




**FEBRABAN**

Federação Brasileira de Bancos

# GUIA | **BOAS PRÁTICAS DE COMPLIANCE**

*Edição revista e atualizada 2018*



*Compliance* transcende a ideia de “estar em conformidade” às leis, regulamentações e autorregulamentações, abrangendo aspectos de governança, conduta, transparência e temas como ética e integridade.

# GUIA | BOAS PRÁTICAS DE COMPLIANCE

*Edição revista e atualizada | 2018*



**COMPLIANCE**

Win! Win!



# 1. INTRODUÇÃO

A regulação do mercado financeiro está sempre em evolução e o ritmo de implantação de novas regras normalmente é alterado mediante situações de crises. Um marco, nesse sentido, foi a crise internacional de 2007-2009, conhecida como *subprime* e marcada por uma bolha imobiliária, novas e complexas formas de securitizações e falta de transparência e regulação, culminando em falências e intervenções em Instituições Financeiras.

Nesse contexto, têm sido implementadas novas regulamentações internacionais com a intenção de promover o aumento da transparência e a melhoria da qualidade da relação entre as Instituições que fazem parte do sistema financeiro e seus clientes e investidores, em temas relacionados a fraude, corrupção, atos ilícitos e denúncias. Como exemplos, podem ser mencionados: *Dodd-Frank Act*, *Foreign Account Tax Compliance Act* (FATCA), *Common Reporting Standard* (CRS) e *UK Bribery Act*.

No Brasil, também foram publicadas novas leis e regulamentações reforçando a necessidade de maior governança das empresas e Instituições Financeiras em relação à prevenção e ao combate à corrupção e a outros atos ilícitos, com destaque para a Lei Anticorrupção (nº 12.846/13), regulamentada pelo Decreto nº 8.420/15, e a Lei nº 12.683/12, que reforça os mecanismos de prevenção à lavagem de dinheiro previstos na Lei nº 9.613/98. Foi ainda publicada, em nosso país, regulamentação exigindo que as Instituições Financeiras implementem política que garanta a manutenção da transparência, responsabilidade e diligência na oferta e venda de produtos e serviços a seus consumidores; trata-se da Resolução CMN nº 4.539/16. Mais recentemente, foram divulgadas a Resolução CMN nº 4.595/17 e a Circular Bacen nº 3.865/17 exigindo que Instituições Financeiras, Administradoras de Consórcio e Instituições de Pagamento implementem Política de *Compliance* (Conformidade).

Tendo em vista essas e outras mudanças recentes no ambiente regulatório, a crescente globalização do mercado financeiro e a exigência de padrões éticos cada vez mais altos pelos diversos *stakeholders*, as Instituições Financeiras estão sendo compelidas a evoluir e reestruturar suas estratégias, estruturas organizacionais e tecnologias.

Nesse ambiente, a função de *Compliance* ganha cada vez mais importância como mecanismo de prevenção, detecção e resposta a práticas indevidas que possam implicar descumprimento de normas e de padrões de ética e conduta, ajudando a proteger a imagem e reputação e desenvolver valor para as Instituições Financeiras.

Em razão da relevância do tema, do aumento da abrangência e da evolução do escopo de atuação de *Compliance* ocorrida ao longo dos últimos anos e para possibilitar o melhor entendimento da interface entre *Compliance* e outras estruturas, como Controles Internos, Gestão de Riscos e Auditoria Interna, na governança corporativa, foi constituído, na Subcomissão de *Compliance* da Febraban e no Comitê de *Compliance* da ABBI, um grupo de trabalho para:

- atualizar e aprimorar a discussão proposta na versão anterior deste documento;
- sugerir bases para a discussão sobre tendências de atuação de *Compliance*.

É importante ressaltar que este documento tem como objetivo compartilhar boas práticas relacionadas à função de *Compliance*, mas que elas devem ser adaptadas ao porte, complexidade, estrutura, perfil de risco e modelo de negócio de cada Instituição.

Além da atuação preventiva e detectiva, *Compliance* cada vez mais tem se tornado uma atividade também consultiva, dando suporte aos objetivos estratégicos e fazendo parte da missão, visão, valores, cultura e gerenciamento de riscos das Instituições.

## 2. CONCEITOS GERAIS

A adoção da função de *Compliance* contribui para a prevenção e mitigação de exposições a riscos regulatórios (locais e internacionais) e de conduta e danos à imagem da Instituição, por meio de medidas internas que disciplinam as suas atividades.

*Compliance* transcende a ideia de “estar em conformidade” às leis, regulamentações e autorregulamentações, abrangendo aspectos de governança, conduta, transparência e temas como ética e integridade.

Além da atuação preventiva e detectiva, *Compliance* cada vez mais tem se tornado uma atividade também consultiva, dando suporte aos objetivos estratégicos e fazendo parte da missão, visão, valores, cultura e gerenciamento de riscos das Instituições.

### 2.1 Risco de *Compliance*

É o risco de sanções legais ou regulatórias, perdas financeiras ou danos reputacionais, bem como de medidas administrativas ou criminais decorrentes da falta de cumprimento de disposições legais e regulamentares, normas de mercado local e internacional ou decorrentes de compromissos assumidos por meio de códigos de autorregulação, padrões técnicos ou códigos de conduta.

