REVISTA Contabilidade & Inovação
Revista Contabilidade & Inovação | UFG | ISSN: 2764-3336 DOI: 10.5600/rci.v1i1.71870

Os Programas de *Compliance*: como a Análise de Dados e a Gestão de Riscos atuam no Desenvolvimento das Organizações

Compliance Programs: how Data Analysis and Risk Management work in the Development of Organizations

Programas de Compliance: cómo funcionan el Análisis de Datos y la Gestión de Riesgos en el Desarrollo de las Organizaciones

Calígena Batista de Paiva Silva
Universidade Federal do Rio Grande do Norte, UFRN, Brasil.

Liliana Bastos Pereira Santo de Azevedo Rodrigues
Faculdade de Direito da Universidade de Coimbra, FDUC, Portugal.

RESUMO

O *Compliance* abrange um conjunto de procedimentos com o objetivo de preservar a credibilidade da organização no mercado, através do chamado Programa de *Compliance*. Esses procedimentos concretizam-se através de uma prévia análise de dados, que será convertida em uma posterior avaliação de riscos para implementação de mecanismos de prevenção e mitigação de desvios de conduta empresarial. Assim, para discorrer sobre como atua uma análise de dados eficiente como procedimento prévio para uma gestão de riscos nos programas de *Compliance* das organizações, o trabalho se vale da pesquisa bibliográfica e documental a fim de aprimorar a compreensão do leitor acerca do conceito e relevância prática do *Compliance* e de seus programas, abordando os principais pilares necessários para um efetivo suporte gerencial às organizações. Tratamos, também, da análise de dados e da gestão de riscos dentro dos programas de *Compliance*, apontando alguns de seus documentos base, concluindo pela sua fundamental importância como suporte para a tomada de decisões estratégicas e do gerenciamento das empresas, consolidando o aumento do valor de mercado da organização

Palavras-chave: *Compliance*; Gestão de Riscos; Risco; Análise de Dados; Prevenção e mitigação de Riscos.

ABSTRACT

Compliance encompasses a set of procedures with the objective of preserving the organization's credibility in the market, through the so-called Compliance Program. These programs are implemented through a prior analysis of data, which will be converted into a subsequent risk assessment for the implementation of mechanisms for the prevention and mitigation of business misconduct. Thus, we start from the premise: how does an efficient data analysis act as a prior procedure for risk management in organizations' Compliance programs?. The work uses bibliographic and documentary research to improve the reader's understanding of the concept and practical relevance of Compliance and Compliance programs, addressing the main pillars necessary for effective managerial support to organizations. Thus, we also deal with data analysis and risk management within the Compliance programs, pointing out some of its base documents, concluding for its fundamental importance as a support for strategic decision-making and the management of companies, consolidating the increase in the value of organization's market.

Keywords: Compliance; Risk management; Risk; Data analysis; Risk Prevention and Mitigation.

ABSTRACTO

Objetivo de preservar la credibilidad de la organización en el mercado, a través del denominado Programa de Cumplimiento. Estos programas se implementan a través de un análisis previo de datos, que se convertirá en una evaluación de riesgos posterior para la implementación de mecanismos para la prevención y mitigación de conductas comerciales indebidas. Así, partimos de la premisa: ¿Cómo actúa un análisis de datos eficiente como procedimiento previo para la gestión de riesgos en los programas de Cumplimiento de las organizaciones? El trabajo utiliza la investigación bibliográfica y documental para mejorar la

comprensión del lector sobre el concepto y la relevancia práctica de los programas de Cumplimiento y Cumplimiento, abordando los principales pilares necesarios para el apoyo gerencial efectivo a las organizaciones. Así, también abordamos el análisis de datos y la gestión de riesgos dentro de los programas de Cumplimiento, señalando algunos de sus documentos base, concluyendo por su fundamental importancia como soporte para la toma de decisiones estratégicas y la gestión de las empresas, consolidando el incremento del valor de mercado de la organización.

Palabras clave: *Compliance*; Gestión de riesgos; Riesgo; Análisis de datos; Prevención y Mitigación de Riesgos.

Artigo apresentado no I Concurso de Artigos Científicos da Controladoria Geral do Estado de Goiás

Data de submissão: 16/02/2022

Data de aprovação: 01/06/2022

Introdução

O compliance surgiu na década de 50, nos Estados Unidos da América, na sequência de novas imposições regulamentares impostas às instituições financeiras, no âmbito de políticas públicas criadas para combater o tráfico de drogas e a lavagem de dinheiro (Block, 2017). Com efeito, as referidas instituições implementaram novos funcionários com a função de acompanhar e cumprir as novas regras dentro das organizações (Coimbra, 2010). Na década seguinte, rapidamente se estendeu às funções destes profissionais a efetiva gestão de riscos, com o propósito de analisar situações que pudessem fragilizar a imagem destas organizações para o seu público alvo. Conta a história que foi com essa ampliação que surgiu, pela primeira vez, o conceito de *compliance officer*, como o profissional responsável por garantir o cumprimento normativo imposto às organizações, realizar um gerenciamento de riscos eficaz e, consequentemente, garantir a credibilidade no mercado (Block, 2017).

A amplitude do conceito tornou necessário o desenvolvimento de verdadeiros programas capazes de implementar na prática toda a responsabilidade que esses profissionais assumiram. Como área interdisciplinar, cujo conceito inicial foi importado da economia, mas rapidamente se estendeu a outras áreas como a gestão, administração e o direito, foi necessário organizar uma equipe de profissionais que pudessem assumir a diversidade de funções assumidas (Block, 2017). Afinal, para o cumprimento normativo e a implementação de uma gestão de riscos eficaz, vários procedimentos são necessários para que se possa obter os benefícios almejados.

Os programas de *compliance* são criados sem que exista um modelo específico, uma vez que eles precisam, em primeiro lugar, adaptar-se às características das organizações onde são implementados (Zenkner, 2019). Esse, inclusive, é o ponto de partida para a estruturação das especificidades necessárias a serem implementadas. Na sequência, são identificados alguns

pilares fundamentais que, apesar de variarem na sua forma de implementação, seguem um critério geral comum a todos esses programas (Benedetti, 2014).

Inicialmente, a organização precisa dar o suporte ao programa para que os *compliance officers* tenham uma certa autonomia para a execução e tomada de decisões estratégicas. Apesar de não se fazerem substituir à alta administração de uma organização, esses profissionais acompanham todo o gerenciamento sugerindo os melhores caminhos a serem trilhados. Na sequência, para o cumprimento da regulamentação imposta, outros procedimentos são implementados, a exemplo da criação de um código de ética e de conduta próprios que devem ser divulgados para o público interno e externo.

O treinamento e comunicação referente às novidades implementadas deve ser constante, possibilitando a todos os intervenientes acompanharem e participarem ativamente na execução dos programas. A implementação de um canal de comunicação é igualmente importante, para aproximar as partes e possibilitar um canal direto para o envio de denúncias e irregularidades. Com a criação destes instrumentos, deve ser incluído um procedimento específico de investigação, com o propósito de averiguar e punir, se necessário, as denúncias que foram recebidas.

A *due diligence* é um procedimento de coleta de informações prévias, que deve ser realizado com o objetivo de auxiliar na tomada de decisões na organização. Essas informações auxiliam o levantamento de riscos e, na sequência, possibilitam que seja realizada na sequência a avaliação de riscos. Esses riscos são um dos fatores mais sensíveis no âmbito de qualquer organização e também de qualquer programa implementado. Eles devem ser identificados e trabalhados para que possam ser criados mecanismos internos de prevenção ou mitigação dos impactos não desejados. Por fim, os programas devem ser alvo de constante monitoramento para aperfeiçoamento e uma maior eficiência dos serviços prestados (Bertoccelli, 2019).

O objetivo geral deste trabalho consiste em demonstrar se é possível integrar uma análise de dados eficiente como procedimento prévio para uma gestão de riscos nos programas de *compliance* das organizações.

