M3L pode ser facilmente sabotado se o conselho ou a administração superior falharem em: defender a L3 (a independência da auditoria interna é o teste final do *tone at the top*. Qualquer tentativa de influenciar o escopo de trabalho, os achados ou o reporte da auditoria desmantela a confiança no M3L); responsabilizar a L1 (se gestores operacionais que ignoram as políticas de risco da L2 não forem responsabilizados, a mensagem enviada à organização é que o controle é opcional); investir em treinamento (a liderança deve garantir o financiamento adequado para o treinamento contínuo das três linhas, sinalizando que a gestão de riscos é um investimento estratégico, e não apenas um custo).

O IIA é enfático ao afirmar que, embora o conselho estabeleça a governança, a efetividade do modelo depende da sua aceitação e promoção pela alta gerência[151]. No Brasil, as investigações de casos de corrupção e desvios mostram que o ponto de falha não estava na ausência de programas de *compliance* (estrutura), mas na sua fragilidade decorrente da falta de compromisso ético da liderança (cultura).

Desse modo, tem-se que a aplicação do M3L no Brasil é permeada por desafios que exigem mais do que apenas uma mudança estrutural. As dificuldades práticas, a ameaça de programas de fachada e, especialmente, a ausência de um *tone at the top* inabalável representam as principais limitações à sua plena efetividade. Para que o modelo cumpra sua promessa de gestão de risco e criação de valor, é imperativo que as empresas nacionais superem as barreiras culturais, invistam na real independência das funções de controle e demonstrem um compromisso ético que permeie as Três Linhas, transformando a conformidade de obrigação em vantagem estratégica.

3.5 – Perspectivas de Aprimoramento e Recomendações

Após analisar a estrutura funcional e os desafios da aplicação do Modelo das Três Linhas no contexto corporativo brasileiro, torna-se imprescindível delinear as

[151] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

perspectivas de aprimoramento e recomendações concretas. O objetivo não é apenas adaptar o modelo para mitigar suas limitações intrínsecas, mas transformá-lo em uma ferramenta mais dinâmica, inteligente e eficaz para a criação e proteção de valor em ambientes complexos.

Nesse sentido, a evolução do M3L exige uma abordagem dupla: de um lado, a adoção de boas práticas de gestão oriundas do cenário internacional; e de outro, o engajamento proativo do sistema regulatório e institucional nacional, para incentivar e dar suporte a sua implementação.

3.5.1. Boas práticas internacionais adaptáveis ao contexto brasileiro

As empresas brasileiras podem elevar a eficácia do M3L mediante a importação e adaptação de práticas que priorizam a integração, a digitalização e a agilidade, em contraste com a abordagem tradicionalmente burocrática e baseada em *checklists*.

Uma das principais limitações do M3L reside na potencial tendência à rigidez e à operação em silos. O aprimoramento está justamente na transição de um modelo de "linhas estanques" para um "ecossistema de riscos e controles", conforme sugerido pelo próprio IIA (2020).

Para tanto, a integração deve ocorrer em três níveis diferentes. O primeiro diz respeito à integração horizontal entre as funções da L2. Aqui é importante que as funções de risco, *compliance*, segurança da informação e sustentabilidade operem sob uma visão unificada (*Integrated Risk Management*). Em vez de relatórios isolados, as organizações devem estabelecer um único comitê de controle da L2 que consolide métricas e reporte de forma coordenada à administração.

O segundo nível se refere à governança ágil (*Agile* GRC). A velocidade do risco, especialmente o cibernético e o tecnológico, requer que as funções de controle e auditoria adotem metodologias ágeis. Isso implica substituir auditorias anuais e longas por asseguramento contínuo e microsserviços de consultoria integrados aos projetos da L1. O controle aqui deve ser incorporado ao desenvolvimento (*DevSecOps*) e não adicionado ao final do processo.

Por fim, o terceiro nível aborda o uso de tecnologia e análise de dados (*Data-Driven GRC*). A adaptação mais crítica é a incorporação de inteligência artificial (IA) e aprendizado de máquina (*Machine Learning*) para o monitoramento contínuo. Tais tecnologias permitem que a L2 realize o denominado *Continuous Control Monitoring* (CCM), analisando 100% das transações em busca de desvios, passando a não mais

depender de testes amostrais[152]. Essa prática internacional libera a L3 para focar no julgamento estratégico e na eficácia dos processos, ao invés de realizar uma mera detecção de falhas operacionais.

