CNseg

PROGRAMA

EDUCAÇÃO EM SEGUROS

GOVERNANÇA, RISCO E *COMPLIANCE* NO SETOR DE SEGUROS

A OPERAÇÃO DE SEGUROS

CNseg

PROGRAMA

EDUCAÇÃO EM SEGUROS

GOVERNANÇA, RISCO E *COMPLIANCE* NO SETOR DE SEGUROS

A OPERAÇÃO
DE SEGUROS

Objetivos deste livreto

Este livreto tem o objetivo de apresentar os fundamentos da Governança Corporativa e das funções de Gestão de Riscos e de *Compliance* no setor de seguros às associadas da CNseg, aos poderes Executivo, Legislativo e Judiciário, aos órgãos de imprensa, às instituições acadêmicas e ao público em geral.

"O conhecimento é poder. A informação é libertadora. A educação é a premissa do progresso, em todas as sociedades, em todas as famílias."

Kofi Annan

Índice

Introdução

Capítulo 1

1.1 GRC: Significado e motivação para um modelo integrado

A expressão Governança, Risco e *Compliance*, mais conhecida pela sigla GRC, passou a ser recentemente utilizada no mundo dos negócios. No entanto, só utilizá-la não basta para compreendê-la, sendo imperativo entender cada um dos seus três componentes a partir da constatação de que cada um deles, isoladamente, já faz parte do vocabulário do mundo corporativo há bem mais tempo.

Cada componente da GRC vem ganhando exponencial relevância no cenário brasileiro e mundial nas últimas décadas. Infelizmente, menos em decorrência de iniciativas voluntárias para prevenção de ameaças, e mais por indução de leis ou regulamentos que buscam atacar as causas de desvios de conduta, como famosos casos de fraude a exemplo da que envolveu a empresa americana Enron, que acabou resultando, em 2002, na aprovação, pelo Congresso dos Estados Unidos, da Lei Sarbanes-Oxley, mais conhecida como SOX. A lei veio a estabelecer padrões rígidos de GRC para as companhias com ações negociadas em bolsas de valores americanas.

No Brasil, exemplos recentes são os casos de corrupção advindos das investigações da Operação Lava-Jato, associada à promulgação da Lei nº 12.846/13, conhecida como Lei Anticorrupção, que redundaram, entre outros efeitos, na celebração de acordos de leniência e em reconhecimentos públicos de grandes empresas nacionais de que não aplicavam princípios importantes da GRC, assumindo o compromisso de passar a observá-los.

A fim de compreender de forma individualizada cada um dos seus três elementos, é necessário mencionar que as práticas de Governança Corporativa compõem a primeira letra da sigla GRC. As primeiras discussões organizadas sobre o tema remontam à década de 1990, tendo como marco inicial a publicação do relatório Cadbury, em 1992, na Inglaterra. No Brasil, pode-se considerar como marco a fundação, em 1995, do Instituto Brasileiro de Governança Corporativa (IBGC), referência nacional para o tema, e que elaborou seu primeiro código de melhores práticas em 1999.

Pode-se, de forma geral, dizer que a governança de uma empresa está relacionada com a forma como uma organização é dirigida, ou seja, com a definição e, principalmente, com o exercício de práticas que permitem alinhar as expectativas não só de acionistas e administradores, mas também das demais partes interessadas (pessoal, consumidores, fornecedores, credores, governo e a sociedade em geral). Nesse contexto, emergem as bases da Governança Corporativa: a transparência, a equidade, a prestação de contas e a responsabilidade corporativa, fazendo com que o controle seja tão importante quanto a gestão.

A segunda letra da sigla GRC está relacionada à Gestão de Riscos. O conceito de risco evoluiu ao longo do tempo e é dependente do contexto em que está inserido. Porém, para essa abordagem inicial, vamos utilizar a definição que está expressa na norma ISO:31.000, de 2009, que trata risco como "*o efeito da incerteza nos objetivos*". A Gestão de Riscos, realizada ao longo do desenvolvimento humano de forma intuitiva, ganhou maior notoriedade a partir de alguns compromissos internacionais como o Acordo da Basileia e a Diretiva de Solvência II. Aqui, também se veem reações a casos de escândalos financeiros que resultaram na criação de frameworks de referência como o The Committee of Sponsoring Organizations - COSO, que teve sua primeira versão em 1992, e a já citada norma ISO:31.000, de 2009.

Por fim, a última letra refere-se a um termo já bastante utilizado no Brasil, o *Compliance*. Em linhas gerais, estar em *Compliance* ou em conformidade, em uma tradução livre para o Português, significa ter seus negócios e atividades conduzidos nos estritos padrões da legislação e dos regulamentos oficiais vigentes e de acordo com as políticas empresariais e normas internas de procedimentos que, obviamente, não podem colidir com as primeiras. Mais do que o cumprimento de normas, a função de *Compliance* tem a ver com o zelo pela integridade da organização, que está ancorado no comportamento adotado por seus administradores, colaboradores e representantes em cada situação cotidiana. Apesar de o termo ter se popularizado no Brasil recentemente, as primeiras menções a essa função remontam à metade do século XX.

Pode-se dizer, portanto, que GRC, muito mais que apenas uma reunião dessas três práticas, é algo bem mais elevado como, por exemplo, definem Nicolas, WEIPPL, Edgar e SEUFERT, Andreas:

GRC é uma abordagem holística e integrada, para toda a organização, de governança, riscos e Compliance que garanta uma atuação ética e de acordo com o seu apetite ao risco, políticas internas e regulamentações externas através do alinhamento da estratégia, processos, tecnologia e pessoas, melhorando assim a eficiência e eficácia.

(A Frame of Reference for Research of Integrated Governance, Risk and *Compliance* (GRC), tradução livre, 2014, p.9)

Pensar em Governança, Risco e *Compliance* de uma forma combinada agrega valor superior à mera existência isolada dessas três práticas, mediante a criação de uma vantagem competitiva. Ou seja, tratar cada um desses elementos da GRC de forma segregada,

cada qual em uma área de atuação específica, como se fossem células sem qualquer interconexão, pode levar à perda da oportunidade de uma maior efetividade no processo.

A não coordenação desses assuntos, por um lado, faz com que seja necessário alocar diversos profissionais com habilidades específicas atuando de forma individual sobre temas que, quando integrados, resultam em ganho de escala e de eficácia; isso ocorre não só para aqueles que cuidam desses temas nas organizações, mas também, por exemplo, para as áreas de negócio, que acabam por dispensar maior atenção e tempo às atividades e demandas individualizadas de governança, riscos e *Compliance*, em detrimento das atividades fim da empresa e da busca pelo resultado operacional. Por isso, não é raro que gestores das áreas de negócio questionem o fato de terem de gastar tempo excessivo com atividades que, em suas visões, se mostram redundantes ou, até mesmo, mais grave, contraditórias, quando não há um modelo integrado de GRC.

A integração desses três componentes em uma iniciativa coordenada e sinérgica proporciona uma atuação que vai da participação na orientação estratégica às atividades mais

operacionais de uma companhia. Portanto, o sucesso dessa integração depende de um elemento fundamental quando se fala de governança, risco e *Compliance*: a adequação da cultura organizacional ou, como bem define o COSO, do "ambiente de controle".

A cultura organizacional é, pois, além de necessária, o fator fundamental para o pleno desenvolvimento de uma estrutura eficiente de GRC, porque, como se viu, não basta juntar os três temas em um arranjo organizacional de uma única área, mas sim pensar e atuar com esses temas de uma forma integrada, coordenada e colaborativa, buscando melhor comunicação, melhora do trabalho com as diferentes equipes e, principalmente, gerenciamento da informação.

O desenvolvimento de um modelo integrado de GRC deve, portanto, levar em consideração aspectos da cultura organizacional antes de olhar para os aspectos regulatórios e comerciais, uma vez que, sem essa visão de cunho cultural interno, não há como gerar e influenciar a governança, o ambiente de gestão de risco e os procedimentos e práticas de *Compliance*, por mais sofisticados e dispendiosos que eles possam parecer sob uma ótica individualizada e meramente operacional. Com isso, por um lado, se evitará que essas práticas estejam desalinhadas com o objetivo de um modelo integrado de GRC e, por outro, que haja resistência de serem aceitas e seguidas por todos os envolvidos.