Quanto aos objetivos específicos, tem-se em análise os seguintes: i) revisar a base bibliográfica da implementação dos programas de *compliance*, investigando as suas principais características; ii) conceituar risco e a gestão de riscos de forma a poder criar uma avaliação eficiente e os procedimentos necessários para a prevenção e mitigação dos riscos; e iii) adoção de parâmetros necessários através de uma prévia análise de dados, que será enquadrada como parâmetro no processo de gestão de riscos.

O trabalho foi estruturado da seguinte forma. Em um primeiro momento, apresentamos ao leitor o conceito e relevância prática do *compliance* e dos programas de *compliance*, abordando os principais pilares necessários para um efetivo suporte gerencial às organizações. Referimos os requisitos mínimos de um programa efetivo, dando ênfase ao grande diferencial destes programas, qual seja, o gerenciamento de riscos. Apesar de, tradicionalmente, este conceito estar relacionado ao cumprimento normativo, atualmente a doutrina é unânime na relevância que um processo de gestão de riscos agrega às organizações (Paula, 2018).

Tendo esse ponto de partida, damos sequência ao conceito de risco, gestão de riscos e procedimentos de prevenção e mitigação de riscos. Dependendo do apetite de risco de cada organização, qualquer desvio em relação ao que se espera, seja positivo ou negativo, deve ser identificado para auxiliar na estratégia de negócio, resultando na identificação de oportunidades ou ameaças institucionais. Abordamos algumas das principais referências nacionais e internacionais de padronização de sistemas de gerenciamento de riscos para que possamos compreender como funciona o processo de identificação, análise e tratamento de riscos.

Por fim, identificamos processos que permitem facilitar a análise de dados para estabelecer previamente os riscos e dar início à fase de gestão de riscos. A documentação e catalogação de dados servirá de norte para coleta de

informações relevantes, uma vez que serão analisados para um melhor funcionamento da organização com informações importantes para a gestão de riscos.

Para que essa análise seja implementada, é necessário ainda que haja segurança com relação ao uso dos dados, através da aplicação das regras sobre proteção de dados – Lei Geral de Proteção de Dados – respeitando o cumprimento normativo que os programas de *compliance* pretendem alcançar.

Os Programas de *Compliance*

Com foco no âmbito empresarial, o trabalho irá tratar o Compliance e seu conceito sob essa óptica. Assim, tem-se que o conceito de Compliance surgiu pela primeira vez nas instituições financeiras com o principal objetivo de auxiliar o cumprimento da regulamentação interna e logo se tornou um requisito regulatório (Rodrigues, 2020a). De acordo com Benedetti (2014), outros setores como a indústria farmacêutica ou de telecomunicações aderiram a esse conceito.

Atualmente, o compliance é aplicado nas mais diversas áreas de atuação, inclusive em empresas de capital aberto e fechado, entidades do terceiro setor e órgãos públicos, espalhando-se por todo o mundo.

O compliance provém da economia e foi introduzido em áreas como o direito, gestão e administração, representando um conjunto de esforços, com uma dinâmica interdisciplinar, significando a conformidade com normas legais e regulamentares, não necessariamente de origem jurídica (Block, 2017). Coimbra (2010) afirma que um dos principais pontos de atuação é evitar ou mitigar os riscos inerentes à sua área de atuação, visando com isso preservar a imagem da organização perante os seus clientes e sociedade. Através de um programa de compliance efetivo, as organizações terão um forte papel no combate ao crime, fraude e corrupção, aumentando a sua competitividade no mercado.

Os programas de compliance efetivam-se através de procedimentos específicos que podem ser concretizados através dos seguintes pilares fundamentais: i) suporte da alta administração; ii) implementação de código de ética e de conduta; iii) comunicação e treinamento; iv) canal de comunicação; v) meios de investigação; vi) gestão de riscos; vii) procedimentos internos; viii) due diligence; e ix) auditoria e monitoramento.

Em suma, Rodrigues (2020b) conceitua o termo como "um conjunto de ferramentas capazes de melhorar a gestão de uma organização, cumprindo as leis que lhe são impostas, fazendo um gerenciamento de riscos eficaz e preservando a sua credibilidade perante os seus stakeholders." Na sequência, continua a autora, o programa de compliance pode ser materializado através da disseminação de uma cultura mais íntegra, um modo de ser, de atuar, uma ideologia a ser incorporada numa organização. Marcelo Zenkner (2019) defende que "a integridade implica a exata correspondência entre os relevantes valores morais e a realização desses valores no momento em que, diante das situações-problema do dia a dia, uma escolha é reclamada a fim de que uma ação ou omissão sejam realizadas."

O *Compliance* é voltado para as técnicas de concretização da missão, visão e ainda para os valores das organizações, envolvendo uma estratégia para padronizar o seu comportamento, com foco no desenvolvimento econômico e na integridade da instituição. Trata-se de "um conjunto de regras, padrões, procedimentos éticos e legais, que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como a atitude dos seus funcionários" (Candeloro, Rizzo & Pinho, 2012, p. 30).

Portanto, o programa de Compliance objetiva assegurar, juntamente com as equipes dos setores das empresas em que irá atuar, que o sistema de diretrizes, leis e regulamentos da instituição seja fortalecido, com maior controle nos processos para mitigar os riscos das práticas de atuação. Leal (2019, p. 2) aponta que a gestão de riscos se trata do "processo de identificar, analisar, avaliar, monitorar, tratar, comunicar" os riscos. Além disso, as

instituições devem "estabelecer protocolos para tratá-los ou até mesmo definir ações para minimizá-los", para que assim se possa fazer com que os riscos das organizações se tornem menores.

A definição de Compliance, seus objetivos e forma de implantação podem ser extraídos de documentos e regras formatados por diversos órgãos internacionais voltados para determinado ramo de atuação ou ainda por analogia, como mostram Ribeiro e Diniz (2015) em seu trabalho acerca do Compliance e Lei Anticorrupção nas empresas.

Nesse sentido, de acordo com Ribeiro e Diniz (2015) e ainda com Candeloro, Rizzo e Pinho (2012), de forma não taxativa, tem-se que entre esses órgãos estão

> o Bank for Internacional Settlements – BIS, o Comitê de Supervisão Bancária da Basiléia, o Acordo da Basiléia I – 1998, o Acordo da Basiléia II – 2004, o Acordo da Basiléia III – 2010, o Fundo Monetário Internacional – FMI, o Grupo de Ação Financeira Internacional – GAFI, a International Organization of Securities Commissions – IOSCO, The Committee of Sponsoring Organizations of the Treadway Commission – COSO, o Wolfsberg Group, The Egmont Group of Financial Intelligence Units, a Convenção das Nações Unidas contra a Corrupção, a Convenção Interamericana contra a Corrupção e a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais (Candeloro & Rizzo, 2012, p. 343-347).

Ademais, não somente no âmbito internacional existem órgãos reguladores, pois o Brasil também adota regras semelhantes, por exemplo

> o Banco Central do Brasil (em especial as Circulares nos 3.461 e 3.462 de 24 de julho de 2009), a Comissão de Valores Mobiliários – CVM, a Superintendência Nacional de Previdência Complementar – Previc, a Superintendência de Seguros Privados – Susep; bem como nos órgãos autorreguladores, como a BM&FBovespa Supervisão de Mercados – BSM, a Cetip S.A. Balcão Organizativo de Ativos e Derivativos, a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – Anbima e a Associação dos Analistas e Profissionais de Investimento

> do Mercado de Capitais – Apimec, além da Lei no 9.613/1998 e da Lei no 12.846/2013 (Lei Anticorrupção Empresarial) (Candeloro & Rizzo, 2012, p. 342).

Assim, o cumprimento das regras estabelecidas com o Compliance se alinha com a proteção das empresas, indo de acordo com as exigências e orientações internacionais e nacionais com relação à adoção de práticas para combater ainda os riscos que podem levar ao descumprimento das regras vigentes. Ou seja, a gestão de riscos é um fator que irá influenciar diretamente o trabalho do Compliance, facilitando sua implementação, evitando maiores danos à empresa. Gerir os riscos proporciona um equilíbrio entre as metas que são almejadas pela organização e os perigos que podem ser encontrados ao longo do percurso, conectando a gestão e o Compliance, assim como afirmam Neves e Figueiroa (2019).