### 2.2 Responsabilidades Gerais Relacionadas à Atividade de *Compliance*

A Alta Administração deve estabelecer as diretrizes da atividade de *Compliance* na Instituição e disponibilizar os recursos necessários, além de disseminar a cultura de *Compliance* pelo exemplo (tone at the top).

A estrutura de *Compliance* pode ser estabelecida por meio da adoção de linhas de defesa, para atribuição de papéis e responsabilidades, assegurando independência e a adequada segregação de funções.

O profissional de *Compliance* deve fornecer à Alta Administração informações sobre o gerenciamento do risco de *Compliance*, mas cabe destacar que cada colaborador, independentemente do nível hierárquico ou do tipo de contrato de trabalho ou serviço que presta à Instituição, deve estar comprometido com a prática e a disseminação da cultura de *Compliance*.

As responsabilidades estão detalhadas ao longo deste documento.

### 2.3 Programa de Compliance

O Programa de *Compliance* é composto de políticas, procedimentos e planejamento de atividades que visam fortalecer as Instituições direcionando as ações para a condução dos negócios de forma adequada, em relação ao cumprimento das leis e regulamentações, questões de ética e conduta, aspectos concorrenciais e socioambientais, contratos com terceiros, normas contábeis, entre outros.

Para construção de um programa efetivo, devem-se considerar as boas práticas disponíveis globalmente e adequá-las ao porte, à complexidade, à estrutura, ao perfil de risco, ao modelo de negócio e à base legal e regulatória a que a Instituição está submetida.

A estrutura da área de *Compliance* bem como suas responsabilidades devem estar aderentes às exigências legais e regulamentares aplicáveis nas jurisdições em que a Instituição opera.

O Programa de *Compliance* deve definir processos que abranjam a identificação, mensuração e priorização, resposta ao risco, monitoramento e reporte dos riscos, levando em consideração a Abordagem Baseada em Risco e o modelo de Linhas de Defesa que serão tratados na sequência, assim como a gestão integrada com os demais riscos a que a Instituição esteja sujeita.

O estabelecimento de um Programa de *Compliance* efetivo e perene pode gerar muitos benefícios, mantendo a Instituição protegida em um ambiente de negócios complexo, repleto de mudanças regulatórias, e gerando confiança em seus *stakeholders*.

### 2.4 Abordagem Baseada em Risco

Considerando a crescente complexidade e a dinâmica do mercado financeiro em nível global, cada vez mais se faz necessária a adoção de gestão de *Compliance* baseada em risco, para garantir foco nos aspectos mais relevantes.

A Abordagem Baseada em Risco pressupõe que cada Instituição adote uma avaliação de risco de *Compliance* de acordo com seu modelo de negócios, apetite ao risco e ambiente regulatório a que está sujeita, não existindo assim um modelo uniforme para todas as Instituições. Identificar, avaliar e classificar esses riscos é um dos passos mais importantes na criação de um programa sólido de *Compliance*.

O risco é dinâmico e deve ser periodicamente revisado, sendo essencial que as classificações de risco reflitam adequadamente os riscos presentes e resultem em avaliações que gerem medidas práticas para mitigá-los e controlá-los.



## 2.5 Linhas de Defesa

O engajamento de toda a Instituição na atividade de *Compliance*, estabelecendo a adequada segregação de funções e independência das áreas, pode ser alcançada por meio da adoção do modelo de Linhas de Defesa.

Cada uma dessas “linhas” desempenha um papel distinto dentro da estrutura de governança da Instituição, atuando de forma interdependente.

Essa estruturação é aplicável a qualquer Instituição, não importando seu tamanho ou complexidade.

### 1ª Linha de Defesa: Atividades de Negócios e Operacionais

Os gestores de negócio, de suporte e operacionais devem ser os responsáveis primários por identificar, avaliar, tratar, controlar e reportar os riscos de suas áreas, de forma alinhada às diretrizes internas, regulamentações, políticas e procedimentos aplicáveis.

### 2ª Linha de Defesa: Atividades de *Compliance*, Controles Internos e Gerenciamento de Riscos

Essas unidades corporativas devem ser independentes da gestão das linhas de negócio (1ª Linha de Defesa) e atuar como facilitadoras na implementação de práticas eficazes de gerenciamento de riscos e metodologia de Controles Internos e *Compliance*, bem como dar suporte às áreas de negócios e operacionais de forma consultiva.

São responsáveis também por testar e avaliar a aderência à regulamentação, políticas e procedimentos, mantendo padrões de integridade alinhados aos princípios, diretrizes e apetite ao risco adotados pela Instituição e reportando sistemática e tempestivamente à Alta Administração os resultados de suas análises em relação à conformidade.

Para serem efetivas, essas funções devem ter autoridade, recursos e acesso à Alta Administração da Instituição.

### 3ª Linha de Defesa: Auditoria Interna

A Auditoria Interna tem o papel de fornecer aos órgãos de governança e à Alta Administração avaliações abrangentes, independentes e objetivas relativas aos riscos da Instituição.

A independência da atuação desta linha permite que esta revise de modo sistemático a eficácia das duas primeiras linhas de defesa, contribuindo para o seu aprimoramento.

A close-up photograph of a hand holding a rectangular wooden block. The block is light-colored with a visible wood grain. The word "PRINCÍPIOS" is engraved in a bold, red, sans-serif font on the side of the block. The block is being held in a way that it is slightly elevated above a stack of other similar wooden blocks. The background is dark and out of focus.