1.2 Referências teóricas de GRC

Entre as referências teóricas de GRC, destaca-se a *International Organization for Standardization – ISO* – que, por sua natureza independente e não governamental, auxilia o mercado na padronização de assuntos, aproximando-o dos seus reguladores e sendo fonte riquíssima de conteúdo. Devem-se destacar a ISO 31.000, que trata da Gestão de Riscos, e a ISO 37.001, que trata de sistemas de prevenção à corrupção, como documentos ligados à GRC.

Como outra referência, é importante citar o COSO, que tem como objetivo produzir e divulgar documentos que ajudam os mercados a respeito de Gestão de Riscos, controles internos e prevenção à fraude. O COSO foi fundado por entidades ligadas a contabilistas, auditores internos e executivos de finanças, seus principais documentos foram publicados a partir de 1992 (sobre Controles Internos), com diversas revisões ao longo dos anos. Em 1999, ocorreu a primeira publicação sobre Prevenção à Fraude e, em 2004, a publicação a respeito da Gestão de Riscos Corporativos, esta revista em 2017, com a inclusão da perspectiva da integração com as estratégias e desempenho das empresas.

No Brasil, há que se destacar o já citado Instituto Brasileiro de Governança Corporativa (IBGC), que reconhece

a Gestão de Riscos como fator determinante para a perenidade de uma empresa e como assunto necessariamente ligado aos Conselhos de Administração.

1.3 Aplicação do conceito de GRC no mercado segurador

No mercado de seguros, os componentes do GRC começaram a ter um marco regulatório elaborado pela Susep a partir da publicação, em 2004, da Circular Susep nº 249, que tinha como objetivo a implantação de um sistema de controles internos. Tal norma foi a primeira no contexto do mercado segurador a mencionar o ambiente de controle, tratando de aspectos relacionados às características, responsabilidades, monitoramento e supervisão desse ambiente. Apesar de não tratar explicitamente de *Compliance*, há elementos característicos como a necessidade de cumprimento de normas e regulamentos e algumas atividades de controle em relação a isso.

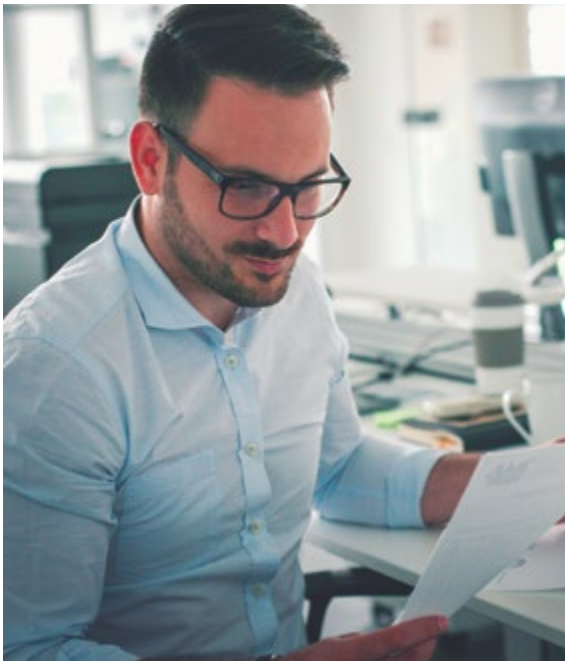
Com o passar do tempo, outros normativos foram adicionados ao arcabouço regulatório que trata do tema, no qual se destaca a Circular Susep nº 344, de 2007, que trata de controles para prevenção à fraude;

a Circular Susep nº 380/08, e, posteriormente, a Circular Susep nº 445/12, que abordam a necessidade de controles para a prevenção à lavagem de dinheiro; até, por fim, chegar ao desenho da Circular Susep nº 521/15, que trata da implantação da Estrutura de Gestão de Riscos.

A despeito de o componente de avaliação de riscos estar presente já na Circular Susep nº 249/04, o amadurecimento regulatório do tema se deu com a publicação da Circular Susep nº 521/15, junto com as alterações da Circular Susep nº 561/17. Essa norma está alinhada com o que é praticado principalmente na União Europeia em decorrência da Diretiva de Solvência II, que busca promover a gestão baseada em riscos com visão integrada e adequada à complexidade de cada empresa, e que associa a necessidade de capital de uma empresa ao seu amadurecimento em termos de governança corporativa, de gestão de riscos e de *Compliance*.

É importante destacar o fomento dado para que cada empresa busque os próprios modelos e metodologias para se adequar ao objetivo pretendido pela mencionada Circular, sem determinar um escopo limitado, o que ajuda a promover as discussões dentro das empresas e contribuir para a evolução da cultura de riscos.

A promulgação desses diversos normativos de forma separada



O desenvolvimento de um modelo integrado de GRC deve, portanto, levar em consideração aspectos da cultura organizacional antes de olhar para os aspectos regulatórios e comerciais.

acabou por criar estruturas e atividades operacionais apartadas em cada empresa a fim de cumprir essas regulações. Tal fato reforça a importância de se pensar na visão integrada do GRC no mercado de seguros visto que, dessa forma, tais assuntos seriam tratados conjuntamente de forma mais eficiente, o que permitiria a melhor gestão da informação e das ações a serem realizadas para gerar valor ao acionista e segurança para o regulador.

No campo da Saúde Suplementar, a Agência Nacional de Saúde Suplementar (ANS) colocou em consulta pública (nº 67), em junho de 2018, proposta de Resolução Normativa que dispõe sobre a adoção de práticas de governança corporativa, com ênfase em Controles Internos e Gestão de Riscos pelas operadoras de planos de saúde. A proposta de normativo contemplou a heterogeneidade do setor e teve como base Nota Técnica e Relatório de Análise de Impacto Regulatório elaborados pela Diretoria de Normas e Habilitação das Operadoras, além de contribuições do setor apresentadas em audiência pública realizada em maio de 2018. Até a publicação deste livreto, a Resolução Normativa não havia sido publicada.

1.4 GRC: Desafios e benefícios da integração

A integração das funções de GRC sob uma única estrutura gera melhor alocação de recursos e tempo, porque elimina trabalhos redundantes ou contraditórios, menor demanda sobre as áreas de primeira linha de defesa dos objetivos estratégicos (as de negócios, as operacionais e as de *back-office*), bem como maior eficiência para as de segunda linha de defesa (aquelas inerentes a riscos, aspectos atuariais e *Compliance*). Procedimentos, práticas de *Compliance*, controles internos e gestão de processos estarão desenhados com um melhor

entendimento do que é preciso para cumprir com o que foi estabelecido pela empresa como seu apetite a risco e, portanto, alinhado com os objetivos estratégicos. Ademais, facilita-se a atuação da auditoria interna, como atividade de terceira linha de defesa, quando do monitoramento periódico e sistemático da qualidade e do desempenho das atividades de primeira e de segunda linhas de defesa.

É esse alinhamento com a estratégia e a proximidade da alta administração e dos principais grupos de interesse com o assunto, que permite o desenvolvimento e o aprimoramento de uma cultura organizacional fundamental para a criação de um ambiente de controle com alto grau de maturidade e o mais próximo possível do estado da arte, no que diz respeito à governança, risco e *Compliance*.

O sucesso ou o fracasso de um modelo integrado de GRC depende fortemente, como já se ressaltou, da cultura da empresa. Ela é essencial na busca de maior eficiência das práticas de governança, risco e *Compliance* de forma a criar um desempenho superior e maior transparência, fundamentais em um cenário concorrencial cada vez mais acirrado, que exige um foco maior na eficiência operacional. Eficiência esta

A aplicação de práticas de GRC nas empresas resulta em inúmeros benefícios, como por exemplo, a interação entre áreas e a melhoria da performance e dos resultados, e a diminuição de custos, decorrente da eficiência dos projetos.

que pode ser alcançada pela melhoria do contexto interno focado na visão da GRC como provedora de uma vantagem competitiva.

1.4.1 Principais desafios

O arranjo necessário entre a definição dos escopos, planejamento, execução e integração dos processos das funções de Governança, *Compliance*, Gestão dos Riscos Corporativos e Gestão de Pessoas, executadas por diversas áreas de uma organização, pode não ser de fácil solução prática, motivo pelo qual um dos principais desafios do desenvolvimento de um ambiente de GRC integrado na organização é a busca pela sinergia entre as áreas, resultando na utilização de recursos e processos eficientes.