Conceito de risco e gestão de riscos

Existem diversos tipos de riscos. De acordo com a norma internacional que trata sobre a gestão de riscos, International Organization for Standardization (ISO) 31000:2018, chama- se risco o efeito de incerteza causado sobre os objetivos da organização, um desvio com relação ao que se espera, podendo ser ele negativo ou positivo, e até mesmo ambos, criando ou resultando em oportunidades e ainda ameaças à organização.

Os riscos podem englobar diversas áreas, embora cada empresa tenha o seu modo de operação. Na Tabela abaixo trazemos os principais riscos que podem ser encontrados nas empresas, de acordo com Azevedo et al., (2017), em seu artigo sobre o compliance e a gestão de riscos nos processos organizacionais.

Tabela 1.
Principais riscos empresariais

Riscos	Descrição
Riscos estratégicos	Englobam a capacidade para lidar com os objetivos estabelecidos.

Riscos	Descrição
Riscos de conformidade	São referentes ao não atendimento às legislações vigentes, que afetam diretamente as atividades da organização.
Riscos financeiros	Sucedem devido à má gestão com aplicações equivocadas dos recursos disponíveis em operações.
Riscos na gestão de pessoas	Ocorrem com a desarticulação na estratégia da empresa de estimular os funcionários no cumprimento da missão.
Riscos ambientais	Com a ineficiência no atendimento das demandas e exigências da responsabilidade corporativa com relação ao meio ambiente.
Riscos de tecnologia de informação e telecomunicações	Se dão pela falta de investimentos que pode acarretar diversos prejuízos.
Riscos operacionais	Decorrem da falta de treinamento e disseminação equivocada das políticas da empresa.
Riscos estratégicos	Englobam a capacidade para lidar com os objetivos estabelecidos.

Fonte: Os autores, baseado em dados do IPEA (2015)

E, além dos riscos já citados por Azevedo et al. (2017), em estudo desenvolvido pela KPMG no ano de 2019, a Pesquisa Maturidade do Compliance no Brasil: 4ª Edição, aponta que entre os riscos mais relevantes detectados, os principais são: Riscos na gestão de contratos e de terceiros (82%); Riscos trabalhistas, segurança do trabalho, previdenciários e tributários (82%); e Riscos concorrenciais, de informação privilegiada e conflito de interesses (79%).

A gestão de riscos é uma atividade que se dá de forma progressiva e deve ser realizada por profissionais confiáveis. Ademais, esta deve ser capaz de identificar possíveis falhas e quais são os impactos que elas poderão proporcionar à empresa (Nunes, 2018). Isto se faz necessário devido à importância de se conhecer tanto as situações do mercado, como também as necessidades da própria instituição.

Pode-se afirmar que "a gestão dos riscos preserva a imagem corporativa interna e externa, diminui a probabilidade de fraudes internas, gera ambiente mais seguro e ético e aumenta a eficácia das organizações" (Santos, 2011, p.

12). Partindo disso, o artigo se desenvolve para demonstrar um pouco da importância de implementar a gestão de riscos nas organizações.

Leal (2019) aponta que a gestão de riscos pode ser vista como o processo estruturante que pode ser utilizado para mitigar os efeitos dos riscos, ou também como um processo proativo para apoiar a tomada de decisão, ou seja, antecipar e minimizar as possíveis consequências de eventos futuros, através da identificação, análise, avaliação e planejamento para monitorar e controlar os riscos. O autor afirma ainda que esse processo faz o desenvolvimento de atividades complexas e multifuncionais e o desenvolvimento de projetos tenham mais probabilidades de sucesso.

Chega-se, afinal, à indagação "como ocorre a gestão de riscos?". Azevedo et al., (2017) explicam que,

> A gestão de riscos corporativos é um processo conduzido em uma organização pelo Conselho de Administração, diretoria e demais empregados, para estabelecer estratégias, formuladas para identificar em toda a organização eventos em potencial capazes de afetá-la, e administrar os riscos, de modo a mantê-los compatíveis com o apetite de risco da organização, e possibilitar garantia razoável do cumprimento de seus objetivos (Azevedo et al., 2017, p. 8).

Desse modo, a gestão de riscos traz estratégias formuladas para identificar e tratar os eventos que poderão trazer consequências para a empresa de modo a ter impacto contrário aos seus objetivos, isto é, a gestão de riscos cria estratégias para administrar os riscos, fazendo com que não ultrapassem os limites aceitáveis para a empresa. As estratégias irão trazer a boa administração dos riscos, possibilitando que a empresa cumpra a sua missão, preservando a sua integridade.

O que é a Análise de Dados

A análise de dados é um processo por meio do qual se faz uma observação minuciosa do contexto em que a instituição está inserida, para que se possa calcular o impacto que possíveis falhas podem causá-la. Esse recurso faz-se

importante por proporcionar a possibilidade de antecipar desafios, usando a tecnologia para buscar informações internas sobre os processos realizados nas empresas (Maestri, 2020).

Nesse processo, encontra-se o Due Diligence, que avalia a reputação de potenciais parceiros e colaboradores que podem ter participação em casos de corrupção. Este é realizado por meio da execução aprofundada da análise dos dados coletados durante a observação das informações internas da empresa e é tido como um dos parâmetros para a mitigação dos riscos. A análise da reputação dos potenciais parceiros e colaboradores é realizada pelo fato de que "é fundamental que as empresas tomem precauções necessárias para garantir que tenham relações com parceiros idôneos" (Ayres, 2016).

A fase da análise de dados se dá, geralmente, antes de iniciar a fase da gestão de riscos, pois é quando o profissional de compliance irá iniciar os estudos sobre a empresa, para, assim, definir quais os possíveis riscos que podem atingir a empresa e quais soluções podem ser aplicadas para mitigá-los e até resolvê-los. Como afirmam Sibille e Serpa (2016),

> É muito importante que antes de se falar em avaliação de riscos, se conheça os objetivos de sua empresa e do seu programa de compliance, pois este pilar é uma das bases do sucesso do programa de compliance, uma vez que o código de conduta, as políticas e os esforços de monitoramento deverão ser construídos com base nos riscos que forem identificados como relevantes durante esta fase de análise. A efetiva condução de uma análise de riscos envolve uma fase de planejamento, entrevistas, documentação e catalogação de dados, análise de dados e estabelecimento de medidas de remediação necessárias. (Sibille & Serpa, 2016, p. 06)

Dessa forma, a análise de dados se faz fundamental para estabelecer os riscos e dar início à fase de gestão de riscos. A documentação e catalogação de dados, como, por exemplo, os dados sobre os procedimentos internos existentes na empresa, servirá de norte para a análise de quais deles poderão ser relevantes para o aprimoramento da empresa, visto que eles serão

analisados para melhorar o funcionamento dela, trazendo informações úteis para a gestão de riscos.

A análise de dados nem sempre irá realmente fazer essas previsões de riscos, pois ela tem mais de uma abordagem. Ela pode ser, por exemplo, apenas descritiva e contar o que aconteceu durante o histórico da empresa, não levantando realmente quais riscos ela pode correr.

Assim, a análise pode ser descritiva (descrevendo situações e buscando explicar o que aconteceu), prescritiva (tendo como propósito direcionar gestores até ações específicas), preditiva (buscando fazer uma previsão do que poderá acontecer utilizando dados passados), ou ainda diagnóstica (visando explicar o motivo por trás de alguma alteração inesperada na empresa).

Metodologia

De acordo com Gerhardt e Silveira (2009), a pesquisa qualitativa se preocupa com o aprofundamento da compreensão de um grupo social, de uma organização, etc., sobre um determinado tema, buscando explicar o porquê das coisas, sendo as principais características desse tipo de pesquisa ações de descrever, compreender e explicar alguns fenômenos. Sob essa perspectiva, esse trabalho buscou compreender e explicar como a análise de dados e gestão de riscos contribuem para o desenvolvimento organizacional.

Desse modo, trata-se de uma pesquisa de abordagem qualitativa e de natureza básica, pois se preocupa com a compreensão do público acerca do tema em questão e não envolve necessariamente uma aplicação prática.