**PRINCÍPIOS**

## 3. PRINCÍPIOS DE COMPLIANCE E RESPONSABILIDADES

### 3.1 Em relação às Responsabilidades do Conselho de Administração

O Conselho de Administração, quando existente, é responsável por acompanhar o gerenciamento do risco de *Compliance* da Instituição Financeira, devendo:

- aprovar a Política de *Compliance*, de acordo com regulamentação vigente;
- assegurar:
  - a. adequada gestão da Política de *Compliance* da Instituição;
  - b. efetividade e continuidade da aplicação da Política de *Compliance*;
  - c. comunicação da Política de *Compliance* a todos os colaboradores e prestadores de serviços terceirizados relevantes;
  - d. disseminação de padrões de integridade e conduta ética como parte da cultura da Instituição;
- garantir que a Alta Administração, com apoio da função de *Compliance*, implemente medidas corretivas para não conformidades identificadas;
- prover os meios necessários para que as atividades relacionadas à função de *Compliance* sejam exercidas adequadamente, incluindo pessoas em quantidade, capacitação e experiência suficientes;
- avaliar, pelo menos anualmente, a efetividade do gerenciamento do risco de *Compliance*.

Na inexistência do Conselho de Administração, suas responsabilidades devem ser incorporadas pela Alta Administração.

O Conselho de Administração e a Alta Administração permanecem responsáveis pela conformidade e efetividade de possíveis atividades da função de *Compliance* que sejam terceirizadas.

### 3.2 Em relação às Responsabilidades do Comitê de Auditoria

O Comitê de Auditoria, quando existente, deve:

- avaliar a Política de *Compliance* antes da aprovação pelo Conselho de Administração;
- analisar, no mínimo anualmente, a efetividade do gerenciamento de *Compliance* em relação a aspectos como independência, estrutura e recursos, papéis e responsabilidades, aderência à regulamentação e cumprimento da Política de *Compliance*;
- encaminhar ao Conselho de Administração sua avaliação sobre a efetividade do gerenciamento de *Compliance*;
- avaliar resultados de inspeções e trabalhos de reguladores e autorreguladores, resultados das auditorias internas e externas e apontamentos relevantes.

### 3.3 Em relação às Responsabilidades da Alta Administração

A Alta Administração da Instituição Financeira é responsável por:

- gerenciar efetivamente o risco de *Compliance*;
- implantar e divulgar a Política de *Compliance*, bem como assegurar sua observância;
- estabelecer área de *Compliance* permanente, efetiva, independente, com acesso a qualquer informação ou área da Instituição e com recursos adequados;
- adotar medidas corretivas para tratamento de não conformidades identificadas;
- manter o Conselho de Administração informado a respeito do gerenciamento do risco de *Compliance*;
- reportar tempestivamente ao Conselho de Administração falhas relevantes de *Compliance* que possam gerar riscos legais, sanções regulatórias, perdas financeiras ou de reputação relevantes.

A Alta Administração deve ainda, no mínimo anualmente, com o suporte da função de *Compliance*:

- avaliar os principais riscos de *Compliance* e respectivos planos de ação;
- informar o Conselho de Administração sobre a efetividade do gerenciamento do risco de *Compliance*.

### 3.4 Em relação à Função de *Compliance*

A função de *Compliance* deve ser baseada nos seguintes princípios:

- independência no exercício de suas funções, que pressupõe (i) a formalização de suas responsabilidades, (ii) a existência de um gestor responsável e com senioridade para condução dos trabalhos de gerenciamento dos riscos de *Compliance*, (iii) a ausência de conflito de interesses e (iv) o acesso a qualquer informação, colaborador ou administrador da Instituição;
- segregação em relação às áreas de negócios, operacionais e Auditoria;
- comunicação direta com a Alta Administração e o Conselho de Administração (se existente);
- alocação de pessoas em quantidade e com perfis adequados, bem como de recursos financeiros suficientes, para o desempenho efetivo das responsabilidades relacionadas à função de *Compliance*;
- remuneração independente do desempenho direto das áreas de negócios, de forma a evitar conflitos de interesses.

As sugestões de práticas para cumprimento desses princípios são apresentadas no item “Atribuições ou Funções de *Compliance*”.



## 4. POLÍTICA DE COMPLIANCE

A Instituição deve elaborar e manter Política de *Compliance* compatível com a natureza, porte, complexidade, estrutura, perfil de risco e modelo de negócio, a qual deve ser aprovada pelo Conselho de Administração (ou, na sua ausência, pela Alta Administração), estabelecendo, no mínimo:

- objetivo e escopo das atribuições de *Compliance*;
- diretrizes a serem seguidas por todos os administradores, colaboradores e terceiros e principais processos utilizados para identificação e gestão dos riscos de *Compliance* por todos os níveis da Instituição;
- definição clara de responsabilidades, de modo a evitar possíveis conflitos de interesses;
- alocação adequada de pessoal (quantidade, capacitação e experiência);
- posição na estrutura organizacional;
- garantia de independência e autoridade dos responsáveis;
- alocação de recursos adequados para desempenho das atividades;
- livre acesso às informações necessárias para o exercício das atribuições;
- canais de comunicação com a Alta Administração, o Comitê de Auditoria e o Conselho de Administração para reporte das atividades e das não conformidades identificadas;
- processos de coordenação com as demais áreas de Gestão de Riscos, Controles Internos e Auditoria Interna da Instituição.