Para ilustrar essa dificuldade, tome-se como exemplo a gestão dos riscos emergentes, que constitui relevante desafio às estruturas de GRC existentes. Com efeito, nem sempre é fácil estabelecer padrões sobre como antecipar riscos emergentes como, por exemplo, os derivados da introdução de novos regulamentos ou de alterações substanciais de normas já existentes, os relacionados ao lançamento de novos produtos pela companhia, os oriundos da entrada de novos competidores e as outras grandes mudanças que possam gerar riscos futuros para a companhia. No entanto, essa visão ficará facilitada se, em vez de atualizarem de forma isolada a governança, a gestão de riscos e o *Compliance*, atuarem de maneira coordenada.

1.4.2 Benefícios da integração

A aplicação de práticas de GRC nas empresas resulta em inúmeros benefícios, dentre os quais se destacam: (i) interação entre áreas e a melhoria da performance e dos resultados; (ii) diminuição de custos, decorrente da eficiência dos projetos, dos processos e dos controles existentes; (iii) maior segurança e confiabilidade nas informações obtidas, o que pode ser traduzido na geração de valor perceptível pelos acionistas e investidores e; (iv) diminuição de fraudes e maior controle dos processos.

Governança

Capítulo 2

2.1 Contexto

A crescente necessidade de leis, regulamentos e normas sobre governança, aliada à necessidade de definição de fatores de riscos e ao imperativo do *Compliance*, tem obrigado as organizações a repensar o seu modelo de negócio. As práticas de governança corporativa, se tratadas separadamente da gestão de riscos e do *Compliance*, podem se tornar redundantes e gerar conflitos de interesses, inconsistências e ineficiências. Por outro lado, adotar boas práticas de governança significa estar alinhado à evolução do ambiente de negócios, o que passou a ser mandatório.

2.2 Definição de Governança

Há diversas definições para governança de empresas, governança corporativa ou simplesmente governança:

Conjunto de mecanismos organizacionais que tem como objetivo delimitar os poderes e também influenciar as decisões dos gestores; dito de outra forma, que governam a sua condução e definem o seu poder discricionário."
(Charreaux, 1997)

"A governança corporativa é um termo abrangente que inclui questões específicas decorrentes de interações entre alta administração, acionistas, conselhos de administração e outras partes interessadas."
(Cochran et Watrick, 1988);

"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." ***(site do IBGC)***

Embora sejam várias as definições, pode-se concluir, no entanto, que governança é um conjunto de mecanismos cujo objetivo principal é a convergência dos anseios de diferentes partes interessadas, delimitando seus escopos de atuação e poderes de decisão.

2.3 Princípios

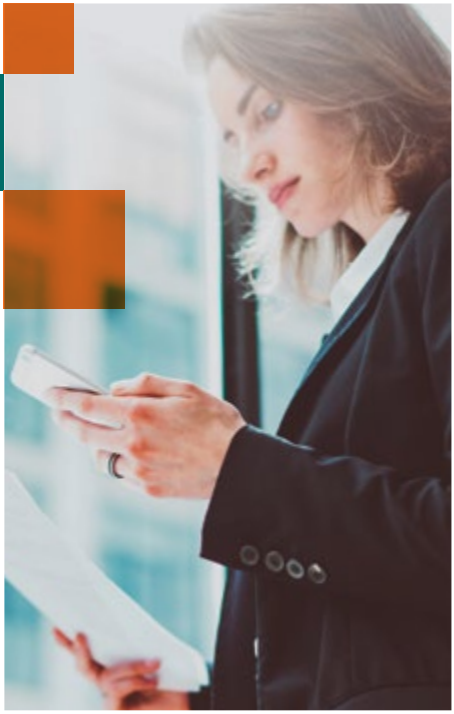
De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), as boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum. O IBGC cita quatro princípios básicos, já mencionados anteriormente: a transparência, a equidade, a prestação de contas e a responsabilidade corporativa.

O princípio da **transparência** consiste na disponibilização de informações de relevância a todas as partes interessadas, não se resumindo somente àquelas exigidas por mecanismos externos (leis, regulamentos). Já a **equidade** diz respeito à igualdade de tratamento a ser dada às partes interessadas. O princípio da **prestação de contas** trata da transparência da atuação dos agentes de governança, compreendendo a responsabilidade integral dos seus atos e omissões e a atuação diligente e responsável no âmbito dos seus papéis. Por fim, o princípio da **responsabilidade corporativa** trata da perenidade da empresa, levando em consideração os diversos capitais (financeiro, humano, reputacional etc).

2.4 Integração entre as áreas – GRC e *Tone at the Top*

Uma gestão de riscos eficaz, perfeitamente inserida nos princípios do GRC, se inicia por meio de uma estrutura organizacional que possibilite às lideranças do primeiro escalão tomarem decisões alinhadas com o apetite a riscos estabelecido e se envolverem ativamente no tema. Uma prática comum é a criação de um comitê de riscos, órgão de governo interno que monitora continuamente os processos de identificação, avaliação e resposta aos principais riscos corporativos e garante comunicação fluida com o conselho de administração e os outros órgãos de governança, no tocante às diretrizes e à estratégia corporativa de gestão de riscos.

Tais mecanismos promovem transparência, previsibilidade e confiança, além de permitirem que as empresas tenham maior qualidade na gestão empresarial e na governança e, portanto, possam enfrentar momentos de crise e de intensa pressão com maior resiliência.



Uma gestão de riscos eficaz se inicia por meio de uma estrutura organizacional que possibilite às lideranças do primeiro escalão tomarem decisões alinhadas com o apetite a riscos estabelecidos e se envolverem ativamente no tema.

Outra consequência direta é o chamado "*Tone-at-the-Top*", que pode ser traduzido como o compromisso dos acionistas, conselheiros e líderes empresariais em vivenciar, promover e propagar a cultura organizacional vinculada às práticas de governança corporativa e conformidade.

A gestão da empresa se transforma e passa a sustentar e patrocinar os processos e soluções integradas de GRC para agregar valor ao negócio de qualquer companhia. Esse compromisso da alta administração é comunicado de forma clara e eficiente aos colaboradores dos demais níveis e também ao mercado, passando a integrar a missão, a visão e os valores da sociedade.

2.5 Mecanismos de Governança

Já se viu que a governança corporativa é um conjunto de mecanismos que tem como objetivo, sobretudo, a criação de valor para a companhia. Segundo Shleifer e Vishny (1997), esses mecanismos funcionam para reduzir os conflitos de agência e também os conflitos entre acionistas majoritários e minoritários.

A teoria da agência (Jensen e Meckling, 1976) propõe que o funcionamento de tais mecanismos implique uma empresa mais eficaz. Charreaux (1997) definiu uma tipologia para esses mecanismos, como segue:

Mecanismos específicos: Conselho de Administração e seus Comitês, sistema de remuneração, auditoria interna, entre outros.

O Conselho de Administração é um dos principais promotores do alinhamento dos interesses de acionistas e gestores no sistema de governança corporativa de uma companhia. Entre suas principais atribuições, destaca-se a definição da estratégia, a nomeação, destituição e acompanhamento dos diretores executivos, a aprovação e supervisão orçamentária, a escolha dos auditores independentes e o estabelecimento das políticas de GRC, incluindo o apetite a riscos da organização.

Para auxiliá-lo, podem ser estabelecidos comitês especializados, como os comitês de Auditoria, Riscos, Finanças, Remuneração, entre outros. O Comitê de Auditoria tem como atribuições principais o acompanhamento e a avaliação da qualidade da atuação da auditoria interna e da auditoria independente, tanto na companhia como em suas controladas.

O Comitê de Remuneração atua na revisão da política ou no sistema de remuneração e no modelo de gestão de pessoas, podendo contribuir de forma relevante na gestão de riscos. Os esquemas de remuneração em forma de opções de ações, por exemplo, são formas úteis e legítimas de alinhamento dos gestores e acionistas.

Por fim, os comitês de risco e financeiro, compostos por único comitê ou separadamente, acompanham e avaliam, monitoram e criam planos de ação para a gestão dos riscos corporativos.

O Conselho de Administração é um dos principais promotores do alinhamento dos interesses de acionistas e gestores no sistema de governança corporativa de uma companhia.

Mecanismos não específicos: ambiente legal e regulatório, sindicatos, auditores externos, entre outros. Os mecanismos externos de governança referem-se a tudo aquilo que não é inerente à empresa. Em outras palavras, são instituições formais tais como: leis e regulações, regras econômicas e políticas, códigos de condutas e valores, entre outros. Silveira (2002) destaca a influência exercida pelo ambiente externo no modelo de governança corporativa no que tange ao seu aperfeiçoamento e eficácia.