Superar o problema dos "programas de fachada" demanda que as métricas de desempenho das Três Linhas sejam ligadas à cultura. Boas práticas internacionais sugerem que a remuneração dos gestores da L1 deve estar atrelada não apenas aos resultados financeiros, mas também a sua adesão às políticas de risco e *compliance* estabelecidas pela L2. Essa prática reforça o princípio de que o risco é de propriedade da operação e traduz o *tone at the top* em consequências financeiras tangíveis.

3.5.2. Incentivos regulatórios e institucionais à adoção do modelo

Apesar dos marcos regulatórios existentes no Brasil, como a Lei Anticorrupção e regras específicas do Banco Central (BC) e Comissão de Valores Mobiliários (CVM), a adesão ao M3L ainda carece de incentivos positivos mais amplos. A regulamentação atual tende a ser punitiva (focada em multas e sanções), negligenciando o potencial de incentivos institucionais que promovem a governança proativa.

Nesse mote, é precípuo que os órgãos reguladores e as instituições financeiras de fomento reconheçam a maturidade do M3L. O incentivo pode se dar pela aplicação do princípio da proporcionalidade, em que o nível de exigência e burocracia regulatória seja inversamente proporcional à robustez do sistema de controle da empresa.

Assim, recomenda-se como incentivo financeiro a oferta de linhas de crédito mais favoráveis ou a redução das taxas de juros por bancos estatais para empresas que comprovem um M3L maduro, auditado de forma independente.

Sugere-se ainda a adoção de vantagens em licitações públicas, atribuindo-se pontuação adicional em processos licitatórios para empresas que demonstrem um sistema de gestão de risco e *compliance* alinhado ao M3L e que possuam uma L3 independente, nos moldes das diretrizes do “Código das Melhores Práticas de Governança Corporativa do IBGC”[153].

As instituições brasileiras devem criar mecanismos de reconhecimento público para as melhores práticas de governança. A CVM ou a B3[154], por exemplo, poderiam

[152] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ref. 140.
[153] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC), ref. 1.
[154] Bolsa, Brasil, Balcão. Empresa que administra a bolsa de valores oficial do Brasil.

estabelecer um selo ou índice de governança de risco que vá além dos critérios de listagem tradicionais. Esse tipo de reconhecimento não apenas confere prestígio e atrai investimentos ESG, mas também serve como um indicador para o mercado sobre a resiliência e a estabilidade da empresa em longo prazo, reduzindo o custo de capital.

3.5.3. Propostas para o aperfeiçoamento do marco regulatório nacional

Apesar de o Brasil ter avançado na regulação de *compliance* após 2013, o marco regulatório ainda pode ser aprimorado para solidificar a implementação do M3L, mormente quanto à independência da Segunda e da Terceira Linhas.

O grande ponto de fragilidade no país é a ambiguidade de deveres na L2. Dessa forma, propõe-se a criação de diretrizes setoriais – BC, SUSEP[155] e CVM – que estabeleçam a segregação de deveres, ou seja, a exigência formal de que as funções-chave da L2 (como o *Chief Risk Officer* e o *Chief Compliance Officer*) não acumulem responsabilidades operacionais (L1) nem de asseguramento independente (L3).

Outrossim, com vistas ao aprimoramento, sugestiona-se a implementação de uma estrutura de "reporte funcional", em que os líderes da L2 devam se reportar diretamente a um comitê do conselho. Tal exigência garantiria a preservação do *status* e autoridade dos líderes, mesmo que eles se reportem administrativamente ao CEO.

O aperfeiçoamento regulatório deve também focar em blindar a independência da L3 (auditoria interna). Nesse trilhar, incluem-se duas propostas. A primeira trata do reporte obrigatório e exclusivo ao conselho. Assim, em empresas de capital aberto ou em setores regulados, deve-se exigir que o chefe da auditoria interna (CAE) se reporte apenas ao conselho de administração, ou a um comitê de auditoria forte e composto por membros independentes[156].

A segunda proposta versa sobre a implantação de mecanismos de proteção e *whistleblowing*. Trata-se de um reforço regulatório da proteção legal e institucional do CAE contra retaliação e demissão imotivada, garantindo sua capacidade de exercer o ceticismo profissional. Além disso, a L3 deve ter acesso garantido e protegido a canais de denúncia (*whistleblowing*), para monitorar a eficácia e a resposta da administração aos relatórios.