**REGULA**

**Guidel**

**Rule**

**LAW**

**Procees**





## 5. ATRIBUIÇÕES OU FUNÇÕES DE COMPLIANCE

Recomenda-se a definição de unidade específica responsável pela coordenação das funções de *Compliance*. Independentemente da existência da referida unidade específica, os responsáveis pelas funções de *Compliance* deverão dar suporte ao Conselho de Administração e à Alta Administração no gerenciamento efetivo dos riscos de *Compliance* por meio das atividades exemplificadas abaixo, que devem ser adequadas de acordo com a realidade de cada Instituição.

Nem todas as “atribuições ou funções de *Compliance*” precisam ser obrigatoriamente conduzidas por uma área ou departamento de *Compliance*, mas as divisões de responsabilidades devem ser claras, não deve haver conflitos de interesses e o responsável por *Compliance* deve ser capaz de exercer suas responsabilidades de forma efetiva.

### 5.1 Consultoria, Orientação, Treinamento e Capacitação

- **Garantir disseminação da cultura e temas de *Compliance*, apoiando a Alta Administração na definição de treinamento e capacitação adequada a todos os colaboradores e prestadores de serviços terceirizados relevantes.**

Sugestões de práticas:

- a. Disseminar permanentemente a cultura de *Compliance* em todos os níveis e linhas de defesa da Instituição.
  - b. Definir os canais de comunicação e plano de treinamento e capacitação aplicáveis aos colaboradores e prestadores de serviços terceirizados relevantes.
  - c. Identificar as áreas com necessidades de treinamento específico e capacitação em *Compliance*, ética e conduta para atuação prioritária.
  - d. Estabelecer canal para tratamento de dúvidas relacionadas a *Compliance*.
  - e. Divulgar apropriadamente o canal de denúncias de atos ilícitos, descumprimentos regulatórios, condutas inapropriadas ou ilícitas ou práticas que firam os princípios e padrões éticos.
- **Atuar como área consultiva nos temas relacionados a *Compliance*.**

Sugestões de práticas:

- a. Orientar e aconselhar os gestores e colaboradores da Instituição (incluindo os membros da Diretoria e do Conselho de Administração), em relação à conformidade com leis, regulamentações e autorregulamentações.
- b. Elaborar pareceres e opiniões sobre temas de *Compliance* de forma a assegurar a avaliação correta de eventuais riscos e estratégias para controle e mitigação.

- c. Revisar o conteúdo, adequação e conformidade de materiais e documentos (como regulamentos, materiais de divulgação, termos de adesão e ciência de riscos e *disclaimers*).
  - d. Auxiliar na solução de questões relacionadas a *Compliance*, ética e conduta, evidenciando os pontos sensíveis e respectivas sugestões e apoiando a tomada de decisões pelos gestores e colaboradores da Instituição.
- **Assegurar a existência de normativos internos (políticas, circulares, manuais etc.) e processos e procedimentos atualizados.**

Sugestões de práticas:

- a. Assegurar a elaboração e atualização de diretrizes institucionais em relação a valores, princípios, padrões éticos e normas de conduta, incluindo elaboração e disponibilização de Código de Conduta acessível a todos os colaboradores.
- b. Garantir a existência de fluxo e critérios de elaboração, aprovação e atualização dos normativos internos (políticas, circulares, manuais etc.), sua divulgação eficaz para todos os colaboradores impactados, definição de prazos para sua revisão e coerência com os processos e atividades da Instituição e as demandas regulatórias.
- c. Assegurar que os colaboradores tenham conhecimento de seus papéis e responsabilidades e propiciar a comunicação adequada entre as áreas da Instituição, garantindo o seu claro entendimento.
- d. Certificar a existência de processo apropriado para criação e revisão da estrutura funcional das áreas e distribuição de responsabilidades, contemplando a segregação adequada de atividades e mitigando os potenciais conflitos de interesses.
- e. Garantir processos adequados de remuneração, incentivos e gestão de desempenho que mitiguem conflitos de interesses.
- f. Assegurar a existência de diretrizes relacionadas a medidas disciplinares.

## 5.2 Identificação, Mensuração e Priorização de Riscos de *Compliance*

- **Atuar proativamente na definição e manutenção de programas relacionados a *Compliance*.**

Sugestões de práticas:

Definir metodologia para: (i) identificação dos riscos de forma proativa, por exemplo, por meio do acompanhamento de mudanças e tendências do ambiente regulatório, nos negócios ou em produtos; (ii) mapeamento e registro atualizado dos riscos; (iii) critério de classificação dos riscos para utilização da Abordagem Baseada em Risco.

- **Identificar e avaliar a aderência da Instituição ao arcabouço legal e regulatório, às recomendações de órgãos de supervisão e autorregulação e aos códigos de conduta e riscos envolvidos.**

Sugestões de práticas:

- a. Identificar reguladores, autorreguladores e demais entidades no Brasil e no exterior (quando aplicável) que norteiam os mercados de atuação da Instituição.
  - b. Estabelecer, conjuntamente com as demais áreas pertinentes da Instituição, os processos para captura e avaliação das leis, normativos, regulamentos, resoluções, instruções, circulares, códigos, termos de compromisso, termos de ajustamento de conduta, recomendações e códigos, políticas e procedimentos internos etc.
  - c. Definir a metodologia de análise legislativa e normativa e acompanhar a adequação da Instituição à legislação, regulamentação e autorregulamentação aplicáveis, identificando responsáveis e prazos para implantação de planos de ação a fim de assegurar aderência e cumprimento.
  - d. Identificar e registrar os riscos inerentes e possíveis riscos residuais de *Compliance*, relacionados não somente à conduta e ética, mas também riscos de *Compliance* relativos a riscos operacionais e de crédito, liquidez, mercado, entre outros. Entre os exemplos de temas relevantes a serem abordados, estão aqueles concernentes à gestão socioambiental, gestão de terceiros e contratos, defesa da concorrência, propriedade intelectual, informação privilegiada e conflitos de interesses, fraude e prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, práticas contábeis, trabalhistas e tributárias.
  - e. Definir metodologia de mensuração e priorização de riscos de *Compliance* de acordo com critérios objetivos.
  - f. Acompanhar as tendências dos órgãos reguladores e autorreguladores no Brasil e no exterior (quando aplicável) e dos avanços tecnológicos, visando a uma atuação preventiva na mitigação de riscos.
- **Participar na aprovação de produtos e serviços e de potenciais parceiros e clientes.**

Sugestões de práticas:

- a. Assegurar a existência de processo adequado para avaliação de produtos ou serviços em relação aos padrões corporativos e às legislações e regulamentações vigentes.
- b. Emitir pareceres sob a perspectiva de riscos de *Compliance* quando da aprovação e revisão dos produtos e serviços nos fóruns pertinentes da Instituição.
- c. Assegurar a implantação dos planos de ação para mitigação dos possíveis riscos de *Compliance* identificados em produtos ou serviços.

- d. Garantir a existência de metodologia de análise dos riscos de conduta e de reputação envolvendo parceiros, representantes e clientes, mediante a análise de dados cadastrais, informações na mídia, identificação de beneficiários finais e Pessoas Expostas Politicamente (PEPs), de forma a prevenir a realização de negócios com contrapartes inidôneas, suspeitas de envolvimento em atividades ilícitas ou que possam causar dano à imagem e reputação da Instituição.

- **Atuar proativamente na definição e manutenção de programas relacionados a *Compliance*.**

Sugestões de práticas:

Desenvolver proativamente programas para temas específicos, adequados à natureza, porte, complexidade, estrutura, perfil de risco e modelo de negócio da Instituição e de acordo com a evolução do ambiente regulatório, como, por exemplo:

- a. “Programa de Integridade, Ética e Prevenção à Corrupção” – para garantir a existência de código ou política relacionada à integridade, ética ou conduta de acordo com os princípios e valores da Instituição e as diretrizes sobre a forma de atuação em relação a todos os *stakeholders*.
- b. “Programa Socioambiental” – para assegurar a implantação de normativos internos sobre riscos socioambientais e sustentabilidade, incluindo critérios para mitigar riscos socioambientais na avaliação de clientes e concessão de crédito e acompanhando as tendências e boas práticas nacionais e internacionais.
- c. “Programa de Relacionamento com Clientes” – para assegurar a definição de normativo interno com diretrizes para o relacionamento com clientes e usuários da Instituição, acompanhando as iniciativas para avaliar as questões de conduta de colaboradores, de segurança da informação e de oferta de produtos e serviços e mitigando os riscos inerentes do relacionamento com clientes e usuários.
- d. Programa de Barreiras de Informação” – para assegurar o desenvolvimento e aplicação de diretrizes a fim de garantir o fluxo apropriado de informações privilegiadas, com monitoramento adequado, observando os aspectos legais, de *e-mails*, mensagens eletrônicas, telefones e demais meios de comunicação corporativos.
- e. “Programas de Certificação” – para garantir a identificação das regulamentações que exijam avaliação e emissão periódica de relatório em relação às atividades de *Compliance*.
- f. “Programa de *Suitability*” – para garantir que o perfil de investimento dos clientes investidores seja avaliado, de maneira a assegurar a adequação do investimento recomendado ao respectivo cliente.
- g. “Programa de Prevenção e Resolução de Conflitos de Interesses” – para identificar e administrar potenciais conflitos de interesses dentro da Instituição.

- **Assegurar a existência de processos definidos para atendimento a regulamentações específicas.**

Sugestões de práticas:

Auxiliar no desenvolvimento de processos e sistemas, que podem ou não estar diretamente sob responsabilidade da área de Compliance, mas que precisam ser avaliados e acompanhados, como, por exemplo:

- a. “Sistema de Segurança da Informação” – assegurar a implantação de sistema que permita o acesso restrito e controlado a informações sensíveis, estabelecendo um fluxo de aprovação capaz de verificar as solicitações de acesso e o adequado acesso compatível com as funções dos colaboradores e garantindo a confidencialidade das informações sigilosas e a inexistência de conflito de interesses.
- b. “Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo” – assegurar a adoção de medidas como: (i) disseminação da cultura de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, por meio de treinamento e capacitação adequados (presenciais ou via e-learning) de todos os colaboradores e prestadores de serviço terceirizados relevantes, incluindo correspondentes no país; (ii) análise apropriada do “conheça seu cliente”, “conheça seu fornecedor”, “conheça seu parceiro” e “conheça seu colaborador”, com o intuito de identificar, por meio de metodologia baseada em risco, os clientes de baixo, médio e alto risco, identificando até o nível dos beneficiários finais e Pessoas Expostas Politicamente (PEPs) e demais atributos classificados como “especial atenção”; (iii) monitoramento das transações e mídias, com o objetivo de detectar operações atípicas, prevenir a realização de negócios com contrapartes inidôneas, suspeitas de envolvimento em atividades ilícitas ou que possam causar dano à reputação da Instituição; (iv) condução de investigações e diligências reforçadas quando necessário; (v) elaboração de relatórios e comunicações tempestivas às áreas competentes da Instituição e aos órgãos reguladores pertinentes.
- c. “Monitoramento de Práticas Abusivas” – assegurar a existência de processos adequados de *trade surveillance* para prevenir ou corrigir práticas e condutas ilícitas ou inapropriadas por parte de colaboradores e clientes, monitorando sistemática e permanentemente as transações, elaborando relatórios e estabelecendo comunicação tempestiva e adequada com as áreas de negócios e administrativas da Instituição e órgãos reguladores pertinentes.
- d. “Vedações e Sanções Comerciais” – assegurar a adoção de procedimentos para evitar que a Instituição realize negócios e pagamentos com partes vedadas ou sancionadas, observando regras dos órgãos reguladores e autorreguladores e dos organismos internacionais pertinentes.

### 5.3 Monitoramento, Testes e Reporte

- **Monitorar a exposição aos riscos de *Compliance* e testar os controles.**

Sugestões de práticas:

- Instituir critérios e metodologia para monitoramento (acompanhamento periódico), como, por exemplo, por meio da utilização de indicadores.
  - Estabelecer metodologia para testes dos controles, levando-se em consideração a Abordagem Baseada em Risco.
  - Definir programa de monitoramento e testes, abrangendo riscos de conduta inapropriada ou ilícita, à reputação e regulatórios.
  - Acompanhar multas e passivos relevantes gerados por não conformidades.
  - Monitorar situações que possam afetar a reputação da Instituição para possibilitar reporte adequado interna e externamente, conforme aplicável.
- **Relatar sistemática e periodicamente os resultados das atividades relacionadas a *Compliance* ao Conselho de Administração, à Alta Administração e aos demais níveis organizacionais.**

Sugestões de práticas:

- Comunicar periodicamente a situação de conformidade aos níveis adequados da Instituição, incluindo, por exemplo, avaliações de risco de *Compliance*, mudanças nos perfis de risco, indicadores, falhas identificadas e evolução dos planos de ação.
- Definir periodicidade da comunicação dos resultados das atividades relacionadas à função de *Compliance* ao Conselho de Administração e demais níveis organizacionais pertinentes.
- Estabelecer canal de comunicação com a Alta Administração e o Conselho de Administração para: (i) reporte tempestivo de alterações relevantes da legislação aplicável, dos riscos e dos controles; (ii) planos de ação a fim de sanar eventuais não conformidades, independentemente dos reportes periódicos definidos acima.
- Prestar suporte à Alta Administração e ao Conselho de Administração da Instituição na execução de suas responsabilidades e na garantia do cumprimento da Política de *Compliance*.
- Manter a Alta Administração e o Conselho de Administração informados sobre alterações ou atualizações relevantes dos procedimentos de *Compliance* e nível de aderência da Instituição à regulamentação aplicável.
- Elaborar relatório de conformidade, com periodicidade mínima anual, consolidando os resultados das atividades de *Compliance* e incluindo as recomendações e ações tomadas, além do resultado do gerenciamento dos apontamentos apresentados em relatórios anteriores.
- Apresentar o relatório de conformidade ao Conselho de Administração e mantê-lo à disposição dos reguladores pelo prazo mínimo de cinco anos.

## 5.4 Relacionamento com Reguladores, Autorreguladores, Entidades de Representação e Auditores Independentes

- **Garantir relacionamento ético e íntegro com reguladores, autorreguladores, entidades de representação e auditores independentes, assegurando o atendimento adequado.**

Sugestões de práticas:

- a. Assegurar a existência de processos apropriados para o atendimento tempestivo e com qualidade adequada das demandas de reguladores, supervisores e autorreguladores, informando, sempre que necessário, a Alta Administração e o Conselho de Administração sobre o andamento dos trabalhos e resultados.
- b. Assegurar a definição de processo para envio ou disponibilização de informações regulatórias consistentes e tempestivas.
- c. Revisar e acompanhar os planos de ação para cumprimento dos apontamentos relacionados aos casos de não conformidades legais apresentadas pelos reguladores e auditores independentes.
- d. Estabelecer critérios de acompanhamento dos referidos planos de ação, identificando as áreas responsáveis, definindo os prazos de implantação e informando, sempre que necessário, a Alta Administração e o Conselho de Administração.
- e. Participar de reuniões e grupos de trabalho, organizados por reguladores, autorreguladores e entidades de representação, com o intuito de contribuir com as discussões dos temas de *Compliance*, auxiliando na revisão de práticas e regras de mercado, bem como da melhor forma de atender à legislação aplicável, sempre em linha com as necessidades dos negócios da Instituição.





## 6. SINERGIA ENTRE COMPLIANCE E AS DEMAIS ÁREAS DA INSTITUIÇÃO

A função de *Compliance* atua de forma interdisciplinar e com interação constante com as demais áreas da Instituição.

### 6.1 *Compliance* e Controles Internos

Os Controles Internos, independentemente do porte da Instituição, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas.

