KPMG

Guia prático do Compliance: O que você precisa saber para começar

Livro Colaborativo
KPMG Business School

Curso Certificação em Compliance
Novembro, 2020

KPMG
BUSINESS SCHOOL

Co-Autores

a. Capítulo 1
i. Carla Micheline Israel
ii. Gildo Manuel Rodrigues
iii. Paula da Silva Carvalho
iv. Priscila Minami Ujihara
v. Silvia Maria Andrade de Faria Nascimento

b. Capítulo 2
i. Ana Cristina Costa Cruz de Rezende
ii. Ariana Amorim de Oliveira
iii. Renata Pinto Bravo Reis
iv. Rodrigo Lazzarini
v. Vanuza Pereira Caju

c. Capítulo 3
i. Emanuela Lima
ii. Mario Jorge Menezes Cardoso
iii. Odair Oregoshi
iv. Paulo Renato Aidar Lopes
v. Thayna Ohana Machado

d. Capítulo 4
i. Fabricia de Cassia Constancio Jacob
ii. João Batista Brandelli
iii. Luigi Dutra Facchinetti Cardia
iv. Paulo Roberto Bacchmi
v. Shaila Santos da Silva

e. Capítulo 5
i. Bernardo C Fontenelle
ii. Joyce Dias Berrocozo Monteiro
iii. Monica Fernandes Pereira
iv. Patrícia de Queiroz Costa
v. Raquel Silva d'Albuquerque

f. Capítulo 6
i. Caroline Cavalcante de Almeida Faleiros
ii. Fernando Placoná Vieira da Silva
iii. Pedro Henrique de Sousa Malvezzi
iv. Rita Knop

g. Capítulo 7
i. Fernando Aguiar Fernandes Filho
ii. Luciane Pinto Carvalho
iii. Luciane Maria Radichi
iv. Rodrigo Morais

h. Capítulo 8
i. Caroline de Souza Iglesias Teixeira
ii. Danielle Campany Salles
iii. Isabel Scorcio Hildebrandt
iv. Natalia Moura Ferreira
v. Nathalia De Paula dos Santos
vi. Sabrina Maria Santos Farah Pessoa
vii. Soraya Fonseca Salomão Pacheco
viii. Valeria Ribeiro

i. Capítulo 9
i. Andrezza de L. C. Knauer Santos
ii. Janaina N Miranda
iii. Luiz Fernando Nobrega

Orientadores da KPMG

Alessandro Gratão Marques
Carolina Ferreira Paulino
Emerson Buziles de Melo
Marcelo Pereira de Lira
Raphael Rodrigues Soré
Renata Santana
Sheila de Lima Valdevino

Sumário

Prefácio 6

Capítulo 1 – Governança e Cultura 9

1.1. Desafios e responsabilidades dos conselheiros 27

1.2. Desafios e responsabilidades dos executivos 30

1.3. Tornando a função de compliance estratégica 30

Capítulo 2 – Avaliação de Riscos de Compliance 34

2.1. Compliance - Contexto Geral 35

2.2. Como se define risco? 35

2.3. Lavagem de dinheiro 37

2.4. Legislação de Prevenção aos Crimes de Lavagem de Dinheiro (Lei de PLD) 37

2.5. Sanções internacionais 40

2.6. Corrupção e suborno 40

2.7. Terceiros 43

2.8. Práticas Anticoncorrenciais 44

2.9. Imagem e reputação 45

2.10. Riscos Regulatórios 45

2.11. Risco Socioambiental 46

2.12. Violação de privacidade de dados 47

2.13. Conflito de interesse 48

2.14. Cyber Security 48

2.15. Trabalhista 49

2.16. Tributário 50

2.17. Evolução do gerenciamento de riscos 51

2.18. Avaliação de riscos de compliance 51

2.19. Riscos emergentes e a pandemia 53

2.20. Riscos mais aparentes no cenário de pandemia 54

Capítulo 3 – Pessoas e Competências 56

3.1. Papéis e responsabilidades 57

3.2. Due diligence e background check 59

3.3. Pesquisa de dados 61

3.4. Definição e avaliação das informações 61

3.5. Avaliação contínua de competências 62

3.6. Gestão de desempenho, incentivos e remuneração 63

3.7. Aplicação de medidas disciplinares 65

Capítulo 4 – Políticas e Procedimentos 67
4.1. Introdução e Objetivos 68
4.2. Código de Conduta 69
4.3. Compromissos 70
4.4. Conceituações e Diferenças em Relação a Políticas, Normas e Procedimentos 70
4.4.1. Políticas 70
4.4.2. Normas 71
4.4.3. Procedimentos 71
4.5. Estruturação dos documentos normativos 71
4.6. Açõs que Contribuem para Maior Efetividade das Políticas e dos Procedimentos 73
4.6.1. Planejamento 73
4.6.2. Execução 74
4.6.3. Implementação (Divulgação) 76
4.7. Aspectos Pós-Implementação (Monitoramento, Revisão e Atualização) 76
Capítulo 5 – Comunicação e Treinamento 78
5.1. Introdução 79
5.2. Legislação - Lei n° 12.846/13 e Decreto n° 8.240/15 79
5.3. Iniciativas e práticas de comunicação e treinamento 80
5.3.1. Fácil acesso ao programa 80
5.3.2. Embaixadores de compliance 80
5.3.3. Treinamentos disponíveis para toda força de trabalho 81
5.3.4. Evidências/Rastreabilidade dos treinamentos 81
5.3.5. Vídeos e teatros sobre o tema 82
5.3.6. Campanha de endomarketing 82
5.3.7. E-learning 84
5.3.8. Revisão periódica dos treinamentos 84
5.3.9. "Compliance day" ou "Dia do Compliance" 84
5.4. Indicadores - Key Performance Indicators (KPIs) 85
5.4.1. Principais KPIs 85
5.5. Considerações gerais 86
Capítulo 6 – Tecnologia e Análise de Dados 88
6.1. Contextualização 89
6.2. Data Analytics 90
6.2.1. O que é? 90

6.2.2. Objetivo 91
6.2.3. Benefícios 91
6.3. Estrutura da análise de dados (framework) 93
6.3.1. Tipos de análises de dados 93
6.4. O Compliance Officer e o Data Analytics 94
6.5. Canal de denúncias no tratamento e análise de dados 94
6.5.1. O que é? 94
6.5.2. Objetivo 94
6.5.3. Benefícios 95
6.6. Estrutura de tratamento das denúncias (framework) 95
Capítulo 7 – Monitoramento e Testes 96
7.1. Monitoramento e sinergia das três linhas de governança 97
7.2. Testes
Capítulo 8 – Gerenciamento de Deficiências e Investigações
8.1. Conceito, Finalidade e Abrangência 103
8.2. Tipos de Investigação Corporativa 108
8.3. Procedimentos 109
8.4. Considerações gerais sobre o tema 110
Capítulo 9 – Reporte 112
9.1. O papel do reporte na efetividade dos Programas de Compliance 115
9.2. Desafios no processo de reporte 116
9.3. Monitoramento 117
9.4. Canal de Denúncias e suas tratativas de reporte 118
9.5. Como definir a periodicidade dos reportes 119
9.6. Compliance na gestão de crise 120
121
Referências Bibliográficas 122
124

Prefácio

Embora muito se discuta nos dias de hoje os efeitos deletérios da corrupção sobre as organizações privadas e públicas sua repercussão sobre as sociedades devido aos impactos sobre os serviços públicos gerados ou, ainda, sobre a relação de rent seeking entre o público e o privado — é certo que esse fenômeno remonta a origem e a organização da humanidade.

Quando fazemos um olhar retrospectivo sobre os principais esforços nacionais e internacionais acerca do enfrentamento deste tema, que embora talvez esteja muito presente já nas primeiras relações de trocas, percebemos que a institucionalização de arranjos legais e institucionais é relativamente recente.

O paradigma de um enfoque no enfrentamento às práticas de corrupção do ponto de vista das relações com o Estado ocorreu em diversos países em momentos distintos, fomentado, em especial, por meio da mudança das relações comerciais voltadas para cadeias globais e uma economia globalizada. Nesse particular, é internacionalmente reconhecido o protagonismo americano a partir da Lei Federal de Práticas de Corrupção no Exterior em 1977 — Foreign Corrupt Practices Act (FCPA) —, tendo no Reino Unido a Lei de Suborno em 2010 (Bribery Act) como sua legislação referencial, sendo importante também destacar a Convenção de Mérida, promulgada em 2003, que culminou com a assunção do compromisso por 140 países de combater à corrupção e às suas práticas.

O nosso País, mesmo possuidor de diversos dispositivos legais de tipificação de atos de corrupção e seu enfrentamento, teve melhoria no seu marco legal com a sanção da Lei n° 12.846/2013, conhecida como Lei Anticorrupção (LAC). Esta lei veio a estabelecer punições gravosas na esfera administrativa para empresas corruptoras nas relações com o Estado, com base na responsabilidade objetiva de seus agentes, permitindo ao País alinhar-se às boas práticas internacionais, trazendo inclusive ao ordenamento jurídico nacional o instrumento de resolução negocial por meio da celebração de acordos de leniência. Certamente, o avanço nacional recente no enfrentamento da corrupção não decorreu somente do avanço legal e infralegal, mas também do amadurecimento e da profissionalização de organizações públicas de defesa do Estado, do fortalecimento da cultura ética e da governança corporativa de organizações privadas e estatais que se sujeitam à abrangência desse arcabouço normativo e institucional.

O caráter transnacional da corrupção exige esforços que perpassam para

muito além da construção de um arcabouço legal e o fortalecimento de instituições para o seu combate no âmbito nacional, fazendo-se mister a construção de um consenso internacional da sua relevância e da sua urgência de agenda. Requer a construção de mecanismos de detecção tempestivos que permitam identificar responsáveis e a extensão dos atos, uma melhor compreensão de mecanismos e fatores que levam algumas pessoas a cometer atos de corrupção, o enfrentamento de paraísos fiscais e outros meios de ocultação de patrimônio e bens. As últimas décadas têm sido muito profícuas, tanto no avanço de compartilhamento de informações entre instituições nacionais e internacionais para o seu combate, como também pelo avanço na realização de experimentos no ramo das ciências comportamentais e sociais, que nos ajudam a melhor entender questões relativas a conflitos de interesse, viés comportamental e incentivos que podem impactar uma atuação não íntegra.

O avanço progressivo na detecção e na punição no contexto externo de atuação das organizações traz não somente uma preocupação para o reforço de uma cultura alinhada a valores, balizada pela ética e pela integridade para o atingimento de seus objetivos, como também requer que estas busquem utilizar, ao máximo, os potenciais que os modelos computacionais proporcionam na melhoria dos controles internos, tanto para o diagnóstico quanto para a construção de avaliações preditivas.

Nas economias de mercado, as organizações privadas assumem papel primordial na criação de valor, na construção de relações equilibradas dentro de uma sociedade e na promoção contínua de inovações que proporcionem saltos de produtividade, ampliando a riqueza gerada pela nação. Porém, este ciclo virtuoso somente é possível por meio da construção de relações pessoais e interorganizacionais baseadas na confiança, na ética e na competição de mercado. As organizações para permanecerem neste mercado, a cada dia mais desafiador e dinâmico, deverão ser capazes de gerenciar riscos das perspectivas mais diversas, desde estratégicos, operacionais, de tecnologia da informação, financeiros e de compliance.

As sociedades de países desenvolvidos e as novas gerações vêm demonstrando valoração crescente não apenas com a qualidade e o custo dos produtos e dos serviços, mas como também associados a uma adequada responsabilidade corporativa com os valores ambientais e sociais, em uma visão whole approach. Marcas anteriormente valorizadas e consumidas podem rapidamente perder valor na velocidade digital em uma sociedade interconectada

quando questionada quanto aos valores esperados.

As organizações devem estar preparadas para competir em um ambiente cada vez mais volátil, incerto, complexo e ambíguo, como vem sendo preconizado por diversos especialistas e reforçado de forma muito concreta neste momento atual de enfrentamento da pandemia mundial. Para desenvolver esta capacidade, as organizações deverão investir no desenvolvimento de competências de seus colaboradores internos, estruturar sua governança, seus controles internos e sua gestão de riscos de forma equilibrada para suportar o alcance das estratégias para criação de valor dentro do apetite de risco aceito, bem como fazer uso intensivo das novas tecnologias para ser eficiente no ambiente de competição, sem abrir mão dos valores sólidos compartilhados por todos dentro da organização e respeitados pelos seus colabores externos.

Nesse sentido, o aprimoramento da qualidade das interlocuções entre os setores público e privado passa obrigatoriamente pelo investimento de suas áreas de compliance, sobretudo em decorrência de novos diplomas legais, como a Lei Geral de Proteção de Dados e a Lei da Liberdade Econômica, mas especialmente por novos temas em discussão legislativa os quais trarão grandes impactos nessa temática, como a regulamentação do lobby.

Esta publicação, a qual discute temas e processos fundamentais para o aprimoramento da governança e da gestão, não somente permite aos participantes sedimentar conteúdos como também contribuir para o fomento de uma discussão de qualidade necessária ao nosso País para uma retomada de seu dinamismo econômico.

Gustavo de Queiroz Chaves
Secretário Federal de Controle Interno-Adjunto
da Controladoria Geral da União (CGU)

Capítulo 1

Governança e Cultura

KPMG

KPMG BUSINESS SCHOOL

Há alguns anos, enquanto enumerava razões para convencer as organizações a dar atenção ao *compliance*, o ex-procurador-geral de justiça americano Paul McNulty proferiu uma expressão que viria a ficar famosa nos Estados Unidos: *"If you think compliance is expensive, try non compliance."* Em português, pode ser traduzida como "se você pensa que o *compliance* é caro, experimente não atendê-lo" e, nos últimos anos, pudemos observar, seja nos Estados Unidos, seja no Brasil, assim como em qualquer parte do mundo, inúmeros casos que corroboram essa afirmação.

A repercussão de casos de corrupção, especialmente os nacionais, que levaram a crises agudas empresas conceituadíssimas, aceleraram ainda mais o amadurecimento desse setor no País. O bordão de McNulty não é mera retórica jurídica.

Mudanças regulatórias, risco de danos à reputação, multas vultosas aplicadas por órgãos de fiscalização, pressão dos acionistas e dos *stakeholders*. Todos esses fatores fizeram com que os executivos passassem a enxergar o *compliance* como um investimento e não como um custo, tornando os debates mais latentes no C-Level. Contribuíram também para que sua definição, antes restrita às questões regulatórias e legais, ganhasse contorno mais flexível e passasse a englobar ética, sustentabilidade, cultura corporativa, risco cibernético, gerenciamento de dados e informações de clientes, cadeia de suprimentos, trabalho remoto, entre outros diversos riscos emergentes.

O complexo cenário regulatório de *compliance* atualmente requer que as organizações avancem nas suas práticas de governança corporativa, para que efetivamente gerenciem e monitorem seus riscos e implementem os processos e a cultura de *compliance*, alinhada e homogênea em toda a organização.

A adoção de boas práticas de governança e a implementação de uma estrutura robusta não apenas melhora sua gestão e contribui para a geração de melhores resultados, mas principalmente promove a confiança e a transparência da organização perante seus *stakeholders*[1] e seus principais *shareholders*[2]. A governança corporativa é um dos fatores essenciais para a sustentabilidade das organizações no longo prazo.

Sob a perspectiva das práticas de Governança Corporativa, alguns riscos inerentes aos processos de negócio representam uma constante preocupação do Conselho de Administração, assim como a existência de uma adequada estrutura de Governança, Riscos e Compliance (GRC) para minimizar a ocorrência e o impacto desses riscos, por exemplo:

- Riscos desconhecidos e não gerenciados e que podem afetar a reputação, a imagem, os resultados e até a continuidade da empresa.
- Baixa conformidade a políticas, normas e procedimentos estabelecidos.
- Autuações fiscais pelo não cumprimento das leis e dos regulamentos.
- Perdas financeiras nas operações/transações com clientes, fornecedores e prestadores de serviço.
- Perdas financeiras ou de ativos decorrentes de fraudes, desvios, roubos ou falta de controles adequados.
- Falta de confiança nas informações gerenciais.
- Gastos acima do que foi estimado e/ou receitas abaixo do esperado.
- Erros e retrabalhos contínuos no processamento das transações e das operações do dia a dia.
- Pouco monitoramento das operações pelas gerências.

Diante deste cenário, as funções de gerenciamento de riscos estão inseridas na estrutura de governança corporativa das organizações e são pilares fundamentais do que é denominado "As 3 Linhas de Defesa" da governança, que permeiam os diversos níveis hierárquicos, e nos quais atuam as quatro principais atividades de GRC: Controles Internos, Gestão de Riscos, Compliance e Auditoria Interna, conforme ilustrado na figura a seguir:

Fonte: IIA (Instituto dos Auditores Internos do Brasil)

[1] Parte interessada de uma organização. Exemplo: colaboradores, comunidade, clientes, fornecedores, entre outros.

2 Acionistas de uma organização.

Cada uma das linhas desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

Na **1ª linha** estão os gerentes operacionais que gerenciam os riscos e têm propriedade sobre eles, assim como são os responsáveis por implementar as ações corretivas para resolver as deficiências nos processos e nos controles internos.

A Gerência Operacional identifica, avalia, controla e mitiga os riscos para implementação das políticas, para que as atividades estejam de acordo com os objetivos estratégicos e de conformidade da empresa e, por meio de suas equipes, implementem os controles por meio de sistemas, processos, atividades e tarefas que estão sob a orientação e a gestão, em prática, garantir a conformidade pelos controles. Faz parte ainda testar a aderência e efetividade deles.

Já a **2ª linha** conta com os especialistas das áreas (Gerência de Risco, Controles Internos, Compliance, Financeiro, Controladoria, Tecnologia da Informação, Segurança Patrimonial e Meio Ambiente) os quais estabelecem diversas funções e gerenciamento de riscos e conformidade para ajudar a desenvolver e/ou a monitorar os controles da primeira linha de defesa, fornecendo conhecimento e ferramentas adequadas.

Podem existir também dentro da empresa múltiplas funções de conformidade com responsabilidade específica de monitoramento da conformidade, como qualidade, suprimentos, saúde, recursos humanos. A função de controladoria monitora os riscos financeiros e as questões de reporte financeiro. Estas funções podem intervir diretamente com subsídios legais e operacionais, de modo a adequar e proporcionar as melhorias necessárias aos controles e aos procedimentos.

Na **3ª linha**, considera-se que os auditores internos fornecem à estrutura de governança e à Alta Administração avaliações baseadas no maior nível de independência e objetividade dentro da organização, com avaliação da gestão de riscos, controles e governança.

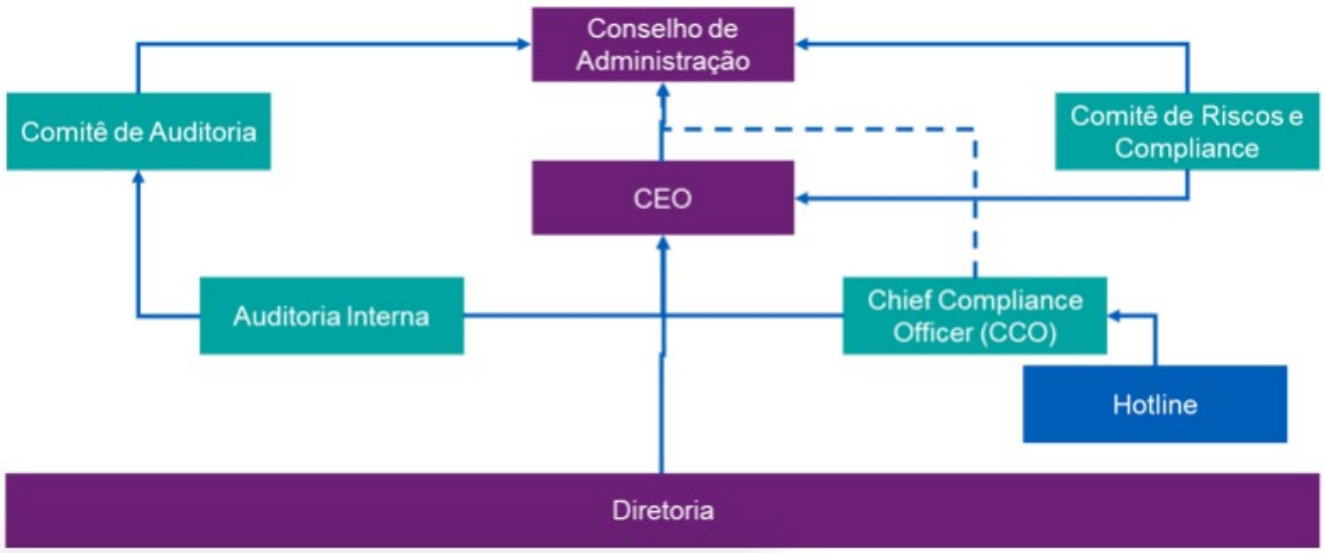
Segundo o professor Marcos Assi, a auditoria interna provê avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos de gerenciamento de riscos e controle. O escopo dessa avaliação é reportado à Alta Administração e ao órgão de governança e controles.

No contexto de *compliance*, as práticas de governança corporativa são fundamentais para o alinhamento do compromisso com a ética em toda a organização.

O que é governança corporativa? Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas,

envolvendo os relacionamentos entre sócios, Conselho de Administração, Diretoria, órgãos de fiscalização e controle e demais partes interessadas (IBGC, 2015).

A seguir apresentamos uma sugestão de posicionamento e responsabilidades de cada organismo de governança corporativa em um Programa de Compliance para reflexão dos leitores:



Destacamos na figura anterior as seguintes responsabilidades dos organismos de Governança Corporativa (GC), conforme apresentadas no quadro abaixo:

ORGANISMO (GC)	RESPONSABILIDADES
CONSELHO DE ADMINISTRAÇÃO	- Exercer suas atribuições considerando os interesses de longo prazo da organização. - Definir os valores e os princípios éticos da organização e zelar pela manutenção da transparência da organização no relacionamento com todas as partes interessadas. - Exercer o papel de guardião dos princípios, dos valores, dos padrões de conduta ética e do Programa de Compliance, bem como definir a atuação da função de compliance no nível estratégico. - Monitorar os riscos derivados da atitude dos gestores (*tone at the top*) e a cultura da organização. - Avaliar periodicamente a exposição da organização a riscos e a eficácia do Programa de Compliance. - Eleger e destituir o Chief Compliance Officer (CCO) e deliberar sobre papéis, responsabilidades e atribuições, bem como sobre eventuais necessidades do Comitê de Riscos e Compliance. - Aprovar a estrutura de Governança de Compliance, Código de Conduta, papéis e responsabilidades, Comitê de Auditoria, Comitê de Riscos e Compliance, políticas,

ORGANISMO (GC)	RESPONSABILIDADES
CONSELHO DE ADMINISTRAÇÃO (continuação)	canal de linha ética, matriz de riscos, estrutura de auditoria interna, entre outros mecanismos. - Assegurar a autoridade, a independência, a autonomia e a responsabilidade da função de *compliance*. - Aprovar orçamento anual, investimentos e demandas adicionais (por exemplo: investigações). - Aprovar o Plano Anual do Programa de Compliance compatível com as estratégias de negócios. - Rever anualmente o Programa de Compliance para aprimorá-lo. - Supervisionar e patrocinar a implementação e a efetividade do Programa de Compliance e recomendar ações de aprimoramento da função de *compliance* alinhadas às boas práticas.

ORGANISMO (GC)	RESPONSABILIDADES
COMITÊ DE AUDITORIA	- Assessorar o Conselho de Administração no monitoramento e no controle da qualidade das demonstrações financeiras, nos controles internos, no gerenciamento de riscos e em *compliance*, visando à confiabilidade e à integridade das informações, bem como à proteção da empresa e de todas as partes interessadas. - Ser formado, em sua maioria, por membros independentes e coordenado por um conselheiro independente. - Ter ao menos um de seus membros independentes com experiência comprovada nas áreas Contábil-societária, de Controles Internos, Financeira e de Auditoria, cumulativamente. - Possuir orçamento próprio para a contratação de consultores para assuntos contábeis, jurídicos ou outros temas, quando necessária a opinião de um especialista externo. - Assegurar que as áreas de Auditoria Interna e Compliance estão atentas aos principais riscos do negócio. - Monitorar o impacto do ambiente regulatório, de

ORGANISMO (GC)	RESPONSABILIDADES
COMITÊ DE AUDITORIA (continuação)	*compliance* e do ambiente de negócios, bem como do *tone at the top* e da cultura corporativa nos Programas de Compliance da empresa. - Poderá assumir os papéis e as responsabilidades do Conselho de Administração em relação ao Programa de Compliance, se designado formalmente pelo CA.

ORGANISMO (GC)	RESPONSABILIDADES
COMITÊ DE RISCOS E COMPLIANCE	- Zelar pela imagem e pela reputação da organização. - Revisar e aprovar as revisões sugeridas pela área de Compliance no Código de Conduta, na Política de Compliance e Anticorrupção, bem como demais políticas relacionadas a diretrizes, padrões éticos e de integridade e submeter a aprovação do CA. - Revisar o Plano Anual de Compliance. - Acompanhar a execução do Plano Anual de Compliance. - Revisar o orçamento para estruturação e manutenção do Programa de Compliance. - Aprovar o plano de divulgação, conscientização e disseminação do Código de Conduta e Políticas de Compliance da organização e monitorar sua adequada implementação, propondo e aprimorando ações voltadas para o fortalecimento e o desenvolvimento da consciência e dos padrões de conduta ética na organização. - Exercer o papel de assessoramento de dúvidas e/ou conflitos de interpretação das disposições do Código de Conduta, Política de Compliance e Anticorrupção e demais políticas relacionadas a diretrizes, padrões de conduta ética e de integridade. - Analisar as denúncias, realizadas por meio do Linha Ética (*Hotline*) de eventos em desconformidade com o código de conduta, com as políticas da organização, recomendar quanto à aplicação de medidas disciplinares, conforme a política de medidas disciplinares, independentemente do nível hierárquico, em casos de desvio e/ou falhas relacionadas a compliance e recomendar planos de ação

ORGANISMO (GC)	RESPONSABILIDADES
COMITÊ DE RISCOS E COMPLIANCE (continuação)	preventivos, educativos e corretivos. - Acompanhar o processamento das denúncias, na forma e na periodicidade definidas por seu regimento. - Conduzir e/ou autorizar investigações em qualquer matéria dentro de seu escopo de atribuições. - Tomar decisões sobre assuntos relacionados ao Código de Conduta. - Assegurar a existência e a manutenção da Linha Ética (Hotline) como um canal de comunicação permanente e direto com o Comitê de Riscos e Compliance. - Monitorar e analisar os relatos de desvios e o andamento dos planos de ação do Programa Anual de Auditoria e Compliance, alertando o Conselho de Administração e a Alta Administração sobre a iminência da materialização de riscos, podendo manifestar-se a respeito e sugerir providências. - Monitorar a exposição a riscos, dos sistemas de controles internos e do cumprimento de leis, normas, regulamentos e políticas da organização. - Aprovar e monitorar o plano de comunicação e treinamento do Programa de Compliance. - Analisar os indicadores de riscos e desempenho do Programa de Compliance. - Aprovar e recomendar sobre os indicadores de risco de terceiros. - Monitorar a implementação e efetividade do Programa de Compliance. - Revisar e aprovar as diretrizes da estrutura de Gestão de Riscos da organização (papéis, responsabilidades, metodologia, sistemas, processos, entre outros). - Apoiar e propor a disseminação da cultura de Gestão de Riscos como ferramenta de gestão. - Revisar e manifestar-se sobre a Política de Gestão de Riscos. - Aprovar o Plano de Ação de Gestão de Riscos.

ORGANISMO (GC)	RESPONSABILIDADES
COMITÊ DE RISCOS E COMPLIANCE	- Entender e avaliar a metodologia do cálculo do Apetite a Risco. - Assessorar a Diretoria na discussão sobre a definição do Apetite a Risco aceitável da empresa. - Validar o portfólio de riscos estratégicos e a régua de impacto. - Obter com a Diretoria a aprovação dos riscos estratégicos a ser priorizados e seus respectivos planos de ação e contingência (se aplicável). - Efetuar reporte à Diretoria acerca do gerenciamento dos riscos estratégicos. - Monitorar as variações de criticidade dos riscos priorizados e reportar variações significativas à Diretoria. - Avaliar e opinar sobre possíveis conflitos de interesses.