---

[155] Superintendência de Seguros Privados, uma autarquia federal responsável por regular e fiscalizar o mercado de seguros, previdência privada aberta, capitalização e resseguros no Brasil.
[156] THE INSTITUTE OF INTERNAL AUDITORS, ref. 82.

Para evitar redundâncias entre as linhas e o consequente desperdício de recursos, a regulamentação poderia também fomentar o asseguramento coordenado (*Combined Assurance*). O regulador poderia emitir um guia, em linha com as práticas globais, que estimule a coordenação formal entre a auditoria interna, auditoria externa e demais funções de asseguramento (L2), garantindo, pois, uma cobertura de risco eficiente e sem sobreposições.

A partir dessas considerações, observa-se que o aprimoramento do Modelo das Três Linhas no Brasil é um imperativo estratégico. Não basta a simples adoção formal, é necessário investir na inteligência do modelo, por meio da integração, do uso de tecnologias de *continuous monitoring* e da cultura de *accountability*[157]. No ponto, as recomendações regulatórias, que incluem a criação de incentivos positivos e a solidificação da independência da L2 e da L3, são cruciais para transformar o M3L de um requisito de *compliance* em um pilar de resiliência corporativa. Ao fortalecer o marco regulatório e a cultura ética[158], o Brasil pode assegurar que o M3L funcione não apenas como uma defesa contra falhas, mas como um sistema íntegro para decisões estratégicas mais informadas e seguras.

[157] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO), ref. 140.
[158] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC), ref. 1.

CONCLUSÃO

A análise das principais normas que integram o ordenamento jurídico brasileiro – em especial as Leis n.º 12.529/2011, 12.846/2013, 13.303/2016, 13.709/2018, 14.133/2021 e o Decreto n.º 11.129/2022 – demonstra que o Modelo das Três Linhas se consolidou como estrutura funcional e normativa para o fortalecimento da integridade, transparência e governança institucional no país.

Trata-se de uma evolução gradual e sistêmica: o Direito Concorrencial introduziu o *compliance* como instrumento de prevenção de ilícitos econômicos e de estímulo à autorregulação (Lei n.º 12.529/2011); o Direito Anticorrupção o transformou em critério legal de mitigação de responsabilidade e de avaliação da conduta corporativa (Lei n.º 12.846/2013 e Decreto n.º 11.129/2022); o Direito Administrativo Empresarial incorporou o *compliance* como exigência estrutural de governança nas empresas públicas (Lei n.º 13.303/2016); o Direito Digital o expandiu para o campo da proteção de dados e privacidade (Lei n.º 13.709/2018); e o Direito das Contratações Públicas consolidou a integridade como requisito jurídico e contratual nas relações público-privadas (Lei n.º 14.133/2021).

Essas normas, interpretadas em conjunto, revelam que o *compliance* deixou de ser mera prática de gestão para tornar-se instituto jurídico transversal, incorporado a múltiplos ramos do direito e estruturado segundo a lógica do Modelo das Três Linhas. Nesse modelo, a primeira linha (formada por gestores e executores das atividades) é responsável pela aplicação direta dos controles; a segunda linha (composta pelas funções de *compliance*, gestão de riscos e controle interno) garante a supervisão e a coerência dos processos; e a terceira linha (constituída por auditorias internas e externas) exerce papel independente de verificação, reporte e aprimoramento.

O avanço do arcabouço normativo brasileiro é inegável. O país passou a dispor de uma base legal robusta, compatível com os padrões internacionais de integridade corporativa, especialmente aqueles preconizados pela OCDE, pelo U.S. Department of Justice (DOJ), pelo UK Ministry of Justice e pelo Institute of Internal Auditors (IIA). Contudo, o principal desafio permanece na efetividade prática dessas estruturas.

A persistência de programas de fachada, a insuficiência técnica das equipes de *compliance* e a limitada autonomia das áreas de auditoria e controle ainda fragilizam a implementação do Modelo das Três Linhas no contexto brasileiro. Mais do que leis,

é necessária a internalização cultural da integridade, isto é, o compromisso ético e institucional com a conformidade e a transparência.