2.6 Linhas de defesa

O *Institute of Internal Auditors* (IIA), uma das entidades que conceberam a estrutura COSO, recomenda o modelo de Três Linhas de Defesa como forma de gerenciamento de riscos que possam comprometer os objetivos estratégicos e como implantação de atividades de controle para mitigá-los, por meio do esclarecimento dos papéis e responsabilidades essenciais a cada nível da empresa. O modelo apresenta uma visão sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de Governança, Gestão de Riscos e *Compliance* e é aplicável a qualquer organização, não importando seu tamanho ou complexidade.

PRIMEIRA LINHA DE DEFESA

É responsável por manter controles internos eficazes e por conduzir procedimentos e controles de risco. Tem como principais objetivos:

- Identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos.
- Garantir que as atividades estejam de acordo com as metas e objetivos.
- Desenvolver e implementar procedimentos detalhados de controles.
- Assegurar a conformidade, reportando falhas de controle, processos inadequados e eventos inesperados.

SEGUNDA LINHA DE DEFESA

É responsável por facilitar e monitorar a implementação de políticas eficazes de gerenciamento por parte da gerência operacional. Seus principais objetivos são:

- Auxiliar os proprietários dos riscos a definir a meta de exposição ao risco e a reportar adequadamente informações relacionadas a riscos em toda a organização.
- Monitorar os diversos riscos específicos, tais como: a não conformidade com leis e regulamentos aplicáveis e com políticas e normas internas.
- Reportar diretamente à alta administração e, em alguns setores de negócio, diretamente ao órgão de governança.

- Monitorar algumas conformidades específicas.

TERCEIRA LINHA DE DEFESA

É responsável por avaliar a eficiência e eficácia das operações. São seus principais objetivos:

- Reportar análises ao Conselho de Administração, quando houver, ou à alta administração, nos casos em que não houver.
- Aferir a confiabilidade e a integridade dos processos de reporte.
- Atestar que os procedimentos internos estejam em conformidade com as leis aplicáveis.
- Verificar se os procedimentos internos estão alinhados aos regulamentos, políticas e normas.

2.7 Benefícios de se ter Governança

Os principais objetivos gerados por uma estrutura eficiente e robusta de governança giram em torno de algumas temáticas centrais: (i) o aprimoramento do processo decisório com base em riscos; (ii) a deliberação de temas vinculados à gestão de riscos e *Compliance* na agenda do Conselho de Administração e administradores; (iii)

o tratamento transparente e equânime com os públicos interno e externo e; (iv) a observância do apetite a riscos estabelecido na organização.

Importante ressaltar que a Governança Corporativa a ser buscada pelas sociedades não trata do mero cumprimento de regras e recomendações contidas no código de ética e conduta ou em políticas institucionais, tampouco deve ser entendida apenas como uma validação de práticas a serem observadas sem qualquer vinculação com o cotidiano da empresa com o objetivo de passar uma boa imagem para o público externo e satisfazer regulações.

A Governança a ser almejada é a praticada no cotidiano da empresa, e seu valor se torna perceptível quando:

- O aprimoramento do processo decisório resulta na descentralização do poder, no gerenciamento dos conflitos de interesse e em deliberações sustentáveis, que objetivam o interesse de longo prazo da organização.
- Seus colaboradores cumprem as normas de maneira consciente e manifestam um comportamento ético.
- Prevalece uma atitude transparente e equânime, que gera confiança e reflete em uma percepção externa positiva e na boa reputação da organização.
- Há um relacionamento estruturado entre a Administração, os conselheiros e os acionistas.
- A meritocracia é praticada por meio do aperfeiçoamento de mecanismos de avaliação de desempenho e de um sistema de incentivo, que priorizam o interesse da sociedade a médio e longo prazos.
- As estruturas de gestão de riscos e controles internos asseguram efetivamente a aderência às regras, diminuindo as chances de surpresas negativas.
- Prevalece a transparência com as partes interessadas e os seus acionistas exercem seus direitos de forma equitativa.

Tais benefícios gerados pela governança resultam no aumento do valor do negócio e, consequentemente, as empresas percebidas como bem administradas se tornam mais atraentes para investidores e mais confiáveis para consumidores.

A excelência em Governança Corporativa tem sido buscada, cada vez mais, pelos acionistas e demais partes interessadas e pode ser traduzida em processos e boas práticas que passam a ser visíveis na sociedade e que efetivamente agregam valor a ela, alinhando a tomada de decisão com o apetite a riscos estabelecido.

Portanto, a organização deve analisar a governança corporativa com a sua devida importância, a fim de assegurar a sua perenidade e direcionar as principais mudanças organizacionais e práticas por meio de uma "agenda de governança" eficaz, que possa ser adotada a curto, médio e longo prazos.

Gestão de Riscos

Capítulo 3

3.1 Princípios da Gestão de Riscos

A Gestão de Riscos deve fazer parte da rotina corporativa, estar aliada às práticas e aos princípios de Controles Internos e servir como suporte às áreas de negócio e aos administradores da companhia na tomada de decisões. Refere-se aos princípios, à estrutura e ao processo para mitigar os riscos que eventuais fraquezas internas e ameaças externas trazem aos negócios, seja por sua probabilidade de ocorrência, seja pelos impactos negativos que podem vir a gerar caso se materializem.

3.2 Ambiente de Controle

O Ambiente de Controle deve dar o ritmo a uma organização por meio de uma cultura de Controles Internos que influencie e conscientize as pessoas que nela trabalham. Com base na estrutura integrada publicada pelo COSO, foram estabelecidos princípios que permitem às empresas avaliar os seus sistemas próprios de controle, melhorando o desempenho e a governança das organizações. Tais princípios abordam a estrutura de controles internos de uma organização sob diversas perspectivas de ações, em especial:

1. Uniformizar definições de controle interno.
2. Definir componentes, objetivos e objetos do controle interno em um modelo integrado.
3. Delinear papéis e responsabilidades da administração, reforçando a independência em relação aos seus executivos.
4. Estabelecer padrões para implementação e validação dos controles.
5. Criar um meio para monitorar, avaliar e reportar os controles internos.
6. Demonstrar o comprometimento com a integridade e os valores éticos.

3.2.1 Diretrizes da Estrutura de Gestão de Riscos

Considerando definições presentes em documentos de melhores práticas e regulamentos associados ao tema, a Estrutura de Gestão de Riscos deve, principalmente:

- Ser compatível com a natureza, escala e complexidade das operações da organização, além de estar alinhada com o ambiente de controles internos;
- Prever processos, metodologias e ferramentas para identificar, avaliar, mensurar, tratar e monitorar a exposição a riscos.
- Adotar os tratamentos e controles adequados, compatíveis com cada risco, com o objetivo de, entre alternativas possíveis, evitá-lo, mitigá-lo, compartilhá-lo ou mesmo aceitá-lo de forma consciente e controlada.
- Descrever o conjunto de riscos a que a companhia se encontra exposta, de acordo com os processos

e metodologias empregados para a identificação de riscos, definindo um apetite a risco e descrevendo a forma de alcançar seus objetivos estratégicos para criar valor aos seus acionistas.

- Considerar a elaboração de um Plano de Continuidade de Negócios, contendo os procedimentos e informações necessários para a manutenção das atividades críticas de uma organização diante de situações que afetem seu funcionamento normal.

É de extrema importância observar que o departamento responsável pela gestão dos riscos corporativos deve estar subordinado, conforme o caso, ao Conselho de Administração ou à Diretoria da companhia, devendo dispor da independência necessária para o exercício de suas atribuições.

3.2.2 Identificação dos riscos

A identificação e a avaliação dos riscos deverão considerar, entre outras possíveis, pelo menos as seguintes tipologias de riscos:

a) Riscos Estratégicos: são os riscos associados com as decisões estratégicas da organização para atingir os seus objetivos de negócios ou decorrentes da falta de capacidade ou habilidade da companhia e suas subsidiárias para proteger-se ou adaptar-se a mudanças no ambiente.
b) Riscos Financeiros: são os riscos associados à exposição das operações financeiras da companhia e suas subsidiárias. Os riscos financeiros podem ser classificados entre riscos de Mercado, de Crédito e de Liquidez.
c) Riscos Operacionais: são os riscos decorrentes da falta de consistência e adequação dos sistemas de informação, processamento e controle de operações, bem como de falhas no gerenciamento de recursos e nos controles internos ou fraudes que tornem impróprio o exercício das atividades da companhia ou de suas controladas diretas ou indiretas.