São algumas das responsabilidades dos Controles Internos:

- mapear os processos, riscos e controles críticos para atingimento dos objetivos da organização, em linha com as diretrizes de *frameworks* mundialmente aceitos, como *The Committee of Sponsoring Organizations of the Treadway Commission* (COSO);
- certificar, de forma independente, a existência, a efetividade e a execução dos controles;
- elaborar e aplicar *Control Self-Assessment* (Autoavaliação de Controles ou CSA) para assuntos administrativos e operacionais de menor relevância;
- elaborar e aplicar *Entity-Level Controls* (Controles de Nível de Entidade) para verificar a estrutura de governança da Instituição;
- executar os Testes de Aderência;
- emitir parecer em relação aos riscos de Controles Internos e assuntos correlatos.

Em algumas Instituições, a área de Controles Internos pode ser responsável por atividades relacionadas à função de *Compliance*, como, por exemplo, a realização de testes de conformidade com leis e regulamentações. Nesses casos, as responsabilidades de cada área devem estar claras e formalizadas, devendo haver coordenação adequada para a realização das atividades e avaliação dos resultados.

## 6.2 Compliance e Auditoria Interna

As Instituições devem implementar e manter atividade de Auditoria Interna compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da Instituição.

A Auditoria Interna é uma atividade independente, de avaliação objetiva de todo o processo de governança e validações por meio de testes dos processos e controles, sempre baseados no perfil de risco da Instituição.

São algumas das responsabilidades da Auditoria Interna:

- realizar auditorias com metodologia aderente aos padrões reconhecidos nacional e internacionalmente, conforme cronograma do Plano Anual;
- analisar a efetividade e a eficiência dos sistemas e processos de *Compliance* e Controles Internos, de gerenciamento de riscos e de governança corporativa, considerando os riscos atuais e potenciais riscos futuros;
- avaliar a confiabilidade, a efetividade e a integridade dos processos e sistemas de informações gerenciais;
- assegurar a observância ao arcabouço legal, à regulamentação infralegal, às recomendações dos organismos reguladores e aos códigos de conduta internos aplicáveis aos membros do quadro funcional da Instituição;
- salvaguardar os ativos e as atividades relacionadas à função financeira da Instituição, bem como atender às demandas específicas de órgãos reguladores e autorreguladores, Conselho de Administração, Alta Administração e comitês.

Em geral, os trabalhos de Auditoria Interna são realizados mediante abordagem sistemática, realizada de maneira aleatória e temporal, por meio de amostragens, e *Compliance* efetua essa abordagem de forma rotineira e permanente.

*Compliance* deve acompanhar os planos de ação de apontamentos da Auditoria Interna relacionados à conformidade, podendo também levar em conta os resultados dos trabalhos da Auditoria Interna em sua avaliação do ambiente de *Compliance*.

A área de *Compliance* deve estar no escopo de avaliação regular e periódica da Auditoria Interna, devendo haver independência entre elas.

### 6.3 Compliance e Jurídico

O Departamento Jurídico orienta sobre a forma pela qual o negócio pode ser conduzido, dentro do arcabouço regulatório do país onde a atividade se desenvolve.

São algumas das responsabilidades do Jurídico:

- assessorar em questões legais;
- elaborar parecer quanto aos riscos legais envolvendo produtos, serviços e processos operacionais, sob a ótica da doutrina e jurisprudência;
- emitir parecer quanto à aplicabilidade de determinada norma legal ou regulamentar, quando houver obscuridade ou controvérsia a seu respeito.

O Jurídico faz parte da primeira linha de defesa, e *Compliance* da segunda linha de defesa. Embora, em algumas Instituições, *Compliance* e Jurídico possam estar subordinados à mesma estrutura organizacional, *Compliance* deve ter garantida sua independência de atuação.

*Compliance* deve posicionar-se em relação a temas que, mesmo legais no sentido jurídico, possam ir contra valores éticos ou de conduta da Instituição.

### 6.4 Compliance e as Áreas de Negócios, Produtos e Suporte

Como quase toda a atuação das Instituições Financeiras é regulamentada, deve existir parceria entre as áreas da primeira linha de defesa e *Compliance* para a boa condução dos negócios.

A atuação de *Compliance* é importante para orientação das áreas sobre eventuais penalidades que possam ser aplicadas pelos órgãos reguladores e autor-reguladores e pela própria Instituição, no caso de inobservância de legislações, regulamentações, autorregulamentações ou mesmo normas internas.

Os produtos e serviços comercializados pela Instituição devem estar em conformidade às diversas regulamentações existentes; para tanto, *Compliance* deve participar e acompanhar a criação, manutenção, alteração e oferta deles, pois sua atuação visa proteger a Instituição tanto no sentido de eventuais sanções legais ou regulatórias quanto no que se refere a perdas financeiras e danos reputacionais.

Além disso, alguns outros temas exigem constante interação entre as áreas, como, por exemplo, os relacionados a: conduta em relação a clientes e mercado, conflitos de interesses, barreira de informações, *suitability*, prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo, responsabilidade socio-ambiental e privacidade.

## 6.5 *Compliance* e os Comitês

*Compliance* tem atuação interdisciplinar e deve envolver-se nas tomadas de decisões estratégicas da Instituição, especialmente quando se referem a produtos, serviços, relacionamento com o cliente ou com o mercado, interpretação de leis e regulamentações, planos de ação para cumprimento de requerimentos legais ou regulatórios, entre outros; para tanto, é imprescindível que participe dos comitês que tratam desses assuntos.