O amadurecimento da governança pública e privada brasileira exige a superação da visão punitivista e a adoção de um paradigma de regulação preventiva e colaborativa, no qual o *compliance* atue como eixo integrador entre controle, gestão e auditoria. Essa transição reflete o movimento global de substituição da “cultura do medo da sanção” pela “cultura da integridade”, na qual o Modelo das Três Linhas funciona como arquitetura de governança e gestão de riscos voltada à sustentabilidade organizacional.

Conclui-se, portanto, que o Modelo das Três Linhas, hoje incorporado a diversos diplomas legais brasileiros, representa mais do que uma ferramenta de controle interno: trata-se de paradigma normativo de governança democrática e responsabilidade corporativa, que redefine a relação entre Estado, mercado e sociedade. Sua consolidação dependerá da profissionalização das funções de integridade, da autonomia das estruturas de controle, e do engajamento ético das lideranças, de modo que o *compliance* deixe de ser um requisito formal para se tornar expressão concreta de cidadania institucional e confiança pública.

Nesse intento, propõe-se neste trabalho algumas sugestões com vistas ao aprimoramento do sistema já existente, como a criação de diretrizes setoriais, a implementação de uma estrutura de “reporte funcional”, o reporte obrigatório e exclusivo do o chefe da auditoria interna ao conselho de administração (ou a um comitê de auditoria), a implantação de mecanismos de proteção e *whistleblowing* e, por fim, o fomento do asseguramento coordenado.

REFERÊNCIAS

AGUIAR, André Amaral de. **Responsabilidade objetiva na Lei Anticorrupção e compliance:** construção do conceito de culpabilidade de empresa na busca de uma política pública eficiente. São Paulo: Editora Dialética, 2022.

ALENCAR, C. H. R.; VARELLA, M. D. Combate globalizado à corrupção: da gênese do modelo norte-americano à sua implementação internacional. **Revista de Direito Internacional Econômico e Tributário – RDIET**, Brasília, v. 16, n. 2, p. 184–226, jul./dez. 2021. Disponível em: https://portalrevistas.ucb.br/index.php/rdiet/article/view/13486. Acesso em: 12 out. 2025.

ALMEIDA, Luiz Eduardo de. Governança Corporativa. *In*: ALVIM, Tiago Cripa et al (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024.

ASSI, Marcos. **Governança, riscos e compliance:** mudando a conduta nos negócios. São Paulo: Saint Paul Editora, 2017. *E-book*. ISBN 9788580041279. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788580041279. Acesso em 26 set. 2024.

ASSI, Marcos. **Gestão de compliance e seus desafios:** como implementar controles internos, superar dificuldades e manter a eficiência nos negócios. São Paulo: Saint Paul Editora, 2013.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo - Atuação do encarregado pelo tratamento de dados pessoais**. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/copy_of_guia_da_atuacao_do_encarregado_anpd.pdf. Acesso em: 6 nov. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: ANPD, 2022. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 6 nov. 2025.

BACIGALUPO, Enrique. **Compliance y Derecho Penal**. Pamplona, Thomson Reuters, 2011.

BAKER MCKENZIE. **United States: Why compliance still matters**. InsightPlus – Baker McKenzie, 13 fev. 2025. Disponível em: https://insightplus.bakermckenzie.com/bm/investigations-compliance-ethics/united-states-why-compliance-still-matters. Acesso em: 12 out. 2025.

BANCO DE COMPENSAÇÕES INTERNACIONAIS. Comitê de Supervisão Bancária da Basileia. **Sound management of risks related to money laundering and financing of terrorism**. Basel: Bank for International Settlements, July 2020. Disponível em: https://www.bis.org/bcbs/publ/d573.pdf. Acesso em: 22 fev. 2025.

BANCO DE PAGAMENTOS INTERNACIONAIS. Comitê de Supervisão Bancária da Basileia. **Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering**. Basileia: Bank for International Settlements, 1988. Disponível em: https://www.bis.org/publ/bcbsc137.pdf. Acesso em: 20 fev. 2025.

BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: ALVIM, Tiago Cripa et al (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024.

BITENCOURT, C. M. A inteligência artificial nos órgãos constitucionais de controle de contas públicas: tornar transparente suas funções e resultados. **Revista Interdisciplinar de Controle e Gestão Pública**, 2023. Disponível em: https://www.scielo.br/j/rinc/a/WJgdHhvqpvyr7XnHhMN39Wz/?lang=pt. Acesso em: 8 nov. 2025.