ORGANISMO (GC)	RESPONSABILIDADES
CHIEF COMPLIANCE OFFICER (CCO)	- Zelar pela imagem e pela reputação da organização. - Assegurar a atuação da função de *compliance* no nível estratégico da organização, participando das reuniões de Conselho de Administração (CA) e/ou comitê designado pelo CA. - Definir e disseminar a governança e a cultura de compliance, em conjunto com a Alta Administração, em todos os níveis da organização. - Elaborar o orçamento e o Plano Anual da função e submeter para aprovação do Conselho de Administração e/ou do comitê por este órgão designado. - Interagir e aconselhar a 1ª e a 2ª linha de defesa da organização (áreas de Negócio), no que diz respeito a ética, *compliance*, políticas corporativas aplicáveis e regulação local, sempre zelando pelos mais altos padrões éticos. - Estabelecer sinergia eficiente com as demais áreas (por exemplo: GRC). - Analisar, priorizar e implementar todas as estratégias

ORGANISMO (GC)	RESPONSABILIDADES
CHIEF COMPLIANCE OFFICER (CCO) (continuação)	de compliance, monitorar sua efetividade, por meio de indicadores e reportar ao Conselho de Administração e/ou ao comitê por este órgão delegado, de forma regular e frequente. - Coordenar e interagir com as áreas de Negócio e de Controle a efetiva comunicação com reguladores e facilitar a estruturação de serviços, o desenvolvimento de negócios, buscando encontrar soluções criativas e inovadoras para questões tanto de ética e compliance como regulatórias. - Monitorar continuamente o ambiente regulatório, avaliar o impacto na organização e contribuir para estabelecer processos e controles internos adequados, bem como no monitoramento da efetividade. - Promover a padronização dos processos e dos controles internos relacionados ao Programa de Compliance. - Estabelecer um processo apropriado de gerenciamento de riscos e manter os processos, os controles internos e o Programa de Compliance alinhado às boas práticas e aderente às necessidades da organização (adequados ao porte, aos riscos e à complexidade das atividades). - Estabelecer a política, a metodologia, o processo e a matriz de gestão de riscos relacionados ao Programa de Compliance e realizar o monitoramento contínuo, contemplando, mas não limitado a: - Critérios de impacto e probabilidade de ocorrência dos riscos de *compliance* (por exemplo: ética, imagem, reputação, proteção de dados, fraude, corrupção, ambiental, regulatório, suborno, terceiros, cyber, licenças, AB&C, PEP, conflito de interesse, lavagem de dinheiro, pagamentos etc.). - Taxonomias de riscos e categorização do risco bruto, controle e risco residual. - Construção de cenários e análise de tendências.

ORGANISMO (GC)	RESPONSABILIDADES
CHIEF COMPLIANCE OFFICER (CCO) (continuação)	- Processos, atividades e transações críticas. - Mudanças regulatórias e avaliação de impacto. - Oportunidades de melhorias, potenciais desvios e indicadores de monitoramento. - Propor, em conjunto com a Alta Administração, a régua de impacto e probabilidade, atualizá-la sempre que necessário, calcular e atualizar o valor do apetite a risco e estabelecer critérios para mapeamento, avaliação e classificação de riscos. - Estabelecer indicadores de compliance e riscos e assegurar que estes sejam aplicados na avaliação de desempenho dos profissionais e de terceiros da organização. - Estabelecer a política, a metodologia e o processo para elaboração, revisão, aprovação e divulgação de políticas e procedimentos relacionados a compliance e riscos. - Elaborar o código de conduta e políticas inerentes a compliance e submeter para aprovação do Conselho de Administração e/ou do comitê por este órgão designado. - Promover a disseminação e a conscientização dos padrões de conduta ética e das políticas de compliance e riscos, criando e mantendo mecanismos que visem a assegurar o seu cumprimento. - Elaborar e submeter para aprovação, conforme limite de alçada, as políticas que suportam as transações, os processos e as atividades de controles relacionados aos principais aspectos do Programa de Compliance e Riscos. - Disseminar e disponibilizar as políticas relacionadas ao Programa de Compliance e Riscos à organização. - Revisar anualmente o código de conduta e as demais políticas e procedimentos do Programa de Compliance e Riscos e submeter para aprovação, conforme alçada estabelecida.

ORGANISMO (GC)	RESPONSABILIDADES
CHIEF COMPLIANCE OFFICER (CCO) (continuação)	- Administrar os temas de compliance e riscos, monitorando a exposição a riscos, os sistemas de controles internos e o cumprimento de leis, normas e regulamentos e políticas da organização. - Adotar Política de Compliance (incluindo apuração e investigação de relatos/denúncias), aprovada pelo Conselho de Administração, que inclua a definição dos riscos para os quais se busca proteção, a estrutura organizacional para gerenciamento de riscos, a avaliação da adequação da estrutura operacional e os processos de controles internos na verificação da sua efetividade, além de definir diretrizes para o estabelecimento dos limites aceitáveis de apetite a riscos da organização. - Manter e atualizar arcabouço regulatório aplicável à empresa, com base nas informações capturadas pelas áreas e reportar à Alta Administração. - Zelar pela existência de um processo formal e ferramentas adequadas para a captura e a avaliação do impacto de normas e regulamentações, aplicáveis à organização. - Empenhar esforços, em conjunto com as demais áreas, para desenvolver mecanismos que visam à conformidade com as leis e os regulamentos. - Atrair, reter e capacitar talentos para atuação na função de compliance e riscos adequados ao porte, aos riscos e à complexidade das atividades a ser desempenhadas. - Assegurar a autoridade, a independência, a autonomia e as responsabilidades da função de compliance e riscos. - Realizar a avaliação de riscos de terceiros (due diligence), monitorar a exposição a riscos e, se necessário, vetar o relacionamento que possa ter impacto na imagem, na reputação e no financeiro. - Estabelecer o Plano Anual de comunicação e

ORGANISMO (GC)	RESPONSABILIDADES
CHIEF COMPLIANCE OFFICER (CCO) (continuação)	treinamento do Programa de Compliance e Riscos e aplicar as sessões de treinamentos (presenciais ou remotos), mantendo o registro de conformidade. - Desenvolver conteúdo de comunicação (interno e externo) sobre o Programa de Compliance e Riscos. - Monitorar a aderência aos treinamentos por meio de indicadores. - Realizar workshops e reuniões com a liderança (incluindo Conselho de Administração, Comitês e Alta Administração). - Estabelecer e gerir o canal Linha Ética (Hotline). - Assegurar o anonimato, a existência de protocolos de registro, a independência do canal e que o canal Linha Ética seja amplamente divulgado e nos idiomas adequados. - Realizar as apurações e as investigações com equipe técnica capacitada em técnicas forenses e aplicar as ações necessárias para cessar a ocorrência de relatos e/ou desvios de mesma natureza. - Monitorar os relatos/denúncias, elaborar análise de tendências e planos de ação para adequação dos processos e do ambiente de controles. - Assessorar a organização na implementação de sistemas que permitam a realização de monitoramento da efetividade do Programa de Compliance de forma tempestiva (compliance analytics). - Realizar testes, processos, atividades, transações e controles. - Reportar regular e frequentemente ao Conselho de Administração e/ou ao comitê por este designado. - Zelar pela existência e pela aplicação de mecanismos para orientações e medidas disciplinares. - Coordenar o Comitê de Riscos e Compliance.

ORGANISMO (GC)	RESPONSABILIDADES
AGENTES DE COMPLIANCE	- Disseminar a cultura de *compliance*. - Interagir com as áreas para que estas cumpram as diretrizes do Programa de Compliance. - Ser o ponto focal para esclarecimentos sobre aspectos de *compliance*. -Auxiliar na divulgação dos mecanismos de compliance, por exemplo: código de conduta, políticas e procedimentos, Linha Ética (Hotline), comunicação e treinamento e, se necessário, testes dos processos, atividades, transações e controles internos com reporte ao Compliance Officer. - Apoiar a implementação dos planos de ação de compliance. - Sugerir melhorias no Programa de Compliance da organização. - Contribuir na realização dos treinamentos do Programa de Compliance. - Auxiliar na identificação e na avaliação dos riscos de compliance. - Assessorar no monitoramento da efetividade do Programa de Compliance. - Zelar pela imagem e pela reputação da organização. - Zelar pela imagem e pela reputação da organização.

ORGANISMO (GC)	RESPONSABILIDADES
DIRETORIA	- Executar a estratégia de negócio alinhada às diretrizes de compliance aprovadas pelo CA. - Fornecer fluxos de informações adequados ao Conselho e apresentar resultados de avaliação de riscos e métricas que aumentam o conhecimento do Conselho para tomada de decisão. - Patrocinar ativamente as diretrizes do CA para estruturação e implementação do Programa de Compliance. - Assegurar autoridade, independência, autonomia,

ORGANISMO (GC)	RESPONSABILIDADES
DIRETORIA	orçamento e investimento aprovado pelo CA para funcionamento do Programa de Compliance. -Promoverdebatesecomunicaçõessobreaimportância do *compliance* na estratégia da organização. - Disseminar a estratégia de compliance e os padrões de conduta ética e políticas estabelecidas. - Monitorar os principais riscos de compliance da organização. - Promover investimentos em tecnologia, análise de dados e automação de *compliance* para suportar a eficácia e a sustentabilidade do programa. - Receber e analisar relatórios regulares e significativos para entender a situação do *compliance*, bem como avaliar os impactos e as tendências dos riscos no negócio. - Manter-se atualizada acerca das últimas alterações de *compliance* e regulatórias, avaliar as implicações das novas regulamentações. - Assegurar os recursos e a estruturação da equipe de Compliance alinhados à complexidade do negócio e dos riscos inerentes (risk based approach). - Estabelecer a cultura correta de compliance, expressar uma forte liderança pelo exemplo e modelar e comunicar ativamente uma governança e a cultura de compliance. - Avaliar como os incentivos impactam os esforços de compliance. - Demonstrar seu comprometimento com ética e *compliance* de forma regular e frequente. - Prover informações necessárias paras as atividades de auditoria interna, compliance e investigação quando solicitado. - Assegurar resultados eficazes e eficientes relacionados ao Programa de Compliance.

Como apresentado, os agentes de governança representados por sócios, conselheiros, administradores ou órgãos de governança de uma organização são essenciais na implementação da cultura de *compliance* e são responsáveis por "assegurar que toda a organização esteja em conformidade com os seus princípios e valores, refletidos em políticas, procedimentos de controle e normas internas, leis e dispositivos regulatórios a que esteja submetida." (IBGC, 2015).

Os princípios de transparência, equidade, prestação de contas e responsabilidade corporativa[3], definidos pelo Instituto Brasileiro de Governança Corporativa (IBGC) para a governança da organização, são hoje os pilares para a implementação de um Programa de Compliance efetivo.

Segundo pesquisa realizada pela KPMG, sobre a maturidade do *compliance* no Brasil, 73% dos respondentes afirmaram que os executivos seniores reforçam periodicamente que a governança e a cultura de *compliance* são essenciais para a estratégia da empresa. Reforçada no exemplo de que 71% dos executivos revisam e aprovam anualmente o Programa de Ética e Compliance na sua organização (KPMG, 2019).

Esse resultado mostra a relevância do tema na sobrevivência da empresa e porque o envolvimento da Alta Liderança então se faz necessário.

No entanto, infelizmente os reportes e o monitoramento do tema levados até à Alta Administração pode não estar ocorrendo da forma necessária. Segundo a mesma pesquisa, para 13% dos respondentes, o reporte da área de Compliance para à Alta Administração é realizado apenas quando necessário e para 3% dos que responderam à pesquisa não há nenhuma comunicação. O que reforça a importância de melhorar esse envolvimento dos agentes de governança com o tema.

---

[3] Princípios Básicos de Governança Corporativa, de acordo com o IBGC, 2015: "Transparência: Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que conduzem à preservação e à otimização do valor da organização.
Equidade: caracteriza-se pelo tratamento justo e isonômico de todos os sócios e as demais partes interessadas (stakeholders), levando em consideração direitos, deveres, necessidades, interesses e expectativas destes.
Prestação de contas (accountability): os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e suas omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis.
Responsabilidade corporativa: os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional etc.) no curto, médio e longo prazos.

Nos últimos anos, as demandas regulatórias nacionais e internacionais com foco na prevenção e na punição de casos de fraudes e corrupção cresceram e se tornaram mais restritivas e exigentes. Nesse contexto, os agentes de governança são peças-chave na implementação e no cumprimento desses requisitos, pois são os responsáveis em dar o exemplo no cumprimento do código de conduta, o qual exerce um papel de guardião dos princípios e dos valores da organização e que deve ser a base para o Programa de Compliance.

No cenário americano, a Lei Sarbanes-Oxley (Sarbanes-Oxley Act, normalmente abreviada em SOX ou Sarbox), criada em 2002, trouxe como obrigatório um conjunto de medidas para aumentar os controles, a segurança e a transparência na condução dos negócios e inseriu boas práticas de governança corporativa. Dentre essas práticas, podemos citar:

- Aprovação das demonstrações financeiras e eficácia dos controles e dos procedimentos de divulgação internos pela Alta Liderança, geralmente CEO e CFO, certificando e aprovando a exatidão.
- Inclusão de todos os passivos, as obrigações ou as transações nas demonstrações financeiras.
- Publicação de informações em relatórios anuais sobre o escopo e a adequação da estrutura de controle interno e os procedimentos para relatórios financeiros. Adicionalmente, a empresa de contabilidade registrada deve, no mesmo relatório, atestar e informar sobre a avaliação da eficácia da estrutura de controle interno e dos procedimentos de apresentação de relatórios financeiros.
- Divulgação tempestiva ao público das informações sobre mudanças significativas na condição financeira ou nas operações da organização.
- Aplicação de multas e penalidades no caso de alteração, destruição, ocultação e/ou falsificação de registros, documentos ou objetos tangíveis com a intenção de obstruir, impedir ou influenciar uma investigação legal, inclusive para o auditor.

A lei também trata a responsabilidade por fraude corporativa ou criminal e aumento das penalidades para crimes de colarinho branco.

A partir daí, no Brasil, o tema começou também a se tornar cada vez mais relevante nas mesas de debate da Alta Administração e de executivos, principalmente por conta dos casos de corrupção que vieram à tona e que não apenas destruíram empresas, mas famílias também, e comprometeram setores inteiros. Novos modelos de negócio e de gestão precisaram ser criados a partir daí.

Desde a criação da Lei Sarbanes-Oxley e impulsionadas pelos relevantes fatos de corrupção ocorridos no Brasil, foram elaboradas e aprovadas diversas legislações, normas e orientações relevantes relacionadas à governança na esfera do *compliance*, as quais podemos citar:

- Lei n° 12.846/2013 ("Lei Anticorrupção") e seu decreto regulamentador (Decreto nº 8.420/2015).
- Lei n° 13.303/2016 ("Lei das Estatais").
- ISO 19600:2014 - Sistema de Gestão de Compliance - Diretrizes.
- ISO 37001:2016 - Sistemas de Gestão Antissuborno.
- Código das Melhores Práticas de Governança Corporativa (IBGC).
- Guia sobre *compliance* concorrencial do Conselho Administrativo de Defesa Econômica (Cade).
- Revisão do regulamento do Novo Mercado da B3.
- Manual para Implementação de Programas de Integridade - Orientações para o setor público - Ministério da Transparência e Controladoria-Geral da União (CGU).
- Programa de Integridade: Diretrizes para Empresas Privadas - Controladoria-Geral da União (CGU).
- Guia Prático de Gestão de Riscos para a Integridade - Ministério da Transparência e Controladoria-Geral da União (CGU).
- Manual para Implementação de Programas de Integridade - Ministério da Transparência e Controladoria-Geral da União (CGU).
- Manual Prático de Avaliação de Programa de Integridade em PAR - Ministério da Transparência e Controladoria-Geral da União (CGU).

Uma questão relevante que deve ser considerada na governança de um Programa de Compliance é a implementação de uma cultura que seja difundida e assimilada por toda organização, e que fomente uma conduta de respeito aos valores e à legislação, sendo os agentes de governança da organização responsáveis por dar exemplos positivos (tone of the top), como: código de ética, código de conduta, código de boas práticas etc. De acordo com o IBGC, 2017, "O grande desafio é estabelecer uma cultura ética verdadeira, coerente com a identidade da organização e baseada no exemplo da liderança."

Ainda, destaca-se também outros aspectos que devem ser levados em conta na implementação de uma cultura de *compliance*:

- Engajamento real da Alta Direção.
- Definição dos responsáveis pelo compliance na organização.

- Engajamento e responsabilização dos colaboradores com o tema.
- Identificação dos riscos de *compliance*.
- Definição de regras claras, políticas, códigos, valores e princípios que definem a cultura almejada.
- Monitoramento, avaliação e reporte da cultura de *compliance*.
- Estabelecimento de uma linha ética.

É importante lembrar que a efetividade da implantação de uma cultura de *compliance* alinhada com toda a organização só será possível a partir do engajamento dos seus conselheiros, de executivos e do alinhamento com os valores da organização.

1. 1 Desafios e Responsabilidades dos Conselheiros

Uma estrutura de *compliance* com o intuito de atender às demandas de órgãos reguladores nacionais e internacionais deve contemplar práticas condizentes relacionadas à governança corporativa, à gestão de riscos e do próprio *compliance*.

"Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional, etc.) no curto, médio e longo prazos." (IBGC, 2020)

Conforme vimos anteriormente, governança corporativa envolve o desenvolvimento de um sistema que associe as relações entre os acionistas, a Gestão Operacional e o Conselho da Administração.

O Conselho de Administração é responsável por acompanhar o gerenciamento do risco de *compliance* da empresa e, pelo menos uma vez ao ano, deve avaliar a efetividade do gerenciamento do risco de *compliance*.

O Conselho de Administração tem suas diretrizes definidas pela Lei nº 6.404/76 - Sociedades Anônimas (arts. 140 a 160).

O art. 142 aborda sobre as suas competências, conforme os seus incisos II, III e VI abaixo:

- II - eleger e destituir os diretores da companhia e fixar-lhes as atribuições, observado o que a respeito dispuser o estatuto;
- III - fiscalizar a gestão dos diretores, examinar, a qualquer tempo, os livros e papéis da companhia, solicitar informações sobre contratos celebrados ou em via de celebração, e quaisquer outros atos;
- VI - manifestar-se previamente sobre atos ou contratos, quando o estatuto assim o exigir."

O art. 153 também se aplica ao Conselho de Administração e cita: "O administrador da companhia deve empregar, no exercício de suas funções, o cuidado e diligência que todo homem ativo e probo costuma empregar na administração dos seus próprios negócios."

E por fim, o art. 158, que também se aplica ao Conselho de Administração, aborda: "O administrador não é pessoalmente responsável pelas obrigações que contrair em nome da sociedade e em virtude de ato regular de gestão; responde, porém, civilmente, pelos prejuízos que causar, quando proceder:

- I - dentro de suas atribuições ou poderes, com culpa ou dolo;
- II - com violação da lei ou do estatuto."

Dando continuidade, o Conselho de Administração é responsável por:

- Assegurar que a Alta Administração, com apoio do *compliance*, implemente medidas corretivas para não conformidades identificadas.
- Aprovar a Política de Compliance, de acordo com os requisitos legais vigentes.

Também cabe ao Conselho de Administração garantir:

- Apropriada gestão da Política de Compliance da empresa.
- Comunicação da Política de Compliance a todos os colaboradores e os prestadores de serviços terceirizados relevantes.
- Divulgação de padrões de integridade e conduta ética como parte da cultura da empresa.
- Efetividade e continuidade da aplicação da Política de Compliance.
- Fornecer os meios necessários para que as atividades relacionadas à função de *compliance* sejam realizadas adequadamente, incluindo pessoas em quantidade, capacitação e experiência suficientes.
- Revisar, 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 são responsáveis pela conformidade e pela efetividade de possíveis atividades da função de *compliance* que sejam realizadas por terceiros.

A responsabilidade dos Conselhos de Administração no monitoramento dos temas de *compliance* é uma figura cada vez mais importante da agenda moderna da governança corporativa. As ações dos comitês de auditoria buscam responder a essa demanda em auxílio ao Conselho.

O Conselho de Administração tem o papel fundamental em definir as estratégias e implementar mudanças para assegurar a continuidade futura dos negócios de organizações familiares.

Identificar as questões-chave e os eventos importantes que podem mudar a direção dos negócios, assim como ter a coragem de encarar uma nova realidade, recomendar e supervisionar as mudanças fundamentais que irão garantir o crescimento sustentado dos negócios são prioridades de uma governança efetiva — daí a importância da participação do Conselho de Administração.

Os Conselhos de Administração necessitam compreender não só o cenário econômico, para definir a melhor estratégia a ser aplicada — por exemplo: como criar valor para a organização, apontar as oportunidades que deve investir e as competências necessárias para isso —, como também executar um plano de melhoria e quais metas e indicadores deverão nortear a implementação.

Todos os conselheiros devem saber com clareza os objetivos e as estratégias da organização, compreendendo como criar valor, desenvolvimento da governança corporativa e quais as métricas que irão monitorar o seu progresso. Existem algumas estratégias que são comuns a qualquer Conselho Administrativo, como aumentar o retorno dos investimentos, valorizar o negócio e proteger os interesses de todas as partes interessadas.

Organizações de qualquer porte ou natureza jurídica podem determinar a criação de um Conselho Administrativo, as quais devem atentar-se para pensar não só no tamanho da operação hoje, mas também nos planos futuros de expansão e crescimento.

Ainda, de acordo com a Instrução CVM nº 586, de 8 de junho de 2017, o Conselho de Administração deve ter membros de perfil diversificado, número adequado de conselheiros independentes e tamanho que permita a criação de comitês, o debate efetivo de ideias e a tomada de decisões técnicas, isentas e fundamentadas.

Sem dúvida, o Conselho Administrativo de uma organização é a máquina de tomada de decisões, as quais podem levar a empresa tanto ao sucesso quanto ao insucesso, tudo isso em um cenário que traz mais ameaças do que contribuição e em que a atuação dos conselheiros é essencial para o enfrentamento e a superação dos possíveis eventos disruptivos do negócio.

1.2 Desafio e Responsabilidade dos Executivos

Nos últimos anos, principalmente após o surgimento da lei anticorrupção, o *compliance* vem ganhando destaque no sistema de governança das organizações, tornando-se essencial e trazendo muitos benefícios, como oportunidades de negócios, vantagens competitivas, atração de investimentos, prevenção de riscos corporativos, identificação de problemas antecipadamente, correção de não conformidades e sustentabilidade do negócio.

A Lei nº 12.846/2013 trouxe a responsabilização objetiva administrativa e civil para as empresas pela prática de atos contra a Administração Pública. Dessa forma, as empresas são responsáveis por prevenir os atos ilícitos praticados por seus colaboradores, portanto, os executivos são os principais responsáveis por assegurar o cumprimento da legislação e as normas por todos os colaboradores e os terceiros que agirem em seu nome.

Os executivos fazem parte da Alta Administração de uma organização, representada pela Diretoria. Segundo o IBGC, a Diretoria é responsável por colocar em prática o plano estratégico, elaborar e implementar os processos operacionais, financeiros e de compliance da organização.

A responsabilidade da organização de estar em conformidade com legislação, normas e políticas internas que ela está submetida, não é só de compliance, mas de todos na organização, principalmente da Alta Administração, que precisam assegurar que isso aconteça. Uma maneira de demonstrar seu compromisso é dando o exemplo, reforçando constantemente a importância da empresa em estar em conformidade, dessa forma contribui para o desenvolvimento da cultura de compliance.

Portanto, os executivos, além de fazer com que a empresa atinja seu objetivo, de dar retorno do capital investido, têm o desafio de manter o negócio em conformidade com as leis e as regras para manter a confiança de clientes e investidores.

1.3 Tornando a função de *compliance* estratégica

Um dos riscos fundamentais que todo negócio deve se preocupar é com relação à violação da privacidade dos dados de seus clientes. As organizações precisam garantir e respeitar a privacidade de seus clientes para o bom desempenho e a continuidade dessa parceria.

O fornecimento de dados dos clientes a terceiros, a fim de obter algo em troca, induz que a organização esteja atuando fora dos padrões de conformidade,

podemos citar como exemplos: corrupção, branqueamento de capital ou fazer mal uso de informação privilegiada (CAMARGO, 2018).

O *compliance* visa a agregar valor ao negócio e assegura a sobrevivência da organização na nova abordagem de trabalho, com base em boas práticas de governança, melhora a questão de ausência de orientações normativas, desalinhamento às legislações aplicáveis, falhas na gestão de processos internos, falta de ferramentas preventivas adequadas e operação sem uma estrutura de sistema de informação.

A implementação do *compliance* nas organizações objetiva o contínuo funcionamento do negócio, uma vez que:

- Proporciona redução de incidência de fraudes e desconformidades, que geram desvios de recursos.
- Evita riscos de sansões legais, perdas financeiras e perda de reputação.
- Aumenta a qualidade das decisões dentro da organização.
- Reduz o custo operacional.
- Garante o retorno de investimento, com base na implementação de boas práticas de governança.

Além dos benefícios já apresentados, a organização com um bom Programa de Compliance ganha credibilidade por parte das pessoas interessadas no negócio e na abertura de mercado externo. Também tem um significativo aumento da eficiência e da qualidade dos serviços e dos produtos, além de melhoria da governança corporativa.

A adoção de *compliance* vem trazer melhoria na qualidade e na economia de recursos, evitando gastos com multas, punições e cobranças judiciais. A implementação de boas práticas de governança também fortalece a marca no mercado nacional e internacional devido à seriedade organizacional.

Se exercer a visão de futuro, chegaremos à conclusão de que será por meio de implementação de *compliance* que as organizações se consolidarão no mercado e alcançarão seus objetivos estratégicos, táticos e operacionais de forma segura ao longo prazo, com criação de programas preventivos e de monitoramento contínuo.

A adoção de boas práticas, alinhadas a missão, visão e valores de um negócio, favorece não apenas a satisfação de investidores, colaboradores e fornecedores, como abre portas para transações mercantis internacionais.

Não estar em compliance significa estar assumindo riscos potencialmente desnecessários que podem levar a perdas financeiras, patrimoniais, de mercado e

muitas outras.

É importante refletir e mudar a abordagem de gestão, ajustar a forma como as informações da empresa são tratadas e como as pessoas se comportam no dia a dia, para alcançar nível de excelência em compliance, independentemente do segmento de atuação e do tamanho da organização.

A tomada de decisão geralmente parte dos processos de informação e interpretação nas organizações e as decisões estão relacionadas aos diversos modos de interpretação (WEICK, et al 2005).

Essas decisões podem ser de caráter racional, para enfatizar as análises das informações e as relações de causa e efeito, algo científico ou que sejam antecipadas ações estratégicas da empresa.

É importante ressaltar que a comunicação é uma via de mão dupla, ou seja, quando o ambiente favorece a comunicação e a aproximação das partes interessadas, o gestor da organização também recebe mais informações e, para isso, existem os meios de comunicação internos, como jornais, e-mail, telefones e cartazes. Eles devem trazer informações relevantes e livres de filtros.

Isso não significa que o filtro não tem uma origem justificada, porém, quando isso acontece, revela uma falta de confiança na equipe, o que apresenta como resultado outro problema: falha na formação de colaboradores.

Abordaremos aqui um exemplo de tomada de decisão em que ser e estar em *compliance* faz muita diferença. É o caso da empresa que deseja transferir sua base de dados de um servidor interno para um servidor remoto.

Nesse caso, o Programa de Compliance vai prever a gestão de riscos que a transferência de servidores podem eventualmente trazer. Afinal, nenhuma organização quer que informações confidenciais fiquem expostas, por exemplo que dados sensíveis de colaboradores e clientes caiam em mãos erradas.

O programa também visa a garantir a proteção de dados com implementação de mecanismo de segurança, com base em protocolos para um ambiente em nuvem.

Para garantir que esse processo seja realizado da maneira mais segura possível, um Programa de Compliance bem estruturado inicia com treinamento dos colaboradores de maneira a garantir que todos estejam alinhados sobre as normas internas e à legislação em vigor. Os respetivos treinamentos devem pautar pelo código de ética da empresa e também pelas leis e pelas normas nacional e internacional.

Para a identificação de anomalias que possam afetar o processo, é necessário

contar com um controle de qualidade interno, além de um serviço de auditoria externa.

E, por fim, a inserção de um canal de denúncias com o intuito de comunicar as irregularidades de forma anônima no sentido de proteger o colaborador contra represálias.

Neste caso, o programa também visa a garantir proteção de dados com a implementação de mecanismos de segurança, com base em controles internos e conformidade, tais como:

- Linha Ética, que vai possibilitar o recebimento de denúncias internas e externas, bem como mecanismo de proteção que impeça qualquer espécie de retaliação à pessoa que utilize esse canal.
- Código de ética e integridade, tendo como princípio valores e missão alinhados ao negócio da empresa, de forma a prevenir conflitos de interesses e vedação de atos de corrupção e fraude.
- Previsão de sansões, que são aplicáveis em caso de violação às regras do código de conduta e integridade em vigor na organização.
- Programa de capacitação de pessoal, de forma periódica sobre a política de gerenciamento de risco.

Por fim, a área ou a função de *compliance* que é responsável pela atualização e pela aplicação do código de conduta e integridade.

Capítulo 2

Avaliação de Riscos de Compliance

2.1. Compliance - Contexto Geral

Com a complexidade crescente no ambiente de negócios e a (até então) globalização das empresas, o termo *compliance* entrou de vez na agenda dos executivos brasileiros — pela necessidade de transparência com investidores ou mercado, pela manutenção de um ambiente de trabalho ético e com valores alinhados com às diretrizes da empresa e de seus acionistas e para resgatar a credibilidade de empresas afetadas por escândalos e fraudes corporativas.