Quanto aos procedimentos utilizados, foram aplicadas a pesquisa bibliográfica e a pesquisa documental, através de uma busca ativa em livros, artigos e documentos oficiais que abordam os temas discutidos, como o Decreto Regulamentador Federal n.º 8.420/2015, a norma internacional de gestão de riscos chamada "*International Organization for Standardization*"

(ISO) 31000:2018 e ainda o livro "Manual de *Compliance*", que aborda temas como a gestão de riscos, canal de denúncias e análise de dados.

Gestão de Riscos nas Organizações

A gestão de riscos se dá por meio de um processo contínuo, que deve começar desde a alta administração da instituição, apoiando os processos e dando exemplo de ética e organização, para que os demais funcionários tenham um espelho de como devem atuar. O processo de gestão de riscos se inicia após a definição de quais riscos a empresa está sujeita e, segundo Leal (2019), esse processo varia dependendo das normas que os definem, possuindo diferentes abordagens e padrões, além de passos diversificados.

As principais abordagens são as do padrão do Institute of Risk Management (IRM), o padrão internacional de 2009, *International Organization for Standardization* (ISO) 31000:2018, atualizado em 2018, e o British Standard (BS) 31100. Todos os processos envolvem pelo menos três passos entre "definição de escopo, contextos e critérios; identificação de riscos; análise de riscos; avaliação de riscos; tratamento dos riscos; monitoramento e análise crítica dos riscos; comunicação e consulta aos riscos" (Leal, 2019, p. 32).

De modo geral, mesmo que variem, os passos são estruturados para identificar, analisar, avaliar e definir um tratamento para os riscos. A seguir, na Figura 1, é apresentado o esquema adaptado dos passos adotados pela ISO 31000:2018 para o processo de gestão de riscos.

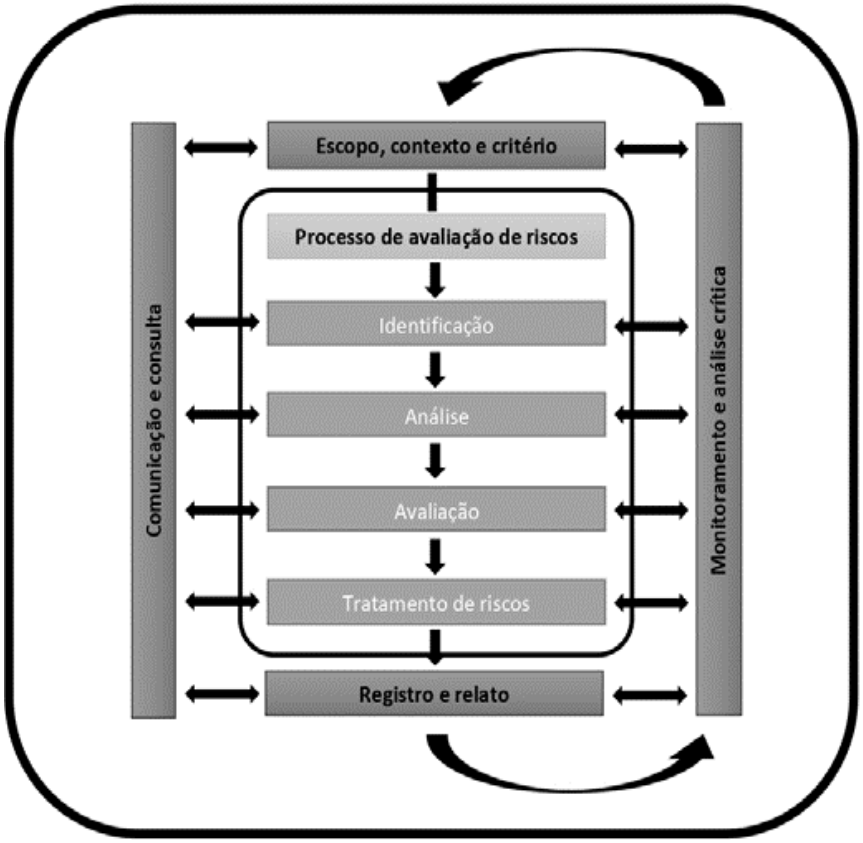

Figura 1: Processo de Gestão de Riscos.

Fonte: Adaptado da ISO 31000:2018

Em geral, a ISO 31000:2018 define o processo de avaliação de riscos nas três etapas mostradas no esquema acima: i) escopo, contexto e critério; ii) registro e relato; e iii) monitoramento e análise crítica. Em um primeiro momento, é trabalhada a identificação dos riscos, que pode ser feita utilizando várias técnicas, para que sejam identificados os riscos que podem afetar a missão da empresa. É importante que todos os riscos sejam identificados, mesmo os que já tenham suas fontes sob controle.

A definição do escopo, do contexto e dos critérios, envolve a definição dos processos organizacionais e a compreensão dos contextos externo e interno, levando a empresa a definir e alcançar seus objetivos, isto porque os fatores organizacionais podem ser fontes de risco. Para definir a significância que determinado risco terá para a organização, são utilizados critérios alinhados à

gestão de riscos, de modo a apoiar os processos de tomada de decisão, levando em conta sua natureza e consequência.

Em seguida, realiza-se a análise dos riscos, que visa compreender a sua natureza e características, desde suas fontes, consequências, probabilidade de eventos, eficácia, entre outros. A análise pode ser realizada através de técnicas qualitativas, quantitativas ou até por uma mescla de ambas as técnicas, geralmente utilizada para analisar eventos com alto teor de incerteza, dependendo do propósito da análise.

Os resultados das análises dos riscos proporcionam discernimento para as decisões, abrindo as portas para a última etapa do processo, que é a etapa de avaliação de riscos. Essa avaliação estabelece uma comparação entre os dados encontrados na análise de risco, com os critérios estabelecidos para que desse modo seja determinado se há necessidade de ser realizada, ou não, uma ação adicional. É o processo de tomada de decisão, em que deve ser considerado o contexto geral e mais amplo, e as reais consequências que podem ocorrer, o resultado deve ser registrado, comunicado e validado nos outros setores da organização.

O tratamento dos riscos é realizado para formular e selecionar opções para planejar e implementar as ações de tratamento, avaliar a sua eficácia e verificar se o que resta dos riscos, ou seja, os riscos remanescentes, são aceitáveis. Em caso negativo, realizam-se ações adicionais, que são realizadas com o objetivo de mitigar os efeitos dos riscos e trazer para as organizações mais possibilidades de êxito em sua missão.

Registro e relato é a parte do processo que visa comunicar as atividades realizadas e os resultados obtidos com a gestão de riscos na organização. Assim, pode-se fornecer informações que irão auxiliar na tomada de decisão e melhorar as ações da gestão, podendo melhorar a qualidade de diálogo entre as partes interessadas e, ainda, apoiar a alta direção e órgãos de supervisão a cumprir as suas responsabilidades que foram definidas previamente (Leal, 2019, p. 42).

A comunicação e a consulta tornam-se fatores importantes neste cenário, porque a comunicação visa auxiliar as partes na compreensão dos riscos, promovendo conscientização e entendimento sobre o risco identificado, enquanto a consulta busca obter retorno e informação para melhor realizar a tomada de decisão. Esse canal deve ser permanente no acompanhamento do processo de gestão de riscos em andamento.

Por fim, há o monitoramento e a análise crítica, a ISO 31000 determina essa etapa para que os riscos sejam constantemente monitorados e revisados para que não existam surpresas, e possam ser identificadas quaisquer alterações no cenário que foi estabelecido no processo de gestão de riscos. Desse modo, pode-se verificar se os resultados da avaliação estão de acordo com a experiência real, se há a necessidade de novas intervenções ou se o que foi feito ainda é suficiente.

Para que se possa gerir os riscos e desenvolver todo o processo de identificação, análise e avaliação, deve-se primeiro realizar uma análise de dados, que irá contornar ou, pelo menos, mitigar os riscos de falhas nos processos a serem realizados. A seguir, será apontado no que consiste a análise de dados.