É de extrema importância observar que o departamento responsável pela gestão dos riscos corporativos deve estar subordinado ao Conselho de Administração ou à Diretoria da companhia, devendo dispor da independência necessária para o exercício de suas atribuições.

d) Riscos de *Compliance*: são os riscos relacionados a sanções legais ou regulatórias, de perda financeira ou dano à reputação que a empresa pode sofrer como resultado da falha no cumprimento da aplicação de normas, leis, acordos, regulamentos, código de ética ou conduta ou das demais políticas e normas internas.
e) Riscos de Segurança da Informação: são os riscos relacionados a controles ineficazes ou inexistentes e a ações indevidas que possam comprometer a confidencialidade, integridade e disponibilidade das informações da companhia ou de suas controladas diretas ou indiretas.

Muitas companhias possuem seus próprios dicionários de riscos, não necessariamente seguindo a tipologia de riscos descrita acima; no entanto, é mister que esses dicionários categorizem e tratem todos os possíveis riscos a que as companhias estão expostas e que sejam adotados como linguagem única de riscos pelas diversas áreas da organização.

Devem ser estabelecidos processos de identificação e priorização do tratamento dos riscos corporativos. Os processos de identificação dos riscos devem abranger pelos menos as categorias de riscos descritas acima e devem contar com o auxílio de bases de dados internas da organização, de fontes de informações externas e ainda com o julgamento de especialistas.

3.2.3 Avaliação dos riscos

Para definir o tratamento que será dado a um determinado risco e sua relevância, deve-se determinar o seu efeito potencial por meio de ferramentas de avaliação de riscos.

Modelos qualitativos podem ser adotados como, por exemplo, a matriz de riscos, que demonstra os pontos de cruzamento da probabilidade de ocorrência e do impacto dos riscos. Dessa forma, pela divisão da matriz em quadrantes, pode-se avaliar a criticidade dos riscos. Quanto maior for a probabilidade e o impacto de um risco, maior será seu nível de criticidade.

		SEVERIDADE				
		PROBABILIDADE				
		MUITO BAIXA	BAIXA	MÉDIA	ALTA	MUITO ALTA
IMPACTO	MUITO BAIXO	Muito baixo	Muito baixo	Muito baixo	Muito baixo	Baixo
	BAIXO	Muito baixo	Muito baixo	Baixo	Baixo	Médio
	MÉDIO	Muito baixo	Baixo	Médio	Médio	Alto
	ALTO	Muito baixo	Baixo	Médio	Alto	Muito alto
	MUITO ALTO	Baixo	Médio	Alto	Muito alto	Muito alto

Quanto à criticidade, pode-se estipular que:

a) Risco no quadrante vermelho: risco inaceitável, que possui alta probabilidade de ocorrência e que, se ocorrer, poderá resultar em impacto extremamente severo.
b) Risco no quadrante laranja: pode ser tanto um risco provável, com alta probabilidade de ocorrência, mas baixo impacto para a consecução dos objetivos, ou um risco inesperado, com baixa probabilidade de ocorrência, mas alto impacto para a consecução dos objetivos.
c) Risco no quadrante amarelo: risco que deve ser quantificado e monitorado de forma rotineira e sistemática;
d) Risco no quadrante verde: risco que representa pequeno problema e causa pouco prejuízo.

Por meio da construção da matriz de riscos, é possível classificar os riscos em diferentes níveis. O Nível de Risco é um índice calculado pela multiplicação da média dos graus de Probabilidade pela média dos graus de Impacto dos riscos presentes nos processos, projetos, áreas ou organizações. Podem, por exemplo, ser classificados como:

a) Mínimo;
b) Baixo;
c) Moderado;
d) Significativo e;
e) Alto.

As matrizes e indicadores podem ser aplicados sobre os riscos inerentes às operações (sem considerar os controles mitigatórios associados), bem como sobre os riscos residuais (após a consideração dos controles mitigatórios associados).

Em estágios mais maduros dos processos de avaliação dos riscos, modelos estocásticos de quantificação dos riscos podem ser adotados. Tais modelos estimam com determinado nível de confiança o impacto para o conjunto de riscos corporativos identificados e priorizados pela organização. Eles levam em consideração técnicas estatísticas, modelagens atuariais, financeiras e econômicas e processos aleatórios

para estimar os impactos financeiros dos riscos bem como, a avaliação do capital econômico necessário para garantir a solvência da seguradora.

3.2.4 Solvência e capital baseado em riscos

Um processo robusto e em estágio avançado de gestão dos riscos deve produzir estimativas próprias do capital econômico mínimo necessário para garantir a solvência da companhia. Tais resultados são possíveis de serem obtidos por meio da construção de modelos internos de capital, independente das exigências regulatórias vigentes. Enquanto o capital mínimo requerido pelos reguladores reflete o risco médio adotado pelo mercado e não leva em consideração a estrutura societária dos grupos seguradores, ignorando algumas correlações entre negócios, os modelos próprios de capital desenvolvido internamente refletem o capital econômico adequado para a exposição ao risco da companhia, tomando em consideração as definições do apetite a riscos vigente, bem como as correlações entre todos os negócios dentro de um mesmo conglomerado econômico segurador.

3.2.5 Tratamento dos riscos

A definição do tratamento a ser dado aos riscos identificados baseia-se no seu grau de exposição e natureza de risco. Após a avaliação do risco, o tratamento envolve a seleção de uma ou mais opções para tratar os riscos e a posterior implementação de controles ou processos para acompanhá-los.

Para mitigar os riscos, a companhia precisa implantar atividades de controle, as quais compreendem desde as políticas corporativas até os manuais de procedimentos elaborados para assegurar que as diretrizes e os objetivos, definidos para minimizar seus riscos, estejam sendo observados nas atividades executadas.

As respostas a riscos classificam-se nas seguintes categorias:

a) ELIMINAR – descontinuação das atividades que geram riscos.
b) MITIGAR – adoção de medidas para reduzir a probabilidade ou o impacto dos riscos.
c) COMPARTILHAR – redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma parcela do risco.
d) ACEITAR – nenhuma medida é adotada para modificar os níveis de probabilidade ou de impacto dos riscos.

3.2.6 Apetite e Tolerância aos Riscos

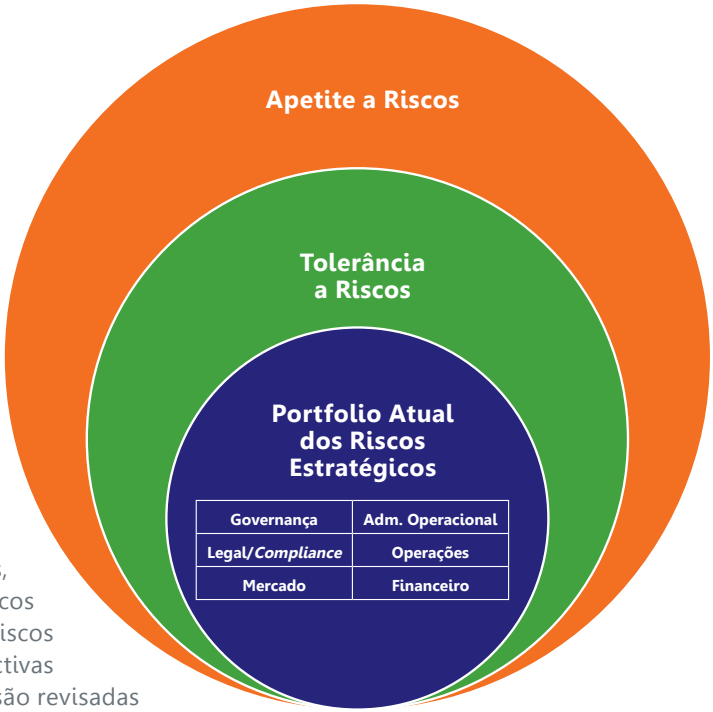
O Apetite ao Risco se refere a quanto de risco que uma organização está disposta a correr para atingir seus objetivos. As declarações do Apetite ao Risco podem ser expressas tanto qualitativa como quantitativamente e geridas em relação a uma iniciativa individual ou agregada.