Comitês de produtos e serviços, de integridade e ética e de riscos são alguns dos quais *Compliance* deve participar e ter liberdade para se posicionar, com independência das áreas de negócio, garantindo que os riscos envolvidos sejam levados à atenção dos participantes.

A função de *Compliance* deve prestar subsídios em relação à interpretação de leis e regulamentos e riscos envolvidos, para a correta tomada de decisão.

## 7. PERFIL DO PROFISSIONAL DE COMPLIANCE

Embora não exista uma formação específica para atuar na função de *Compliance*, o profissional deve ter experiência, conhecimento e qualidades pessoais e profissionais que possibilitem a condução das atividades de forma adequada, como:

- sólidos valores éticos e de integridade, demonstrados por meio de sua conduta e atitudes;
- capacidade de entendimento da cultura da Instituição Financeira, seu contexto e a natureza das atividades;
- conhecimento do ambiente regulatório e de seus impactos na Instituição;
- capacidade de formar parceria com as diversas áreas da Instituição, mantendo sua independência;
- habilidade de comunicação e argumentação com todos os níveis da Instituição e órgãos reguladores, autorreguladores e fiscalizadores, auditorias e entidades de representação;
- capacidade de influenciar e incentivar comportamentos desejados;
- assertividade e habilidade de dizer “não” em situações que configurem risco;
- independência para expressar sua opinião técnica sem receio de retaliações ou ameaças e isenção para que suas decisões e julgamentos não sejam influenciados por relações de afinidade;
- disponibilidade, empatia e acessibilidade para esclarecer dúvidas e tratar questões dos diversos níveis da Instituição;
- capacidade de lidar com pressão;
- análise crítica, mesmo diante de situações atípicas e adversas, e atenção às oportunidades de melhorias nos processos internos;
- habilidade de se manter atualizado e se antecipar às necessidades ocasionadas por mudanças mercadológicas, novas tecnologias e modelos de negócios, produtos e serviços, ausência de regulamentações, metodologias e padrões de nível global.

## 8. DESAFIOS E TENDÊNCIAS PARA A FUNÇÃO DE COMPLIANCE

A evolução dos padrões de comportamento da sociedade e os avanços no uso da tecnologia, com reflexos para a indústria financeira e consequentemente para o profissional de *Compliance*, trazem grandes desafios diante de sua complexidade e impacto nas práticas de negócio.

Há maior expectativa quanto a comportamentos éticos e transparência nas relações comerciais e ao papel e contribuição das Instituições Financeiras em temas socioambientais e de combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção.

Nesse contexto, o risco reputacional passa a constar de forma ampla e definitiva da agenda de reguladores, autorreguladores e profissionais de *Compliance* e da indústria financeira como um todo. O desafio é alinhar as expectativas do mercado à dinâmica organizacional e transmitir uma mensagem robusta e consistente em relação aos padrões éticos da Instituição.

O mercado tem estabelecido diversas medidas e controles para garantir aderência a esses requisitos e evitar a violação e o não cumprimento de normas e regulamentos. Investimentos em controles, desenvolvimento de políticas e procedimentos, aculturação dos colaboradores, entre outras ações, têm se intensificado de maneira expressiva e contínua.

Destaca-se ainda o desafio de encontrar a forma mais adequada de interagir com o Setor Público, como cliente, fornecedor ou fiscalizador, considerando-se as leis e regulamentações de prevenção à corrupção.

A crescente inovação de produtos, serviços e canais, o uso intensivo de tecnologias e o surgimento de diferentes participantes no mercado trazem desafios adicionais à atuação de *Compliance* pela necessidade de atualização constante em relação à essa dinâmica de negócios, identificação e avaliação de novos riscos e entendimento e implementação de diversas regulamentações trazidas pelos reguladores.

As redes sociais trazem a “voz do cliente”, de forma ampla e praticamente instantânea, demandando tratamento e resposta efetivos e endereçando questões que podem representar risco de imagem.

Por fim, ressalta-se a existência de diversos outros temas, como, por exemplo, defesa da concorrência, privacidade, incentivo a denúncias e riscos no relacionamento com fornecedores, que devem estar cada vez mais presentes na agenda de *Compliance*, seja por demandas de leis e regulamentações, seja por demanda ou mudança no comportamento dos diversos públicos com os quais as Instituições interagem.



## REFERÊNCIAS

ASSI, Marcos. *Governança, riscos e Compliance: mudando a conduta nos negócios*. São Paulo: Saint Paul, 2017.

CANDELORO, Ana Paula P.; DE RIZZO, Maria Balbina Martins; PINHO, Vinícius.

*Compliance 360°: riscos, estratégias, conflitos e vaidades no mundo corporativo*. São Paulo: Trevisan, 2012.

GIOVANINI, Wagner. *Compliance: a excelência na prática*. São Paulo: Câmara Brasileira do Livro, 2014.

GONSALES, Alessandra et al. *Compliance: a nova regra do jogo*. São Paulo: LEC, 2016.

SERPA, Alexandre da Cunha. *Compliance descomplicado: um guia simples e direto sobre programas de Compliance*. 2016.

THE INSTITUTE OF INTERNAL AUDITORS. *IIA position paper: the three lines of defense in effective risk management and control*. 2013.



**FEBRABAN**

Federação Brasileira de Bancos

[www.febraban.org.br](http://www.febraban.org.br)