Análise de Dados para uma Gestão de Riscos Eficaz

Para que essa análise seja implementada, é necessário ainda que haja segurança com relação ao uso dos dados, pois deve-se garantir a sua proteção e ainda promover o alcance dos objetivos do negócio. Como afirmam Xavier et al., (2017),

> A segurança da informação é necessária à organização para garantir a proteção das informações de ameaças. [...] Haja vista que garante às empresas minimizar os riscos e dar continuidade aos negócios. Manter a segurança das informações através de processos de apoio, sistemas e redes, são importantes mecanismos para os negócios e necessários, tendo em vista a continuidade, competitividade, o fluxo do caixa, a lucratividade, etc. (Xavier et al., 2017, p. 8)

Visto isso, nota-se que a segurança das informações obtidas para se realizar a análise de dados são mecanismos necessários e importantes para a continuidade da empresa. Inclusive, tendo em vista a Lei Geral de Proteção de Dados - LGPD, publicada em 2018 que entrou em vigor em 2020, encontram-se pontos que devem ser observados pelas empresas para que se garanta a segurança de dados pessoais tratados, por meio de um mapeamento detalhado das informações abordadas durante o funcionamento da empresa, é possível saber onde, como e para que estes dados estão sendo armazenados, bem como quem tem acesso a eles e quais riscos estão associados.

Assim, com a análise de dados no centro das principais estratégias para a gestão dos negócios da empresa e em especial da gestão de riscos, a proteção deles se faz fundamental, para que, além de tudo, a empresa não perca vantagens no campo econômico e também não deixe de cumprir sua missão. Isto porque, ao analisar os riscos, estão envolvidas entrevistas com empregados, análise de documentos, além de fatores como o país em que a organização atua, ramo de atividade, utilização de terceiros, entre outros (Ayres, 2016).

Desse modo, por meio das análises já concluídas, após o planejamento, entrevistas, documentação e catalogação dos dados, dá-se início ao processo de gestão de riscos. Como estabelecido na ISO 31000:2018, deve-se ter em vista o escopo da instituição, os contextos interno e externo e ainda convém que se tenham definidos a quantidade e o tipo de riscos que ela (a instituição) está disposta a assumir.

A partir disso, dar-se-á início ao processo de avaliação dos riscos, como exposto e explicado ponto a ponto no esquema do tópico anterior, na qual será realizada a identificação dos riscos, a análise e a avaliação deles, que levará ao processo de tomada de decisão, em que se definirá qual atitude deverá ser tomada com relação aos riscos identificados.

Em alguns casos, não é necessário realizar nenhuma ação, em outros é necessário realizar novas análises para compreender melhor os riscos, manter os controles existentes ou até reconsiderar os objetivos da empresa. Em outros

casos, porém, é necessário considerar as opções de tratamento dos riscos, em que se irá selecionar e implementar opções para abordar os riscos. Nessa fase existem alguns parâmetros que podem ser adotados para mitigação de riscos, como veremos a seguir.

Adoção de parâmetros para mitigação de riscos

A gestão de riscos, como pilar de um programa de *Compliance* – ou, em outras palavras, programa de integridade – traz em seu desenvolvimento a identificação, mensuração e mitigação/tratamento de riscos críticos à corporação, além da transferência, contingência/diminuição de impactos, assegurando a continuidade dos negócios (Fernandes et al., 2019, p. 3). Assim, para assegurar a mitigação dos riscos, a gestão de riscos traz sugestões de parâmetros que podem ser adotados pela empresa.

Isto porque, como na maioria dos problemas que se pode antecipar, o que se deve fazer é buscar diminuir seus impactos, para que não venham a se tornar maiores e de difícil solução. Desse modo, a gestão de riscos, como visto anteriormente, proporciona a oportunidade de fazê-lo por meio de atitudes a serem adotadas no cenário empresarial.

A fase de implementação de atitudes diz respeito à fase de tratamento de riscos e tomada de decisão. Estas ações irão variar de acordo com o cenário em que a empresa estiver inserida, pois tal etapa é realizada pelos tomadores de decisão do processo, que são os titulares das unidades e os gestores de riscos (Brasil, 2019, p. 33).

Algumas das ações que podem ser tomadas dentro dos programas de *Compliance* para mitigação de riscos, por exemplo, nos cenários interno e externo das organizações são a cooperação através do

> abrandamento dos conflitos e da majoração da importância da perspectiva de futuro, pela valorização dos empregados – existência de um plano de cargos e salários objetivo e automático, que possibilite visualizar a carreira no futuro. [...] realização de contratos de longo prazo, com o incremento da relação de confiança entre as partes, com a

> manutenção da interação constante com os demais atores envolvidos, bem como pelo investimento na credibilidade da marca. através das políticas de *compliance*. (Ribeiro & Diniz, 2015, p. 103)

Como se pode observar, o *Compliance* traz uma visão estratégica e se aplica a todos os tipos de organização, pois a aplicação de condutas legais e éticas, objetivando um modo de agir mais íntegro por parte das empresas tem cada vez mais demanda no mercado. Dessa maneira, as empresas deverão adequar-se de modo a ter sua lucratividade com foco no desenvolvimento econômico e socioambiental para seu progresso, tendo como ponto de partida as normativas já impostas para identificar e tratar os riscos que podem ocorrer no âmbito organizacional.

A ISO 31000:2018, por exemplo, aponta que o objetivo da fase de tratamento de riscos é selecionar e implementar opções para abordar riscos, planejar e implementar o tratamento do risco, avaliar a eficácia do tratamento, definir se o risco remanescente é aceitável e, se não, realizar um tratamento adicional.

O Programa de Integridade da organização encontra suas bases dispostas no Decreto n.º 8.420/2015, que traz, a partir de seu art. 41, os atributos que devem estar contidos no Programa. O Decreto define que o Programa de Integridade é um conjunto de mecanismos internos e procedimentos que devem prezar pela ética, e que incentiva a denúncia das irregularidades que se apresentem. Além disso, o Programa deve fomentar a aplicação efetiva dos códigos de ética, política e as diretrizes que gerem as empresas, para que, assim, as possibilidades de falhas praticadas sejam detectadas e sanadas.

O Decreto traz consigo a necessidade da empresa realizar a implementação e conservar um programa de gerenciamento de riscos juntamente com o Programa de Integridade, pois assim estará fortalecendo seu ambiente operacional. Ademais, esse trabalho em conjunto gera o fortalecimento da governança corporativa, que é outro fator importante a ser levado em conta, pois é o sistema responsável por manter e garantir que as equipes atuem em

conformidade com as boas práticas empresariais, dirigindo, monitorando e incentivando a administração e as atividades da empresa.

Depois de calculado o nível de riscos, processo feito durante a avaliação, e ter em vista não só o nível, mas também como estão distribuídos em termos de probabilidade e impacto, faz-se necessário avaliar se existem parâmetros que atuem a fim de mitigar esses riscos e, em caso positivo, qual sua eficácia. O Guia de Gestão de Riscos, desenvolvido pelo Supremo Tribunal Federal - STF (2019), aponta que esses parâmetros podem ser de três tipos: "preventivos (quando atuam na causa); detectivos (quando estão relacionados com a detecção do evento de risco); e mitigatórios (quando atuam no impacto)" (Brasil, 2019, p. 29).

Dessarte, a fase de tratamento de riscos pode envolver a ação de evitar o risco, não iniciando ou deixando de praticar certas atividades que dão origem a estes, podem ser feitas conferências e verificações segregadas, em que um funcionário realiza determinada tarefa e outro uma diferente para complementar a ação, a fim de detectar possíveis eventos de risco, e também, com a identificação de riscos que possam trazer impactos negativos, a implementação de políticas, uso de certos dispositivos e práticas que visam modificar os riscos, buscando assim a sua mitigação. Pode-se, ainda, como apontado pelo "Guia de Gestão de Riscos", desenvolvido pelo STF, escolher a opção de compartilhar os riscos, transferindo-o ou compartilhando uma parcela deste, um exemplo citado seria a terceirização da atividade que envolve o risco e a contratação de um seguro.