Casos emblemáticos como Enron e WorldCom, bem como os impactos da Operação Lava Jato em nosso País, trouxeram à tona a importância de robustos Programas de Compliance (e demais instrumentos da governança corporativa) na condução dos negócios, e tudo isso começa com a cultura de ética em uma empresa. Mesmo o mais sofisticado ambiente de governança está sujeito a falhar quando não há o patrocínio e o exemplo da Alta Administração.

Dessa forma, um dos primeiros aspectos a se considerar são os riscos em que cada empresa está operando e qual seu arcabouço regulatório, ou seja, a quais legislações essa empresa tem que atender.

2.2. Como se define risco?

- Risco é um evento composto de três elementos: Chance, Escolha e Consequência - Perryman Kuver (1999).
- Um incidente ou uma ocorrência gerada com base em fontes internas e externa, que afeta a realização dos objetivos - COSO ERM.

A integração com estratégia e desempenho reforça a importância do gerenciamento de riscos no planejamento estratégico e na incorporação destes em toda a empresa, uma vez que os riscos influenciam e alinham a estratégia e o desempenho em todos os departamentos e as funções (fonte: COSO ERM).

Para isso, conforme metodologia da KPMG, devemos considerar as seis etapas seguintes para realizar o mapeamento de riscos de *compliance*:

1. **Identificar e analisar os aspectos** de negócio: entender qual o arcabouço regulatório, quais as estratégias e o apetite a risco de cada empresa.
2. **Identificar e categorizar os riscos:** conhecer os riscos e categorizá-los conforme sua natureza é fundamental para entendê-los e dar a resposta mais apropriada. Importante ressaltar que o pior risco é o risco que não é conhecido.
3. **Avaliar os riscos inerentes:** entender os riscos "brutos" da empresa, ou seja, sem considerar ainda nenhuma atividade de mitigação ou resposta.

4. **Avaliar os controles mitigatórios:** entender o ambiente de controles internos de cada empresa e como eles atuam e endereçam os riscos inerentes.

5. **Avaliar o risco residual:** avaliar o impacto do risco, após considerar as atividades mitigatórias. Cabe ressaltar aqui que as ações mitigatórias tendem, na maioria das vezes, a reduzir a probabilidade e não o impacto dos riscos nas organizações.

6. **Remediar os riscos:** responder aos riscos, conforme o apetite da empresa, seja mais conservador, seja arrojado, passando por mitigar, aceitar, terceirizar ou eliminar o risco.

A avaliação dos riscos, via de regra, é pautada pela análise do impacto versus pela probabilidade de o risco se materializar. Nesse ponto, é fundamental não se ater apenas ao julgamento do profissional de *compliance*, mas sim garantir que a avaliação e a resposta aos riscos estejam devidamente alinhadas com as diretrizes da empresa, seu apetite a riscos e aprovadas pelas alçadas competentes.

Nessa jornada, teremos grandes desafios, como sensibilizar a empresa/executivos como um todo da importância desse processo e, mais ainda, das consequências de não fazê-lo adequadamente. E isso leva tempo, insumo precioso que, por vezes, não dispomos na quantidade necessária. Mas isso faz parte do desafio dos profissionais de *compliance* ao redor do mundo, em um processo contínuo de evolução rumo a um mundo mais ético e transparente (ao menos em sua maioria).

Na ISO 31000, risco é definido como o "efeito da incerteza nos objetivos", portanto, podemos conceituar riscos como eventos que, caso se materializem, irão de alguma forma impactar o alcance dos objetivos da empresa.

Partindo da conceituação acima, podemos dizer que risco de *compliance* pode ser caracterizado pelo efeito do não cumprimento das obrigações de *compliance* , definidas como requisitos que a empresa tem de cumprir, ou que decide cumprir nos objetivos da empresa. Esses efeitos seriam as sanções administrativas e pecuniárias à pessoa jurídica e às pessoas físicas com elas relacionadas, por exemplo: multas, impedimento aos executivos de atuar no mercado e cassação da licença de funcionamento da empresa, e danos à reputação/imagem que a empresa pode enfrentar, em razão do descumprimento ou do tratamento inadequado de normas externas (leis, regulamentos, normas de entidades reguladoras e autorreguladoras), e/ou do código de ética e das demais políticas internas.

Abaixo, relacionamos alguns dos principais riscos de *compliance* (taxonomias

de riscos), em nossa visão, e alguns exemplos de controles internos que podem ser implementados para mitigá-los:

2.3. Lavagem de dinheiro

Um tema bastante explorado sob a ótica de *compliance* envolve os mecanismos de prevenção à lavagem de dinheiro que alguns conhecem como PLD, outros como AML e, eventualmente, até como crimes que têm como objetivo disfarçar origens ilícitas de recursos ou transações não adequadas acerca das normas vigentes sobre o tema.

A título de uniformização do conhecimento, normalmente os mecanismos utilizados no processo de prevenção à lavagem de dinheiro envolvem teoricamente três etapas independentes, que, com frequência, ocorrem simultaneamente:

- Colocação - Relativa à inserção dos recursos ilícitos (por exemplo: dinheiro) no sistema econômico, por meio de depósitos, compra de instrumentos ou de bens.

- Ocultação - Consiste em dificultar o rastreamento contábil dos recursos ilícitos com a utilização de eventuais aspectos de confidencialidade em transferências eletrônicas para contas anônimas ou em localidades com menor preocupação sobre o tema.

- Integração - Quando os recursos ilícitos são formalmente incorporados ao sistema econômico. As organizações criminosas buscam investir em empreendimentos que facilitem suas atividades — podendo tais sociedades prestarem serviços entre si.

Neste âmbito, desde 1998, com a promulgação da Lei Ordinária nº 9.613, o Brasil normatizou um conjunto de regras e requerimentos para as empresas que operam no sistema econômico local e suas filiais ou matrizes no exterior, e o tema ganhou embasamento com os outros órgãos de supervisão e controle, por exemplo: Conselho Monetário Nacional (CMN), Comissão de Valores Mobiliários (CVM), Banco Central do Brasil (Bacen) e Conselho de Controle de Atividades Financeiras (COAF), este último vinculado ao Ministério da Fazenda, que tem como objetivo regular, receber e oficiar os órgãos de investigação do Estado em relação a eventuais atipicidades ou suspeitas em transações no sistema econômico.

2.4. Legislação de Prevenção aos Crimes de Lavagem de Dinheiro (Lei de PLD)

A Lei nº 12.683, de 9 de julho de 2012, altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem

de dinheiro, sendo destacado: "Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal."

"Art. 9º Sujeitam-se às obrigações referidas nos arts. 10 e 11 as pessoas físicas e jurídicas que tenham, em caráter permanente ou eventual, como **atividade principal ou acessória, cumulativamente ou não:**

I. - a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira;

II. - a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial;

III. - a custódia, emissão, distribuição, liquidação, negociação, intermediação ou administração de títulos ou valores mobiliários.

Sujeitam-se às mesmas obrigações:

I. - as bolsas de valores, as bolsas de mercadorias ou futuros e os sistemas de negociação do mercado de balcão organizado;

II. - as seguradoras, as corretoras de seguros e as entidades de previdência complementar ou de capitalização;

III. - as administradoras de cartões de credenciamento ou cartões de crédito, bem como as administradoras de consórcios para aquisição de bens ou serviços;

IV. - as administradoras ou empresas que se utilizem de cartão ou qualquer outro meio eletrônico, magnético ou equivalente, que permita a transferência de fundos;

V. - as empresas de arrendamento mercantil (leasing) e as de fomento comercial (factoring);

VI. - as sociedades que efetuem distribuição de dinheiro ou quaisquer bens móveis, imóveis, mercadorias, serviços, ou, ainda, concedam descontos na sua aquisição, mediante sorteio ou método assemelhado;

VII. - as filiais ou representações de entes estrangeiros que exerçam no Brasil qualquer das atividades listadas neste artigo, ainda que de forma eventual;

VIII.- as demais entidades cujo funcionamento dependa de autorização de órgão regulador dos mercados financeiro, de câmbio, de capitais e de seguros;

IX. - as pessoas físicas ou jurídicas, nacionais ou estrangeiras, que operem no Brasil como agentes, dirigentes, procuradoras, comissionarias ou por qualquer forma representem interesses de ente estrangeiro que exerça qualquer das atividades referidas neste artigo;

X. - as pessoas físicas ou jurídicas que exerçam atividades de promoção

imobiliária ou compra e venda de imóveis;

XI. - as pessoas físicas ou jurídicas que comercializem joias, pedras e metais preciosos, objetos de arte e antiguidades.

XII. - as pessoas físicas ou jurídicas que comercializem bens de luxo ou de alto valor, intermedeiem a sua comercialização ou exerçam atividades que envolvam grande volume de recursos em espécie;

XIII.- as juntas comerciais e os registros públicos;

XIV. - as pessoas físicas ou jurídicas que prestem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, em operações de compra e venda de imóveis, estabelecimentos comerciais ou industriais ou participações societárias de qualquer natureza;

a) de gestão de fundos, valores mobiliários ou outros ativos;

b) de abertura ou gestão de contas bancárias, de

c) poupança, investimento ou de valores mobiliários;

d) de criação, exploração ou gestão de sociedades de qualquer natureza, fundações, fundos fiduciários ou estruturas análogas;

e) financeiras, societárias ou imobiliárias; e

f) de alienação ou aquisição de direitos sobre contratos relacionados a atividades desportivas ou artísticas profissionais;

XV. - pessoas físicas ou jurídicas que atuem na promoção, intermediação, comercialização, agenciamento ou negociação de direitos de transferência de atletas, artistas ou feiras, exposições ou eventos similares;

XVI.- as empresas de transporte e guarda de valores;

XVII.- as pessoas físicas ou jurídicas que comercializem bens de alto valor de origem rural ou animal ou intermedeiem a sua comercialização; e

XVIII.- as dependências no exterior das entidades mencionadas neste artigo, por meio de sua matriz no Brasil, relativamente a residentes no País."

Segundo o art. 10º, as instituições devem:

- Fazer a identificação dos clientes e manter os registros e operações atualizados;
- Manter o registro de toda transação em moeda nacional ou estrangeira;
- Implementar políticas, procedimentos e controles internos eficientes, compatíveis com seu porte e volume de operações;
- Cadastrar-se e manter o referido cadastro atualizado no órgão regulador

ou fiscalizador e, na falta deste, no Conselho de Controle de Atividades Financeiras (COAF);

- Comunicar ao COAF as operações atípicas, suspeitas ou com limites superiores aos regulamentados.

2.5. Sanções internacionais

São ações apoiadas pela Organização das Nações Unidas (ONU) e impostas **como uma forma não militar de punir aqueles que ameaçam a paz e a segurança mundial.**

As sanções internacionais podem ser aplicadas a países, organizações e/ou indivíduos.

Procedimento de screening

Basicamente é a "consulta" (investigação/pesquisa) **realizada sobre as partes** (indivíduo e empresas) envolvidas na transação, de modo a apurar se as partes possuem indicações negativas, podendo considerar a inclusão dos respectivos nomes em listas restritivas nacionais e internacionais, pessoas politicamente expostas, exposição em mídias negativas, entre outros.

Penalidades e danos à imagem pelo envolvimento em situações relacionadas à lavagem de dinheiro, em descumprimento à Lei nº 9.613/98, que dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores.

Controles internos

- Disseminação da cultura de prevenção à lavagem de dinheiro por meio de treinamento e capacitação adequados de todos os colaboradores e prestadores de serviço terceirizados relevantes.
- Análise apropriada do "conheça seu cliente", "conheça seu fornecedor", "conheça seu parceiro" e "conheça seu colaborador".
- Procedimentos de Controle e Monitoramento de Operações Suspeitas.

2.6. Corrupção e suborno

Penalidades e danos à imagem pela prática de atos contra a Administração Pública, nacional ou estrangeira, conforme previsto no ordenamento jurídico brasileiro.

Com a finalidade de evitar a prática de atos de corrupção, o ordenamento jurídico congrega diversos instrumentos de combate à corrupção, tais como a Lei nº 8.429/1992 (Lei de Improbidade Administrativa), o Código Penal, as leis

que definem os denominados crimes de responsabilidade (Lei nº 1.079/1950 e Decreto-Lei nº 201/1967), a LC nº 135/2010 ("Lei da Ficha Limpa"), que alterou a LC nº 64/1990 para estabelecer novas hipóteses de inelegibilidade, entre outros diplomas legais.

Recentemente, em função da necessidade de proteção crescente da moralidade, notadamente, a partir da Operação Lava Jato I, justificou a promulgação da Lei nº 12.846/2013 (Lei Anticorrupção), que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a Administração Pública, nacional ou estrangeira.

Pela legislação, constituem-se atos lesivos à Administração Pública, nacional ou estrangeira, todos aqueles praticados pelas pessoas jurídicas, que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da Administração Pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

I - prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II - comprovadamente, financiar, custear, patrocinar ou, de qualquer modo, subvencionar a prática dos atos ilícitos previstos nesta Lei;

III - comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV - no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar licitação pública ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados

com a administração pública;
V - dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

Para as pessoas jurídicas consideradas responsáveis pelos atos lesivos previstos na Lei n° 12.846/2013, cabem as seguintes sanções:

- Multa, no valor de 0,1% (um décimo por cento) a 20% (vinte por cento) do faturamento bruto do último exercício anterior ao da instauração do processo administrativo, excluídos os tributos, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação.
- Publicação extraordinária da decisão condenatória.
- As sanções serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e natureza das infrações.
- Na hipótese que não seja possível utilizar o critério do valor do faturamento bruto da pessoa jurídica, a multa será de R$ 6.000,00 (seis mil reais) a R$ 60.000.000,00 (sessenta milhões de reais).
- Publicação extraordinária da decisão condenatória ocorrerá na forma de extrato de sentença, a expensas da pessoa jurídica, em meios de comunicação de grande circulação na área da prática da infração e de atuação da pessoa jurídica ou, na sua falta, em publicação de circulação nacional, bem como por meio de afixação de edital, pelo prazo mínimo de 30 (trinta) dias, no próprio estabelecimento ou no local de exercício da atividade, de modo visível ao público, e no sítio eletrônico na rede mundial de computadores.

Controles internos

- Implementação de procedimentos e política anticorrupção.
- Disseminação da cultura de prevenção à corrupção por meio de treinamento e capacitação adequados de todos os colaboradores e os prestadores de serviço terceirizados relevantes.
- Criação de uma canal para denúncias de atos ilícitos, descumprimentos regulatórios, condutas inapropriadas ou ilícitas ou práticas que firam os princípios e os padrões.
- Auditorias anticorrupção.
- Implementação da Matriz de Consequências - Medidas disciplinares.

2.7. Terceiros

As empresas de todos os setores dependem cada vez mais de uma rede robusta de terceiros, como terceiros intermediários, fornecedores, distribuidores, agentes, *joint ventures*, alianças, subcontratados, prestadores de serviços, entre outros. Essa rede é fundamental para manter uma presença global, diferencial competitivo e concorrer com eficácia e eficiência no mercado.

Embora os terceiros sejam fundamentais para uma empresa atuar globalmente, os riscos associados a eles não podem ser terceirizados. Há muitos casos em que a falta de supervisão e monitoramento adequado de terceiros gerou graves consequências. As empresas globais foram expostas a riscos significativos, afetando negativamente seu desempenho, sua imagem e sua reputação, além do impacto financeiro.

Os órgãos regulatórios, em todo o mundo, esperam que as empresas tenham uma supervisão e um monitoramento efetivo e eficiente de seus terceiros. As empresas tiveram que priorizar e aprimorar seus esforços de *compliance* em consequência de ações de execução e multas notórias.

Diversos organismos internacionais publicaram regulamentações e boas práticas quanto ao ciclo de vida de terceiros (identificação, avaliação de riscos, *due diligence*, integração, avaliação e monitoramento contínuo) relacionadas à eficácia dos Programas de Compliance. O Departamento de Justiça (DOJ) e a Comissão de Valores Mobiliários (SEC) dos EUA elaboraram um guia conjunto que estipulava como a *due diligence* baseada em riscos é particularmente importante com terceiros e será considerada ao avaliar a efetividade do Programa de Compliance de uma empresa.

Penalidades e danos à imagem por prática de atos de corrupção e de lavagem de dinheiros por parte de terceiros com os quais a empresa se relaciona, direta ou indiretamente.

Controles internos

- Implementação de um programa de gestão de terceiros.
- Inclusão de termos e cláusulas contratuais que visem a assegurar o cumprimento de leis e normas por parte dos terceiros.
- Realização de processo de *due diligence* e avaliação de reputação como o *background check.*
- Monitoramento contínuo.

2.8. Práticas Anticoncorrenciais

Penalidades e danos à imagem advindos do envolvimento em situações anticoncorrenciais e em desacordo com a Lei n° 12.529/2011 - Lei de Defesa da Concorrência (LDC).

A Lei n° 12.529/2011, Lei de Defesa da Concorrência (LDC), estrutura o Sistema Brasileiro de Defesa da Concorrência e dispõe sobre a prevenção e a repressão às infrações contra a ordem econômica.

De acordo com o art. 36 da Lei n° 12.529/11, uma conduta é considerada infração à ordem econômica quando sua adoção tem por objeto ou possa acarretar os seguintes efeitos, ainda que só potencialmente: limitar, falsear ou, de qualquer forma, prejudicar a livre concorrência; aumentar arbitrariamente os lucros do agente econômico; dominar mercado relevante de bens ou serviços; ou quando tal conduta significar que o agente econômico está exercendo seu poder de mercado de forma abusiva.

Em seu art. 37, são definidas as penas pela prática de infração da ordem econômica:

I - no caso de empresa, multa de 0,1% (um décimo por cento) a 20% (vinte por cento) do valor do faturamento bruto da empresa, grupo ou conglomerado obtido, no último exercício anterior à instauração do processo administrativo, no ramo de atividade empresarial em que ocorreu a infração, a qual nunca será inferior à vantagem auferida, quando for possível sua estimação;

II - no caso das demais pessoas físicas ou jurídicas de direito público ou privado, bem como quaisquer associações de entidades ou pessoas constituídas de fato ou de direito, ainda que temporariamente, com ou sem personalidade jurídica, que não exerçam atividade empresarial, não sendo possível utilizar-se o critério do valor do faturamento bruto, a multa será entre R$ 50.000,00 (cinquenta mil reais) e R$ 2.000.000.000,00 (dois bilhões de reais);

III - no caso de administrador, direta ou indiretamente responsável pela infração cometida, quando comprovada a sua culpa ou dolo, multa de 1% (um por cento) a 20% (vinte por cento) daquela aplicada à empresa, no caso previsto no inciso I do caput deste artigo, ou às pessoas jurídicas ou entidades, nos casos previstos no inciso II do caput deste artigo.

§ 1° Em caso de reincidência, as multas cominadas serão aplicadas em dobro.
Controles internos

- Disseminação da cultura de prevenção à lavagem de práticas anticoncorrenciais por meio de treinamento e capacitação adequados de todos os

colaboradores e os prestadores de serviço terceirizados relevantes.

- Inclusão de orientações em um código de conduta, um guia ou uma política.
- Implementação da Matriz de Consequências - Medidas disciplinares.

2.9. Imagem e reputação

Perda de reputação da empresa, confiança dos clientes/investidores e danos à marca em virtude da materialização de riscos de associados ao nome da empresa ou de seus executivos e acionistas.

Controles internos

- Implementação e monitoramento do Programa de Compliance.
- Disseminação permanente de uma cultura ética, através de treinamentos e comunicação interna em todos os níveis da empresa.
- Implementação de metodologia de mensuração e priorização de riscos, de acordo com critérios objetivos.

2.10. Riscos Regulatórios

Penalidades aplicadas pelo órgão regulador por descumprimento de normativos expedidos.

O ambiente regulatório no Brasil vem passando, nos últimos anos, por um processo de aprimoramento e de crescimento das exigências, fazendo com que a necessidade de aprimorar os controles para mitigação do risco seja cada vez maior.

Controles internos

- Auditoria regulatória/testes de aderência à legislação.
- Implementação e gerenciamento de calendário de obrigações.
- Utilização de ferramentas de acompanhamento das normas regulatórias e da legislação.
- Revisão e acompanhamento de planos de ação para cumprimento dos apontamentos relacionados aos casos de não conformidades legais apresentadas pelos reguladores e pelas auditorias.
- Criação de comitês para entender os impactos na empresa das novas regulamentações e definir os processos e os controles que deverão ser implementados e/ou alterados.

2.11. Risco Socioambiental

Penalidades e danos à imagem decorrentes de danos socioambientais por descumprimento da legislação.

Nos últimos anos, uma série de acontecimentos mundiais tem direcionado os investidores a atribuir importância cada vez maior às práticas ambientais, sociais e de governança, chamadas de ESG (sigla em inglês para Environmental, Social and Governance).

A preferência por investir em empresas sustentáveis é crescente. Para se ter ideia, as emissões de títulos voltados para ESG no mundo devem alcançar US$ 350 bilhões ou R$ 1 trilhão em 2020, volume 36% maior do que o registrado em 2019, segundo previsão do Climate Bonds Initiative (CBI).

ESG é um índice que avalia as operações das principais empresas, conforme os seus impactos, em três eixos da sustentabilidade — o Meio Ambiente, o Social e a Governança. A medida oferece mais transparência aos investidores sobre as empresas nas quais eles estão investindo. O critério de Meio Ambiente vê como a empresa atua na gestão da natureza. O Social examina se a empresa viola direitos humanos universais, monitorando as relações da empresa entre os trabalhadores, os fornecedores e as comunidades nas quais atuam. Já a avaliação da Governança envolve práticas de gestão empresarial ligadas ao combate à corrupção e ao compliance.

Controles internos:

- Implementar normativos internos sobre riscos socioambientais e sustentabilidade, incluindo critérios para mitigar riscos socioambientais na avaliação de clientes e concessão de crédito.
- Criar controle de características da operação, atividade da empresa ou informações desabonadoras ligadas a crimes ambientais dos parceiros/ fornecedores.
- Inserir no processo de recrutamento parâmetros para levar a diversidade e a inclusão adiante em toda a organização.
- Incorporar as questões Ambientais, Sociais e de Governança nos processos de investimentos.
- Reforçar, através de comunicação e treinamento, os princípios de transparência nos negócios para colaboradores, clientes e parceiros.

2.12. Violação de privacidade de dados

Penalidades, passivos judiciais e danos à imagem pela quebra da privacidade de colaboradores, fornecedores e clientes e em virtude do descumprimento da Lei n° 13.709, mais conhecida como Lei Geral de Proteção de Dados Pessoais.

A Lei Geral de Proteção de Dados tem como objetivo proteger a liberdade e a privacidade de consumidores e cidadãos. Criada em 2018 e prevista para entrar em vigor em maio de 2021, ela demanda que empresas e órgãos públicos mudem a forma de coletar, armazenar e usar os dados pessoais dos cidadãos, ou seja, terá impactos significativos nas áreas Jurídica, Administrativa e de Segurança da Informação das empresas. E, para que não haja confusão, a lei traz logo de cara o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os dados sensíveis e os sobre crianças e adolescentes.

Desta maneira, os agentes possuem o dever de realizar o tratamento, respeitando os **direitos dos titulares**, dos quais decorrem os seguintes princípios:

- **Finalidade específica** e informada explicitamente ao titular.
- **Adequação** à finalidade previamente acordada e divulgada.
- **Necessidade** do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial.
- **Acesso livre**, fácil e gratuito das pessoas à forma como seus dados são tratados.
- **Qualidade de dados**, deixando-os exatos e atualizados, segundo a real necessidade no tratamento.
- **Transparência**, ao titular, com informações claras e acessíveis sobre o tratamento e os seus responsáveis.
- **Segurança** para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão.
- **Prevenção** contra danos ao titular e a demais envolvidos.
- **Não discriminação**, ou seja, não permitir atos ilícitos ou abusivos.
- **Responsabilização** do agente, obrigado a demonstrar a eficácia das medidas adotadas.

O descumprimento à LGPD acarreta sanções que variam entre advertências ou multa até proibição parcial ou total do exercício de atividades relacionadas ao tratamento [6].

A multa é por infração, no valor de até 2% do faturamento da empresa, limitado até cinquenta milhões de reais, a qual pode ser diária. Ademais, as sanções consistem na publicização da infração, bloqueio ou perda dos dados a que se refere a violação.

Controles internos:

- Utilização de ferramentas de segurança de dados como varreduras de vulnerabilidade e avaliações de risco, monitoramento de atividades de dados e alerta, criptografia e bloqueio.
- Implementação de normativos internos com os papéis e as responsabilidades na proteção dos dados.
- Estabelecimento de processo e controles para garantir o atendimento de direitos dos titulares dos dados.
- Controles para eliminação de dados não necessários.
- Criação de política de violação de dados com prazos de notificação.

2.13. Conflito de interesse

Perdas financeiras e exposição da imagem, em função de decisões pautadas em conflito de interesses.

Conforme a **Lei** nº 12.813/2013, **conflito de interesses** é a situação gerada pelo confronto entre **interesses** públicos e privados, que possa comprometer o **interesse** coletivo ou influenciar, de maneira imprópria, o desempenho da função pública, porém o conflito de interesse pode ocorrer também no âmbito privado.

Controles internos

- Implementação de procedimentos para identificar, analisar e administrar potenciais conflitos de interesses dentro da empresa.

2.14. Cyber Security

Perda financeira, interrupção ou dano à reputação de uma empresa resultante da falha de seus sistemas de tecnologia da informação. O risco cibernético pode se materializar de várias maneiras, como: violações deliberadas e não autorizadas de segurança para obter acesso aos sistemas de informação; violações involuntárias ou acidentais de segurança; ou riscos operacionais de TI devido a fatores como baixa integridade do sistema (fonte: Northbridge Insurance).

Ataques cibernéticos com impactos operacionais, financeiros e de reputação significativos são cada dia mais frequentes. O risco de vazamento de dados e sequestro de dados por meio de *ransomware*, com objetivo de negociar resgates

por meio de criptomoedas, tornaram-se realidade para as empresas do mundo todo.

Os funcionários são cada vez mais vítimas de esquemas de *phishing*, muitas vezes, por negligenciarem políticas e procedimentos de segurança.

A informações ficam mais expostas a vazamento ou roubo de informação com o avanço da tecnologia com o armazenamento em nuvem *(cloud computing)*, redes sociais e até mesmo pelos hábitos como de uso de celulares, *tablets e notebooks.*

Conforme os ataques cibernéticos avançam no mundo inteiro, a conscientização sobre a gravidade desse risco aumenta e os controles para garantir a segurança ficam mais robustos, porém, diante da impossibilidade de se proteger totalmente de ataques, as empresas precisam estar preparadas para lidar com as consequências em casos de violações.

Controles internos:

- Treinamento dos colaboradores quanto aos principais riscos cibernéticos e normas de segurança
- Manutenção de um ambiente de tecnologia atualizado
- Revisões periódicas de segurança
- Plano de resposta a incidentes.

2.15. Trabalhista

Passivos judiciais e danos à imagem da empresa em função do não cumprimento de leis e acordos trabalhistas e convenções coletivas, bem como de normas internas das empresas.

O risco de compliance trabalhista deve ser monitorado com a finalidade de avaliar e estabelecer na empresa regras que atendam a critérios legais envolvendo diversas questões, como:

- Admissão e demissão de colaboradores
- Saúde e segurança no trabalho
- Impactos ambientais
- Relação interpessoal no ambiente laboral.

A identificação e a prevenção de riscos deve focar em evitar conflitos entre empregador e funcionários, acidentes de trabalho e outras situações capazes de fazer com que a empresa seja responsabilizada no âmbito judicial. Assim, é possível mitigar o ajuizamento de judiciais.

Controles internos:

- Auditoria trabalhista para determinar se os procedimentos operacionais da empresa estão sendo realizados de forma correta.
- Formalização e divulgação de plano de cargos e salários.
- Inclusão no código de ética de temas como assédio moral e sexual.

2.16. Tributtário

Resultado tributário inesperado em função da desconformidade à legislação tributária, que não ocorre apenas com o descumprimento das obrigações tributárias acessórias, mas pode ocorrer também com a obrigação tributária principal quando há o pagamento de tributo em valor menor do que o devido.

Controles internos

- Aplicação de treinamentos de atualização de legislação tributária.
- Implementação de ferramenta para acompanhamento de atualização de legislação tributária.
- Tabulação dos resultados de conciliação de contas e da conferência dos lançamentos, comparando-os em relação a períodos anteriores.