A Tolerância ao Risco é a quantidade de incerteza que uma organização está preparada para aceitar no total ou de forma mais restrita dentro de uma determinada unidade de negócio, de uma categoria de risco específica ou relacionada a uma determinada iniciativa. Expresso em termos quantitativos que podem ser monitorados (como, por exemplo, solvência, lucro, capacidade de distribuição de dividendos ao longo de um período específico etc.), a Tolerância ao Risco é o percentual do Apetite a Riscos que servirá de alerta para Administração.

O Apetite a Risco da companhia deve estar alinhado com as respectivas estratégias e com o seu Plano de Negócios e refletido nos limites de riscos aceitáveis.

O Apetite a Riscos e a Tolerância a Riscos deverão ser estabelecidos pelo Conselho de Administração, conforme exemplo no gráfico da página seguinte.

A área de Gestão de Riscos deve acompanhar o desempenho dos indicadores de riscos e os seus limites, bem como supervisionar a implementação e manutenção dos planos de ação mediante gestão contínua e avaliações independentes.



As camadas de Apetite a Riscos, Tolerância a Riscos e Portfólio de Riscos e as suas respectivas quantificações são revisadas de acordo com a Política Interna da companhia.

3.2.7 Comunicação

A comunicação deve ser tempestiva e adequada com as partes interessadas, acionistas, reguladores e outros públicos externos. Deve reforçar sempre a cultura de riscos a ser seguida por todos os colaboradores e administradores e as atitudes da organização perante os ambientes externo e interno.

Como visam compartilhar e fornecer informações para o gerenciamento contínuo de riscos, são processos que devem permear por toda a companhia.

3.2.8 Monitoramento

A Administração deve avaliar continuamente a adequação e a eficácia da Gestão de Riscos. A área de Gestão de Riscos, por sua vez, deve acompanhar o desempenho dos indicadores de riscos e os seus limites, bem como supervisionar a implementação e manutenção dos planos de ação mediante gestão contínua e avaliações independentes.

As atividades de gestão de riscos devem ser adequadamente documentadas como forma de evidenciar sua aderência ao modelo de Gestão de Riscos da companhia.

Compliance

Capítulo 4

4.1 A função de *Compliance* – o que é

A palavra *Compliance* vem do verbo em inglês "*to comply*", que significa "cumprir, executar, satisfazer, realizar o que lhe foi imposto", ou seja, *Compliance* é o dever de cumprir, estar em conformidade no que tange à correção das atividades, dos sistemas de informação e das leis e regulamentos oficiais aplicáveis, assim como de políticas e normas internas e institucionais.

Para que seja efetiva a função de *Compliance*, também diretamente relacionada à Governança Corporativa, as companhias devem desenvolver um programa de *Compliance* eficiente, contendo certas diretrizes, como a seguir relacionadas, porém não se limitando a elas se assim o ambiente exigir:

- Estabelecer e aculturar a conduta ética e fomentar os canais de denúncias em todos os níveis da companhia, considerando todas as diretrizes estabelecidas no Código de Ética, inclusive com alcance irrestrito aos terceirizados, sejam eles fornecedores de bens ou prestadores de serviços.
- Disseminação da cultura de avaliação de riscos e da aplicação de um sistema de controles internos por todos os níveis, juntamente com as demais áreas de Controles Internos, de modo a prevenir e detectar a prática de atos em desconformidade com a regulamentação aplicável, assim como as políticas e normas internas e institucionais.
- Programas de treinamento robustos e cíclicos, que alcancem todos os níveis da sociedade, inclusive terceirizados.
- Canais internos de comunicação para reciclagem de temas relevantes e também para contato interno com a sociedade de forma irrestrita e isenta.
- Monitoramento e implementação das demandas regulatórias e demais normativos legais aos quais a companhia esteja submetida, visando ao estrito cumprimento de tais disposições.

A função de *Compliance* deve ser evidenciada pelo apoio visível e inequívoco da alta direção da sociedade. A Circular Susep nº 234/03 impõe a designação específica de um diretor estatutário como responsável pelas funções de *Compliance* e determina a observância das referidas práticas pelos membros da Diretoria e do Conselho de Administração.

O departamento responsável pela avaliação do cumprimento do programa de *Compliance* deve estar subordinado, conforme o caso, ao Conselho de Administração ou à Diretoria da companhia, devendo dispor da independência necessária para o exercício de suas atribuições.
As exigências relacionadas ao *Compliance* e à Governança Corporativa

podem variar conforme o tipo societário adotado pela companhia, o tamanho de sua estrutura e a complexidade de suas operações, segundo legislação aplicável.

De acordo com a ISO 19600 (sistema de gestão de *Compliance*), convém que, trabalhando em conjunto com a direção, a função de *Compliance* seja responsável por:

a) Identificar as obrigações de *Compliance* com o apoio de recursos pertinentes e traduzir essas obrigações em políticas, procedimentos e processos acionáveis.
b) Integrar obrigações de *Compliance* nas políticas, procedimentos e processos existentes.
c) Fornecer ou organizar apoio contínuo de treinamento para os empregados, para assegurar que todos os empregados relevantes sejam treinados regularmente.
d) Promover inclusão da responsabilidade de *Compliance* em descrições de cargos e processos de gestão de desempenho de empregados.
e) Definir um sistema de relatórios de *Compliance* e documentação em vigor.
f) Desenvolver e implementar processos para a gestão da informação, como reclamações e/ou

retroalimentação por meio de linhas diretas, um sistema de comunicação de irregularidades e de outros mecanismos de execução.
g) Estabelecer indicadores de desempenho de *Compliance* e monitorar e medir o desempenho em *Compliance*.
h) Analisar o desempenho para identificar a necessidade de ações corretivas.
i) Identificar riscos de *Compliance* e gestão desses riscos relativos a terceiros, como fornecedores, agentes, distribuidores, consultores e contratados.
j) Assegurar que o sistema de gestão de *Compliance* seja analisado criticamente em intervalos planejados.
k) Assegurar que haja acesso a aconselhamento profissional adequado no estabelecimento, implementação e manutenção do sistema de gestão de *Compliance*.
l) Fornecer aos empregados acesso a recursos sobre os procedimentos e referência de *Compliance*.
m) Fornecer aconselhamento objetivo para a organização sobre assuntos relacionados ao *Compliance*.

4.2 Focos de um Programa de *Compliance*

Um Programa de *Compliance* pode ser entendido como a formalização e abrangência, pela alta direção da companhia, das ações e atividades que a organização desenvolverá em relação aos temas de *Compliance*.

No Brasil, o programa deve também prever mecanismos e procedimentos internos para disseminar a cultura de *Compliance* e vincular as questões inerentes à integridade trazidas pela "Lei Anticorrupção".

As ações para o cumprimento do Programa de *Compliance* devem envolver toda a estrutura da companhia, contando com o apoio das estruturas de *Compliance* e demais áreas de Controles Internos da organização, e devem ser continuamente aprimoradas, à medida que se identifiquem oportunidades de melhorias.

O Programa deve:

- Incentivar a cultura de *Compliance* e levar em consideração a missão, os valores e o Código de Ética da organização.
- Demonstrar as estruturas e mecanismos de controle adotados pela organização para assegurar a integridade e aderência às leis e regulamentos aplicáveis aos seus negócios.
- Demonstrar as ações que visam assegurar a conformidade dos procedimentos adotados diante das exigências externas e normativos internos.
- Abranger toda a companhia e considerar, na sua composição, as avaliações de riscos, as políticas e procedimentos aprovados,

o programa de treinamento e qualificação de funcionários, as ações de comunicação, os controles internos, os canais de denúncias e as auditorias realizadas.

- Instituir ações de prevenção, detecção, remediação e resposta contra atos lesivos praticados em desfavor da sociedade.

A Lei Anticorrupção, regulamentada pelo Decreto nº 8.420/15, reconhece a importância dos programas de *Compliance* e considera atenuante para aplicação de multas a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e aplicação efetiva de Códigos de Ética e de Conduta. Situação que, sem dúvida, constitui importante incentivo para as empresas estruturarem programas de *Compliance*.

Em complementação, o artigo 42 do Decreto nº 8.420/15 elenca os critérios pelos quais o programa de integridade será avaliado quanto a sua existência e aplicação, o que traz parâmetros importantes a serem considerados pelas empresas.