Outras opções de tratamentos de riscos apontados pela ISO 31000:2018 incluem assumir ou aumentar o risco de maneira a perseguir uma oportunidade; remover a fonte de risco; mudar a probabilidade; mudar as consequências; reter o risco por decisão fundamentada; além das opções já citadas anteriormente, como o compartilhamento de riscos, por contratos e financiamento dos riscos; e evitá-los, não iniciando ou descontinuando atividades que deem origem aos riscos.

Selecionar as opções de tratamento de riscos que seria mais apropriada para implementação na instituição em que se está trabalhando envolve o balanceamento dos benefícios potenciais derivados em relação ao alcance dos seus objetivos, tendo em vista os custos, esforços ou desvantagens da implementação (Abnt, 2018). Isto porque as empresas não têm sempre as mesmas condições, como dito no decorrer do presente trabalho, desse modo requerem avaliações feitas por meio das análises descritas anteriormente. Assim, a aplicação dos parâmetros de tratamento de riscos pode ser realizada utilizando uma ou mais das opções citadas, e ainda muitas podem não se adequar a determinadas circunstâncias, por isso se faz necessária a avaliação.

Um dos parâmetros que podem ser aplicados para conseguir identificar possíveis riscos é a realização do *due diligence*, principalmente para empresas que atuam por meio de parceiros, representantes ou revendedores. A adoção do *due diligence* irá fazer uma avaliação prévia, levantando informações como o histórico dos potenciais agentes e outros parceiros comerciais, verificando se eles têm histórico de práticas comerciais antiéticas ou que podem expor a empresa a realização de negócios inaceitáveis ou que envolvam riscos legais (Sibille & Serpa, 2016, p. 16).

Na realização do *due diligence*, Sibille e Serpa (2016) apontam que as empresas deverão fazer o registro de como foram realizadas as etapas de avaliação, para que assim possam demonstrar que seus programas estão funcionando. Devendo a empresa manter os registros e informações tanto dos terceiros que contrataram como também dos que não foram contratados. Isso irá demonstrar os critérios adotados pela empresa para a realização de parcerias e contratações.

Em geral, os Programas de *Compliance* irão implementar nas empresas canais de comunicação como o canal de denúncia. Este canal fornece “aos funcionários e parceiros comerciais uma forma de alertar a empresa para potenciais violações ao Código de Conduta, a outras políticas ou mesmo a respeito de condutas inadequadas de funcionários ou terceiros que agem em nome da empresa” (Sibille & Serpa, 2016, p. 13). Dessa maneira, o canal de

denúncia possibilita que funcionários e terceiros denunciem de forma anônima suas preocupações com relação a possíveis irregularidades que possam estar ocorrendo, para que a empresa possa atuar removendo a fonte de risco, evitando ou mitigando este tipo de conduta.

Sibille e Serpa (2016) apontam que o canal de denúncia é a principal fonte de identificação de fraudes, usando como base dados da *Association of Certified Fraud Examiners* (ACFE), que apontou o canal de denúncia como o que mais identificou fraudes nas empresas no ano de 2015, com cerca de 43%. Sendo assim, nota-se a importância da implementação do canal de denúncia nas empresas, para que elas possam ter melhor desempenho na identificação de irregularidades institucionais.

Sob essa perspectiva, a denúncia "é o aviso, o alerta lançado para a avaliação de outrem sobre algo que pode parecer passível de responsabilização" (Alvim & Carvalho, 2019, p. 02). Para atender às denúncias reportadas, as organizações devem realizar investigações internas, garantindo que os fatos sejam verificados. Estes podem ser diversos, abarcando ações ou inações inapropriadas, como:

> Cometimento de fraudes em geral; atos de corrupção lato sensu; atuação ou não atuação em não conformidade com regulação externa ou interna à instituição; atos inapropriados de gerência e gestão de pessoas; ações ou inações que representem ou possam representar conflitos ou transgressões éticas; atos que atentem contra a dignidade de outrem. (Alvim & Carvalho, 2019, p. 02)

Visto isso, as investigações realizadas irão ocorrer de acordo com o tipo de denúncia feita. A principal consequência da denúncia, segundo Alvim e Carvalho, é a responsabilização dos agentes; se a denúncia for interna à instituição, as providências cabíveis à situação podem ser a investigação interna para identificar a irregularidade, seus autores e demais responsáveis, além de identificar os procedimentos que podem ter permitido esse desvio de conduta. Ocorrida essa identificação, parte-se para a responsabilização dos envolvidos, onde se pode, eventualmente, informar às autoridades públicas, e

realizar a comunicação interna com colaboradores e parceiros comerciais, para tomada de demais medidas pertinentes (Alvim & Carvalho, 2019, p. 04).

Após realizar o tratamento dos riscos, planejando e implementando as ações, avaliando sua eficácia e verificando se os riscos remanescentes são aceitáveis, faz-se o registro e relato, que é quando se faz o registro das atividades e os resultados obtidos com a realização delas, e se comunica à alta direção e demais órgãos de supervisão para auxiliar no processo de tomada de decisão.

Por fim, realiza-se o monitoramento e a análise crítica. Essa etapa se dá para que os riscos sejam constantemente monitorados e revisados, buscando evitar o aparecimento de surpresas, identificando previamente alterações no cenário que se estabeleceu no processo de gestão de riscos.

Desse modo, verifica-se no dia a dia o funcionamento dos resultados da avaliação de riscos, se as ações implementadas estão funcionando corretamente ou se há a necessidade de novas intervenções. Por exemplo, se no canal de denúncias houver uma alta taxa de recebimento de denúncias em determinado setor, isso irá indicar haver falhas na gestão deste e, assim, pode-se verificar ainda que devem ser tomadas medidas para que a organização possa trazê-lo aos eixos.

Vantagens de Aplicar os Programas de Compliance nas Organizações

Os Programas de *Compliance* garantem para as empresas a possibilidade de estar em conformidade com as normas e leis vigentes, e ainda proporcionam o alinhamento das práticas organizacionais com os seus valores, bem como com sua missão. Desse modo, e de acordo com o que foi explanado anteriormente, pode-se explorar a importância da implementação de tais Programas nas empresas.

O alinhamento das práticas organizacionais com os valores que estão definidos dentro de cada setor faz com que as empresas tenham mais

credibilidade no mercado, e assim também com os órgãos fiscalizadores e clientes. Isto porque, ao estar em conformidade, a organização vem a estabelecer um padrão de qualidade para suas práticas internas, mantendo-se íntegra e mais transparente.

De acordo com a Pesquisa Maturidade do *Compliance* no Brasil, são benefícios das boas práticas de implantação da avaliação de riscos de *Compliance*: compreender *gaps* na mitigação de riscos corporativos; a capacidade de implementar controles em toda a empresa, quando necessário; melhoria na comunicação, coordenação; a alta administração se mantém informada; há ainda a possibilidade de identificar controles duplicados e priorizar os riscos.

Além disso, a Pesquisa aponta benefícios da avaliação do incentivo de seus colaboradores e terceiros e das políticas e procedimentos a serem adotados, sendo estes: o recrutamento eficiente, ações disciplinares que impactem as performances e a avaliação destas performances, papéis e responsabilidades definidos, integrando ainda a tecnologia.

Para a implantação de um Programa de *Compliance* eficaz, é necessário ainda o treinamento e a comunicação, para maior envolvimento dos colaboradores. Algumas vantagens desse processo são: a mitigação dos riscos de *Compliance*, melhorias na gestão do Programa de Ética e *Compliance*, além de reforçar a mensagem do Código de Ética e Conduta da empresa e da cultura de *Compliance*.

O estudo realizado pela KPMG traz ainda os benefícios integrados à análise de dados e da visualização desses dados como ferramentas cada vez mais importantes para um gerenciamento de riscos mais proativo, auxiliando na tomada de decisões dos negócios. São eles: a análise da "causa-raiz" e tendências dos riscos que podem ser encontrados; a identificação tempestiva dos riscos e a resposta rápida; a aplicação do *Compliance* em tempo real; a visão agregada dos riscos; a integridade dos dados e os controles automatizados; entre outros.