O tema riscos de *compliance* possui relevância crescente, principalmente, pelas consequências danosas que a materialização desse risco pode significar para as empresas e as pessoas, conforme alguns exemplos que relatamos a seguir:

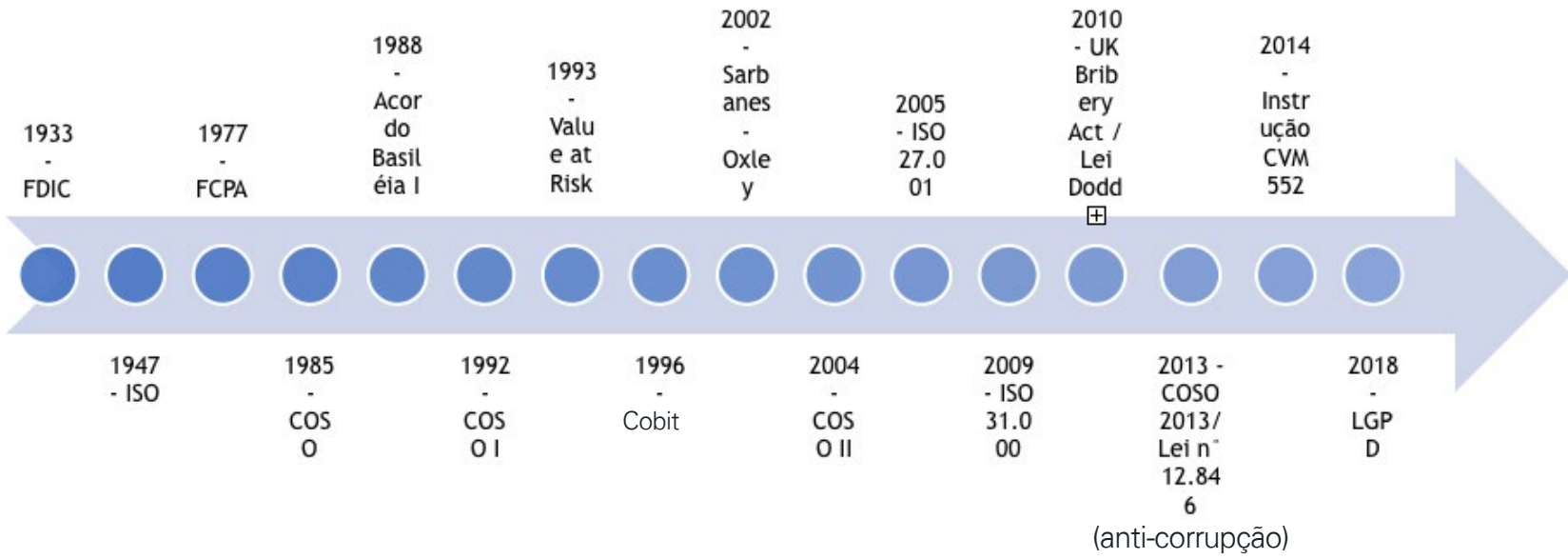
- O Banco Central multou recentemente um banco brasileiro em R$ 92,2 milhões por deficiência nos controles internos de prevenção à lavagem de dinheiro.
- O órgão de controle da concorrência da França multou uma gigante de tecnologia em 1,1 bilhão de euros (1,23 bilhão de dólares), alegando que a empresa é culpada de comportamento anticompetitivo devido à sua rede de distribuição e varejo.
- Uma fabricante europeia de aeronaves foi considerada culpada por subornar autoridades em 16 países ao redor do mundo. A empresa deverá pagar US$ 4 bilhões em multas após uma longa investigação de quatro anos, que acusou a fabricante europeia de conspirar através de uma vasta rede de corrupção global.
- Recentemente uma empresa que administra uma famosa rede social recebeu a decisão da Comissão Federal do Comércio dos Estados Unidos de que a empresa deveria pagar uma multa histórica de US$ 5 bilhões de dólares para encerrar a investigação do governo americano sobre suas práticas de privacidade. A

multa é a já imposta a qualquer empresa por violar a privacidade dos consumidores.

Dessa forma, é necessária uma adequada gestão de riscos de *compliance*, que pode ser definido como um processo confiável de identificação, mensuração, priorização e minimização de riscos de *compliance*, que possam impactar os objetivos da empresa, sendo eles de curto, médio ou longo prazos.

O desafio é fazer com que todos dentro da empresa respeitem e sigam as leis e as normas internas, já que, muitas vezes, os riscos de *compliance* acabam se materializando em razão do desconhecimento de regras, leis e normas e falhas na execução dos procedimentos.

2.17. Evolução do gerenciamento de riscos



Cadernos de Governança Corporativa - Gerenciamento de Riscos Corporativos: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21794/Riscos%20cad19.pdf

2.18. Avaliação de riscos de compliance tributário

A avaliação de risco é a base do Sistema de Gestão de Compliance. O detalhamento dessa avaliação dependerá do porte da empresa o dos objetivos que pretende alcançar.

A ISO 31000 é uma norma internacional para a Gestão de Risco. Nela, o processo de avaliação de riscos estratégicos engloba as etapas de identificação, análise e avaliação de riscos. Essa metodologia de avaliação pode ser utilizada para os demais tipos de risco.

A primeira etapa é a identificação de riscos, cuja finalidade é preparar, de forma abrangente, uma lista de riscos baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da organização. A identificação abrangente é crítica, uma vez que um risco não identificado nesta fase

não será tratado nas fases seguintes. É preciso levar em consideração possíveis causas e cenários que apontem para as possíveis consequências. Todas as causas e as consequências significativas deverão ser consideradas. A participação das pessoas estratégicas de cada área envolvida é essencial no processo de identificação dos riscos.

A etapa seguinte é a análise de riscos. O objetivo é desenvolver a compreensão dos riscos, a apreciação das causas e as estratégias e os métodos mais adequados de tratamento. O risco é analisado, as consequências e a probabilidade são mapeadas. As consequências podem ser expressas em termos de impactos tangíveis e intangíveis.

Na fase final, temos a avaliação de riscos, processo que auxilia na tomada de decisões. Consiste em comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Com base nesta comparação, a necessidade do tratamento pode ser considerada. As decisões devem levar em conta o contexto mais amplo do risco e considerar a tolerância aos riscos. Convém que as decisões sejam tomadas de acordo com os requisitos legais e regulatórios. A decisão pode ser em se aprofundar mais na análise ou de não se tratar o risco. Essa decisão será influenciada pela atitude perante o risco da empresa e pelos critérios de risco que foram estabelecidos.

A ISO 19600, que está sendo readaptada para a ISSO 37.301, contém as diretrizes do Sistema de Gestão de Compliance. O objetivo das normas ISO 19600:2014 é orientar às empresas na elaboração de seus Programas de Compliance.

Esse conjunto de normas tem sua estrutura com base no ciclo PDCA:

P - Plan - Planejar o sistema de gestão, elaborar o plano de ação. Definir as medidas a ser adotadas no enfrentamento dos riscos mapeados.

D - Do - Executar, adotar ações para implementar o plano de ação e estabelecer mecanismos de acompanhamento.

C - Check - Verificar a eficácia dos controles implementados. Investigar se o planejado está sendo executado e se está sendo eficaz. Se não funciona, precisa ser tomada alguma ação corretiva.

A - Act - Agir, tomar alguma ação; aprender com a experiência. Levando em consideração os resultados, os casos de não conformidade devem ser tratados e o sistema deve ser aperfeiçoado em um ciclo contínuo.

O objetivo é impulsionar o sistema de gestão, e a liderança da empresa é a engrenagem desse ciclo. A liderança é composta por um grupo de pessoas, os gestores da empresa.

2.19. Riscos emergentes e a pandemia

De acordo com o Conselho Internacional de Governança de Riscos (IRGC), riscos emergentes são aqueles identificados como "novos" ou riscos que se tornam mais aparentes devido a condições incomuns.

Devido à sua própria natureza, a avaliação desse tipo de risco se torna um desafio ainda maior. Por surgirem em contextos nunca vistos ou em cenários de muita instabilidade, a identificação do risco pode levar mais tempo que o normal.

A sua compreensão pode ser limitada pela falta de informação e, partir daí, o desenvolvimento de estratégias e métodos para mitigação podem ser falhos ou insuficientes.

Ainda, além de serem complexos de avaliar, quantificar e mitigar, riscos emergentes podem causar grandes impactos para as empresas e a sociedade como um todo e, por isso, merecem muita atenção.

Então como identificar riscos emergentes? De acordo com Martin Weymann e Rainer Egloff, em publicação para revista The Actuary , como a percepção de risco varia de acordo com cultura, sociedade, educação e contextos, a diversificação de grupos para identificação desses riscos é essencial. Outro ponto fundamental para o tratamento desse tipo de risco é a compreensão de seu possível impacto e não necessariamente na probabilidade de sua ocorrência.

No livro *A Lógica do Cisne Negro*, Nassim Taleb trata de sua visão sobre o mundo, principalmente em como a sociedade lida com o improvável e como a percepção sobre a suposta verdade pode trazer uma terrível sensação de segurança. Taleb contextualiza sua tese com a descoberta da Austrália, momento em que os ingleses, que até então só conheciam cisnes brancos, se depararam com cisnes negros.

O cisne negro simboliza o evento imprevisível, mas que gera grande impacto. Até serem descobertos, a premissa era de que não existiam cisnes, que não os brancos, já que nunca se tinha visto cisnes de outra cor. Mas, de acordo com Taleb, negar o imprevisível, a exemplo de uma possível existência de um cisne de outra cor, a sociedade limita a sua percepção de realidade àquilo que já experienciou e nega a possibilidade de o imprevisível ocorrer.

No entanto, constantemente a sociedade se depara com o improvável e, por esta razão, o ideal é priorizar suas crenças de acordo com os danos que elas podem causar e não com a chance de elas acontecerem. E como quando falamos de riscos emergentes tratamos do imprevisível, essa metodologia deve ser adotada.

Contextualizando a lógica de Taleb, poderíamos considerar a pandemia da

COVID-19 como um cisne negro? Segundo o próprio escritor, não. Em participação no evento Expert XP, este alegou que "Algo que você espera que vá acontecer possivelmente não é um cisne negro." De acordo com ele, como na história vivenciamos outros momentos de pandemia e tínhamos o conhecimento da gravidade do vírus antes de ele se propagar, possuíamos informações o suficiente para tomarmos medidas simples de mitigação do risco.

É certo que o conceito de cisne negro é relativo. Ao não ter ou ao não considerar as informações relevantes, provável será que seremos muito mais surpreendidos por cisnes negros.

2.20. Riscos mais aparentes no cenário de pandemia

- Teletrabalho: o teletrabalho ganhou uma força significativa como uma alternativa de forma de trabalhar em um contexto de maior segurança. É claro que com esse aumento os riscos advindos desse formato de trabalho também foram intensificados, entre eles os riscos trabalhistas advindos das condições de ergonomia no teletrabalho e o aumento significativo de ciberataques. Riscos esses analisados abaixo:

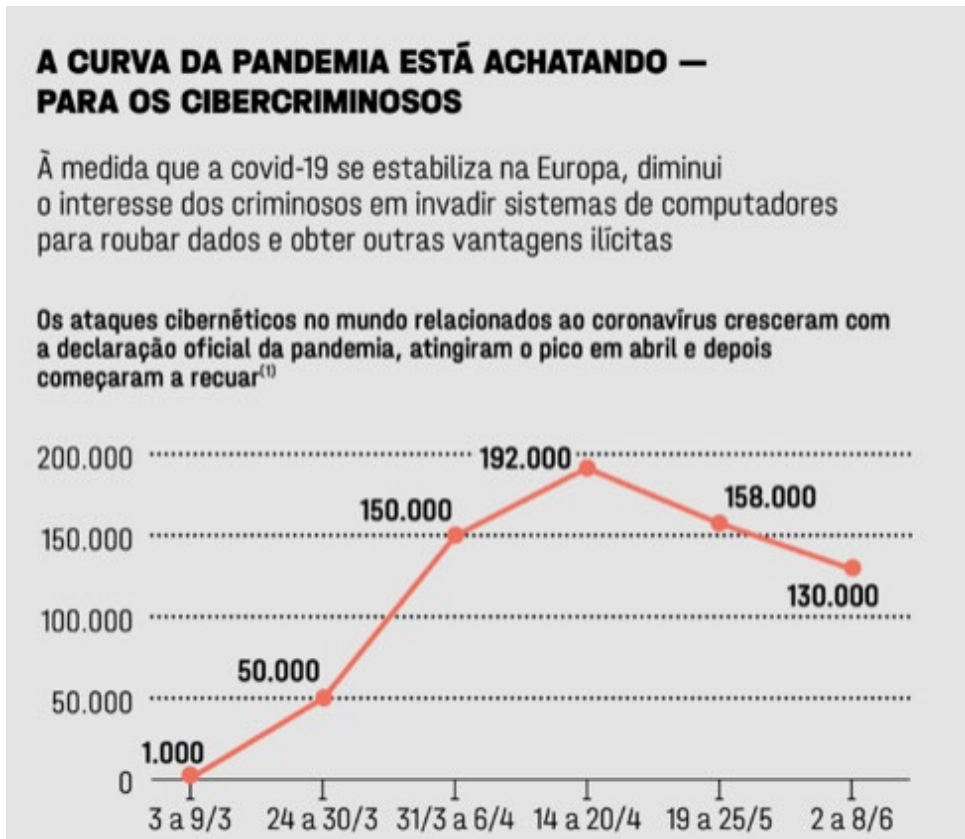
A) Ergonomia do trabalho: abaixo exploramos um caso concreto em que uma empresa de energia se viu respondendo a um processo devido à falta de estrutura disponibilizada para funcionários trabalhando em home office durante o período da pandemia:

Em 8 de julho, uma empresa de energia foi obrigada, por meio de liminar, a disponibilizar mobiliário ergonômico e arcar com custos do teletrabalho para todos os seus profissionais colocados em regime de *home office* (o que representa 90% de seus empregados alocados no Estado do Rio de Janeiro). De acordo com a decisão, a empresa também foi obrigada a providenciar a entrega do mobiliário, além de arcar, a partir da data da distribuição da ação até o seu trânsito em julgado, com todos os custos com equipamentos de informática, pacotes de dados e energia elétrica, necessários ao regular desempenho do teletrabalho. Foi estabelecida uma multa no valor de R$ 5 mil, em relação a cada empregado prejudicado, na hipótese de descumprimento.

Posteriormente, por entender que não ficou provado que os funcionários da empresa não teriam condições de atuar em *home office*, a desembargadora competente decidiu pela suspensão da liminar, mas o processo permanece em andamento.

B) Aumento de ciberataques: abaixo exploramos a relação do ciberataque com a necessidade do teletrabalho ao longo da pandemia:

De acordo com matéria publicada na revista exame, dados do Check Point, empresa israelense especializada em segurança digital, mostram que as tentativas de cibercrimes, durante o período da pandemia, aumentaram significativamente (gráfico a seguir). Muito embora, a situação da pandemia e do cibercrime tenham se estabilizado ao longo do tempo, não se pode negar que os criminosos digitais ganharam ainda mais espaço com a adoção massiva de teletrabalho por todo o mundo, intensificando, portanto, a necessidade de atenção a crimes como esses.



Fonte: Revista exame, dados do Check Point

Capítulo 3

Pessoas e Competências

3.1 Papéis e responsabilidades

Quais os papéis e as responsabilidades do Compliance Officer nas organizações? Esta questão é sempre debatida em diversos fóruns, entre os profissionais de Compliance, administradores, diretores, membros do Conselho de Administração, consultores, auditores, agentes de regulação do mercado, entre outros, devido à sua complexidade e também pelo fato de a função de Compliance ser recente no mercado brasileiro em nosso ambiente de negócios.

Especialistas e profissionais no tema convergem para os principais papéis e responsabilidades do Compliance Officer, desde o papel de guardião das melhores práticas éticas até como o responsável pela disseminação e pela multiplicação da cultura de integridade nas instituições.

Dentre os diversos papéis e responsabilidades amplamente discutidos nos fóruns mencionados, existem alguns pontos essenciais que serão destacados ao decorrer desta análise, por exemplo o papel de multiplicador e guardião do programa de integridade.

Debates incansáveis foram realizados sobre a efetividade dos programas de Compliance nas instituições, em que nos deparamos com vários exemplos reais de companhias multinacionais de grande porte que implementaram o programa de Compliance, seus procedimentos, códigos de conduta, canal de denúncias, treinamentos, dentre outros instrumentos, porém, foram envolvidos em grandes escândalos de desvios de recursos, atos ilícitos, situações de assédio moral, entre outros fatos que abalaram a sua imagem reputacional, além do imenso impacto financeiro nas instituições.

Desta forma, surge invariavelmente o questionamento de quais controles e processos não funcionaram ou não foram cumpridos e, se houve um problema cultural na companhia, ou seja, por que o programa de Compliance não foi efetivo?

É possível explorar os potenciais motivos da não efetividade do programa de Compliance, por exemplo a falta de comprometimento da Alta Administração, imposição de metas extremamente agressivas, falta de treinamentos, canal de denúncias inefetivo, falhas nos processos de comunicação, inexistência de controles internos e falta de comprometimento dos colaboradores com o tema de Compliance.

Mas como mitigar esse processo de cegueira ética? Através da multiplicação e da disseminação dos comportamentos éticos aceitáveis para aquele ambiente e aquela organização, em que seja possível gerar o senso de justiça em todos

os seus elementos[4].

Neste contexto, é possível explorar mais detalhadamente os papéis e as responsabilidades de um Compliance Officer nas companhias, ou melhor, em seu ambiente de atuação.

Um dos papéis e das responsabilidades abordados (não subjugando os demais itens) é o de ser o multiplicador e o disseminador da cultura de integridade.

Neste sentido, o maior desafio é provocar as pessoas a refletir na melhor decisão a se tomar quando postas em situações de conflitos éticos. Tal competência é conquistada através de treinamentos periódicos, comunicações sobre o tema advindas da Alta Administração e da criação de agentes multiplicadores da cultura de Compliance.

Esse papel é fundamental e complexo, pois exige a habilidade do profissional em transmitir os princípios e as diretrizes nos diversos fóruns das companhias, conhecendo o ambiente de negócios, seus principais riscos, processos de controles e o gerenciamento de toda a sua cadeia de relacionamentos.

Outro desafio está relacionado à diversidade do público a ser atingido. O Compliance Officer deve se preocupar em atingir todos os colaboradores da companhia e em todos os níveis hierárquicos, levando em consideração orçamento disponível, grau de instrução do colaborador, cargo, grau de exposição a riscos e diversidade cultural e regional.

Por conseguinte, a comunicação e o treinamento devem ser personalizados para cada tipo de colaborador. O mesmo treinamento utilizado para membros da Diretoria não pode ser utilizado para colaboradores operacionais de uma linha de montagem, por exemplo, dada a complexidade do tema, a abrangência, a exposição a riscos de Compliance, disponibilidade de tempo, dentre outros.

Neste sentido, o Compliance Officer também deve gerir o canal de denúncias, através da divulgação interna e externa da ferramenta, a fim de incentivar os colaboradores, terceiros, parceiros de negócios e consumidores a denunciar condutas ilícitas.

Além disso, o profissional pode possuir uma equipe competente e treinada ou contratar uma consultoria especializada para realizar as investigações sobre as denúncias dispostas no canal. Vale ressaltar que, tanto uma equipe interna quanto a consultoria especializada devem possuir autonomia e independência para

---

[4] DA SILVEIRA, Alexandre Di Micelo. Ética Empresarial na Prática: Soluções Para Gestão e Governança no Século XXI. 1° Edição. Editora Alta Books, 2007.

realizar suas atribuições.

Através das investigações e das diligências, é possível verificar a veracidade dos fatos denunciados, elaborar indicadores sobre os principais atos transgressores e, com base neles, criar planos de ação mitigatórios para que não haja a reincidência desses ilícitos.

Desta forma, através da conscientização de condutas esperadas, por meio da realização de treinamentos, do incentivo do uso do canal de denúncias e de investigações realizadas de forma autônoma e independente, é possível criar um ambiente autorregulado, em que o Compliance Officer deve monitorar constantemente e elaborar planos de ação sob as deficiências encontradas ao longo do programa.

Além disso, também é dever do Compliance Officer integrar a área de Compliance com outras áreas da companhia, a fim de realizar seus trabalhos de forma ampla e interdisciplinar, por exemplo atuar com a área de Auditoria e Controles Internos, com a finalidade de mapear e testar os controles críticos da companhia e identificar possíveis falhas ou riscos de fraude, bem como elaborar políticas e procedimentos internos com o auxílio de outras áreas e outros departamentos.

Semelhantemente, o Departamento Jurídico pode auxiliar no mapeamento de riscos de Compliance e na elaboração de um inventário regulatório, com o intuito de auxiliar na confecção de controles internos e planos de ação para mitigar os riscos identificados e deixar a companhia atualizada sobre o arcabouço regulatório a que está inserida.

Assim, é dever do Compliance Officer, com a Alta Direção e o Conselho de Administração, a criação de uma cultura de integridade, através da colaboração multidisciplinar de toda a companhia, estimulando um ambiente mais íntegro, que inibe ou repulsa a cegueira ética corporativa.

3.2 Due diligence e background check

Due diligence é uma expressão inglesa que significa "diligência prévia". Pode ser conceituada como um processo que envolve estudo, pesquisa e análise detalhada de informações financeiras, fiscal, contábil, legal e de integridade, a fim de avaliar o risco de determinado negócio/relação jurídica, como em operações de aquisição, fusão e cisão de empresas, com ênfase em pessoas jurídicas e corporações.

Este procedimento está previsto no art. 42, incisos XIII e XIV, do Decreto nº 8.420/15, que prevê como critério de efetividade do programa de Compliance, pois,

além de atuar como um mitigador de riscos, é possível identificar oportunidades e agregar conhecimento ao negócio.

Semelhantemente, o *background check,* que significa "verificação de antecedentes", tem como objetivo encontrar o maior número de informações e dados possíveis para verificar a sua validade, como avaliar o histórico profissional de um candidato à vaga de diretor. Este procedimento prioriza análises de pessoas físicas, podendo abranger, mas não se limitando a:

- Distribuição de ações judiciais.
- Consulta de processos administrativos.
- Situação cadastral do quadro societário.
- Regularidade de CPF e CNPJ.
- Regularidade perante órgãos de controle como Anvisa, CREA, OAB, CRM, dentre outros.
- Confirmação de informações no currículo: formações, experiências anteriores etc.
- Emissão de certidões negativas (tributárias, criminais, cíveis, dentre outras).
- Consulta à Lista Suja do Trabalho Escravo.
- Consulta a listas públicas disponibilizadas pelo governo no Portal da Transparência, como: CEIS - Cadastro de Companhias Inidôneas e Suspensas, CNEP - Cadastro Nacional de Companhias Punidas e CEAF - Cadastro de Expulsões da Administração Federal (aplicado a pessoas físicas e jurídicas), Lista de Acordos de Leniência, PEP - Pessoas Expostas Politicamente.

Dentre os diversos pilares que o programa de Compliance de uma companhia deve possuir, estes procedimentos são um dos mais essenciais e de razoável facilidade de implementação. Para a realização da *due diligence*, o Compliance Officer deve ser atentar para realizar o procedimento de forma adequada, atentando-se para o tamanho da companhia, a complexidade regulatória e jurídica e o ramo de atuação.

Isto posto, é possível estipular os critérios de análise para os stakeholders — clientes, fornecedores, parceiros, bem como quais são as possibilidades da companhia em relação à contratação de cadastros de consulta e análise.

Inobstante as diversas modalidades de busca e consulta cadastral, é de competência do Compliance Officer definir quais serão os critérios efetivamente considerados, devendo, ainda, se comprometer com a revisão de sua política de forma programada, a fim de identificar se os mesmos critérios devem ser mantidos,

ajustados ou ainda alterados.

Adentrando as análises, é possível estipular duas diferentes fases: pesquisa de dados e definição e avaliação das informações. Vejamos:

3.3 Pesquisa de dados

Trata-se da busca dos dados pessoais das pessoas e das companhias envolvidas na negociação para verificação do histórico em fontes de pesquisa aberta.

Uma das buscas mais acessíveis a todas as companhias é a utilização de buscadores na Internet quanto ao nome do possível cliente, fornecedor ou parceiro. Apesar desta modalidade de pesquisa poder culminar em elevado grau de falha, para pequenas companhias que não podem suportar os custos de contratação de companhias de análise de cadastro ou crédito, já se torna um primeiro filtro, que pode interromper o fluxo de uma contratação ou uma negociação em curso.

Outro formato é a contratação de bases de dados oficiais em que é possível realizar a verificação. No entanto, aqui é possível identificar a primeira dificuldade — quando se trata de diversas consultas, será necessário realizar a consulta de cada CPF/CNPJ em cada site de bases oficiais, culminando em um elevado tempo para obtenção de todos os resultados. Ainda neste processo, incorremos em um elevado risco operacional, por erro manual — quando é possível deixar de consultar um cadastro ou ainda repetir o mesmo resultado para outra pessoa.

Em relação às companhias que possuem orçamento disponível, a escolha mais recorrente é a contratação de sistemas ou fornecedores que realizam a busca em todas as bases de dados oficiais, Internet e ainda outros cadastros à escolha. Essa ferramenta permite consolidar todos os resultados existentes, com menor taxa de falha operacional, uma vez que é preciso consultar o dado (seja CPF/Nome ou CNPJ/Razão social), apenas 1 (uma) vez e salvar o resultado para análise.

3.4 Definição e avaliação das informações

O processo de avaliação das informações reunidas desempenha papel fundamental no processo decisório da organização. É neste momento que se identifica e consolida quais informações são significativas para a organização.

Por exemplo, quando tratamos de parceiros comerciais com relevante nome, a identificação de processos judiciais ou ainda relacionados a investigações, como a "Operação Lava Jato"[5], que apura a prática de crimes financeiros e desvio de

[5] http://www.pf.gov.br/imprensa/lava-jato

recursos públicos, em que este esteja envolvido pode ser o indicativo para a organização não realizar negócio, sob pena de atingir o ativo mais importante da organização, sua imagem e sua reputação.

Por outro lado, quando tratamos de pessoas físicas, é possível identificar, por meio das análises, a existência de indícios que podem fazer com que a contratação seja identificada como um cenário de risco. Neste caso, podemos exemplificar como o candidato à analista financeiro em uma área considerada estratégica para a companhia, por realizar o acompanhamento e a movimentação de recursos, que possui apontamentos em aberto na CVM[6] e, por isso, a companhia decide por declinar sua contratação, pois considera como um risco.

Após a conclusão da fase de avaliação das informações, é necessário cruzar as informações consolidadas com as políticas e/ou os manuais internos da companhia. Este documento oficial da companhia determinará quais situações são consideradas como impeditivas ao prosseguimento da relação e quais são passíveis de prosseguimento, mediante medidas como: aprovação de alçadas e/ou acompanhamento regular (com intervalos a ser definidos na política).

Em uma organização que possui um maior grau de maturidade nos seus processos de Compliance, o Compliance Officer deve implementar indicadores como Know Your Client (KYC), Know Your Employee (KYE) e Know Your Partner (KYP) — conheça seu cliente, seu empregado e seu parceiro —, pois, por meio deles, é possível realizar acompanhamentos de forma estratégica e analítica, avaliar periodicamente o grau de risco e permitir seu reporte ao Conselho de Administração.

3.5 Avaliação contínua de competências

A avaliação por competência tem por objetivo, além de avaliar a performance dos funcionários, ajudar a identificar quais são as competências necessárias para o novo momento da companhia ou do empregado, colaborando com o desenvolvimento de competências e habilidades de que contribuirão efetivamente.

As teorias atuais ainda preveem que a avaliação seja realizada em 360 graus — ou seja, por meio de seu superior, seus pares, seus subordinados (se houver) e, ainda, a auto avaliação.

Além disso, a avaliação contínua das competências permite a efetiva redução

---

6 CVM - Comissão de Valores Mobiliários (CVM) - Entidade pública e autárquica vinculada ao Ministério da Fazenda http://www.cvm.gov.br/-jat

dos riscos da companhia. Pense bem: quando se possui a certeza de que determinado funcionário possui as habilidades e os conhecimentos necessários na área, o risco operacional, de erro, por exemplo, é significativamente reduzido. Por outro lado, um funcionário que não possui determinada competência, além de aumentar o risco de falhas manuais, não consegue identificar que determinado processo ou solicitação pode causar outros riscos ou configurar descumprimento das políticas internas. E ainda nem citamos a possibilidade de ser indiferente a fraudes internas ao não possuir as competências necessárias para análise crítica.

A título de exemplo, os profissionais de Compliance devem ter conhecimento sobre o arcabouço regulatório da companhia, seus órgãos de controles e seus conselhos de classe, conhecer os produtos e os serviços oferecidos, tecnologias que suportem a gestão de seu departamento e dominar as normas técnicas de Compliance e anticorrupção.

Já o Compliance Officer, além de possuir todas essas competências, ele também deve ser um profissional comunicativo para conseguir transmitir a mesma mensagem para diversos tipos de público, ter um alto poder de persuasão, a fim de demonstrar a importância de suas ações à Diretoria e ao Conselho de Administração, ser resiliente para enfrentar os desafios financeiros e operacionais, possuir um bom relacionamento com profissionais, ter visão estratégica e contribuir para o crescimento da companhia, dentre outras competências.

De posse das informações consolidadas, a companhia pode definir competências e habilidades que são necessárias para cada cargo e nível hierárquico, além de planejar-se financeiramente em relação àquelas que são obrigatórias para realização da atividade (como a renovação de uma certificação) e ainda proporcionar a elaboração de planos de carreira alinhados às competências que precisam ser desenvolvidas pelo funcionário em prol da manutenção ou da promoção no cargo.

3.6 Gestão de desempenho, incentivos e remuneração

A garantia da integridade de todo um sistema de Compliance é um dos principais pontos de vulnerabilidade e compete a organização estabelecer medidas que incentivem e orientem as pessoas da importância de desempenharem as suas atividades dentro dos requisitos legais, éticos e colaborativos.