Atenta à relevância do tema, a Controladoria Geral da União (atual Ministério da Transparência, Fiscalização e Controladoria-Geral da União) publicou seu "Programa de Integridade – Diretrizes para Empresas Privadas"[1] , com o objetivo de auxiliar as empresas a construir ou aperfeiçoar seu programa de integridade, considerando cinco pilares:

1º Comprometimento e apoio da alta direção – O apoio da alta direção da empresa é condição indispensável e permanente para o fomento de uma cultura ética e de respeito às leis e para a aplicação efetiva do Programa de Integridade.

2º Instância responsável pelo Programa de Integridade – Qualquer que seja a instância responsável, ela deve ser dotada de autonomia, independência, imparcialidade, recursos materiais, humanos e financeiros para o pleno funcionamento, com possibilidade de acesso direto, quando necessário, ao mais alto corpo decisório da empresa.

3º Análise de perfil e riscos – A empresa deve conhecer seus processos e sua estrutura organizacional, identificar seu Programa de Integridade — visão geral da área de atuação e principais parceiros de negócio —, seu nível de interação com o setor público — nacional ou estrangeiro — e, consequentemente, avaliar os riscos de se ver envolvida em atos lesivos.

4º Estruturação das regras e instrumentos – Com base no conhecimento do perfil e riscos da empresa, deve-se elaborar ou atualizar o Código de Ética ou de Conduta e as regras, políticas e procedimentos de

1. https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf

prevenção de irregularidades; desenvolver mecanismos de detecção ou reportes de irregularidades (alertas ou "bandeiras vermelhas"; canais de denúncia; mecanismos de proteção ao denunciante); definir medidas disciplinares para casos de violação e medidas de remediação. Para uma ampla e efetiva divulgação do Programa de Integridade, deve-se também elaborar plano de comunicação e treinamento com estratégias específicas para os diversos públicos da empresa, inclusive prestadores terceirizados.

5º Estratégias de monitoramento contínuo – É necessário definir procedimentos de verificação da aplicabilidade do Programa de Integridade a operação da empresa e criar mecanismos para que as deficiências encontradas em qualquer área possam realimentar continuamente seu aperfeiçoamento e atualização. É preciso garantir também que o Programa de Integridade seja parte da rotina da empresa e que atue de maneira integrada com outras áreas correlacionadas, tais como: recursos humanos, jurídica, auditoria interna e contábil-financeira.

Além dos parâmetros brasileiros sobre Programa de *Compliance*, há outras diretrizes internacionais que orientam sobre o que se deve observar na proposta de criação e manutenção de tal programa, como: OCDE; *U.S. Federal Sentencing Guidelines*; *FCPA Ressource Guide*; *The Bribery Act 2010 (UKBA): Verification of Anti-corruption Compliance Programs*.

4.2.1 Prevenção à lavagem de dinheiro

Nos termos do art. 9º da Lei 9.613/98 (crimes de "lavagem" ou ocultação de bens, direitos e valores, entre outros), as sociedades seguradoras, dentre outras categorias de empresas, são compelidas a compartilhar com o poder público a tarefa de prevenir a ocorrência dos crimes de lavagem de dinheiro. Assim, são obrigadas a identificar seus clientes, manter registro das transações e informar aos órgãos competentes transações suspeitas.

Há, ainda, regulamento aplicável ao mercado segurador que dispõe sobre

os controles internos específicos para a prevenção e combate dos crimes de lavagem ou ocultação de bens, direitos e valores, ou que com eles possam relacionar-se. O regulamento também dispõe sobre o acompanhamento das operações realizadas e as propostas de operações com pessoas politicamente expostas, bem como a prevenção e coibição do financiamento ao terrorismo, que abrange aspectos como:

a. Estabelecimento de relação de negócios com pessoa politicamente exposta.
b. Adoção de política de prevenção à lavagem de dinheiro.
c. Procedimentos e manutenção de registro.
d. Criação de manuais e comunicação de operações.
e. Treinamento.
f. Programa anual de auditoria interna.
g. Manutenção do cadastro.
h. Dispensa do cumprimento de itens pelo diretor responsável, mediante expressa justificativa baseada em estudo de risco.
i. Comunicação de operações com indícios.

4.2.2 Prevenção contra fraudes

As seguradoras devem manter controles específicos para a prevenção, detecção e resposta a fraudes.

4.2.3 Prevenção à corrupção

A "Lei Anticorrupção", que dispõe sobre a responsabilização objetiva administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, introduz importante mudança ao estimular as empresas a adotarem programas de *Compliance*, podendo, em razão disso, atenuar as possíveis sanções administrativas e/ou judiciais. Seus principais dispositivos são:

1. Punição das pessoas jurídicas por atos lesivos à administração pública que atentem contra o patrimônio público, os princípios da administração pública ou

A implantação de um canal de denúncias é de suma importância para as companhias, dado que permite conhecer e, se for o caso, apurar desvios de conduta.

os compromissos internacionais assumidos pelo Brasil.
2. Responsabilidade objetiva dos atos praticados no interesse ou benefício da empresa.
3. Multas elevadas, com base no faturamento anual.
4. Redução das penas para empresas que tiverem programas Anticorrupção e de *Compliance*.
5. Incentivos às empresas que reportarem voluntariamente o ato lesivo e cooperarem com as investigações.
6. Acordos de Leniência: redução de até 2/3 da multa administrativa.

4.3 Boas Práticas

As boas práticas de negócios fortalecem um programa de *Compliance* eficiente e eficaz. A seguir, exemplos de iniciativas consideradas boas práticas.

4.3.1 Implantação de Canais de Denúncias

A implantação de um canal de denúncias é de suma importância para as companhias, dado que permite conhecer e, se for o caso, apurar desvios de conduta.

Entre as vantagens de se manter um canal ativo, pode-se apontar:

- Combate e prevenção a fraudes e a más práticas.
- Difusão de imagem positiva da organização perante o mercado e a sociedade.
- Segurança e transparência para todas as partes interessadas.
- Identificação, redução e administração dos riscos do negócio.
- Melhora do ambiente de trabalho, aumentando a motivação de todos os colaboradores.
- Fortalecimento dos sistemas de monitoramento e controle.
- Maximização dos lucros por intermédio da redução de custos indesejáveis e incorretos, aumentando a eficiência da gestão dos negócios por meio da colaboração de todos.

É importante que todos os empregados que tenham obrigações de Compliance sejam competentes para desempenhá-las de forma eficaz. Essa competência pode ser obtida de várias formas: por meio de educação, treinamento ou experiência de trabalho.

- Redução do passivo judicial.
- Auxílio no cumprimento de leis e regulamentos.

4.3.2 Comunicação

Os planos de comunicação interna e externa devem incluir:

a) O que comunicar.
b) Quando comunicar.
c) Para quem comunicar.
d) Como comunicar.

A comunicação interna deve assegurar que a mensagem do *Compliance* seja ouvida e compreendida por todos os empregados.

A comunicação externa deve abranger todas as partes interessadas (conselhos de administração, clientes, contratados, fornecedores e investidores). Os métodos utilizados podem ser sites, e-mails, imprensa, relatórios, eventos, entre outros.

4.3.3 Treinamento

É importante que todos os empregados que tenham obrigações de *Compliance* sejam competentes para desempenhá-las de forma eficaz. Essa competência pode ser obtida de várias formas: por meio de educação, treinamento ou experiência de trabalho.

O programa de treinamento deve assegurar que todos os empregados tenham competência para executar suas atividades. A ISO 19600 orienta

que a educação e o treinamento dos empregados sejam:

a) Adaptados às obrigações e riscos de *Compliance* relacionados com os papéis e responsabilidades do empregado.
b) Se for o caso, com base na avaliação de lacunas no conhecimento e competência dos empregados.
c) Realizados por ocasião da elaboração da missão da companhia e permanentemente atualizados.
d) Alinhados ao programa de treinamento corporativo e incorporados em planos de treinamentos anuais.
e) Práticos e facilmente compreensíveis pelos empregados.
f) Relevantes para o trabalho do dia a dia dos empregados e ilustrativos da indústria, organização ou setor.
g) Suficientemente flexíveis para levar em consideração uma série de técnicas para satisfazer às diferentes necessidades das organizações e dos empregados.
h) Avaliados quanto à eficácia.
i) Atualizados conforme a necessidade.
j) Registrados e retidos.

4.3.4 Avaliações de Risco

O risco de *Compliance* pode ser caracterizado pela probabilidade de ocorrência e pelas consequências do não cumprimento com as obrigações de *Compliance* da organização.