Com relação aos programas de monitoramento e testes de *Compliance*, que devem ser realizados continuamente, e também ao gerenciamento de deficiências e investigação, bem como o reporte, alguns dos benefícios apontados são: testes e funções de monitoramento centralizados; melhorias em toda a gestão do Programa; métricas avançadas; maior consciência da responsabilidade da primeira linha de defesa e uso efetivo da terceira linha; possibilidade de utilização da análise dos riscos na tomada de decisão; estrutura eficiente de comunicação e metodologia de forma a colaborar para acelerar a implementação e reduzir riscos de remediação. Além disso, a pesquisa aponta que os controles mitigatórios reduzem riscos reputacionais e regulatórios, aumentam a confiança aos *stakeholders* e dão mais consistência aos processos.

Nesse contexto, infere-se a possibilidade do aumento de produtividade do time empresarial, contribuindo para a sua eficiência, não somente com relação às obrigações legais, como também com os processos internos da organização. Desse modo, a implementação do *Compliance* dentro da esfera corporativa mantém a integridade da instituição e seus processos, bem como traz a satisfação interna e externa. Como apontam Ribeiro e Diniz (2015),

> A implantação de uma política de *Compliance* é essencial para empresas que prezam pela eficiência e buscam perenizar e aumentar os seus lucros, pois a transparência, a ética e a confiança são condições legais, e não apenas itens de ostentação. (Ribeiro & Diniz, 2015, p. 102)

Portanto, a implantação de uma política de *Compliance* dentro do setor empresarial irá auxiliar tanto no seu desenvolvimento interno como no desenvolvimento da sociedade, visto que os comportamentos adotados tendem a ser copiados e replicados, fazendo com que a transparência, a ética e a confiança em qualquer relação, sejam estimuladas e tornem-se bases para uma verdadeira sustentabilidade (Ribeiro & Diniz, 2015).

Outro dado relevante a ser ressaltado, refere-se ao custo médio, para as empresas, de estar em conformidade, ou seja, o custo médio do *Compliance*,

em contrapartida com o custo médio de não estar. Segundo a pesquisa "*The true cost of compliance with data protection regulations*" realizada, em 2017, pela *GlobalScape* - empresa pioneira em proteção e automatização do movimento e integração de dados dentro e fora de seus negócios, atuando na venda e suporte de software de transferência de arquivos gerenciados para empresas -, o custo de estar em conformidade alcançava cerca de US$ 5,47 milhões. Já o custo de não estar em conformidade, chegava a US$ 14,82 milhões.

Observando estes dados disponibilizados, pode-se constatar a evidente diferença entre o custo do investimento nas atividades de *Compliance* e o custo do não investimento. Ao se implementar um Programa de *Compliance* evita-se, portanto, não só problemas como a interrupção dos negócios da organização, a queda na produtividade e aplicação de penalidades, como também a perda de receita.

Considerações Finais

A crescente importância que o *Compliance* – e os Programas de *Compliance* – tem assumido nas organizações atualmente, enquanto uma ferramenta de gestão eficiente, torna necessário o desenvolvimento de pesquisas teóricas para auxiliar os profissionais responsáveis por essa missão. O *Compliance* surge como um instrumento que auxilia no cumprimento normativo e cria procedimentos para uma gestão de riscos eficaz, evitando que as empresas passem por incertezas que possam causar prejuízos negativos.

Como instrumento de gerenciamento de riscos, é possível ainda preservar a imagem e a credibilidade que a empresa possui com o público interno e externo, aumentando, assim, o seu valor de mercado.

Os programas de *Compliance* têm procedimentos específicos que devem ser respeitados, muito embora não possamos definir um programa padrão para ser adotado. Cada organização tem as suas características próprias, sua forma

de trabalho, seu mercado, seu público-alvo, o que torna necessário que os programas a serem implementados se adequem a essa realidade.

Porém, identificamos os principais pilares que obrigatoriamente devem fazer parte de um programa efetivo: i) suporte da alta administração; ii) implementação de código de ética e de conduta; iii) comunicação e treinamento; iv) canal de comunicação; v) meios de investigação; vi) gestão de riscos; vii) procedimentos internos; viii) *due diligence*; e ix) auditoria e monitoramento. Todos esses requisitos se concentram na premissa geral de prevenção e mitigação de riscos. Ou seja, trabalhar o efeito da incerteza causado sobre os objetivos da organização, um desvio em relação ao esperado, podendo ser negativo ou positivo, resultando em oportunidades ou ameaças à organização. Os riscos, por sua vez, podem ser classificados de várias formas, a exemplo dos riscos estratégicos, riscos de conformidade, riscos financeiros, riscos na gestão de pessoas, riscos ambientais, riscos de tecnologia de informação e telecomunicações e riscos operacionais.

Abordamos algumas das principais referências nacionais e internacionais de padronização de sistemas de gerenciamento de riscos para que possamos compreender como funciona o processo que envolve pelo menos três passos entre: “definição de escopo, contextos e critérios; identificação de riscos; análise de riscos; avaliação de riscos; tratamento dos riscos; monitoramento e análise crítica dos riscos; comunicação e consulta aos riscos”. O objetivo final é identificar, analisar, avaliar e definir um procedimento específico para o tratamento dos riscos, conforme o planejamento estratégico da empresa.

De acordo com a *International Organization for Standardization*, o processo de avaliação de riscos é dividido em três etapas: i) escopo, contexto e critério; ii) registro e relato; e iii) monitoramento e análise crítica. A definição do escopo, contexto e critério, envolve a definição do processo e compreensão do contexto interno e externo da empresa de forma a que possam ser alcançados os seus objetivos. O registro e relato é a parte do processo que tem por objetivo comunicar as atividades realizadas e os resultados obtidos que irão auxiliar na tomada de decisão estratégica. O

monitoramento e análise crítica determina que os riscos sejam constantemente monitorados e revisados para que não existam surpresas e possam ser identificadas quaisquer alterações no cenário que foi estabelecido no processo de gestão de riscos. Em paralelo, é importante que se mantenha um canal de comunicação e consulta ativo auxiliando as partes na compreensão dos riscos e disseminação da importância destes procedimentos para a organização.

No momento inicial da implementação de um programa de *compliance*, são feitos o diagnóstico inicial e a contextualização da organização, para posteriormente serem definidos os possíveis riscos não desejados e implementar os procedimentos cabíveis de prevenção ou mitigação. A análise de dados torna-se essencial para uma efetiva avaliação dos riscos, pois é um processo por meio do qual há a possibilidade de prever o impacto das possíveis falhas nas organizações, valendo-se de uma observação minuciosa do contexto em que a instituição está inserida.

Desse modo, torna-se possível antecipar desafios e utilizar a tecnologia para procurar informações sobre os processos internos. Com uma aprofundada análise destes dados, podemos incluir ainda informações referentes a potenciais parceiros ou colaboradores que possam ter participação, por exemplo, em casos de corrupção, possibilitando a implementação de precauções necessárias nesses casos.

Para que essa análise seja implementada, é necessário ainda que haja segurança com relação ao uso dos dados, através da aplicação das regras sobre proteção de dados – Lei Geral de Proteção de Dados –respeitando o cumprimento normativo que os programas de *compliance* pretendem alcançar.

Em suma, para a implementação de um programa de *Compliance* efetivo torna-se fundamental trabalhar com uma prévia análise de dados segura, que possa auxiliar o profissional responsável na tomada de decisões estratégicas e no gerenciamento de riscos eficiente, contribuindo, sempre, para a melhoria

dos serviços prestados e, consequentemente, no aumento do valor de mercado das organizações.

Referências

ABNT. **Gestão de Riscos** – Diretrizes. (2018). NBR ISO 31000. Associação Brasileira de Normas Técnicas.

Alvim, T. C. & Carvalho, A. C. (2019) **Linha ética: Funcionamento da denúncia, papel do denunciante e uso do canal de denúncias**. In: Carvalho, A. C.; Bertoccelli, R. de P. et al., (org). Manual de Compliance. Rio de Janeiro: Forense, 102-115.