A gestão de desempenho tem por objetivo desenvolver as competências e as habilidades dos colaboradores, implementando melhorias nos processos internos. O setor de Recursos Humanos precisa inserir na gestão de desempenho da força de

trabalho o conhecimento necessário e a importância do Compliance, sua estrutura organizacional e as ferramentas disponíveis para permitir um controle de ilícitos que possam comprometer a imagem e os recursos da companhia, aprimorando o desenvolvimento das capacidades individuais e das equipes.

A implementação de uma política de gestão de desempenho permite que uma companhia possa aplicar métricas de avaliação, desde o ingresso até o desligamento do colaborador, permitindo uma análise do aprendizado e fixação dos valores éticos e legais adotados pela companhia. Ademais, também permite, ao se verificar desvios, que sejam empregadas medidas tempestivas para correções e ajustes no desenvolvimento das equipes.

Por conseguinte, uma das maneiras para implementar a cultura de Compliance em um grupo é criar incentivos à força de trabalho.

O principal deles é apresentar, de maneira clara, a importância do assunto no dia a dia, os impactos na imagem da companhia, os resultados financeiros e a manutenção dos empregos.

Também poderão ser criadas atividades periódicas, nos moldes dos realizados pela Comissão Interna de Prevenção de Acidentes (CIPA), que permitam uma maior participação de todos os setores nas atividades de Compliance.

Outro artifício que tem apresentado excelentes resultados é de não pagar a participação nos lucros e nos resultados ou outra bonificação salarial ao final do ano, caso o profissional tenha recebido uma advertência ou uma suspensão por comportamentos em desacordo com as diretrizes da companhia.

Em relação ao Compliance Officer, muitas vezes a remuneração não é o fator principal de engajamento. O comprometimento e os valores pessoais são, na maioria das vezes, mais relevantes.

As atividades de Compliance exigem que o profissional tenha ensino superior completo, seja multidisciplinar, analítico, autônomo, criativo, comunicativo, tenha um perfil de liderança e, sobretudo, seja íntegro.

Trata-se de uma profissão com dedicação exclusiva, que lida com assuntos críticos e de alta complexidade, precisa ter remuneração acima da média de seus pares no mesmo nível hierárquico de outras áreas das companhias.

A remuneração acima da média permite uma melhora no recrutamento para a atividade de Compliance, pois o gestor passa a ter um atrativo financeiro para trazer os melhores profissionais, mesmo de outras áreas da mesma companhia para a sua equipe.

3.7 Aplicação de medidas disciplinares

"Compliance é uma obrigação para todos os colaboradores. Portanto, o Código de Conduta Profissional estipula que qualquer colaborador culpado de má conduta terá de contar com consequências disciplinares devido à violação das obrigações do contrato de trabalho, independentemente das sanções previstas na lei".[7]

Uma companhia deve possuir políticas e procedimentos robustos, validados e muito bem comunicados a toda a organização para garantir o cumprimento integral do programa de Compliance, direcionar os colaboradores a seguir as regras ali expostas e garantir que ações e condutas não conforme sejam detectadas e denunciadas.

Quanto mais natural e introjetado na organização for o programa de Compliance, mais eficiente ele será. Por este motivo, seu cumprimento deve buscar ser justo, igualitário e consistente. Esses adjetivos devem ser a base de regras, políticas e procedimentos de conduta.

No intuito de os stakeholders observarem as diretrizes do programa, a companhia deve estabelecer e aplicar medidas disciplinares e punitivas a condutas ilícitas e que vão de encontro com o programa de Compliance estabelecido.

O programa de Compliance deve conter e deixar claro que: condutas que desrespeitem o programa, as diretrizes internas e a falta de reporte de condutas ilícitas serão punidas, independentemente do cargo e do nível hierárquico.

A obrigação do cumprimento do programa é condição sine qua non e envolve certa maturidade de Compliance, pois requer o reconhecimento de que qualquer falha em detectar, reportar pontos ou agir contra o programa de Compliance deve ser punida. Assim, é importante reforçar que as regras e as diretrizes internas devem ser aplicadas a todos, indiscriminadamente.

Um ponto de atenção é que as medidas disciplinares devem estar alinhadas à legislação, portanto é necessário que estas passem por validação do Departamento Jurídico e de Recursos Humanos. Todos os colaboradores devem ter ciência e conhecimento das regras de conduta esperadas e possíveis punições de seu não cumprimento.

Desta forma, é uma prática das companhias utilizar medidas disciplinares progressivas, isto é, a punição aumenta de acordo com a reincidência da mesma infração. As punições podem ser classificadas como:

---

7 https://sousacruz.adv.br/blog/estruturacao-das-regras-e-instrumentos-de-Compliance/ acesso em 12/08/2020.

- Advertência verbal
- Advertência formal por escrito
- Perda ou corte de remuneração variável
- Transferência para outra função
- Treinamento de Compliance
- Suspensão
- Demissão com ou sem justa causa.

Além das medidas supracitadas, caberá à companhia a adoção de medidas legais relacionadas à restituição dos danos.

A medida punitiva deve ser prevista em política, proporcional à conduta transgressora e tempestiva (ocorrer na forma mais rápida possível após a detecção da infração, sem prejuízo do tempo necessário à correta análise do ocorrido).

A prática entre as companhias é punir com demissão condutas inadequadas (agindo com dolo), por exemplo a fraude. Já outras menos graves e intencionais costumam ser punidas com advertência seguida de treinamentos e conscientização. Assim, percebe-se que o canal de denúncias é um dos meios responsáveis para que fraudes, abusos e perdas sejam comunicados às áreas pertinentes da organização. Desta forma, cada colaborador se torna uma peça fundamental no monitoramento do programa.

Capítulo 4

Políticas e Procedimentos

KPMG

KPMG
BUSINESS SCHOOL

4.1. Introdução e Objetivos

As estruturas da organização e seus sistemas de controle devem interagir com os valores, a ética e as suas crenças para produzir normas de comportamento favoráveis aos resultados de compliance.

Como base de toda organização ou empresas, as regras de condutas devem ser elaboradas, aprovadas pelos gestores, difundidas e aplicadas em todos os níveis, para prevenção de sanções, perdas financeiras e danos à reputação e à imagem das organizações.

As regras de condutas são:

Externas - Vindas de órgão governamental e de controle.

Internas - Criadas pela própria organização e servirá para manter o alinhamento de condutas em todos os níveis, bem como com as partes relacionadas. Dentre as regras internas de uma organização, existem aquelas que regulam a **própria organização**, como Estatuto, Regimentos e Acordos de Acionistas, e aquelas que **regulam os seus processos** em diversos níveis. Podemos elencar as mais utilizadas como políticas, normas e procedimentos e, ainda, o Código de Conduta, que regulará, além dos atos internos da empresa, também as partes relacionadas.

O objetivo das regras é prevenir e não deixar condições favoráveis à prática de desvios e pode ser:

- Principal: busca regulamentar e punir para reduzir a vulnerabilidade.
- Secundário: busca o compromisso com o programa de integridade da organização.

Definir quais políticas e procedimentos devem ser utilizados na organização é um dos elementos essenciais para a efetividade do Programa de Compliance.

Com base no conhecimento do perfil e dos riscos da empresa, deve-se elaborar ou atualizar o código de conduta e as regras, as políticas e os procedimentos de prevenção de irregularidades (Programa de Integridade - Diretrizes para Empresas Privadas - CGU).

A cultura da empresa, as suas atividades e os relacionamentos com terceiros são elementos primordiais para a definição das regras.

Para uma maior eficiência, eficácia e confiabilidade, as regras devem ser elaboradas pelas áreas específicas, com consenso e aprovação do compliance.

O gestor de compliance é o guardião dessas regras e não necessariamente aquele que vai elaborá-las, mas sim aquele que vai definir a sua necessidade.

Para apuração robusta e justa de uma denúncia, são necessários elementos que comprovem o desvio de atitude. Estando o ato apurado, previsto nos

procedimentos formais da organização (Código de Conduta e Ética, políticas, normas e procedimentos), facilitará a decisão da Comissão de Ética, que julgará com base em elementos concretos e formais. Daí a importância da organização em ter o maior número de processos formalizados, divulgados e treinados em todos os níveis.

A revisão periódica, a atualização e a adaptação aos riscos têm que sempre estar no radar do compliance, suprindo possíveis deficiências nas apurações de desvio de conduta, inibindo assim futuros casos.

A partir do perfil de riscos, é possível definir as políticas e os procedimentos que devem constar no Programa de Compliance Principais Políticas, devendo levar em consideração as necessidades de cada organização.

Deve-se considerar brindes, doações e patrocínios, presentes e hospitalidades, conflitos de interesse, relacionamento com agentes públicos, uso de informações privilegiadas, práticas de competição, controles financeiros e registros contábeis, entre outros, e, por fim, política de investigação de fraudes e má conduta, esta última essencial para credibilidade e coerência na aplicação das sanções.

4.2. Código de Conduta

A empresa respeita a legislação aplicável e os seus negócios e está plenamente comprometida com a adoção de altos padrões éticos na condução de suas operações. A conduta empresarial é responsável e visa a garantir a sustentabilidade dos negócios.

O mesmo comprometimento demonstrado pela empresa é também exigido de colaboradores, parceiros e clientes. É fundamental que todos saibam que a empresa não tolera desvios de conduta ou nenhum tipo de violação ou descumprimento de obrigações legais e/ou normas internas.

A empresa tem o compromisso de conduzir seus negócios com integridade e com os mais elevados padrões éticos, assim como respeitar a legislação aplicável aos seus negócios e estar plenamente comprometida com a adoção de elevados padrões éticos na condução de suas operações. A conduta empresarial é responsável e visa a garantir a sustentabilidade dos negócios. O Código de Conduta reflete valores, missão e crenças da empresa e, diariamente, deve ser seguido pelos colaboradores e também servir de referência para os parceiros.

Além de nortear os negócios, é também ser uma ferramenta que amplia a comunicação e dá publicidade e garantia de transparência de todas as ações de compliance implementadas pela empresa, pois orienta, conscientiza e esclarece eventuais dúvidas.

Do Código de conduta derivam as principais políticas sobre temas como: anticorrupção, transações com partes relacionadas, conflito de interesses, prevenção à lavagem de dinheiro, leis concorrenciais, recebimento de brindes, relacionamento com entes públicos, dentre outras políticas que serão tratadas individualmente.

4.3. Compromissos

Estabelecer compromissos da empresa com leis e regulamentos, meio ambiente, saúde e segurança, inclusão e diversidade e outros temas relevantes para ela.

Prever condutas e comportamentos esperados com base na integridade e na ética, bem como os não aceitáveis e os intoleráveis.

Estabelecer um canal de denúncia para acolher reclamações e manifestações sobre potenciais desvios de comportamento e não conformidades com valores, crenças e políticas, geridos por empresa independente, com garantia de sigilo para todos os denunciantes que não desejam se identificar, garantindo que não haverá retaliação. Os casos são apurados por grupos de trabalho e reportados periodicamente à Administração e ao Conselho Fiscal.

4.4. Conceituações e Diferenças em Relação a Políticas, Normas e Procedimentos

Embora muito comuns nas organizações, os documentos apresentados a seguir e suas conceituações ainda geram muitas dúvidas em sua correta utilização, acarretando ineficiência, reduzindo a produtividade e a rentabilidade de uma organização.

Para tratarmos desses documentos, explicitaremos seus principais conceitos, suas diferenças e suas semelhanças.

4.4.1. Políticas

A ISO 9000:2015 define "política como sendo intenções e direção de uma organização expressos pela Alta Administração".

Traduzindo a definição da ISO 9000:2015, a política representa a visão e as diretrizes da organização as quais devem ser seguidas para atingir o objetivo estabelecido pela organização.

A política norteia as ações da organização e servem como referência para o estabelecimento das normas e dos procedimentos.

É ligada diretamente à cultura organizacional, devendo estar em consonância com missão, visão e valores da organização.

4.4.2. Normas

De acordo com o Dicionário Michaelis, norma é "tudo que estabelece e regula procedimentos; padrão, preceito, princípio, rédea, regra. "

Fazendo a correlação com a definição acima, as normas são regras que devem ser respeitadas e que permitem ajustar determinadas condutas e atividades.

As normas são aprovadas em consenso de pessoas, departamentos ou órgãos com autoridade reconhecida dentro da organização.

4.4.3. Procedimentos

Trata-se de uma forma específica de executar uma atividade ou um processo, segundo a definição dada pela ISO 9000:2015.

O procedimento é a forma detalhada de descrever uma tarefa a ser executada, através de uma padronização e demonstrando cada resultado da tarefa executada.

Normalmente é detalhado o que deve ser executado, quem a executa, quais medidas são necessárias para a execução, quando e como as etapas são executadas.

Como observamos na conceituação, cada um desses documentos tem um papel fundamental dentro da organização, sendo a política responsável por descrever a visão e as diretrizes a ser seguidas para atingir o objetivo estabelecido pela organização; as normas por estabelecer as regras mínimas e aceitáveis para que tais objetivos sejam cumpridos; e os procedimentos por descrever a forma de execução das atividades necessárias para se atingir os objetivos propostos pela organização.

Cabe ressaltar que um documento não substitui o outro, pelo contrário, são extremamente complementares e fundamentais para as organizações, pois é necessário que políticas, normas e procedimentos estejam claramente definidos, aprovados e publicados. Eles formam um conjunto de ferramentas importante para definir e dar transparência à organização.

4.5. Estruturação dos documentos normativos

Os documentos normativos devem ser diretos, claros, objetivos, preferencialmente em tópicos simples, sem muitas explicações conceituais.

A organização deve escolher o local adequado para o armazenamento dos documentos normativos e estes devem estar permanentemente à disposição de todos os prepostos e empregados de sua organização.

Por fim, é necessário que se eleja qual a área que ficará encarregada da gestão de políticas, normas e procedimentos, ou seja, que fará o controle de sua vigência,

controlará o fluxo de assinaturas e a logística, para que isso ocorra no menor tempo possível.

Abaixo, descreveremos como deve ser a estrutura mínima dos documentos normativos:

- Cabeçalho - Contendo tipo de documento, código do documento, páginas, classificação de publicidade, nome do documento, data de vigência e a versão do documento.
- Objetivo - Descrever qual o objetivo que se espera com a edição, a aprovação e a vigência daquela norma interna (por exemplo: estabelecer padrões mínimos de comportamento para o público interno e externo da empresa XPTO, diante de situações que possam envolver ou caracterizar corrupção ou suborno de agentes públicos ou privados).
- Normas de referências - Relacionar todas as normas externas e internas que são aplicáveis ao caso.
- Âmbito de aplicação - Indicar qual o público a que é destinada a presente normativa (por exemplo: colaboradores, fornecedores, prestadores de serviços, distribuidores, parceiros comerciais, consorciador etc.).
- Definições - Definir termos relevantes presentes na norma (por exemplo: compliance, programa de integridade, corrupção pública, corrupção privada, suborno, extorsão, concussão, vantagem indevida, pagamento de facilitação, agente público, brindes, presentes, entretenimento, viagens etc.).
- Políticas/Procedimento - É a parte mais importante do documento. Apresentar quais são as diretrizes e as orientações de conduta da empresa XPTO para atingir o objetivo. (por exemplo: política anticorrupção da empresa, condutas profissionais esperadas, condutas vedadas etc.).
- Regras de consequências - Indicar o procedimento para comunicação sobre casos de violação da norma, o procedimento para apuração do fato e dos envolvidos, bem como as possíveis medidas a ser adotadas nos casos de violação.
- Áreas envolvidas - Apresentar as áreas da empresa que foram envolvidas na elaboração da norma e qual a responsabilidade de cada uma delas (por exemplo: Diretoria de Compliance, Diretoria Jurídica, Gerência de Recursos Humanos etc.).
- Disposições gerais - Assuntos pertinentes que não foram indicados nos itens anteriores.
- Aprovação/vigência - Procedimento adotado para a aprovação da norma e período de vigência. Estudar a possibilidade de indicar um prazo para revisão, mas sem tirar a vigência.

- Anexos - Documentos relevantes que possam ser anexados à norma (por exemplo: formulários, planilhas, documento-padrão etc.).
- Rodapé - Com as informações de quem elaborou, revisou e aprovou, bem como as respectivas datas.

4.6. Ações que Contribuem para Maior Efetividade das Políticas e dos Procedimentos

Em que pese a existência de um arcabouço robusto em seu portfólio de políticas e procedimentos, muitas organizações têm incorrido em falhas recorrentes na elaboração e na manutenção de seu acervo documental, seja no que se refere ao nível de efetividade, seja na manutenção da vigência desses instrumentos disciplinadores e orientativos para seus processos e suas atividades. A máxima popular "Menos é mais" pode se traduzir em sentimento que se busca na maioria das organizações, ou seja, desenvolver um portfólio de políticas e procedimentos não tão vasto, mas definitivamente efetivo para o atendimento de seus objetivos e, de certa maneira, maduro na cultura da organização contribuiria sobremaneira para que os riscos sejam reduzidos ao menor nível de exposição possível, culminando, dessa forma, com o atingimento dos objetivos estratégicos da organização.

Outra mesa de debates em que esse tema relativo à efetividade das políticas e dos procedimentos é trazido à discussão ocorre nas abordagens relacionadas à auditoria de monitoramento em que, recorrentemente os auditores opinam a essa efetividade e sobre a sua adequação e vigência, opiniões em que, na sua grande incidência, atestam a não aderência (não conformidade) por parte das áreas abrangidas pelo documento, das práticas em relação ao que preconizam tais instrumentos ou uma possível obsolescência dos instrumento em relação à prática atual. O que, de certa forma, expõe o baixo nível de engajamento das pessoas às regra e às disposições emanadas dos documentos (políticas e procedimentos).

Neste contexto, por alcançar maior efetividade das políticas e dos procedimentos nas organizações, algumas ações, ao serem tomadas no primeiro ciclo de maturidade das políticas e dos procedimentos (elaboração e divulgação), podem contribuir para o atingimento desse objetivo (efetividade dos instrumentos de regulação), sobretudo, no que tange à conscientização de todos os envolvidos sobre a real importância da documentação. Essas ações, se implementadas ao longo de todo o desenvolvimento dos documentos, nas fases de Planejamento, Execução e Implementação (Divulgação), tendem a ser mais assertivas na sua finalidade.

4.6.1. Planejamento

A fase de planejamento constitui-se em uma das importantes etapas no contexto do desenvolvimento das políticas e dos procedimentos, uma vez que, adequadamente conduzida, propiciará um produto de relevante qualidade, perfeitamente alinhado à cultura e ao propósito da organização. Dentre as principais ações a ser observadas nessa fase, podemos incluir as seguintes:

1) Entenda a aplicação, a abrangência e as referências legais e normativas que embasam as políticas e os procedimentos

Para o desenvolvimento de instrumentos disseminadores das diretrizes (políticas) e dos normativos (procedimentos), faz-se necessária a realização de uma pesquisa bastante aprofundada sobre a aplicabilidade de tais instrumentos, incluindo: i) áreas abrangidas pelos documentos, seja no nível da organização (institucional), seja no nível do processo/atividade; ii) riscos a ser tratados pelas atividades de controles, procedimentadas nos documentos; iii) legislação ou regulamentação externa que disciplina atividades, processos ou áreas relacionadas à documentação; e iv) inventário e análise a políticas e procedimentos existentes.

2) Associe as políticas e os procedimentos aos riscos identificados para a organização

Alinhado a essa visão, o conteúdo dos documentos deve também contemplar os riscos cobertos por estes, bem como de informações pertinentes às respectivas atividades de controle (por exemplo: (a) responsáveis pela execução das ações/controles; (b) frequência da atividade de controle; (c) nível de formalização; (d) modelos (templates) para formalização do controle; (d) aprovações requeridas; (e) dentre outras informações).

4.6.2. Execução

Adotadas as ações que fundamentam a fase de planejamento, inicia-se a fase de execução, fase caracterizada pela construção, propriamente, dos documentos. Nessa fase, algumas questões importantes devem ser consideradas, de modo que se tenha uma construção consistente e bastante aderente à cultura e ao propósito da organização, como já mencionado anteriormente. Dentre as atividades julgadas importantes, destacam-se as seguintes:

1) Ao estruturar o documento

Estabelecer um padrão de apresentação aplicável a todos os documentos elaborados é fundamental. Ainda que se possa parecer um ponto simples, a adoção dessa medida enriquece muito o trabalho desenvolvido, tanto do ponto de vista de qualidade e apresentação quanto do ponto de vista de engajamento

de todos, uma vez que, existindo uma padronização entre os documentos que integram o portfólio da organização, a tendência é de que os usuários se sintam familiarizados com o manuseio da documentação, de modo que suas consultas ou suas pesquisas se tornem mais objetivas, aumentando, com isso, a frequência em que tais documentos sejam acessados por todos.

2) Ao redigir o documento

Este tópico, se não o mais importante, se qualifica como um dos mais importantes. Não raro, a efetividade e o alcance das políticas e dos procedimentos são comprometidos devido a falhas na condução e na elaboração de sua escrita. A fim de evitar impasses, cabe ao redator manter-se atento a alguns aspectos que podem contribuir para a edição dos documentos. Dentre as preocupações que devem estar constantemente na pauta do redator, destacam-se as seguintes:

a) Adote uma linguagem acessível e comum a todos na organização. A aplicação de uma linguagem alinhada à cultura da organização é fator preponderante para a alavancar o nível de precisão de como a diretriz, a regra ou o procedimento irá atingir a todas as camadas da organização. Utilize termos geralmente empregados internamente (por exemplo: referir-se às pessoas como colaboradores e não funcionários/empregados ou vice-versa). Outro aspecto relevante de se observar se refere à adoção de uma linguagem que se adapte a todas áreas e as regiões de operações da organização. A linguagem formal é necessária, porém formalidade em abundância pode não despertar o interesse e o comprometimento de todos.

Um exemplo de como podem existir variações bem relevantes na linguagem de um determinado documento se observa em documentos institucionais, por exemplo Códigos de Ética e Conduta em que, muitas vezes, são elaborados em diferentes formatos de apresentação e de linguagem, altamente ajustado ao público a quem se destina ou à região a qual se endereça.

b) Busque objetividade

Ser claro e conciso são características essenciais para o atingimento dos objetivos que se buscam com a preparação de políticas e procedimentos. Documentos muito robustos contendo várias páginas se tornam, muitas vezes, inexploráveis perante o público-alvo, haja vista apresentarem um conteúdo maçante e pouco objetivo, não despertando o interesse das pessoas a quem se destina.

Obviamente que é preciso ter muita atenção e cuidado para que não haja uma sintetização excessiva do documento, tornando-o incompleto ou incompreensível. O equilíbrio entre ser sucinto e, ao mesmo tempo, completo se traduz no grande desafio (dilema) do redator.

c) Promova o engajamento

Outro fator relevante e que contribui para o sucesso no desenvolvimento das políticas e dos procedimentos é tornar o documento um compromisso de todos na organização. Para tanto, promova as pessoas ligadas às áreas afins com os documentos em elaboração a exercer o papel ativo e contributivo nesse projeto de desenvolvimento. A partir dessa interação, potenciais resistências (à criação de políticas e procedimentos), que porventura existirem, deixarão de existir no curto prazo. Além disso, o envolvimento de pessoal-chave (executores de atividades, gestores de áreas, donos de processos, donos de riscos, entre outros) com as atividades ou os processos associados ao documento (principalmente ao que tange a procedimentos) não se trata de uma sugestão, mas faz-se necessária, haja vista a complexidade muitas vezes observada nas atividades, no âmbito do processo. Essas pessoas detêm um conhecimento aprofundado dos processos, bem como das suas particularidades, suas atividades acessórias e suas integrações

d) Revise o documento e submeta à aprovação

Uma atividade que pode e deve ser repetida à exaustão diz respeito à revisão do documento elaborado. Utilize sempre medidas conservadoras, ou seja, revise reiteradamente, quantas vezes julgar necessário, já que o nível de aceitação e de credibilidade por parte das pessoas está diretamente associado ao nível de qualidade apresentada no documento, obtida, na maioria das vezes, por meio da sua apresentação e da inexistência de imperfeições ou incorreções. Finda a atividade de revisão, submeta o documento ao processo de aprovação. Nesse ponto é necessário o envolvimento da governança competente (Alta Administração, gestores e donos de processo ou de risco). Nesse estágio de aprovação, é necessário um investimento adicional de tempo, direcionado a discussões corretivas e/ou contributivas para a formalização dos documentos. Nesse estágio, é comum existirem ajustes (adições, correções ou exclusões) demandados pelos aprovadores, portanto, existindo a necessidade de um tempo adicional para aprovação, é prudente que se conceda.

Essa cautela será benéfica para o processo de implementação como um todo. Por outro lado, é preciso ser tempestivo ao submeter à aprovação. As lacunas extensas de tempo entre a elaboração e a aprovação pode comprometer a sazonalidade do documento e a sua divulgação pode não ser tão oportuna quanto se espera.

4.6.3. Implementação (Divulgação)

Conjuntamente à redação do documento, a fase de implementação (ou divulgação) se traduz em uma fase igualmente importante. Avalie a possibilidade

de treinamentos específicos, voltados à capacitação e à conscientização (aculturamento) das pessoas sobre políticas e procedimentos elaborados ou atualizados. Utilize-se dos treinamentos para também abordar sobre a importância do documento, seu objetivo e sua abrangência e, é claro, utilize-se desse momento para exaurir potenciais dúvidas acerca do conteúdo e da aplicação do documento divulgado. Essa ação de capacitar pode ser adotada tanto na divulgação de um documento novo como na divulgação de atualização a documentos existentes.

4.7. Aspectos Pós-Implementação (Monitoramento, Revisão e Atualização)

Não obstante a implementação do Programa de Compliance, são necessários monitoramento, revisão e atualização, que, juntos, garantem a efetividade e a perpetuação da cultura da integridade.

A elaboração de políticas e procedimentos não é capaz de gerar efeitos sem que haja um acompanhamento e um aculturamento constante para internalizar a cultura da integridade e aumentar a adesão às boas práticas.

O monitoramento consiste em verificar se as políticas e os procedimentos estão sendo cumpridos, por meio de:

- Auditoria interna
- Observância do manual de procedimentos de compliance
- Gestão de contratos
- Pesquisas
- Relatórios críticos periódicos
- Investigação (dando efetividade principalmente ao canal de denúncias)
- Sistemas de controle.

Entretanto, os procedimentos citados devem ser utilizados em harmonia e de forma sistematizada, sendo esta etapa parte fundamental do planejamento do Programa de Compliance, de forma a analisar o desempenho e os resultados para adequação e melhoria contínua.

A revisão e a atualização são frutos de monitoramento sério e constante do Programa de Compliance.

Uma vez verificada a efetividade do Programa de Compliance, bem como suas brechas, é hora de identificar, avaliar e classificar os riscos para atualização ou adoção de novas políticas e procedimentos, com base nos resultados obtidos.

O treinamento aliado à avaliação é uma ferramenta fundamental para a efetividade do programa, pois promove conhecimento, aculturamento, atualização das políticas e dos procedimentos, além de identificar pontos deficientes capazes de gerar riscos, possibilitando sua mitigação.

Capítulo 5

Comunicação e Treinamento

KPMG

KPMG
BUSINESS SCHOOL

5.1. Introdução

Neste capítulo, abordaremos a importância da comunicação e do treinamento dentro do Programa de Integridade das empresas, com o propósito de apresentar experiências vividas, práticas de sucesso que possam ser utilizadas dentro das organizações como processo de melhoria contínua e implementação do programa.

5.2. Legislação - Lei nº 12.846/13 e Decreto nº 8.240/15

A Lei n° 12.846, de 1° de agosto de 2013, também chamada de "Lei Anticorrupção", instituiu a responsabilização objetiva administrativa e civil das pessoas jurídicas pela prática de atos lesivos que sejam cometidos em seu interesse ou benefício, contra a Administração Pública, nacional ou estrangeira. A lei foi regulamentada pelo Decreto n° 8.420, de 18 de março de 2015, que estabeleceu as diretrizes para o Programa de Integridade das empresas.

A partir da análise das supracitadas normas, é possível verificar que, além do caráter punitivo, é necessário que as empresas adotem mecanismos e políticas que tenham o condão de prevenir, detectar e remediar riscos e irregularidades concernentes ao cumprimento das leis, principalmente medidas preventivas no combate à corrupção — tais medidas são consideradas na dosimetria das sanções a ser aplicadas, podendo atenuar a responsabilização da empresa.

Dentro desse contexto, o treinamento e a comunicação são medidas essenciais para a efetividade do Programa de Integridade, que deve ser estruturado e adequado conforme as características e os riscos da atividade de cada pessoa jurídica.

Conforme dispõe o art. 42 do Decreto n° 8420/15, o Programa de Integridade deve contemplar, entre outros aspectos, treinamentos periódicos, além de padrões de conduta, código de ética, aplicáveis a todos os empregados e os administradores, que precisam conhecer e entender seus objetivos para que o programa seja bem-sucedido.