BLOK, Marcella. **Compliance e governança corporativa**. 4. ed. *[S.l.]*: Freitas Bastos, 2023. *E-book*.

BOLETIM DE ANÁLISE POLÍTICO-INSTITUCIONAL: Avaliação de Integridade nas Estatais pela CGU. Rio de Janeiro: **Ipea**, n. 15, Jul.-Dez. 2018. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/boletim_analise_politico/180905_bapi_15_cap08.pdf. Acesso em: 4 nov. 2025.

BRAGATO, Adelita Aparecida Podadera Bechelani. **O compliance no Brasil:** a empresa entre a ética e o lucro. 2017. Dissertação (Mestrado em Direito) – Universidade Nove de Julho, São Paulo, 2017.

BRASIL. Banco Central do Brasil. **Recomendações de Basileia**. Brasília, DF: Banco Central do Brasil, [s.d.]. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/recomendacoesbasileia. Acesso em: 22 fev. 2025.

BRASIL. **Decreto nº 8.945, de 27 de dezembro de 2016**. Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias. *Diário Oficial da União*: seção 1, Brasília, DF, 28 dez. 2016.

BRASIL. **Decreto nº 11.129, de 11 de julho de 2022.** Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e altera o Decreto nº 8.420, de 18 de março de 2015. *Diário Oficial da União: seção 1*, Brasília, DF, 12 jul. 2022.

BRASIL. **Lei nº 12.529, de 30 de novembro de 2011**. Estrutura o Sistema Brasileiro de Defesa da Concorrência. Diário Oficial da União, Brasília, DF, 1 dez. 2011.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Diário Oficial da União, Brasília, DF, 2 ago. 2013.

BRASIL. **Lei nº 13.303, de 30 de junho de 2016.** Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios. *Diário Oficial da União*: seção 1, Brasília, DF, 1 jul. 2016.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021**. Lei de Licitações e Contratos Administrativos. *Diário Oficial da União*, Brasília, DF, 1 abr. 2021.

CARNEIRO, Claudio; SANTOS JUNIOR, Milton de Castro. **Compliance e boa governança:** pública e privada. Juruá Editora, 2018.

CARVALHO, Victor Aguiar de. **Corrupção empresarial e administração pública:** diagnóstico e estratégias de enfrentamento. Belo Horizonte: Fórum, 2022.

COELHO, N.; HERINGER, H. M. L. Análise da Foreign Corrupt Practices Act (FCPA) e a crítica ao imperialismo. **Revista Jurídica UNICURITIBA**, Curitiba, v. 1, n. 46, 2017. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2004/1285. Acesso em: 12 out. 2025.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Enterprise Risk Management – Integrating with Strategy and Performance**. New York: COSO, 2017.

CONGRESS (United States). *S. 4548* – **Foreign Extortion Prevention Technical Corrections Act**. Projeto de lei — 118th Congress, 2023-2024. Disponível em: https://www.congress.gov/bill/118th-congress/senate-bill/4548/text. Acesso em: 12 out. 2025.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Guia de programas de compliance concorrencial.** Brasília, DF: CADE, 2016. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-compliance-versao-oficial.pdf. Acesso em: 15 out. 2025.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). **Regimento interno.** Aprovado pela Resolução nº 22, de 19 de junho de 2019. Brasília, DF: CADE, 2019. Disponível em: https://cdn.cade.gov.br/Relatoriorios%20de%20gestao/2020/Cap.%201/Resolu%C3%A7%C3%A3o%2022%20de%2019%20de%20junho%20de%202019_Regiment%20Interno.pdf. Acesso em: 15 out. 2025.

CONTROLADORIA-GERAL DA UNIÃO (CGU). **Portaria Normativa SE/CGU nº 226, de 9 de setembro de 2025**. Estabelece diretrizes para implementação e monitoramento de programas de integridade no âmbito da Administração Pública Federal direta, autárquica e fundacional. Brasília, DF: CGU, 2025. Disponível em: https://www.gov.br/ana/pt-br/acesso-a-

informacao/integridade/normativos/arquivos/portaria-normativa-se_cgu-no-226-de-9-de-setembro-de-2025.pdf. Acesso em: 4 nov. 2025.