Ayres, C. (2016). **Análise prática de programas de compliance: a operacionalização dos principais elementos de um programa de compliance nas pessoas jurídicas no âmbito da Lei 12.846/2013**. São Paulo: JOTA, 2016. Recuperado de: https://www.jota.info/opiniao-e-analise/artigos/coluna-do-trench-rossi-analise-pratica-de-programas-de-compliance- 01022016. Acessado em: 27 jun. 2021.

de Azevedo, M. M., Cardoso, A. A., Federico, B. E., Lima, M. A. F., & Duarte, J. G. (2017). O compliance e a gestão de riscos nos processos organizacionais. **Revista de Pós-Graduação Multidisciplinar,** 1(1), 179-196. Recuperado de: http://www.fics.edu.br/index.php/rpgm/article/view/507. Acessado em: 31 mai. 2021.

Benedetti, C.R. (2014). **Criminal Compliance. Instrumento de prevenção criminal corporativa e transferência de responsabilidade** penal. São Paulo: Quartier Latin,

BERTOCCELLI, R. DE P. (2019) **COMPLIANCE.** IN: CARVALHO, A. C.; BERTOCCELLI, RODRIGO DE PINHO ET AL (ORG). MANUAL DE COMPLIANCE. RIO DE JANEIRO: FORENSE,42

BLOCK, M. (2017) **COMPLIANCE E GOVERNANÇA CORPORATIVA**. RIO DE JANEIRO: FREITAS BASTOS, 15 E SS.

BRASIL. (2019) SUPREMO TRIBUNAL FEDERAL (STF). **GUIA DE GESTÃO DE RISCOS [RECURSO ELETRÔNICO]**. BRASÍLIA: STF, SECRETARIA DE GESTÃO ESTRATÉGICA, ESCRITÓRIO DE GESTÃO APLICADA, 49.

CANDELORO, A. P. P & RIZZO, M. B. M. PINHO, V. (2012). **COMPLIANCE 360°: RISCOS, ESTRATÉGIAS, CONFLITOS E VAIDADES NO MUNDO CORPORATIVO**. 1. ED. SÃO PAULO: TREVISAN EDITORA UNIVERSITÁRIA.

COIMBRA, M. A. & MANZI, V. A. (2010). **MANUAL DE COMPLIANCE**. PRESERVANDO A BOA GOVERNANÇA E A INTEGRIDADE DAS ORGANIZAÇÕES. SÃO PAULO: ATLAS.

LEAL, M. M. (2019); **PROCESSO DE GESTÃO DE RISCOS NO DIÁRIO OFICIAL DO DISTRITO FEDERAL: ISO 31000:2018**. DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM COMPUTAÇÃO APLICADA. BRASÍLIA: UNIVERSIDADE DE BRASÍLIA. RECUPERADO DE: HTTPS://REPOSITORIO.UNB.BR/HANDLE/10482/36123. ACESSADO EM: 10 DE MAIO DE 2021.

MAESTRI, C. & COSTA, N. (2020). **POR QUE A ANÁLISE DE DADOS É TÃO IMPORTANTE NA TOMADA DE DECISÃO? USO DE DADOS E INFORMAÇÕES INTELIGENTES AJUDA A DIRECIONAR AÇÕES COM MAIS ASSERTIVIDADE ALÉM DE ANTECIPAR DESAFIOS.** PARANÁ: RPC, 2020. RECUPERADO DE: HTTPS://WWW.NEGOCIOSRPC.COM.BR/DEOLHONOMERCADO/INOVACAO/2020-05-27-POR-QUE-ANALISE-DE-DADOS-E-TAO-IMPORTANTE-NA-TOMADA-DEDECISAO/. ACESSADO EM: 27 JUN. 2021.

NEVES, E. C. & FIGUEIROA, C. C. GESTÃO DE RISCOS. IN: CARVALHO, A. C.; BERTOCCELLI, R. DE P. ET AL (ORG). **MANUAL DE COMPLIANCE**. RIO DE JANEIRO: FORENSE, 2019, P. 29-36.

NUNES, L. A. (2019) COMPLIANCE COMO FATOR ESTRATÉGICO NAS ORGANIZAÇÕES. **REVISTA ESPECIALIZE** ON-LINE IPOG. GOIÂNIA: IPOG. 9(16): 01.

PAULA, M. A. DE .(2018). COMPLIANCE - **GESTÃO DE RISCOS E COMBATE À CORRUPÇÃO.** BELO HORIZONTE: FÓRUM, 2018.

PESQUISA, K. P. M. G. (2019) **MATURIDADE DO COMPLIANCE NO BRASIL**. RECUPERADO DE: HTTPS://HOME.KPMG/BR/PT/HOME/INSIGHTS/2019/10/PESQUISA-MATURIDADE-COMPLIANCE.HTML. ACESSADO EM: 10 ABRIL. 2022.

PONEMON INSTITUTE LLC, SPONSORED BY GLOBALSCAPE (2017) THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS. DISPONÍVEL EM: <HTTPS://DYNAMIC.GLOBALSCAPE.COM/FILES/WHITEPAPER-THE-TRUE-COST-OF-COMPLIANCE-WITH-DATA-PROTECTION-REGULATIONS.PDF>. ACESSO EM: 15 ABRIL. 2022.

RIBEIRO, M.C. P. & DINIZ, P. D. F (2015) COMPLIANCE E LEI ANTICORRUPÇÃO NAS EMPRESAS. **REVISTA DE INFORMAÇÃO LEGISLATIVA**, 52(205) 87-105, 2015.

RODRIGUES, L.S. DE A. (2020) **COMPLIANCE – CONCEITO**. NATAL: EDUCOMPLIANCE, 2020, A. RECUPERADO DE: HTTPS://EDUCOMPLIANCE.COM.BR/COMPLIANCE-CONCEITO/. ACESSADO EM: 27 JUN. 2021.

RODRIGUES, L. S. DE A. (2020) **COMPLIANCE COMO INSTRUMENTO DE ENFRENTAMENTO À PANDEMIA. NATAL: EDUCOMPLIANCE**. DISPONÍVEL EM: HTTPS://EDUCOMPLIANCE.COM.BR/O-COMPLIANCE-COMO-FERRAMENTA-DE-ENFRENTAMENTO-DA-PANDEMIA/. ACESSO EM: 27 JUN. 2021.

SANTOS, R. DE A. DOS ET AL. (2011) **COMPLIANCE COMO FERRAMENTA DE MITIGAÇÃO E PREVENÇÃO DA FRAUDE ORGANIZACIONAL**. DISSERTAÇÃO DE MESTRADO EM ADMINISTRAÇÃO. SÃO PAULO: PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO, RECUPERADO DE: HTTPS://TEDE.PUCSP.BR/BITSTREAM/HANDLE/979/1/RENATO%20DE%20ALMEIDA%20DOS%20SANTOS.PDF. ACESSADO EM 26 JUN. 2021.

SIBILLE, D. & SERPA, A.C. (2016) **OS PILARES DO PROGRAMA DE COMPLIANCE: UMA BREVE DISCUSSÃO**. SÃO PAULO: LEC, RECUPERADO DE: HTTPS://WWW.EDITORARONCARATI.COM.BR/V2/PHOCADOWNLOAD/OS_PILARES_DO_PROGRAMA_DE_COMPLIA NCE.PDF. ACESSADO EM: 26 JUN. 2021.

XAVIER, D. F. S.ET AL. (2017) COMPLIANCE UMA FERRAMENTA ESTRATÉGICA PARA A SEGURANÇA DAS INFORMAÇÕES NAS ORGANIZAÇÕES. **IN:** SIMPÓSIO INTERNACIONAL DE GESTÃO DE PROJETOS, INOVAÇÃO E SUSTENTABILIDADE. ANAIS DO VI SINGEP. SÃO PAULO.

ZENKNER, M. (2019) **INTEGRIDADE GOVERNAMENTAL E EMPRESARIAL. UM ESPECTRO DA REPRESSÃO E DA PREVENÇÃO À CORRUPÇÃO NO BRASIL E EM PORTUGAL**. 2.ª REIMPRESSÃO. BELO HORIZONTE: FÓRUM.