De acordo com a Controladoria Geral da União (CGU), "o investimento em comunicação e treinamento é essencial para que o Programa de Integridade da empresa seja efetivo".

Dessa forma, quando da aprovação do planejamento e do orçamento anual da empresa para o desempenho de suas atividades, a autoridade competente para deliberar sobre a matéria, normalmente o Conselho de Administração ou a Diretoria Executiva, deve aprovar uma verba específica, adequada ao porte e à complexidade de atuação da empresa, que será destinada ao plano de capacitação

e comunicação do Programa de Integridade, garantindo, assim, sua efetividade.

5.3. Iniciativas e práticas de treinamento e comunicação

Considerando a relevância do treinamento e da comunicação na estruturação do Programa de Integridade, cumpre ressaltar a necessidade de ampla divulgação de suas diretrizes por parte das empresas.

5.3.1. Fácil acesso ao programa

As principais políticas da organização devem ser acessíveis a todos os interessados, em uma linguagem clara e precisa. A divulgação pode ser feita no portal e nas notícias na rede corporativa, além de e-mails, banners e newsletters direcionados aos diversos públicos de interesse.

Adicionalmente, observa-se que várias empresas divulgam o Código de Ética/ Código de Conduta em seu website, possibilitando que todos os stakeholders (fornecedores, clientes, investidores etc.) conheçam os preceitos que pautam sua forma de atuação no mercado.

No que tange aos treinamentos, importante, outrossim, que as empresas possuam um plano de capacitação com o objetivo de treinar periodicamente colaboradores, administradores e partes interessadas, revisando e atualizando o conteúdo dos assuntos a ser abordados, conforme a legislação e o contexto da atividade empresarial da organização.

Nesse sentido, para exemplificar os pilares de treinamento e comunicação, destaca-se o momento atual das empresas, tendo em vista os impactos causados pela pandemia em razão do coronavírus (COVID-19), sendo oportuno reforçar orientações a respeito de temas como doações e contratações emergenciais com os entes públicos — questões normalmente abordadas nos programas de integridade das organizações.

5.3.2. - Embaixadores de compliance

Algumas empresas apoiam-se em uma rede de representantes para dar capilaridade ao Programa de Compliance, de modo a difundir políticas, práticas e conectar os negócios e as funções com a área de Compliance.

Esses representantes, denominados embaixadores de compliance, são

---

8 Controladoria Geral da União: Programa de Integridade - Diretrizes para empresas privadas - 2015.

9 Exemplos de empresas que divulgam Programa de Integridade/Código de Ética/Código de Conduta em sítio externo (acesso dia 12/07/2020): i) Petróleo Brasileiro S.A. - Petrobras - Programa Petrobras de Prevenção da Corrupção (PPPC) (fonte: site: petrobras.com.br); ii) Suzano Papel e Celulose S.A. - Código de Conduta (fonte: site: suzano.com.br); iii) Vale S.A. - Código de Conduta (fonte: site vale.com).

colaboradores selecionados nas próprias áreas, que são formados e preparados nos temas de compliance de tal forma que podem unir a teoria à prática, mapeando riscos, ministrando e replicando treinamentos e estimulando o movimento de compliance dentro de suas respectivas áreas.

É essencial que o embaixador esteja inteiramente comprometido com o seu papel, bem como cada líder esteja comprometido com o apoio, o estímulo e a viabilização prática desse papel no dia a dia das áreas.

O Departamento de Compliance deve coordenar atividades dos embaixadores e dar-lhes todo o suporte técnico necessário, conforme mencionado a seguir no item 2.6 Campanha de endomarketing.

5.3.3. Treinamentos disponíveis para toda força de trabalho

Os treinamentos devem acometer toda a força de trabalho, ou seja, desde os colaboradores das áreas operacionais, como fábricas, até a Alta Administração. Além disso, o conteúdo e a forma de apresentação devem estar alinhados com a linguagem de cada público.

Importante existir uma preocupação com os recém-contratados, que devem conhecer, entender e estar comprometidos com o código de conduta e com o Programa de Integridade da empresa, além disso a empresa deve estabelecer treinamentos de reciclagem periódicos.

Boas práticas de mercado indicam a realização de treinamentos, no mínimo, anuais sobre ética e integridade ou, se houver mudança no ambiente de compliance, que requeira atualização das equipes internas ou externas envolvidas.

5.3.4. Evidências/Rastreabilidade dos treinamentos

Os treinamentos devem acometer toda a força de trabalho, ou seja, desde os colaboradores das áreas operacionais, como fábricas, até a Alta Administração. Além disso, o conteúdo e a forma de apresentação devem estar alinhados com a linguagem de cada público.

Importante existir uma preocupação com os recém-contratados, que devem conhecer, entender e estar comprometidos com o código de conduta e com o Programa de Integridade da empresa, além disso a empresa deve estabelecer treinamentos de reciclagem periódicos.

Boas práticas de mercado indicam a realização de treinamentos, no mínimo, anuais sobre ética e integridade ou, se houver mudança no ambiente de compliance, que requeira atualização das equipes internas ou externas envolvidas.

5.3.5. Vídeos e teatros sobre o tema

Uma prática bastante utilizada para engajar os colaboradores nos pilares de ética e integridade são os vídeos institucionais em que são tratados temas de interesse, com ênfase nos principais assuntos relativos ao Programa de Integridade. A gravação pode ser do presidente, de diretores ou executivo da área de Compliance e são simples de ser realizados e disponibilizados aos colaboradores seja por e-mail, intranet, comunicação interna, entre outros.

Outra forma mais lúdica e que empresas vêm adotando para trazer o tema da ética para o dia a dia dos colaboradores são teatros. Como exemplo, podemos citar uma empresa do ramo varejista de grande porte que fez uma apresentação teatral para as equipes da fábrica e do centro de distribuição, de aproximadamente uma hora, com encenação de atores que representavam o diabo e o anjo e discutiam dilemas éticos vivenciados constantemente na empresa e na vida pessoal dos colaboradores. Antes da apresentação, os dois atores circularam nas dependências da empresa e da fábrica para gerar a curiosidade dos colaboradores e maior participação. O evento repercutiu de forma positiva, engajando e, ao mesmo tempo, fazendo com que os colaboradores refletissem sobre a ética, mas de forma leve e divertida. A apresentação teatral foi gravada e disponibilizada na intranet da empresa para acessos posteriores dos colaboradores, além de novos profissionais da empresa.

5.3.6. - Campanha de endomarketing

É importante refletir que uma parte das pessoas não tem interesse em comunicações internas relacionadas ao compliance por uma simples razão: já nos consideramos éticos e se, por acaso, não tivermos sido em alguma situação, sempre haverá uma boa justificativa.

No entanto, apesar do desinteresse inicial, podemos tornar a comunicação de compliance mais efetiva através do endomarketing, que pode ser aplicado à realidade de cada empresa, trabalhando internamente o conjunto de percepções do público interno.

Mas o que é endomarketing? Trata-se de um conjunto de ações estratégicas desenvolvidas com técnicas e ferramentas de marketing com foco nos próprios colaboradores. Neste caso, cria-se o inesperado pelas pessoas e assim é possível surpreender o público interno. O endomarketing não é uma ação isolada e sim um processo que precisa ser estruturado, sistematizado e integrado.

- Consumidor -» Público interno (colaboradores)
- Produto -» Informação de compliance.

A implementação do Programa de Compliance pode ser realizada através de uma importante campanha de endomarketing, considerando na sua estratégia:

- Mesma programação visual e de linguagem (conceito criativo).
- Comunicação sistemática e atrativa.
- Espaços específicos para conteúdos importantes.
- Canais estruturados de comunicação interna (e-mail informativo, newsletter, revista interna, jornal de parede, mural digital, intranet, Apps internos e outros).
- Ambientação (instalação de peças em alguns espaços de grande movimentação do público, por exemplo: adesivo no torniquete de entrada e saída dos colaboradores; placa na cancela para entrada e saída de veículos; banner na entrada dos prédios e/ou nas áreas de convivência; display de mesa para salas de reunião; papel de bandeja no refeitório; adesivo nos espelhos dos banheiros e outros).
- Peças informativas e motivacionais.

Em 2018, uma empresa do setor aeronáutico incluiu como sustentação da sua campanha de endomarketing o desenvolvimento de uma peça exclusiva para os embaixadores de compliance, chamada de "Jornada do Exemplo". Cada embaixador recebeu uma caixa em formato de calendário com o total de 32 compromissos semanais que deveriam ser cumpridos ao longo do ano. A cada segunda-feira, o embaixador lia a orientação com a atividade que deveria ser realizada na área de atuação, por exemplo: reflexão sobre os capítulos do Código de Ética e Conduta; organização de uma sessão conjunta para assistir ao vídeo sobre o canal de denúncia; orientações sobre atualização de políticas e procedimentos de compliance; visita à área de Compliance, entre outros. Esse instrumento criou um ritual para manter o tema de compliance sempre em pauta.

5.3.7. E-learning

O e-learning (eletronic learning) é um modelo de ensino que acontece através do meio digital, apoiado principalmente pelo uso de Internet. Essa ferramenta ajuda principalmente as empresas que atuam em muitas localidades do Brasil, e até em outros países, a disseminar a cultura de ética e integridade aos colaboradores.

Muitas vezes, os treinamentos realizados na modalidade on-line contemplam mecanismos de avaliação de aprendizagem, o que garante a avaliação da aderência ao conteúdo sugerido, por exemplo ética, integridade e combate à corrupção.

Outra forma lúdica de avaliar a aderência da ética no dia a dia da empresa é elaborar jogos on-line para testar o conhecimento e avaliar a retenção das informações pelos colaboradores a respeito do código de ética.

5.3.8. Revisão periódica dos treinamentos

Oportuno mencionar a importância da revisão periódica dos treinamentos por parte das empresas, pois regularmente faz-se necessário atualizar seu conteúdo, considerando, por exemplo, o segmento de atuação da empresa, o modelo de capacitação e a legislação aplicável.

Cabe citar, outrossim, que investigações internas, relatórios de auditoria, mudanças no ambiente interno ou externo são fatores que podem acarretar a revisão do Programa de Integridade, inclusive, no que tange aos treinamentos e à forma de comunicação por parte da empresa.

Dentro desse contexto, o Programa de Integridade deve ser aprovado pela autoridade competente — normalmente o Conselho de Administração — com o compromisso de ser revisitado periodicamente para atualização e melhoria contínua do Programa.

5.3.9. "Compliance day" ou "Dia do Compliance"

Muitas empresas adotam como prática períodos do ano para intensificar a importância da ética e do Programa de Integridade em sua rotina, seja um dia, uma semana ou um mês.

A Petrobras, por exemplo, realiza anualmente a "Semana Petrobras em Compliance", com foco em ética e integridade, a iniciativa amplia o público alcançado e traz nomes de peso entre autoridades, acadêmicos, profissionais de diversas empresas e representantes de empresas envolvidas no combate à corrupção para discutir temas relacionados a *compliance*, governança e ética[10].

A GPA também realiza com seus colaboradores o "Compliance day", com

palestras sobre o Programa de Integridade e também com peças teatrais para abordar questões éticas[11].

5.4. Indicadores - Key Performance Indicators (KPIs)

De acordo com a FCPA, em complemento à existência do plano de comunicação e treinamento, uma empresa deveria desenvolver medições apropriadas, que seriam utilizadas para melhor guiar e direcionar as atividades de seu Programa de Ética e Compliance. Essas medições ajudariam a identificar a urgência de algumas medidas e a garantir que o Programa de Ética e Compliance está sendo entendido e cumprido apropriadamente em todos os níveis da empresa.

Os famosos Key Performance Indicators (KPIs) de treinamento nada mais são do que essas medições e baseiam-se em estatísticas, que devem ser monitoradas pelas equipes de Compliance, com o objetivo de demonstrar o valor do compliance para o negócio da empresa.

5.4.1. Principais KPIs

Um Programa de Compliance organizado utilizará os KPIs de treinamento para ter uma visão global do alcance do programa e para definir estratégias, baseadas em dados, e assim continuar com a disseminação da cultura de compliance pela empresa. A seguir, estão elencados alguns exemplos:

Aprovação/Reteste/Reprovação: Com a utilização de testes mais genéricos, aplicados à empresa de forma conjunta, identificar percentuais de aprovação, pessoas que refizeram os testes e pessoas que reprovaram pode ser importante para entender em qual setor da empresa está com maior dificuldade, ou até mesmo entender a efetividade destes.

- Resposta ao treinamento: Receber o feedback e analisar as respostas das pessoas ao treinamento compõem um bom diagnóstico para identificar a utilidade, a forma como foi recebido, o que foi feito errado e corrigir os erros para as turmas futuras.
- Integração dos treinamentos com os embaixadores de compliance: Esse KPI está diretamente integrado com as áreas de Negócio e demonstrará o aprendizado e a aplicação dos treinamentos no dia a dia. Os embaixadores de

---

10 Informações obtidas no site: https://petrobras.com.br/fatos-e-dados/semana-petrobras-em-compliance-foca-em-etica-e-integridade

11 Informações obtidas no site: https://www.gpabr.com/pt/noticias/gpa-realiza-1o-compliance-dayConduta (fonte: site: suzano.com.br); iii) Vale S.A. - Código de Conduta (fonte: site vale.com).

compliance deverão identificar, na prática, se os treinamentos geraram o efeito esperado e reportar à equipe de Compliance os pontos de atenção para os próximos treinamentos.

- Testes de avaliação de retenção de conhecimento: A aplicação de novos testes, algumas semanas após a finalização dos treinamentos, servirá para demonstrar o conhecimento adquirido pelos funcionários e também para melhor atestar a eficácia do treinamento inicial.
- Metas de treinamento atreladas ao Programa de Compliance: Comumente, empresas definem metas de treinamentos anuais para seus funcionários. Se essas metas forem atreladas a treinamentos de compliance, definindo um percentual mínimo de cursos a ser realizados anualmente contemplando o tema, a empresa demonstrará, não só uma forma de comprometimento com compliance, como também garantirá o contato contínuo de seus funcionários com o Programa de Compliance.

5.5. Considerações gerais

Diante dos exemplos e das vivências práticas demonstradas neste capítulo, nota-se que comunicar e treinar é um trabalho árduo, que se realiza de diversas maneiras, com caminhos alternativos que podem ser adaptados à realidade de cada empresa, tratando compliance de forma leve e criativa, permitindo captar a atenção dos trabalhadores, proporcionando entendimento e esclarecimentos, com o intuito de demonstrar qual é o papel e a responsabilidade de cada um dentro desse trabalho e como são importantes para efetivação do programa dentro da empresa.

Além disso, fica evidenciado que o investimento em treinamento e capacitação de equipes é um grande aliado para o sucesso do compliance dentro das empresas, tendo em vista que a capacitação motiva trabalhadores, traz engajamento, tornando-se peça-chave para o sucesso do programa, garantindo uma cultura organizacional positiva e assegurando que a reputação da empresa seja preservada, além de demonstrar conhecimento e domínio sobre aquilo que é esperado da empresa.

Como sugestão de treinamentos obrigatórios, elenca-se abaixo alguns temas sugeridos dentro de vários outros existentes como melhores práticas:

- Código de Ética.
- Funcionamento do e acessibilidade ao Canal de Denúncias (Após esse tipo de treinamento, nota-se que o número de relatos cresce bastante em virtude de uma eventual demanda reprimida.

- Independência profissional e reporte voluntário em situações de conflito de interesse.
- Matriz de consequências em casos de desvios éticos (abrangendo desde uma advertência verbal até demissão por justa causa).
- Valores da empresa.
- Outros.

Importante destacar que esses temas listados podem ser aplicados em qualquer um dos formatos sugeridos ao longo deste capítulo e precisam ser revisitados e/ou atualizados, imediatamente sempre que ocorrer mudança externa ou interna de compliance da empresa.

Destaca-se ainda que comunicar é necessário, treinar é importante e documentar é fundamental, tendo em vista que o processo precisa ser documentado e apresentado quando se fizer necessário.

Comunicar bem e treinar de forma eficaz promovem a padronização de um ambiente de trabalho produtivo, saudável e ético.

Capítulo 6

Tecnologia e Análise de Dados

KPMG

KPMG BUSINESS SCHOOL

6.1. Contextualização

Com o grande avanço tecnológico na última década, diversas ferramentas de análise de dados — Data & Analytics (D&A) —, inteligência de negócios — Business Inteligence (BI) — e inteligência artificial — Artificial Inteligence (AI) — foram desenvolvidas e implementadas nos mais diversos ramos de atividades.

Essas ferramentas têm como objetivo principal prover ao negócio indicadores-chave de risco e performance (KRIs e KPIs), dashboards e relatórios de tendências. Se bem implementadas, as ferramentas proporcionam, de maneira clara e objetiva, uma melhor compreensão dos detalhes do negócio e amplificam a visão da Administração sobre o que está acontecendo no negócio, desde pequenos reembolsos de despesas até questões de *compliance* (legislação, normas e diretrizes) interno e externo.

De acordo com a Pesquisa Maturidade do Compliance no Brasil - 3ª Edição, 68% dos respondentes afirmaram que não conhecem ou não aproveitam a tecnologia para apoiar suas iniciativas de compliance.

Neste capítulo, abordaremos algumas dessas técnicas e dessas tendências que são amplamente difundidas e utilizadas pela função de compliance das organizações mais modernas na detecção de desvios e contribuem para o amadurecimento do ambiente de controle do negócio. Nesse contexto, a tecnologia é utilizada para apoiar o Programa de Compliance de uma empresa.

Antes de iniciarmos a parte técnica e metodológica do tema de tecnologia em compliance, é preciso fazer as seguintes perguntas: Como a transformação digital impactou a gestão de risco? Como as áreas de Compliance terão que se adaptar a esse modelo disruptivo? O que precisamos fazer para nos adequar a este modelo?

Esta é uma questão de estabelecer uma nova cultura organizacional. É preciso entender que para alcançar a transformação digital é necessário estabelecer uma nova forma de lidar com o risco que permita dar autonomia às equipes. Abrir mão do formato de gestão, comando e controle e migrar para modelos que suportem times multidisciplinares capazes de experimentar, serem ágeis na solução dos próprios problemas e gerenciar suas entregas do início ao fim, dentro de um fluxo de valor.

Na era digital, o "mar" de normas que abrange a maior parte das atividades — da mobilidade urbana à saúde, de telecomunicações à indústria, de varejo a serviços — não pode se tornar empecilho para o desenvolvimento das empresas e suas inovações, e sim agir a seu favor, estimulando o crescimento econômico e a melhora geral das atividades, para a indústria, o setor público e o privado.

A transformação digital requer um novo olhar em relação ao risco, em que, tradicionalmente, os formatos de controle — assim como as próprias normas e leis das quais a área é guardiã — são um reflexo do passado e não do futuro. Fazer gestão de riscos baseada em um ambiente de mercado que já não existe mais é fazê-la pelo retrovisor, desestimulando a experimentação e a inovação.
É preciso interpretar e lidar com as normas e os riscos olhando para frente, de maneira que a empresa se adeque aos novos tempos sem abrandar a austeridade. Assim, a pergunta que não quer calar é: compliance é barreira ou parceiro para a transformação digital de uma organização? A resposta é simples: os profissionais da área de Compliance vivem um momento crucial, com a transformação digital das empresas, o aumento do volume de dados a ser tratados, a deleção do BackOffice para o cliente (self-service), os canais omini channel, o abre alas para os grandes ataques cibernéticos, e os riscos digitais exponencializados. Portanto, não há como resistir, é preciso integrar essa nova cadeia de gestão de riscos, alguns deles difíceis de serem detectados, entretanto ser preditivo é essencial para esse modelo disruptivo de gestão.

Considerar este contexto é importante para conhecer o que vem sendo feito, e o que há de moderno em termos de metodologias, tecnologias e nível de maturidade de gestão de compliance na era digital.

6.2. Data Analytics

6.2.1. O que é?

Data Analytics é o uso aplicado de dados, análises e raciocínio sistemático para seguir em um processo de tomada de decisão muito mais eficiente. Isto é, pesquisar e responder perguntas com base em dados e com uma metodologia clara.

Analytics podem ser aplicados em diversos negócios e departamentos, conforme segue:

- Compras - Ordens de compras, limites de compras.
- Contas a pagar - Desembolsos indevidos, créditos perdidos, cotações e contratos, conta inativa ou fornecedores fictícios.
- Folha de pagamento - Pagamentos precisos e autorizados, funcionários e esquemas de folha de pagamento inexistentes, pagamentos precisos e autorizados, horas extras e comissões razoáveis.
- Contabilidade - Lançamentos contábeis manuais, atividades de fechamento e ajustes.
- Cadastro mestre (Master File) - Clientes, funcionários, fornecedores e

estoque de materiais.

- Viagens e entretenimento.
- Qualidade dos dados - Razoável, dentro do intervalo esperado, validade e completo.
- Conformidade - FCPA, SOX, impostos e transações regulamentadas.
- Fornecer valor e descobertas (insights) mais profundos aos parceiros de negócios.
- Ajudar o negócio a aumentar a eficiência, enquanto melhora a qualidade da avaliação de riscos e controles.
- Mudança fundamental dos relatórios baseados em exceção para relatórios baseados em descobertas.

6.2.2. Objetivo

A relação entre a tecnologia nas empresas e o *compliance* é estreita. Compliance é conformidade e quanto maior for o controle tecnológico das atividades nas empresas, maior será o grau de assertividade do negócio para com as suas obrigações legais e regulamentares, evitando-se penalidades, assim como mitigando danos à sua imagem.

Utilizar a inteligência analítica está diretamente ligado com a possibilidade de melhorar o desempenho com relação aos domínios fundamentais de uma empresa ou um negócio utilizando, basicamente, análise de dados.

É de fundamental relevância que as empresas tenham as ferramentas tecnológicas adequadas para fomentar e promover a análise de dados para o preventivo rumo ao controle e ao monitoramento de sua conformidade.

6.2.3. Benefícios

Discorreu-se até aqui acerca da transformação digital que ocasiona uma efetiva mudança de paradigma nas operações das empresas no mundo, tendo papel de destaque na conformidade dada a quantidade de legislações, regras e regulamentos a que as empresas estão sujeitas, sejam entes públicos sejam privados; da primordial função da Data Analytics diante da conformidade; assim como da efetiva necessidade de um Canal de Denúncia, preferencialmente tecnológico e terceirizado para uma melhor transparência e idoneidade no trato das informações.

A tomada de decisão de uma grande parte das empresas parte da análise de seus dados tecnológicos e assim segue com a conformidade. O uso da tecnologia por parte das empresas proporciona grande eficácia na gestão dos dados, em seus

mais variados itens, tanto na pequena quanto na multinacional, desde a pública para a privada, nas mais variadas atividades empresariais. A tecnologia serve ao mapeamento e à análise mais aprofundados dos dados e, com a integração dos sistemas nas empresas, o cruzamento dos dados, a extração e a análise final, há a possibilidade de se antecipar toda a sorte de consequências indesejáveis mitigando sanções e penalidades.

A importância da tecnologia para a conformidade é tanta que a análise de dados obtidos por meio da automatização está diretamente conectada ao nível de maturidade das empresas quanto ao atendimento às regras do compliance.

Inclusive a 4ª edição da Pesquisa Maturidade do Compliance no Brasil, realizada pela KPMG Auditoria em 2019, especificamente no item 34 - Análise de Dados e Tecnologia, traz que a inovação tecnológica em compliance é tema de debate/diálogo em 51% de um total de 250 empresas respondentes. Do total, apenas 33% se trata de multinacionais.

Referido dado confirma, especificamente no Brasil, que metade das empresas já se ocupam em dialogar com a inovação com um aparato tecnológico próprio e voltado ao tema conformidade.

A mesma pesquisa segrega em cinco grandes pilares a curva da maturidade para análise de dados e tecnologia. Sendo eles Fraco: inexistência de base tecnológica para análise de dados relacionados a compliance; Sustentável: informações relacionadas a alguns aspectos de compliance estão em base tecnológica para departamentos específicos e disponíveis somente para análises manuais de dados; Maduro: processos críticos de compliance suportados por base tecnológica, mas não centralizados em um sistema único; Integrado: o Programa de Ética e Compliance é integralmente suportado em base tecnológica, permitindo monitoramento constante de seus pilares; e Avançado: sistema de gestão de compliance totalmente automatizado com a tecnologia de GRC integrada. Sistema de GRC captura integralmente informações de outros sistemas operacionais.

E neste quesito, a curva da maturidade se encontra entre os níveis Sustentável e Maduro com a nota 2,29. Qual seja, disciplinando que as empresas possuem tecnologia para o sistema de compliance, extraem relatórios consolidados com indicadores, conseguem antecipar medidas de prevenção, mas que ainda não monitoram integralmente os pilares de sua conformidade e que ainda não conquistaram um sistema de gestão completo para Governança, Riscos e Compliance, ou GRC.

Deste modo, muito embora as empresas estejam vivenciando a transformação

digital contando com inúmeras frentes de apoio tecnológico na mitigação de riscos empresariais, ainda se mostra tímido o investimento para a detecção e a análise de dados na mitigação de riscos e atendimento da conformidade.

A utilização de ferramentas de análise de dados pode também adicionar valor à função de compliance de uma empresa. Os principais benefícios são:

Foco nas atividades que geram valor:

- Economia na recuperação de custos com a identificação de duplicatas e pagamentos em excesso à medida que ocorrem.
- Fugas e ineficiências do processo.
- Eficiências obtidas com o gerenciamento automatizado de exceções.
- Identificação de fraude antes que ela aconteça.

Aumento da eficácia do compliance:

- Indicadores de alerta precoce de risco ou falha de controle.
- Capacidade de monitorar continuamente os principais indicadores de performance e riscos (KPIs e KRIs) em tempo real.
- Monitoramento de tendências.

Melhora na eficiência do compliance

- Redução nos custos de treinamento e integração para a nova equipe de Compliance, fornecendo acesso a um repositório seguro de testes comprovados.
- Auditorias com escopo reduzido, pois o monitoramento contínuo de dados fornece garantia suficiente.
- Recursos humanos de compliance e auditoria e custos de viagem reduzidos.

6.3. Estrutura da análise de dados (framework)

A estrutura de análise de dados abordará quatro principais aspectos, conforme segue:

6.3.1. Tipos de análises de dados

- Modelagem estatística
- Previsão (forecasting)
- Data & Text Mining
- Otimização
- Delineamento de experimentos etc.

Com todos os avanços na área de Tecnologia da Informação e também com o aumento da quantidade de dados disponíveis, existem diversas oportunidades para se aplicar análises bem estruturadas.

6.4. O Compliance Officer e o Data Analytics

A função de Compliance Officer é responsável pela interpretação dos dados que motivará a decisão de um gestor baseado na regra de negócio, suportada pelos dados.

Os dados são geralmente apresentados em formato de dashboards, KPIs e KRIs criados através da extração de dados crus (Raw Data) diretamente da fonte e posteriormente tratados em ferramentas específicas para essa finalidade. A apresentação final dos dados é realizada em formato amigável (Friendly Version) com o objetivo de facilitar a compreensão dos fatos do passado e das tendências. Será também utilizada para avaliações de aderência aos controles internos e políticas internas (compliance).

Exemplo de áreas de cobertura

A utilização de ferramentas de análise de dados pode abrir um vasto campo de trabalho para os profissionais de Compliance. Áreas que possuem grande quantidade de dados, informações desconectadas e informações incompletas podem ser monitoradas pela função de Compliance com a ajuda de ferramentas adequadas que buscam os dados desejados na origem e, após compilados, são analisados e relatórios gerenciais (dashboards) são fornecidos.

6.5. Canal de denúncias no tratamento e análise de dados

6.5.1. O que é?

O Canal de Denúncias é o meio de comunicação utilizado para realizar uma denúncia de um desvio de conduta praticado por qualquer pessoa que se relacione com a entidade ou que em seu nome atue.

6.5.2. Objetivo

O Canal de Denúncias tem por objetivo estabelecer um método sistemático para as partes interessadas que desejarem denunciar quaisquer situações que violem os princípios éticos e os padrões de conduta formalmente estabelecidos pela organização, ou que caracterizem atos ilícitos como corrupção, suborno, fraude, nepotismo, assédio, lavagem de dinheiro etc. Acolher relatos de denúncias, de

modo a prevenir e combater desvios e ilícitos, é um compromisso com a integridade e a transparência da organização com as partes interessadas e a sociedade.

6.5.3. Benefícios

Podemos listar alguns itens como os principais benefícios de se implantar um Canal de Denúncias:

- Aumento da capacidade de detecção dos indícios de ilicitude
- Sistematização do registro e apuração das denúncias
- Aumento da eficácia do compliance.

Aumento da capacidade de detecção dos indícios de ilicitude

- Possibilidade de denúncias anônimas, passando, dessa forma, maior segurança ao denunciante.
- Capacidade para atendimento de denúncias em âmbito nacional, ou até mesmo mundial.

Sistematização do registro e apuração das denúncias
ento da capacidade de detecção dos indícios de ilicitude

- Padronização e alinhamento do Canal de Denúncia com as políticas da entidade.
- Controle sistêmico de todas as etapas do processo de apuração das denúncias.
- Definição clara e objetiva das funções no processo de tratamento.