CONTROLADORIA GERAL DA UNIÃO (CGU). **Programa de Integridade:** Diretrizes para Empresas Privadas (vol. II). Brasília: CGU, 2024. Disponível em: https://www.gov.br/cgu/pt-br/assuntos/noticias/2024/10/cgu-publica-novo-guia-de-diretrizes-para-empresas-privadas/GuiaDiretrizes_v14out1.pdf. Acesso em: Acesso em 23 mar. 2025.

CONTROLADORIA-GERAL DA UNIÃO (CGU). **Plano de Integridade da Controladoria-Geral da União 2023–2025**. Brasília, DF: CGU, 2023. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/93464/1/Plano_Integridade_CGU_2023_2025.pdf. Acesso em: 1 nov. 2025.

CONTROLADORIA-GERAL DA UNIÃO (CGU). **Relatório de Gestão – 2024**. Brasília, DF: CGU, 2024. Disponível em: https://www.gov.br/cgu/pt-br/acesso-a-informacao/auditorias/arquivos/2024/RelatorioGestao2024.pdf. Acesso em: 8 nov. 2025.

COZENDEY, Carlos Márcio B. **Instituições de Bretton Woods:** desenvolvimento e implicações para o Brasil. Brasília: FUNAG, 2013.

DE LA TORRE, M. J. **The Foreign Corrupt Practices Act:** Imposing an American Definition of Corruption on Global Markets. Cornell International Law Journal, Ithaca, v. 49, n. 2, 2016. Disponível em: http://scholarship.law.cornell.edu/cilj/vol49/iss2/5. Acesso em: 12 out. 2025.

DEPARTMENT OF JUSTICE (DOJ). Criminal Division. **Evaluation of Corporate Compliance Programs**. Washington, D.C.: U.S. Department of Justice, 2024. Disponível em: https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=. Acesso em: 1 nov. 2025.

DEPARTMENT OF JUSTICE (DOJ). **Foreign Corrupt Practices Act. [S.l.]:** DOJ, 1977. Disponível em: https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act. Acesso em: 10 out. 2025.

DEPARTMENT OF JUSTICE (DOJ). **Relatório de Justificativa**. Disponível em: https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/houseprt-95-640.pdf. Acesso em: 18 abr. 2025.

DEPARTMENT OF JUSTICE (DOJ); SECURITIES AND EXCHANGE COMMISSION (SEC). **A Resource Guide to the U.S. Foreign Corrupt Practices Act**. 2. ed. Washington, D.C.: DOJ/SEC, 2020. Disponível em: https://www.justice.gov/criminal-fraud/file/1292051/download. Acesso em: 10 out. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.

FAUSTO, Boris. **História do Brasil**. 13. ed. rev. e atual. São Paulo: Edusp, 2015.

FERNANDES, Nelson Ricardo; FIGUEIROA, Caio; e NEVES, Edmo. Gestão de Riscos. *In*: ALVIM, Tiago Cripa *et al* (Coord.). **Manual de Compliance**. 4 ed. Rio de Janeiro: Forense, 2024.

FREEMAN, R.E. **Strategic Management:** A stakeholder approach. Boston: Pitman, 1984.

FONTES-FILHO, Joaquim Rubens. A governança corporativa em empresas estatais brasileiras frente à Lei de Responsabilidade das Estatais (Lei nº 13.303/2016). **Revista do Serviço Público**, Brasília, v. 69, edição especial "Repensando o Estado Brasileiro", p. 181-209, dez. 2018. Disponível em: https://repositorio.enap.gov.br/jspui/bitstream/1/5373/1/A%20governança%20corporativa%20em%20empresas%20estatais%20brasileiras%20frente%20à%20Lei%20de%20Responsabilidade%20das%20Estatais%20(Lei%20nº%2013.303-2016).pdf. Acesso em: 2 nov. 2025.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Padrões Internacionais de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação - As Recomendações do GAFI**. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Feburary%202025%20FATF%20Recommendations.pdf. Acesso em: 5 out. 2025.

HESS, David. Ethical infrastructures and evidence-based corporate compliance and ethics programs: policy implications from the empirical evidence. **New York University Journal of Law & Business**, v.12, n. 2, p. 325, 2016. Disponível em: https://www.nyujlb.org/12-2. Acesso em 03 mai. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/24640/2023_C%c3%b3digo%20das%20Melhores%20Pr%c3%a1ticas%20de%20Governan%c3%a7a%20Corporativa_6a%20Edi%c3%a7%c3%a3o.pdf. Acesso em 17 mai. 2025.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. **O The IIA redesenhará as Linhas de Defesa?** São Paulo: IIA Brasil, [s.d.]. Disponível em: https://iiabrasil.org.br/noticia/o-the-iia-redesenhara-as-linhas-de-defesa. Acesso em: 11 nov. 2025.