A ISO 19600 enfatiza que a extensão e o nível de detalhes da avaliação do risco de *Compliance* dependem da situação de risco, do contexto, do porte e dos objetivos da organização.

4.3.5 ISO 37001

A norma ISO 37001, publicada em outubro de 2016, surgiu após a implementação de diversos normativos relativos à anticorrupção pelo mundo e seu objetivo é padronizar os Sistemas de Gestão Antissuborno, criando um modelo de integridade, transparência e conformidade para as organizações.

Apesar de ainda não ter força de lei, é considerado como um mecanismo de boas práticas na implementação de medidas eficazes de prevenção à corrupção com origem em uma renomada instituição global, reconhecendo a participação de organizações da sociedade e, principalmente, de empresas, no combate a essa prática.

4.4 Benefícios de um Programa de *Compliance*

A adoção de um Programa de *Compliance* revela-se importante ferramenta de controle interno da gestão dos negócios. É suporte fundamental das boas práticas de Governança Corporativa e sua adoção demonstra o comprometimento da empresa com o fortalecimento dos seus negócios em bases sólidas, éticas e sustentáveis.

Compliance, especialmente no que coopera com a boa Governança Corporativa, contribui para aumentar o valor das sociedades e assegurar sua perenidade, finalidades estas que constituem a própria razão de ser dos princípios de governança.

A importância da avaliação da conformidade dos procedimentos – *Compliance* – nas sociedades está em assegurar, com razoável grau de certeza, a aderência das práticas em uso às leis, regulamentos, especificações técnicas, políticas organizacionais, planos, instruções normativas, manuais, contratos etc.

Os benefícios e o valor agregado das boas práticas de *Compliance* são representados em aspectos quantitativos e qualitativos. Entre estes, se destacam:

- Redução de custos e de perdas mediante a identificação de deficiências e a implementação de correções com vistas a mitigar riscos que interferem diretamente no resultado financeiro do negócio.
- Melhora da gestão do caixa da companhia: estudos referentes ao valor agregado pelo *Compliance* indicam que para cada US$ 1.00 gasto em *Compliance* obtém-se economia de US$ 5.00 porque se evitam custos com processos judiciais, danos à reputação e perda de produtividade.
- Aprimoramento do relacionamento com o órgão regulador, permitindo o aperfeiçoamento da regulamentação, maior clareza e eficácia na aderência pelas sociedades e incremento da qualidade das decisões, que passam a ser embasadas e protegidas do ponto de vista regulatório.
- Melhoria na competitividade das sociedades que, ao atuarem em ambientes em conformidade com os regulamentos e com as melhores práticas, obtêm valorização de sua marca e apresentam maior resistência a crises de mercado.
- Melhoria da sensibilidade na gestão a respeito de incertezas e de qualquer indício de oportunidade ou ameaça a ser tratada.

Vale ressaltar, por outro lado, que a não adoção de um Programa de *Compliance* eficiente pode trazer consequências negativas à sociedade, tais como:

- Danos à marca e à imagem.
- Sanções administrativas e pecuniárias a pessoas a ela relacionada(s) ou a ela própria, como, por exemplo, multas, impedimento aos executivos de atuar no mercado e cassação da licença de funcionamento da empresa.
- Custos secundários como os de processos judiciais, tempo de funcionários e executivos etc.

A importância da avaliação da conformidade dos procedimentos – Compliance – nas sociedades está em assegurar, com razoável grau de certeza, a aderência das práticas em uso às leis, regulamentos, especificações técnicas, políticas organizacionais, planos, instruções normativas, manuais, contratos etc.

Conclusão

Capítulo 5

Governança, Risco e Compliance são conceitos complementares que, tratados de forma combinada, agregam valor superior à mera existência isolada das três práticas. No mercado de seguros, os componentes do GRC começaram a representar um marco regulatório elaborado pela Susep a partir da publicação da Circular Susep nº 249/04, que foi complementada pelas Circulares Susep nºs 344/07, 380/08, e 445/12, precedendo o desenho da Circular Susep nº 521/15, que trata da implantação da Estrutura de Gestão de Riscos. O apoio da alta administração é fundamental para a implantação das melhores práticas de GRC, conferindo robustez ao conjunto de disciplinas para cumprir normas legais e regulamentares, políticas e diretrizes estabelecidas para o negócio e para as atividades de uma empresa.

O apoio da alta administração é fundamental para a implantação das melhores práticas de GRC, conferindo robustez ao conjunto de disciplinas para cumprir normas legais e regulamentares, políticas e diretrizes estabelecidas para o negócio e para as atividades de uma empresa.

Glossário

Capítulo 6

Acordo de Basileia: Acordo estabelecido pelo Comitê de Supervisão Bancária da Basileia, ligado ao *Bank for International Settlements*, que trata de exigências de capital para instituições financeiras. Existem três acordos de Basileia: Basileia I (1988), Basileia II (2004) e Basileia III (2010).

ANS: Agência Nacional de Saúde Suplementar.

COSO: *Committee of Sponsoring Organizations of the Treadway Commission*. O COSO é uma iniciativa do setor privado que estabeleceu um modelo comum de controle interno, contra o qual as empresas e organizações podem avaliar os seus sistemas próprios de controle, e está empenhado em melhorar o desempenho e governança das organizações.

IBGC: Instituto Brasileiro de Governança Corporativa. O instituto é uma grande referência e um promovedor da discussão dos temas relacionados ao tema de Governança Corporativa;

IIA: *The Institute of Internal Auditors*. Associação profissional internacional que desenvolve a condição profissional de auditoria interna, além de disseminar o conhecimento a respeito de riscos, controles, auditoria e governança.

ISO: *International Organization for Standardization* (Organização Internacional de Normalização).

ISO 31.000: Norma com princípios gerais de gestão de risco elaborada pela *International Organization for Standardization*.

ISO 37.001: Norma com requisitos para uma elaboração de um Sistema de Gestão Antissuborno elaborada pela *International Organization for Standardization*.

OCDE: Organização para a Cooperação e Desenvolvimento Econômico. É uma organização internacional, composta por 34 países e com sede em Paris, França. A OCDE tem por objetivo promover políticas que visem ao desenvolvimento econômico e ao bem-estar social de pessoas por todo o mundo.

Solvência II: Diretrizes aprovadas, em 2007, pelo Parlamento Europeu que visam estabelecer uma metodologia de apuração da necessidade mínima de capital mais sensível ao risco.

SOX: Lei americana Sarbanes-Oxley formulada, em 2002, como resposta a diversos casos de fraude corporativa, sendo o principal motivador o caso da Enron.

Susep: Superintendência de Seguros Privados.

Nossa missão

é congregar as lideranças do setor segurador, elaborar o planejamento estratégico do setor, colaborar para o aperfeiçoamento da regulação, coordenar ações institucionais e representar as associadas junto a autoridades e entidades nacionais e internacionais.

O seguro

tem importante papel na economia e na sociedade brasileira. Ele contribui significativamente para o desenvolvimento da infraestrutura, a geração de renda e o acesso à Saúde Suplementar no País.

Promover

maior integração de todos os participantes do mercado segurador: líderes pensando juntos, empresas compartilhando experiências, proximidade dos órgãos reguladores, consumidores e sociedade em geral, para a construção de uma agenda que favoreça a expansão do seguro e seu crescimento sustentável.

CNseg
Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização

Autoria

– Comissão de Controles Internos da CNseg.
– Comissão de Gestão de Riscos da CNseg.
– Superintendência de Acompanhamento Técnico da CNseg.

Federações filiadas à CNseg

FenSeg
Federação Nacional de Seguros Gerais

FenaPrevi
Federação Nacional de Previdência Privada e Vida

FenaSaúde
Federação Nacional de Saúde Suplementar

FenaCap
Federação Nacional de Capitalização

Rio de Janeiro
Rua Senador Dantas, 74 - 16 andar
Centro | CEP 20031-205
Tel. 21 2510-7777

Brasília
SCN Quadra 1 bl.C
Brasília Trade Center, salas 1601 a 1612
Brasília | CEP 70711-902
Tel. 61 3424-9337 | Fax 61 3328-1904

Projeto gráfico
APPROACH COMUNICAÇÃO

PROGRAMA

EDUCAÇÃO EM SEGUROS

www.cnseg.org.br

APPROACH COMUNICAÇÃO

CNseg

Confederação Nacional das Empresas de Seguros Gerais, Previdência Privada e Vida, Saúde Suplementar e Capitalização