Aumento da eficácia do compliance
ento da capacidade de detecção dos indícios de ilicitude

- Emissão de relatórios realizados de forma automatizada
- Utilização dos insumos para identificação dos riscos de compliance
- Base de dados padronizada e consolidada.

6.6. Estrutura de tratamento das denúncias (framework)

Um software de canal de denúncias eficiente traz a possibilidade de gestão de toda a cadeia de tratamento das denúncias.

Capítulo 7

Monitoramento e Testes

KPMG

KPMG
BUSINESS SCHOOL

Atualmente vivenciamos, principalmente nas grandes capitais, um contexto de organizações que já possuem Programa de Compliance considerável e a avaliação dos seus requisitos, sua efetividade, sua aderência e seus controles é fundamental para avaliar se os controles existem, se são efetivos, para medir a cultura de ética e integridade ou para propor melhoria contínua e evolução necessária do Programa de Compliance.

A estruturação de um Programa de Compliance está baseada no art. 42 do Decreto nº 8.420 de 18 de março de 2015, em que apresenta 16 parâmetros entre os quais estão:

"comprometimento da alta direção (Tone of The Top); padrões de conduta, código de ética, políticas e procedimentos de integridade; treinamentos periódicos, monitoramento contínuo do programa de integridade visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência dos atos lesivos previstos no art. 5º da Lei nº 12.846, de 2013."

Neste capítulo, iremos tratar do monitoramento e dos testes:

O monitoramento contínuo que será tratado não tem começo, meio e fim, ou seja, não tem periodicidade e sim objetivo de avaliar todos os processos e os requisitos formais do Programa de Compliance, sendo então importante estabelecer indicadores de performance para cada um dos pilares do programa e sua interação com toda a organização.

Podemos estabelecer ainda os Testes de Controle que são instrumento de gerenciamento dos riscos de compliance, que têm objetivo avaliar a aderência de políticas, controles internos, código de ética, entre outras responsabilidades do programa.

Com os resultados obtidos nos processos de monitoramento contínuo e nos testes de controle e a organização com uma visão holística dos riscos, desde sua operação até a Alta Administração, as três linhas de defesa nas suas funções (gestão operacional, funções de gerenciamento de riscos, conformidade e auditoria interna) têm papel fundamental para avançar nos riscos e assegurar que a resposta seja apropriada.

7.1. Monitoramento e sinergia das três linhas de governança

A empresa quando toma a consciência dos riscos detectados deve tomar as ações a partir dos responsáveis dos processos em que todos os níveis da empresa, ou seja, desde a Alta Administração até a operação para prevenir, detectar e mitigar os riscos. Neste ponto, encontramos desafios para as atividades de controles,

então as responsabilidades devem estar claras, definidas e delimitadas para ação e obtenção de resultados.

Conforme exposto no capítulo 1 sobre Governança e Cultura, as três linhas de defesa publicadas pelo Instituto de Auditores Internos (IIA) deixa também claro que a Administração é a principal responsável pela gestão de risco de uma empresa e deve atuar de forma eficaz para proteção do negócio sem se apoiar em avaliações de terceiros para identificar as irregularidades.

De modo geral, as linhas de defesa têm como propósito: o controle da Gerência

Operacional é a primeira linha de defesa no gerenciamento de riscos, assim como o controle diário; as diversas funções de controle de riscos e supervisão de conformidades estabelecidas pela Gerência são a segunda linha de defesa; e a avaliação independente é a terceira.

Com o advento da Operação Lava Jato, deflagrada em 2014, muito se mudou no Brasil, inclusive os padrões de conduta, resultando em uma maior visibilidade e nível de pertencimento do compliance.

De acordo com o Decreto nº 8.420, de 18 de março de 2015, no art. 41, Programa de Integridade é definido da seguinte forma:

"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 detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira".

A Política de Integridade vai muito além de missão, visão e valores de uma empresa, de políticas e condutas éticas, é essencial analisar a maturidade da empresa, com pesquisas e questionários internos para elaboração e estruturação de compliance conforme a empresa.

Podemos considerar como diretrizes essenciais do compliance: verificação dos instrumentos normativos para bom código de éticas e políticas acessórias, elaboração de boa matriz de risco institucional de integridade, risk assessments de compliance, canal de denúncias com amplo acesso, comunicação, treinamento, monitoramento contínuo e execução periódica de testes.

Os objetivos de um Programa de Integridade é uma atuação em conformidade com a legislação vigente, com as diretrizes estabelecidas pela empresa, e seguindo os padrões de integridade, ética e transparência em todas as atividades da empresa, bem como no relacionamento entre colaboradores, stakeholders, meio ambiente

e sociedade.

O compliance deve:

1. Promover a cultura da conformidade e da integridade.
2. Potencializar o constante cumprimento das normas internas e daquelas dispostas no ordenamento jurídico.
3. Fomentar a cultura de gestão de risco, endereçando controles preventivos ou detectivos que possibilitem identificar ou prevenir não conformidade.
4. Disseminar a cultura da adoção das melhores práticas de acordo com os mais altos padrões.
5. Impulsionar a formalização e endossar a constante atualização das políticas e dos procedimentos internos por todas as pessoas ligadas à empresa.
6. Consolidar todas as iniciativas de compliance.

O monitoramento contínuo é o quinto pilar do Programa de Integridade da Controladoria Geral da União (CGU) determinante para prática de compliance, pois define procedimentos de verificação e aplicabilidade do Programa de Integridade. Segundo a CGU, no Eixo 4 - Estratégias de Monitoramento do Programa de Integridade:

"As estratégias de monitoramento contínuo objetivam acompanhar as ações previstas neste Plano de Integridade e aprovadas pela Alta Administração, com vistas a avaliar os resultados alcançados pelo Programa." No escopo do monitoramento contínuo, incluem-se as medidas de tratamento dos riscos à integridade, as iniciativas de capacitação de líderes e colaboradores, as medidas de fortalecimento das instâncias relacionadas ao tema e os meios de comunicação e reporte utilizados pelo Programa".

A aplicação de políticas de conformidade, códigos de ética, sistemas de monitoramento e de controle, auditorias internas e externas são imprescindíveis, mas o monitoramento é um dos pilares para atingir níveis maiores de maturidade do Programa de Compliance.

Sabemos ainda que a implementação de Programas de Compliance ocorre de forma gradativa e, embora não seja fundamental implementar todos os pilares no início do programa, é necessário garantir a evolução no sentido de proteger as maiores prioridades da empresa, sendo elas: risco de imagem e reputação, perdas financeiras decorrentes de multas, fraudes e corrupção, pressão de órgãos reguladores, descumprimento das obrigações do compliance.

O *compliance* alinhado a uma boa estrutura de controles internos e gestão

de riscos sendo incorporados às políticas das organizações tende a assegurar eficiência, porém é necessário estabelecer um plano de monitoramento contínuo do código de ética, das políticas e dos indicadores de compliance que destacamos:

- Comunicação interna e externa com grande abrangência e adaptada aos níveis da empresa, podendo ser estabelecidos diversos meios para coleta das informações, como e-mails, pesquisa impressa, entrevistas.
- Treinamentos, mas que a métrica não deve somente ser a quantidade % de empregados capacitados, mas também a aderência, ou seja, quantas violações da política ocorreram x quantos empregados treinados.
- Aderência às políticas pelos colaboradores e pelos terceiros por detecção de incidentes adversos.
- Não atingimentos dos objetivos de compliance e da empresa.
- Avaliação das maiores incidências no canal de denúncias. O compliance pode aplicar pesquisa semestral sobre o canal, tais como: O empregado foi informado de que a empresa dispõe de um canal de denúncias, sabe acessar o canal? Se acessou, se teve dificuldades?
- Acompanhamentos específicos como: auditoria interna anual na qual se avalia os riscos e verifica se os riscos foram avaliados, classificados e seguidos, se os manuais foram seguidos, tecnologias aplicadas aos processos; pós-contratação — contratos vencidos e vigentes sem interrupção da prestação e dos serviços.

Para realizar o monitoramento, é necessário mapear os processos da empresa e, sobretudo, identificar os dados necessários e confiáveis, garantido assim que não ocorram distorções nos indicadores/transações monitorados. A seguir, apresentamos alguns dos dados que podem ser utilizados, bem como os indicadores gerados:

- Relatórios das rotinas do Programa de Integridade

Apresentação ao Conselho de Administração de relatórios das rotinas com análise do desempenho do compliance relacionados ao código de ética, riscos à integridade (abuso de posição, nepotismo, conflito de interesses, vantagens indevidas, influência sobre subordinados para violar sua conduta, ações de retaliações, utilização de recursos públicos em favor de interesses privados).

- Relatórios de investigação

Nos relatórios é possível a obtenção de informações e documentos de comprovação do assunto sob apuração e entendimento dos fatos para ações de prevenção, contingenciando perdas de mesma natureza no futuro pela mesma não conformidade, observando ainda a estrutura organizacional em que a investigação

está acometida.

Nesta ferramenta de coleta, podem-se criar evidências do cumprimento ou não dos compromissos e aprimorar as normas internas da empresa.

- Reclamações de clientes

A gestão de reclamações e a qualidade dos dados são importantes para integrar os canais e aprimorar a experiência dos clientes nos diferentes canais de comunicação (URA, SAC, Ouvidoria, SMS, e-mail, chat, entre outros).

Exemplo de monitoramento de integração de canais: se o cliente mandou um e-mail e depois telefonou, o operador precisa do conteúdo da mensagem para dar continuidade e resposta da reclamação. Caso isso não esteja estabelecido, o risco de reputação é elevado e de não fidelização do cliente, e quando há uma formatação adequada na coleta e no processamento dos dados é possível conhecer melhor o cliente e utilizar como ferramenta de comunicação da empresa, podendo alcançar mais facilmente a satisfação.

- Tendências do canal de denúncias

Maior responsável pela maioria das descobertas das não conformidades, detecção de perda financeira, de imagem, entre outras.

Quando o canal de denúncia não tem usabilidade, podemos considerar que o Programa de Compliance não está sendo efetivo ou não tem credibilidade.

Conforme pesquisa Linha Ética KPMG, os três assuntos mais frequentes são: Conduta e Comportamento correspondem a 68% das denúncias, Fraude com 11% e Assédio com 9%, e o restante se enquadra no descumprimento das políticas, roubo e desvio de recursos, e segurança no trabalho.

Com base nas denúncias, a empresa deverá tê-las no monitoramento com a medição das políticas de contenção, então é necessário:

- Monitorar as denúncias pendentes de resolução
- Gerenciar relatórios com indicadores
- Detectar as causas e os temas mais observados e/ou críticos
- Detectar e gerenciar as denúncias reincidentes
- Revisitar as políticas e os procedimentos para adequações
- Visitar e treinar áreas principalmente as de maior número de denúncias
- Desenvolver e divulgar relatórios gerenciais periodicamente
- Desenvolver hotline para assuntos recorrentes.
- Modificações regulatórias

Imprescindível acompanhar as evoluções e as atualizações dos regulamentos internos e externos, em qualquer ambiente, pois sua ausência pode acarretar

múltiplos riscos, tais como: operacional, legal, de mercado, de liquidez, de reputação, de fraude e corrupção, de crédito, de integridade de dados, de impedimentos de participação de concorrências, em que o risco dependerá do objetivo determinado pela empresa.

É recomendável o monitoramento dos controles internos com abordagem de ambientes regulatórios, interno e externo, sendo:

Ambiente regulatório interno: políticas, manuais e procedimentos.

Ambiente regulatório externo: leis, regulamentos, permissões, licenças e outras formas de autorização, regras ou recomendações de agências reguladoras, jurisprudências, convenções, compromissos ambientais, ou seja, enquadrar a empresa no seu ambiente regulatório. O investimento nesta área dependerá do montante de regulatórios que o negócio está submetido.

- Monitoramento de transações críticas identificadas na matriz de risco de *compliance*

Com a utilização de ferramentas sistêmicas, é possível implementar conceitos de business intelligence para monitorar, de forma independente, as transações que apresentam maiores riscos de exposição da empresa e assim tomar ações tempestivas, reduzindo o impacto ocasionado pela materialização desses riscos ou mesmo até impedindo a materialização destes. Dentre elas, destacamos alguns processos passíveis de monitoramento:

- Doações: utilização de Data Analytics para monitorar as contas contábeis de doações, bem como se as empresas que receberam esses pagamentos estão em conformidade com o Programa de Compliance.
- Gestão de terceiros: implementar relatórios que demonstrem o risco em atuar com terceiros, com base em informações obtidas a partir da due diligence, qualidade do serviço prestado, valor total pago para a empresa e dependência financeira.
- Comunicação com agentes públicos: utilização de ferramentas de monitoramento de dados e e-mails para identificar comunicações com agentes públicos.
- Vazamento de informações: utilização de ferramentas de Data Loss Prevention como barreira para impedir que informações sensíveis sejam divulgadas, bem como monitorando os responsáveis por tais atos.
- Cyber attack: relatórios que demonstrem a efetividade de ferramentas de proteção (por exemplo: firewall e antivírus), alertando a indisponibilidade das ferramentas e as tentativas de invasão.

- Pagamentos a distribuidores e funcionários: utilização de Data Analytics para monitorar pagamentos indevidos e/ou duplicados.

Cabe ressaltar que as atividades que devem ou podem ser monitoradas variam conforme segmento da empresa, estrutura tecnológica disponível e apetite ao risco assumido pela empresa. Outro fato importante é considerar a quantidade de exceções que podem ser tratadas pela equipe, pois na identificação de não conformidades no monitoramento as exceções terão que ser tratadas de forma tempestiva por algum colaborador, garantindo assim a efetividade no monitoramento.

7.2. Testes

A última etapa deste pilar consiste na execução de testes de aderência e eficiência do Programa de Compliance para prevenção e detecção. Assim, entendemos como importantes:

- Control and Risk Self-Assessment - Evidências de que os controles associados aos riscos de compliance estão sendo executados (Matriz de Riscos).
- Certificações (auditorias independentes).
- Auditorias (O Programa de Integridade deve fazer Plano Anual de Auditoria Interna).
- Riscos de *compliance* que afetam o negócio.

Para termos uma análise da aderência ao Programa de Integridade, é necessária a realização de testes, a fim de assegurar a eficiência dos controles internos implementados para mitigar os riscos que possam impactar a organização no que se refere ao compliance.

Desta maneira, podemos elencar diversas ferramentas que podem dar segurança para o devido cumprimento do Programa de Integridade. Iremos abordar os testes de maior relevância e efetividade.

- Linhas de governança e Control and Risk Self-Assessment (CRSA)

Inicialmente trazemos a metodologia conhecida como Control and Risk Self-Assessment (CRSA), que nada mais é que a auto avaliação de riscos e controles pelos "donos" dos processos. Com isso, esses gestores são responsáveis pela identificação dos riscos considerando duas variáveis: a probabilidade do risco se materializar e o impacto caso isso ocorresse.

Posteriormente a essa fase, são realizados questionários de controles, a fim de mapear se os riscos identificados já estão sendo controlados ou não. Em caso

de identificação de riscos que não estão devidamente mapeados por controles da organização, serão definidos planos de ação com prazo para implementação desses controles.

Ademais, também podem ser implementados controles compensatórios enquanto os controles definitivos são elaborados, com o objetivo de minimizar os erros que podem ocorrer no processo.

Portanto, nessa ferramenta, é necessária a colaboração entre primeira e segunda linha de defesa. Os gestores dos processos devem receber a assessoria dos componentes da segunda linha de defesa, as áreas especializadas em riscos e controles internos. Além disso, segundo o The IIA, essas duas linhas são responsáveis pela gestão do atingimento dos objetivos corporativos.

É valido ressaltar que diversos tipos de controle podem ser implementados para mitigar riscos relacionados aos processos. Primeiramente, podem ser preventivos, que possuem a característica de serem executados no início do processo, prevenindo a ocorrência de erros ou irregularidades do processo, já mitigando o risco na fonte do processo, ou podem ser detectivos, que são controles que são executados durante o processo para encontrar erros que dificilmente são previstos.

Além disso, os controles podem ser manuais, quando é necessária a análise de uma pessoa para conferir ou executar alguma tarefa para analisar se houve alguma falha, ou automáticos, no caso de serem executados através de sistemas informatizados e que não necessitam de interação humana na sua execução.

- Certificações

Outra maneira de testar a eficácia do Programa de Integridade é por meio das certificações externas. Hoje temos normas ISO que abordam sobre o compliance como um todo, são elas as normas ISO 19600 (ISO Compliance), 37001 (Sistema de Gestão Anticorrupção) e 31000 (Gerenciamento de Riscos).

Essas normas não são conflitantes, mas, na verdade, complementares. A primeira traz sobre uma visão de compliance sobre a necessidade de a área de Compliance ser formada por um conjunto de normas e regras que regulamentem as políticas e as diretrizes internas, identificando desvios e estabelecendo planos de ação para saná-los.

Já a norma 37001 traz maiores especificidades em relação ao compliance anticorrupção, ou seja, define que a organização deverá ter um sistema mais robusto de combate a atos ilícitos através de uma cultura de integridade, transparência, além de estar em conformidade com as leis e as regulamentações em vigor.

E, finalmente, a ISO 31000, que aborda sobre o gerenciamento de risco, que é essencial para a análise da eficácia do Programa de Integridade.

- Auditoria interna

Complementando esse ciclo, temos a terceira linha de defesa, composta pela área de Auditoria Interna. Responsável por prestar avaliação e assessoria independentes e objetivas sobre a eficácia da governança e do gerenciamento de riscos, conforme descrição do The IIA.

A área de Auditoria Interna, em relação ao Programa de Integridade, deverá incluir no Plano Anual de Atividades de Auditoria Interna (PAINT) para testar a efetividade dos controles implementados relacionados aos riscos de compliance identificados, seguindo uma metodologia para testar todos os pilares do Programa de Integridade em um plano plurianual.

Hoje não se considera mais que a Auditoria Interna, apesar de necessitar ser independente para realizar as suas avaliações, não deve ser um corpo isolado do restante da organização. Portanto, deve interagir de maneira regular com as demais áreas de gestão, no intuito de estar alinhada ao planejamento estratégico definido, ser relevante para a organização, bem como poder agregar valor à atividade.

- Testes periódicos em atividades de risco de compliance

Outra maneira eficaz de contribuir com o monitoramento do Programa de Integridade é estabelecer rotinas periódicas de testes em processos intrínsecos aos riscos de compliance, tais como qualificação de terceiros, mapeamento contínuo do ambiente regulatório dos negócios da organização, análise de doações realizadas/recebidas, aderência aos treinamentos voltados para os temas de compliance, entre outros.

Nesses testes, conseguimos fornecer à gestão do Programa de Integridade como estão os Key Performance Indicators (KPIs), que podem ser utilizados para mensurar a efetividade dos controles implementados para mitigar os riscos atribuídos ao compliance.

Com isso, podemos verificar se a Alta Administração está realmente comprometida em apoiar o programa, pois o Tone of the Top (tom do topo) é primordial para o programa ser bem-sucedido na organização e, justamente por isso, é um dos pilares de um Programa de Compliance.

Desta forma, em tempos de constante inovação tecnológica e abundância de informações, saber como fazer a gestão de informações de forma eficiente é a grande sacada do monitoramento, ou seja, coletar, extrair, analisar, classificar, inspecionar e comparar todas as informações que se tem à disposição.

Assim temos o Big Data, que é o conjunto de recursos, ferramentas, armazenagem e processamento de grandes quantidades de dados de maneira mais eficiente, ágil e inovadora. Para o *compliance*, a análise de dados (Data Analytics) é importante para descobrir padrões e gerar intuições (insights) para ajudar a organização em tarefas, por exemplo a identificar fraudes antes mesmo de afetar os processos organizacionais.

Para isto, conta-se com tecnologias de mineração de dados (Data Mining), que têm o processo de encontrar anomalias, padrões e correlações em grandes conjuntos de dados para prever resultados. A base da mineração compreende a análise entrelaçada, utilizando-se de estatística e inteligência artificial.

Estamos falando de ferramentas que auxiliam o profissional de *compliance* a obter avaliação de riscos internos, controle de qualidade, mapeamento de contingência, teste de integridade e, por fim, mas não menos importante, o cumprimento do Código de Ética e Conduta da organização.

A mineração de dados torna mais eficiente o apoio à tomada de decisão, elemento essencial para o conceito de business intelligence, ou seja, auxílio nas estratégias do negócio, pois, na busca por descobrir generalizações nos dados, com o uso da inteligência artificial podendo aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana (machine learning), o que permite automatizar respostas ao usuário, fazendo uma varredura completa nessa imensidão de dados para encontrar padrões e chegar a previsões inimagináveis.

Todavia, caberá ao profissional de compliance a compreensão dos dados gerados pela inteligência artificial, principalmente no início da utilização da ferramenta, pois vários falsos-positivos podem ser encontrados e a expertise do profissional fará toda da diferença onde a equipe deverá concentrar os seus esforços. Isto porque a máquina deverá ser aprimorada de acordo com o tempo de uso e quem deverá orientá-la sobre condutas fora do padrão é o profissional de compliance. Então, se as diretrizes dadas não forem suficientemente boas, a geração de dados pela inteligência artificial poderá não auxiliar, mas sim sufocar a equipe de Compliance com um excesso de informações que não poderão ser checadas por falta de recursos e, possivelmente, algum dado relevante passará sem ser devidamente analisado.

As organizações devem acompanhar o movimento inerente ao avanço de tecnologias, tendo como resultados do investimento em tecnologia: economia de tempo e recursos para se manterem em conformidade com as leis e as

regulamentações; redução de riscos; prevenção contra perdas e fraudes de maneira mais rápida e sem interferências, maximizando os resultados e assim promovendo a sustentabilidade promissora da organização.

Capítulo 8

Gerenciamento de Deficiências e Investigações

KPMG

KPMG BUSINESS SCHOOL

8.1. Conceito, Finalidade e Abrangência

A investigação interna tem origem no termo em inglês "internal investigation". De acordo com Leopoldo Pagotto[12], na década de 1970, o Voluntary Diclousure Program, da Securities and Exchange Commission (SEC), permitia que as investigações internas independentes fossem feitas para a defesa das organizações, com a obrigatoriedade de que fossem criados comitês especiais para a sua condução e sua elaboração de relatórios.

No Brasil, não há expressa regulamentação da condução da investigação interna. Entretanto, a Lei n° 12.846/2013, conhecida como Lei Anticorrupção, demonstra que a investigação interna é uma importante ferramenta garantidora da efetividade do Programa de Compliance.

O documento da CGU denominado como "Programa de Integridade: diretrizes para empresas privadas" norteia o procedimento de investigação corporativa e menciona que "a detecção de indícios da ocorrência de atos lesivos à administração pública, nacional ou estrangeira, deve levar a empresa a iniciar uma investigação interna, que servirá como base para que sejam tomadas as providências cabíveis".[13]

Segundo Leopoldo Pagotto et al., a investigação interna é o conjunto de ações articuladas que objetivam esclarecer fatos em que submerjam a pessoa jurídica e que, de certa forma, servirão de subsídio para tomada de decisão. Esses fatos inserem a pessoa jurídica em atos praticados por seus agentes ou por terceiros que com ela se relacionem. Serpa, complementa que:

> "as investigações devem determinar, de forma plena e com credibilidade, o que aconteceu em relação a um problema – se, de fato, houve uma conduta imprópria, ou não, quais foram as circunstâncias, quem estava envolvido, e se uma violação de leis ou políticas internas ocorreu." (SERPA, 2020, p.2).

As investigações internas podem ser iniciadas a partir de uma denúncia — feita por colaborador, terceiro, acionista, entre outros —, após a identificação de

---

12 PAGOTTO, Leopoldo; ALMEIDA, Silvia Helena Cavalcante de; FERNANDES, Indira. Investigações Internas.In: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otavio (coord.). Manual de Compliance. 2° Ed. Editora Forense, 2020. p. 174.

13 CONTROLADORIA GERAL DA UNIÃO. Disponível em: <https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Acesso em 25 de julho de 2020.

um ato suspeito na auditoria, a partir do monitoramento de processos internos, resultado da análise de riscos ou até mesmo autodeclarações de atos que sejam considerados violações internas, fraudes ou crimes.

As investigações internas podem ser iniciadas a partir de uma denúncia — feita por colaborador, terceiro, acionista, entre outros —, após a identificação de um ato suspeito na auditoria, a partir do monitoramento de processos internos, resultado da análise de riscos ou até mesmo autodeclarações de atos que sejam considerados violações internas, fraudes ou crimes.

Essa ferramenta do Programa de Compliance reduz a incidência de fraudes e inibe a sua ocorrência. Após receber as informações de suposta transgressão, cabe à organização reter materiais, documentos, e-mails ou qualquer outro elemento que possa ser utilizado como prova, bem como manter as fontes de prova seguras. De acordo com o entendimento de Nariman Ferdinian (2018), sob a ótica da Lei Anticorrupção e do Decreto que a regulamenta, as investigações internas operam como balizador do Programa de Integridade, bem como ferramenta de colaboração com a Administração Pública, que, através de acordos de leniência, atenuam eventual sanção.

Cabe destacar que é através dessa ferramenta que as organizações tomam ciência e possuem a oportunidade de averiguar os fatos e interromper eventuais ações de seus colaboradores e terceiros que possam expor sua imagem e sua reputação e causar prejuízos à empresa. Além disso, desenvolver ou aprimorar controles que inibam a reincidência da mesma conduta.

Por fim, como boa prática e elemento capaz de inibir e interromper condutas indevidas, as investigações internas possibilitam à pessoa jurídica que mitigue sanções que a ela recairiam, em caso de inércia diante da fraude ou do crime praticado em seu benefício. Neste sentido, as investigações internas, analisadas sob a ótica da Lei Anticorrupção e dos Programas de Compliance, funcionam no âmbito organizacional, sobretudo, como mecanismo de detecção de ilícitos e de prevenção de riscos.

8.2. Tipos de Investigação Corporativa

Existem diferentes tipos de investigação corporativa que podem ser classificados como: investigações internas propriamente ditas, internas com o auxílio externo, ou externas.

As investigações internas propriamente ditas são as feitas por profissionais da própria empresa; as investigações internas com auxílio externo são investigações

lideradas por pessoas da empresa com o auxílio de um assistente técnico ou um advogado, que direcionará o caminho a ser traçado. Já as investigações corporativas externas ou independentes stricto sensu, por seu turno, são aquelas investigações feitas por uma empresa terceirizada, um terceiro imparcial. Nestes casos, a empresa necessita que a investigação possua maior credibilidade, por isso a necessidade de contratar um terceiro para realizar tal apuração.

O responsável pela investigação tem o dever de verificar a veracidade das informações trazidas, sejam elas através do canal de alertas[14], sejam por quaisquer outros meios. O objetivo principal de uma investigação é averiguar se a conduta imprópria relatada realmente aconteceu. Além disso, através desta será possível identificar os responsáveis pela prática do ato, interromper a continuidade deste e tomar as providências cabíveis ao caso.

Nessa toada, é de suma importância que as empresas possuam normas internas que disponham sobre os procedimentos que serão adotados durante uma investigação, pois, de acordo com Wagner Giovanini[15], esta deverá ser conduzida de forma independente, ou seja, de forma alheia às questões hierárquicas, sem fazer juízo de valor, e afastar conflitos de interesse entre o profissional e o tema ou o objeto da investigação.

Vale ressaltar ainda a existência de mais um tipo de investigação, pouco explorado, e que está disciplinado no Provimento nº 188/2018, do Conselho Federal da Ordem dos Advogados do Brasil (OAB)[16], chamado de investigação defensiva, que é uma qualificação da investigação interna, sendo feita para que a empresa consiga se defender. Através desse provimento, foi regulamentado o exercício da prerrogativa do advogado em realizar diligências investigatórias, a fim de obter acervo probatório lícito para a própria defesa da organização.

Não significa dizer que essa investigação manipulará dados ou informações para possibilitar uma conclusão que auxilie sua defesa, mas sim que o objetivo dela é explorar as teses defensivas em busca de evidências que as corroborem, ou seja, buscar elementos de informação que permitam evidenciar se o fato realmente ocorreu, e como se deu, para que assim a organização tenha argumentos e elementos probatórios robustos para apresentar em sua defesa.

---

14 O canal de alertas é comumente conhecido como canal de denúncias. Não se utilizou a referida nomenclatura, por haver divergências quanto à utilização da palavra "denúncia", que indicaria uma acusação, e a informação levada a conhecimento da organização através do referido canal ainda será apurada.

15 GIOVANINI, Wagner. Compliance: a excelência na prática. São Paulo, 2014. p. 252.

16 ORDEM DOS ADVOGADOS DO BRASIL. Provimento nº 188, de 11 de dezembro de 2018. Disponível em: <https://www.oab.org.br/leisnormas/legislacao/provimentos/188-2018>. Acesso em 20 de julho de 2020.

8.3. Procedimentos

Diante da abordagem trazida, é relevante destacar como funciona, em termos procedimentais, uma investigação corporativa apropriada para seu objetivo de averiguação dos fatos.

Nesse sentido, a partir de distintas fontes, um processo de investigação pode ser desencadeado através de denúncias, de relatórios de auditoria, do monitoramento e de autoconfissões[17].