ISO. **31000:2018(en)**. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en. Acesso em 13 fev. 2025.

KAPLAN, Robert S.; NORTON, David P. **Mapas estratégicos:** convertendo ativos intangíveis em resultados tangíveis. Rio de Janeiro: Elsevier Campus, 2004.

KOEHLER, M. The FCPA, Deferred Prosecution Agreements, and Non-Prosecution Agreements. **U.C. Davis Law Review**, Davis, v. 49, n. 2, 2015.

MARTINS, Simone; TEIXEIRA, Marco Antonio Carvalho; PINEDA NEBOT, Carmen; PEÑA LÓPEZ, María Alejandra. **Transparência, accountability e governança pública**. Brasília, DF: Escola Nacional de Administração Pública (ENAP), 2018. Disponível em: https://repositorio.enap.gov.br/bitstream/1/4161/4/Transparencia.pdf. Acesso em: 2 nov. 2025.

MENDRONI, Marcelo Batlouni. **Lavagem de dinheiro:** prevenção e repressão. 6. ed. São Paulo: Atlas, 2021.

MISALE, Guilherme Teno Castilho. **Programas de compliance à luz do ordenamento concorrencial brasileiro:** instrumentos de conformidade para a política anticartel. 2019. 190 f. Dissertação (Mestrado em Direito) — Faculdade de Direito, Universidade de São Paulo, São Paulo, 2019.

MULITERNO, Paulo Tiago Sulino; e PALAZZI, Leonardo. Corrupção Privada e *Compliance*. *In*: CARNEIRO, Cláudia; e DELLOSO, Ana Ayres (coord.). **Compliance Aplicado ao Direito**. ISBN: 978-65-00-27380-9. ICTS protiviti, 2021.

OLIVEIRA, E. Compliance, Cultura de Integridade e Aliança para Boas Práticas. **Francis Yearbook of Legal Sciences & Human Rights**, Curitiba: Author's Edition, v. 1, n. 1, 2024. ISBN 978-65-00-97652-6. Disponível em: https://dialnet.unirioja.es/descarga/articulo/9571676.pdf. Acesso em: 2 nov. 2025.

OLIVEIRA, Nildete dos Passos. **Governança pública:** um estudo sobre os mecanismos de controle interno e transparência pública no Brasil. 2017. Dissertação (Mestrado em Administração Pública) – Universidade de Brasília, Brasília, 2017. Disponível em: https://repositorio.unb.br/bitstream/10482/31508/1/2017_NildetedosPassosOliveira.pdf. Acesso em: 8 nov. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção das Nações Unidas contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas**, de 1988. Viena: ONU, 1988. Disponível em: https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html. Acesso em: 20 fev. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OECD). **Governments' Assessments of Corporate Anti-Corruption Compliance**. Paris: OECD, 2025. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/governments-assessments-of-corporate-anti-corruption-compliance_6100e758/e798903c-en.pdf. Acesso em: 10 mai. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Guidelines on Corporate Governance of State-Owned Enterprises:** 2015 Edition. Paris: OECD Publishing, 2015. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/11/oecd-guidelines-on-corporate-governance-of-state-owned-enterprises-2015-edition_g1g5a749/9789264244160-en.pdf. Acesso em: 2 nov. 2025. DOI: 10.1787/9789264244160-en.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Manual de Integridade Pública da OCDE**. Paris: OECD Publishing, 2022. Disponível em: https://doi.org/10.1787/db62f5a7-pt. Acesso em 10 mai. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Fortalecendo a Integridade Pública no Brasil:** Consolidando as Políticas de Integridade no Poder Executivo Federal. Paris: OECD Publishing, 2021. Disponível em: https://www.oecd.org/content/dam/oecd/pt/publications/reports/2021/12/strengthening-public-integrity-in-brazil_e7d2d27b/5414ae92-pt.pdf. Acesso em: 2 nov. 2025.

REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho**, São Paulo, v. 214, p. 323-340, nov./dez. 2020. Disponível em: https://www.thomsonreuters.com.br/content/dam/ewp-m/documents/brazil/pt/pdf/other/rdt-214-a-cultura-de-compliance-em-materia.pdf?utm_source. Acesso em: 6 nov. 2025.

SECURITIES AND EXCHANGE COMMISSION (SEC). **Foreign Corrupt Practices Act (FCPA)**. [S.l.]: SEC, [s.d.]. Disponível em: https://www.sec.gov/enforcement/foreign-corrupt-practices-act. Acesso em: 18 abr. 2025.

SPALDING, Andrew Brady. The Irony of International Business Law: U.S. Progressivism, China's New Laissez Faire, and Their Impact in the Developing World (March 25, 2011). **UCLA Law Review**, Vol. 59, 2011. p. 19. Disponível em SSRN: http://dx.doi.org/10.2139/ssrn.1795563 ou https://ssrn.com/abstract=1795563. Acesso em: 03 mai. 2025.

TEPEDINO, Gustavo; FRAZÃO, Ana de Oliveira; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 3. ed., rev., atual. e ampl. São Paulo: Thomson Reuters Revista dos Tribunais, 2023.

THE INSTITUTE OF INTERNAL AUDITORS. **As três linhas de defesa no gerenciamento eficaz de riscos e controles**. Altamonte Springs, FL: The Institute of Internal Auditors, 2013. Declaração de posicionamento. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/as-trs-linhas-d-ippf-00000010-28082019095801.pdf. Acesso em: 11 nov. 2025.

THE INSTITUTE OF INTERNAL AUDITORS. **The IIA's Three Lines Model:** updated guidance. Lake Mary, FL: The Institute of Internal Auditors, 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf. Acesso em: 20 jun. 2025.

THE WHITE HOUSE. **Fact Sheet:** President Donald J. Trump Restores American Competitiveness and Security in FCPA Enforcement. 10 fev. 2025. Disponível em: https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-restores-american-competitiveness-and-security-in-fcpa-enforcement/. Acesso em: 12 out. 2025.

TREVIÑO, Linda K.; NELSON, Katherine A. **Managing Business Ethics:** Straight Talk About How to Do It Right. 8. ed. Hoboken: John Wiley & Sons, 2021.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial básico de governança organizacional:** *3ª edição.* Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2020. Disponível em: https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf. Acesso em: 7 nov. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – RGPD). **Jornal Oficial da União Europeia**, L 119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 6 nov. 2025.

UNITED KINGDOM. **Bribery Act 2010:** Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing. London: Ministry of Justice, 2011. Disponível em: https://assets.publishing.service.gov.uk/media/5d80cfc3ed915d51e9aff85a/bribery-act-2010-guidance.pdf. Acesso em: 05 mai. 2025.

UNITED KINGDOM. **Bribery Act 2010**. London: The Stationery Office, 2010. Disponível em: https://www.legislation.gov.uk/ukpga/2010/23/contents. Acesso em: 05 mai. 2025.

UNITED STATES v. KAY. **Court of Appeals for the Fifth Circuit (5th Cir.)**, 359 F.3d 738, 2004. Disponível em: https://caselaw.findlaw.com/court/us-5th-circuit/1119030.html. Acesso em: 10 out. 2025.

VIOL, Dalila Martins. **Programas de Integridade e Combate à Corrupção:** aspectos teóricos e empíricos da multiplicação do compliance anticorrupção no Brasil. São Paulo: Almedina Brasil, 2021. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556273815.

YOCKEY, G. C. Dueling Cultures of Compliance: The Impact of Cooperation on Internal Ethical Systems in the FCPA Context. **Wisconsin Law Review**, Madison, v. 2012, n. 3, p. 687-718, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029241. Acesso em: 12 out. 2025.

ZAGANELLI, Margareth Vetis. Corrupção empresarial e compliance: um estudo comparado no Brasil e Argentina. **Humanidade & Tecnologia**, Curitiba, v. 57, p. 14–27, abr./jun. 2025. Disponível em: https://revistas.icesp.br/index.php/FINOM_Humanidade_Tecnologia/article/download/6235/3828. Acesso em: 2 nov. 2025.

ZENKNER, Marcelo. **Integridade governamental e empresarial:** um espectro da repressão e da prevenção à corrupção no Brasil e em Portugal. Belo Horizonte: Fórum, 2019.