Os normativos internos, conforme aduz a Controladoria Geral da União (CGU), em sua cartilha: Programa de Integridade - Diretrizes para Empresas Privadas (2015, p. 22), devem estabelecer os trâmites para realização das investigações, indicando os prazos, as pessoas incumbidas para apurar as denúncias e o esclarecimento de quem receberá o reporte das investigações.

Com isso, caso sejam identificados os elementos necessários para uma investigação interna, é preciso, primeiramente, que se delimite a finalidade da investigação e o seu escopo. As pontuações devem ser formalizadas, com a fundamentação da decisão mais o tipo de investigação escolhida[18].

Destarte, deverá ser construído pelo investigador um plano de investigação, com o objetivo de servir de roteiro, podendo ser alterado ao longo do período, se for o caso, para se adequar às novas circunstâncias. O plano pode conter, de acordo com Serpa[19]:

- O objeto da denúncia.
- Os pontos em que há indisponibilidade de dados.
- Os possíveis cenários.
- O rol de pessoas investigadas.
- As pessoas que serão entrevistadas, bem como o cronograma das entrevistas e a posição em que elas serão, individualmente, indagadas.
- A relação de documentos para exame, com a indicação de sua fonte.
- As situações que indiquem a participação da área Jurídica.
- A documentação do processo a ser preservada.

---

17 HENCSEY, Antonio Carlos; BEZERRA, Christina Montenegro; PEREZ, Marisa. Investigações Internas: Condução, Desafios e Melhores Práticas. In: FRANCO, Isabel (org.). Guia prático de compliance. Rio de Janeiro: Forense, 2020. p. 137.

18 PAGOTTO, Leopoldo; ALMEIDA, Silvia Helena Cavalcante de; FERNANDES, Indira. Investigações Internas. In: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otavio (coord.). Manual de Compliance. 2° Ed. Editora Forense, 2020. p. 214.

19 ORDEM DOS ADVOGADOS DO BRASIL. Provimento n° 188, de 11 de dezembro de 2018. Disponível em: <https://www.oab.org.br/leisnormas/legislacao/provimentos/188-2018>. Acesso em 20 de julho de 2020.

Ademais, Giovanini[20] acrescenta que o plano de investigação também pode apresentar o prazo estimado; as perguntas a ser efetuadas nas entrevistas, de maneira geral; a determinação da logística; a definição dos interlocutores para o suporte e a forma de realização dos convites, acrescentando que o investigador deve compreender sobre os processos e as áreas ligadas ao fato investigado.

Por conseguinte, há também, no decorrer do processo investigativo, a possibilidade de se fazer uso das entrevistas como ferramenta. É uma fase primordial e delicada, uma vez que é necessário se atentar para não constranger o entrevistado, mantendo a conformidade com as balizas legais. Seu desfecho pode exigir a verificação de documentos antes não vistos ou a análise dos que foram apresentados pelos entrevistados[21].

O intuito das entrevistas, destaca Serpa[22], é angariar informações desconhecidas ou validar as anteriormente obtidas. Não é útil ao processo entrevistar pessoas que não legitimam tais opções, uma vez que um número mais restrito favorece na preservação da confidencialidade dos fatos, em manter o foco e na não alteração significativa do cotidiano da organização. Assim, o autor preconiza que na entrevista:

- O investigador esteja apto a realizá-la.
- O local deve ser tranquilo e deve considerar: o tempo; a não interrupção e o acesso às necessidades básicas.
- Seja limitada a quantidade de participantes e que seja entrevistado um por vez para evitar o receio em dizer algo.
- É viável a presença de uma pessoa — que não deverá intervir — para fazer anotações, pois possibilita maior atenção e conexão do entrevistador.
- O entrevistado não seja julgado ou intimidado.
- Que o entrevistador não garanta ao entrevistado algo que não ocorrerá.
- Que não sejam prontamente apontadas as mentiras na fala, salvo se auxiliar em conseguir mais informações.
- Que fique claro ao entrevistado, em caso de resistência, que o processo objetiva esclarecer fatos; que ele pode decidir se retirar ou não se manifestar;

---

20 GIOVANINI, Wagner. Compliance: a excelência na prática. São Paulo, 2014. p. 253.

21 PHENCSEY, Antonio Carlos; BEZERRA, Christina Montenegro; PEREZ, Marisa. Investigações Internas: Condução, Desafios e Melhores Práticas. In: FRANCO, Isabel (org.). Guia prático de compliance. Rio de Janeiro: Forense, 2020. p. 137.

22 SERPA, Alexandre da Cunha. Investigações de Compliance antes, durante e depois. p. 06-07. Disponível em: <http://conteudo.lec.com.br/ebook-investigacoes-internas>. Acesso em 19 de julho de 2020.

o entrevistador mostrando-se empático com a situação, mas alertando sobre o propósito.

- O denunciado, se oportuno e geralmente, seja o último entrevistado.

Vale ressaltar, que é relevante que a entrevista seja conduzida na língua do entrevistado, com o uso de um tradutor, se necessário, a fim de evitar algum ruído no diálogo, somada à observância do contexto social para familiaridade com as expressões utilizadas por ele[23].

Além disso, no decorrer do processo investigatório, pode acontecer de ser inevitável a coleta de informações nos e-mails, nos equipamentos ou nos bens da organização, devendo, por cuidado, desde a implantação do Programa de Compliance, esclarecer e comunicar aos colaboradores da possibilidade e do direito desse acesso; firmar um termo de concordância para preparar a defesa, em caso de questionamento judicial por irregularidades, e ter a anuência de profissionais alheios ao processo[24].

Diante disso, ao término da investigação, deverá ser desenvolvido um relatório final com a inserção das informações sobre a investigação, as suas fases especificadas e os resultados obtidos, além do registro substancial das evidências, com reporte dos dados para Alta Direção. É indicada, posteriormente, a publicidade dos resultados para organização, de forma genérica, perante a confidencialidade e respostas não aprofundadas sobre o andamento para o denunciante[25].

Portanto, o resultado da investigação deve ser avaliado por uma instância formada por profissionais de distintos departamentos da organização, que deliberarão sobre o caso e sobre a fixação das medidas disciplinares, se pertinentes[26].

Corroborando com o entendimento acima, a CGU[27] aponta em sua cartilha que, na situação de a investigação concluir que houve a prática de ato lesivo no âmbito da organização, medidas devem ser adotadas, a fim de garantir a cessação da ilicitude; a determinação de soluções e a remediação. Há possibilidade de

---

23 NEVES, Edmo Colnaghi. Compliance empresarial: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan Editora, 2018. p. 75.

24 GIOVANINI, Wagner. Compliance: a excelência na prática. São Paulo, 2014. p. 262-263.

25 HENCSEY, Antonio Carlos; BEZERRA, Christina Montenegro; PEREZ, Marisa. Investigações Internas: Condução, Desafios e Melhores Práticas. In: FRANCO, Isabel (org.). Guia prático de compliance. Rio de Janeiro: Forense, 2020. p. 141-146.

26 NEVES, Edmo Colnaghi. Compliance empresarial: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan Editora, 2018. p. 81.

27 CONTROLADORIA GERAL DA UNIÃO. Disponível em: <https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Acesso em 14 de julho de 2020.

aperfeiçoar o Programa de Compliance para a não repetição da ação e de outras falhas, além do emprego de medidas disciplinares aos responsáveis.

Na necessidade de aplicação de medidas disciplinares, Oliveira e Acocella[28] trazem que estas devem ser suscetíveis a todos da organização, de maneira imparcial, e estabelecidas, conforme a gravidade da irregularidade e o grau de responsabilidade do agente, com a sugestão da determinação das medidas e o seu enquadramento em procedimento.

Com isso, segundo a CGU[29], em sua cartilha, a organização deve se valer das informações adquiridas na investigação interna para estabelecer uma cooperação com a Administração Pública, pois o ato pode auxiliar em possível processo administrativo de responsabilização. Cabe à organização conhecer de antemão quais os órgãos responsáveis por apurar e aplicar sanções, além de trazer em seu programa o passo a passo para fundamentar tal decisão.

Por fim, a investigação interna caracterizada pela imparcialidade, pela não retaliação, pela reanálise de riscos e pela simetria na decisão é um pilar primordial na solidez do Programa de Compliance, uma vez que demonstra que os desvios e os atos lesivos não são, de fato, tolerados pela organização; que há confiança no canal de denúncia e nos controles internos; que o monitoramento está sendo realizado e que existe o comprometimento da Alta Direção, incentivando a responsabilidade de todos na cultura da integridade.

8.4. Considerações gerais sobre o tema

O presente estudo demonstra a necessidade de implementação de Programa de Compliance ou Integridade nas empresas, tendo como objetivo minimizar riscos trabalhistas, fiscais, criminais, entre outros, sendo as investigações corporativas um elemento central desse tipo de programa.

A implementação de forma correta e tecnicamente apropriada das investigações corporativas visa a auxiliar a Alta Administração na tomada de suas decisões, bem como a empresa a verificar a efetividade de suas políticas, prevenir riscos e responder as demandas necessárias, dando credibilidade ao seu Programa de Compliance.

---

28 OLIVEIRA, Rafael Carvalho Rezende; ACOCELLA, Jéssica. Governança Corporativa e Compliance. Bahia: Juspodivm, 2019. p. 40.

29 CONTROLADORIA GERAL DA UNIÃO. Disponível em: <https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Acesso em 14 de julho de 2020.

Capítulo 9

Reporte

KPMG

KPMG
BUSINESS SCHOOL

9.1. O papel do reporte na efetividade dos Programas de Compliance

Alcançar a efetividade nos Programas de Compliance é, sem dúvida, um dos maiores desafios dos profissionais que atuam com conformidade.

É sabido que este patamar de se tornar efetivo exige dedicação, recursos e um nível de maturidade que apenas o tempo e os esforços concentrados da área, sempre somados à Alta Administração, conseguirão.

Importantes componentes para o sucesso da área de Conformidade nas empresas e nas organizações são a transparência e a informação de qualidade. É nesta seara que entram os reportes, que ganham importância fundamental. Mas a pergunta a ser respondida neste capítulo é a seguinte: reportar para quem, o que e quando? Pois então tratemos de dissecar esses pontos, iniciando com o endereçamento dos reportes da área de Compliance.

Alguns deles já estão latentes nas cabeças dos profissionais militantes em compliance, que são os reportes obrigatórios aos reguladores. Aqui, de pronto, pensamos em comunicações ao Conselho de Controles de Atividades Financeiras (COAF), à Receita Federal do Brasil (RFB), ao Banco Central (BC), à Comissão de Valores Mobiliários (CVM), entre tantas outras.

Mas tratando-se de valor agregado ao compliance não só regulatório, tais reportes, a fim de trazer a dita efetividade aos Programas de Compliance, convenhamos, em nada agregam para a tomada de decisão na gestão da empresa, haja vista que são meramente regulatórios.

Então vejamos os reportes à Alta Administração. Estes sim, dependendo de alguns elementos como a periodicidade (que iremos abordar mais à frente), profundidade, independência da área de Compliance e, obviamente, da qualidade do relatório têm sim grande valor agregado para construir um programa efetivo rumo à integridade coorporativa.

Os reportes à Alta Administração precisam conter elementos que levem até o C-Level informações e aspectos sobre como está a integridade na empresa, informações sobre o controle e avaliação de riscos (risk assessment), quantidade de profissionais dedicados à função de compliance, quantidade e tratamento de denúncias, quantidade e qualidade de comunicações de compliance (compliance reminders), andamento de atualização e novas políticas, quantidade de treinamento inerente à ética e à integridade, entre outros.

Tais informações, quando devidamente calibradas para transmitir as ações de conformidade na empresa, darão conforto à Alta Administração quanto ao cumprimento de aspectos de compliance planejados, garantindo que o plano de

ação seja cumprido, ensejando ainda oportunidades de melhoria. Além disso, sejam informadas as ocorrências de não conformidades, falhas ou irregularidades identificadas.

É importante que os reportes tragam informações claras e consolidadas sobre o Programa de Compliance, para que este tenha visibilidade e seja garantida a continuidade das ações.

Permitirão ainda que novos rumos ou diretrizes inerentes ao programa sejam implementados ou abortados e poderão garantir que a Alta Administração tenha o conforto de saber que o programa está sendo cumprido e assim mitigar riscos de condenações e punições aos seus membros.

9.2. Desafios no processo de reporte

Para que o processo de reporte ao Conselho de Administração seja eficaz, a alta gestão deve lidar com alguns desafios. Os maiores desafios incluem os seguintes:

1. Os reportes acontecem conforme desenhado no Programa de Compliance ou estão "apenas no papel"?
2. Há tecnologia e recursos suficientes e apropriados para medir e reportar os fatos e as inconsistências em formatos de relatórios adequados?
3. A comunicação entre os agentes envolvidos no processo de reporte é formalizada, de forma que todo o processo esteja documentado e disponível quando houver necessidade de consulta?
4. Existe um comitê especial e/ou fluxo alternativo, para que seja garantida a independência quando o reporte envolver risco ou evidência de violação por parte de membros da Diretoria ou do Conselho?
5. A periodicidade de reporte planejada é adequada ao cenário e ao momento atuais da empresa?
6. O sistema de monitoramento fornece os dados necessários para a medição de KPIs e KRIs?
7. São desenhados planos de ação específicos para os desvios reportados?

Os KPIs e os KRIs reportados devem estar alinhados à estratégia de gerenciamento de riscos da empresa. O reporte deve incluir informações sobre se os resultados incluem falhas no programa, de forma que seja capaz de sinalizar que algum processo ou controle deve ser revisado. Dessa forma, o processo de reporte fornece instrumentos para que o Conselho de Administração tenha uma visão holística dos resultados do Programa de Compliance.

9.3. Monitoramento

Um Programa de Compliance efetivo depende do monitoramento da sua implementação. As atividades de monitoramento devem ter como objetivo verificar se os processos e os controles estão sendo seguidos efetivamente. As formas de monitoramento dependem do orçamento e da maturidade do Programa de Compliance e podem incluir:

1. Processo independente de avaliação das políticas e dos procedimentos de compliance.
2. Canal de denúncias que garanta o anonimato e a apuração das denúncias por pessoa preparada e que saiba como proceder de forma ágil e consistente.
3. Pesquisas periódicas com terceiros para identificar se os colaboradores têm praticado suas funções de acordo com as políticas da organização.
4. Acompanhamento periódico dos indicadores de compliance.
5. Follow-up das situações identificadas em reportes anteriores e as respectivas ações e respostas.
6. Análise de transações não usuais ou fora dos padrões.

Com a padronização dos processos e a integração sistêmica, é possível monitorar as transações que porventura estejam fora do padrão e avaliar se houve alguma inconformidade. Uma análise de dados torna o compliance incorporado à tecnologia de forma que suporte a eficácia e a sustentabilidade do programa. É importante destacar que esse monitoramento deve ser conduzido nos termos da Lei Geral da Proteção de Dados. A forma com que o processo de monitoramento colhe, trata, armazena e utiliza os dados de clientes, funcionários e terceiros deve ter o consentimento dos titulares das informações.

O canal de denúncias deve ser um complemento para a detecção de eventuais desvios e não a única ferramenta, já que a comunicação espontânea pelos funcionários sobre atos lesivos às políticas e aos valores da empresa, como atos de corrupção ou fraudes, está em fase de maturação inicial.

Além do monitoramento interno, também deve ser feito externamente, de forma a monitorar as transações e as situações com os parceiros de negócio de uma empresa, pois existe o risco de terceiros. Para isso, é importante utilizar as fontes internas e externas de informações disponíveis para que o monitoramento seja contínuo e de acordo com a matriz de riscos de terceiros definida no Programa de Compliance.

9.4. Canal de Denúncias e suas tratativas de reporte

O canal de denúncias conforme já descrito no capítulo 6 sobre "Tecnologia e Análise de Dados" é uma importante ferramenta de gestão e suporte à Governança Corporativa no combate à fraude, à corrupção e à má conduta. Por meio desse termômetro, a Alta Administração consegue medir e direcionar esforços para mitigar as vulnerabilidades encontradas, tais como: fraudes contábeis e financeiras, má conduta, assédio moral, segurança da informação, corrupção e outros ilícitos.

Sobre o ponto de vista de reporte um canal de denúncias eficiente deve estar aberto nas mais diversas formas (urna, telefone, Internet etc.) para colaboradores, fornecedores, terceiros, consumidores e sociedade em geral, permitindo inclusive o recebimento de denúncias anônimas.

Importante destacar que, se os funcionários não se sentirem seguros e confortáveis para utilizar o canal de denúncias disponibilizado, poderão buscar meios externos de fazer suas denúncias, por exemplo por meio de imprensa, Ministério Público e outros órgãos de controle.

Quanto maior a percepção dos funcionários acerca da seriedade, da intensidade e da assiduidade da Alta Administração com o Programa de Compliance, maior o comprometimento em denunciar desvios de conduta. Gerando inúmeros benefícios para a empresa, por exemplo:

- Evita vazamento de informações
- Reduz prejuízos gerados por fraude
- Diminui o número de ações judiciais
- Previne problemas reputacionais.

Uma pesquisa da Universidade de George Washington[30] revelou que quanto maior a atividade interna de denúncias, menor é o volume de processos judiciais e de denúncias externas à organização, ou seja, existe correlação entre o volume de denúncias internas e os melhores resultados financeiros e reputacionais.
Um Programa de Compliance não será plenamente eficaz a menos que os funcionários estejam dispostos a relatar violações à Administração.

No entanto, é fundamental criar e manter um programa de conscientização para a correta utilização dos canais para coibir o mal uso desse importante instrumento,

---

30 Segundo as Universidades de George Washington e de Utah, "More internal whistleblower activity, they found, correlates to fewer material lawsuits against the company, lower litigation settlement costs, fewer whistleblower complaints to outside regulators, less potential for earnings management, and even higher return on assets." Disponível em < http://www.radicalcompliance.com/2018/11/01/internal-reporting-business-outcomes/>. Acesso em 9 de julho de 2020.

em que se deve:

- Tratar a informação com seriedade e profissionalismo
- Assegurar a confidencialidade
- Proibir qualquer tipo de retaliação para o denunciante
- Garantir que a alegação será investigada e que as medidas cabíveis serão aplicadas.

As denúncias devem ser encaminhadas para a área competente (Compliance, Auditoria Interna etc.), para que possam ser investigadas e, caso o resultado seja procedente, aplicar as sanções previstas internamente.

A credibilidade dos mecanismos de compliance será medida pela capacidade que a organização tem de definir as medidas justas e implementá-las rapidamente.

9.5. Como definir a periodicidade dos reportes

Por fim, cabe aqui ressaltar a periodicidade das informações à Alta Administração, que vai variar de acordo com os itens, tais como: porte da empresa, seu segmento empresarial, eventual regulação externa, nível de maturidade do Programa de Compliance (em fase de implementação, a tendência é que os reportes sejam mais frequentes).

De modo geral, os reportes não devem ter intervalos tão longos que se percam informações nem tão curtos que as informações não tragam novidades e sejam enfadonhas.

Adicionalmente aos reportes à Alta Administração, lembrando que a integridade não deve estar limitada ao ambiente interno das empresas, é saudável que estas possam evidenciar sua integridade para fora dos seus muros.

A habitualidade desses reportes com fornecedores, clientes e sociedade cria uma agenda positiva e evidencia as práticas de integridade da empresa. É bem verdade que os portais eletrônicos das empresas já contêm, ou deveriam conter, um bom conteúdo tratando de integridade, mas dar um dinamismo nessas informações evidencia e fortalece o posicionamento ético e íntegro das empresas.

Trazer ao público externo informações sobre novas políticas, treinamentos realizados, comunicações éticas e compromissos da Alta Administração com a integridade são temas que, além de dar ainda mais consistência à posição ética das empresas, podem adicionalmente se tornar um diferencial de mercado.

9.6. Compliance na gestão de crise

Um dos pilares do Programa de Compliance é o apoio da Alta Administração (tone at the top) e, especialmente, em um momento de crise, esse comprometimento deve permanecer rígido e visível para a organização e para os stakeholders.

A situação de crise por si só possui um poder devastador de pressão interna e externa nos funcionários e nos colaboradores e, por isso, é importante reforçar os princípios e as diretrizes do Programa de Compliance existente.

No momento de crise instalada é possível mensurar a capacidade de resposta da empresa, avaliar sua liderança e seus valores, bem como testar sua reputação. A maturidade do processo de gestão e de cada linha de defesa é fundamental na proteção da organização.

Os efeitos econômicos associados à crise têm o condão de gerar ambientes propícios para disseminação de irregularidades, causando especial atenção para a área de Compliance das organizações.

Considerando tratar-se de uma situação excepcional, a área de Compliance deve estar cada vez mais presente nas reuniões de gerenciamento de crise, deixando claro tanto para a Alta Administração como para todos os funcionários que a crise somente será superada dentro de um ambiente de respeito às regras e aos princípios internos e externos.

Pontos de atenção que devem ser reportados pela área de Compliance nas reuniões de gestão de crise são, por exemplo:

- Aspectos regulatórios
- Contratações emergenciais
- Compliance no home office
- Segurança da informação
- Compliance concorrencial
- Aumento de preços
- Fraudes contábeis, entre outros.

Certo é que não existe "risco zero". Cada negócio possui mais ou menos riscos envolvendo sua atividade, razão pela qual toda organização precisa gerenciar crises durante o exercício da empresa.

Ocorre que crises podem ser dinâmicas e imprevisíveis, como o caso atual da pandemia do novo coronavírus, dificultando a sua gestão.

Para tanto, faz-se necessária a criação de um comitê de crise focado em gerenciar tais eventos capazes de comprometer a perenidade e a reputação da organização.

O comitê de crise deve ser composto, pelo menos, pelos principais gestores,

Compliance, Jurídico e Controladoria. Juntos devem ser capazes de gerar respostas rápidas, coordenadas e adequadas, tais como:

- Resposta em tempo real (suporte imediato ao evento crítico).
- Implementação de mecanismo interno e externo de comunicação de crise (investidores, imprensa, mídias sociais e consumidores).
- Monitoramento de indicadores da situação de crise.
- Avaliação de riscos e impactos para o negócio e as partes interessadas.
- Constatação de vulnerabilidades.
- Plano de gestão de crise para recuperação e continuidade do negócio.

Referências Bibliográficas

BRASIL. Lei n° 6.404 de 15 de dezembro de 1976. Dispõe sobre as sociedades por ações. Diário Oficial da União.

CAMARGO, R. F. Gestão de Negócio, Governança Corporativa e Riscos, 2018.

COMISSÃO DE VALORES MOBILIÁRIOS. CVM nº 586, de 8 de junho de 2017. Altera e acrescenta dispositivos à Instrução CVM nº 480, de 7 de dezembro de 2009. Rio de Janeiro. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst586.html Acesso em: 25 de agosto de 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Orientações sobre Comitês de Auditoria. São Paulo, IBGC, 2017 (Série IBGC Orienta).

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. Código das melhores Práticas de Governança Corporativa. São Paulo: IBGC, 5ª edição, 2015.

KPMG: Pesquisa Maturidade do Compliance no Brasil: KPMG, 4ª edição, 2019.

Lei Sarbanes-Oxley - The Sarbanes-Oxley Act, 2002. Disponível em: http://www.soxlaw.com/.

SOUSA NETO, J. A. DE; O compliance e as responsabilidades dos conselhos de administração e dos executivos. Dom Total, maio de 2016. Disponível em: https://domtotal.com/noticia/1026174/2016/05/o-compliance-e-as-responsabilidades-dos-conselhos-de-administracao-e-dos-executivos/.

The Institute of Internal Auditors. Declaração de Posicionamento do IIA: As três linhas de defesa no gerenciamento eficaz de riscos e controles. Janeiro de 2013.

WEICK, K.; SUTCLIFFE, K.M.; OBSTFELD, D. Organizing and the process of sensemaking. Organization Science, n.16, v.4, p.409-421, 2005.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. O que é Governança Corporativa. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 25 de agosto de 2020.

CVM - Comissão de Valores Mobiliários (CVM) disponível em http://www.cvm.gov.br/

DA SILVEIRA, Alexandre Di Micelo. Ética Empresarial na Prática: Soluções Para Gestão e Governança no Século XXI. 1º Edição. Editora Alta Books, 2007.

Estruturação das regras e instrumentos do Compliance. Disponível em https://daniel96313.jusbrasil.com.br/artigos/480261335/estruturacao-das-regras-e-instrumentos-de-Compliance

Exigência de cumprimento e disciplina, resposta e incentivos. Disponível em http://360Compliance.com.br/exigencia-de-cumprimento-e-disciplina-resposta-e-incentivos/

Operação Lava Jato. Disponível em http://www.pf.gov.br/imprensa/lava-jato
Pesquisa Maturidade do Compliance no Brasil. KPMG. 3º edição, 2017-2018.
Programa de Integridade Diretrizes para Companhias Privadas. Disponível em https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-Companhias-privadas.pdf
https://www.Compliancetotal.com.br/Compliance/funcoes
https://clickCompliance.com/Compliance-officer-responsabilidades/#:~:text=Por%20tanto%2C%20o%20profissional%20denominado,para%20o%20neg%C3%B3cio%20em%20quest%C3%A3o.
https://rbnaconsult.com/Compliance-officer-e-o-programa-de-integridade/
COSO - Committee of Sponsoring Organizations of the Treadway Commission. Controles Internos - Alavancar o COSO nas Três Linhas de Defesa. Julho, 2015.
IIA - The Institute Of Internal Auditors. As Três linhas de Defesa no Gerenciamento Eficaz de Risco e Controles. Janeiro, 2013.
ALLIANCE FOR INTEGRITY. Prevenção à Corrupção. Um Guia para Empresas. Dezembro, 2016.
KPMG. Base de Dados Linha Ética. Apresentação Certificação em Compliance. Dados Estatísticos. Últimos 6 meses.
CADE - Conselho de Administrativo de Defesa Econômica. Guia de Programas de Compliance. Janeiro, 2016.
ELETROBRAS, Manual de Compliance Referente às Leis Anticorrupção, 2ª Edição. Dezembro, 2015.
Manual de Compliance Referente às Leis Anticorrupção LEC, 2ª Edição. Dezembro, 2015.
CONTROLADORIA GERAL DA UNIÃO. Riscos à Integridade na CGU - Procedimentos e Análises. Núcleo de Gestão de Riscos e Integridade (NGRI). Março, 2019.
FEBRABAN - Federação Brasileira de Bancos. GUIA | BOAS PRÁTICAS DE COMPLIANCE. Edição revista e atualizada 2018.
TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico de Gestão de Riscos. Abril, 2018.
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. ISO 19600 (ISO Compliance).
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT 37001 (Sistema de Gestão Anticorrupção).
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT 31000

(Gerenciamento de Riscos).
Decreto nº 8.420 de 18 de março de 2015 < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8420.htm>. Acesso em 10 de julho de 2020.
Lei nº 12.846 de 1º de agosto de 2015 < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>. Acesso em 10 de julho de 2020.
ASSI, Marcos. Governança, Risco e Compliance, São Paulo. Janeiro, 2019.

Controladoria-Geral da União. Eixo 4 - Estratégias de Monitoramento. https://www.gov.br/cgu/pt-br/acesso-a-informacao/governanca/programa-de-integridade-da-cgu/eixo-4-monitoramento-continuo. Acesso em 10 de julho de 2020.
BRASIL. Lei nº 12.683, de 09 de julho de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm>. Acesso em 25 julho 2020
CONTROLADORIA GERAL DA UNIÃO. Disponível em: <https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf>. Acesso em 14 de julho de 2020.
GIOVANINI, Wagner. Compliance: a excelência na prática. São Paulo, 2014.
GONZALES, Nariman Ferdinian. Compliance: Investigações Internas e seus limites à luz da privacidade e proteção de dados. São Paulo, 2018.
HENCSEY, Antonio Carlos; BEZERRA, Christina Montenegro; PEREZ, Marisa. Investigações Internas: Condução, Desafios e Melhores Práticas. In: FRANCO, Isabel (org.). Guia prático de compliance. Rio de Janeiro: Forense, 2020.
NEVES, Edmo Colnaghi. Compliance empresarial: o tom da liderança: estrutura e benefícios do programa. São Paulo: Trevisan Editora, 2018.
ORDEM DOS ADVOGADOS DO BRASIL. Provimento nº 188, de 11 de dezembro de 2018. Disponível em: <https://www.oab.org.br/leisnormas/legislacao/provimentos/188-2018>. Acesso em 20 de julho de 2020.
OLIVEIRA, Rafael Carvalho Rezende; ACOCELLA, Jéssica. Governança Corporativa e Compliance. Bahia: Juspodivm, 2019.
PAGOTTO, Leopoldo; ALMEIDA, Silvia Helena Cavalcante de; FERNANDES, Indira. Investigações Internas. In: CARVALHO, André Castro; BERTOCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa; VENTURINI, Otavio (coord.). Manual de Compliance. 2° Ed. Editora Forense, 2020.
SERPA, Alexandre da Cunha. Investigações de Compliance antes, durante e depois. Disponível em: <http://conteudo.lec.com.br/ebook-investigacoes-internas>. Acesso em 19 de julho de 2020.


KPMG


KPMG
BUSINESS SCHOOL