UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
PROGRAMA DE PÓS-GRADUAÇÃO EM
CONTROLE DE GESTÃO- PPGCG

VALDETE APARECIDA ANDRETT

MANUAL DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*: ESTUDO DE CASO EM UMA EMPRESA DE ECONOMIA MISTA

Florianópolis
2021

VALDETE APARECIDA ANDRETT

MANUAL DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*: ESTUDO DE CASO EM UMA EMPRESA DE ECONOMIA MISTA

Trabalho de Conclusão de Curso submetido ao Programa de Pós-Graduação em Controle de Gestão da Universidade Federal de Santa Catarina para obtenção do título em Mestre de Controle de Gestão.

Orientadora:
Prof.ª. Luiza Santangelo Reis, Drª.

Florianópolis
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Andrett, Valdete Aparecida
Manual de Gerenciamento de Riscos de Compliance : Estudo de caso em uma empresa de economia mista / Valdete Aparecida Andrett ; orientador, Luiza Santangelo Reis, 2021.
97 p.

Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro Sócio-Econômico, Programa de Pós-Graduação em Controle de Gestão (MP*), Florianópolis, 2021.

Inclui referências.

1. Controle de Gestão (MP*). 2. Gestão de riscos. 3. Compliance. 4. Manual. I. Santangelo Reis, Luiza . II. Universidade Federal de Santa Catarina. Programa de Pós Graduação em Controle de Gestão (MP*). III. Título.

Valdete Aparecida Andrett

Título: Manual de Gerenciamento de Riscos de *Compliance*

Subtítulo: Estudo de caso em uma empresa de economia mista

O presente trabalho em nível de Mestrado foi avaliado e aprovado por Banca Examinadora composta pelos seguintes membros:

Professor Antônio Celso Ribeiro Brasiliano, Dr.
Fundação Dom Cabral-FDC

Professora Fabricia Silva da Rosa, Dr.(a)
Universidade Federal de Santa Catarina-UFSC

Professor Fernando Richartz, Dr.
Universidade Federal de Santa Catarina-UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Controle de Gestão.

Documento assinado digitalmente
Luiz Alberton
Data: 08/11/2021 08:37:29-0300
CPF: 650.459.989-00
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
Luiza Santangelo Reis
Data: 08/11/2021 08:32:38-0300
CPF: 082.215.979-10
Verifique as assinaturas em https://v.ufsc.br

Prof.ª. Luiza Santangelo Reis, Drª Orientador(a)

Florianópolis, 2021.

AGRADECIMENTOS

Aos meus amados Pais, Ari e Anair, pelo apoio incondicional na minha vida.
Ao meu Filho Gabriel, companheiro constante de caminhada.
Aos Professores e Colegas do Curso pela oportunidade e pelo conhecimento compartilhado.
À minha Orientadora, Professora Dr.ª Luiza Santangelo Reis, por acreditar em meu potencial.
Aos Colegas de trabalho, Facilitadores de Gestão de Riscos, por suas contribuições no Manual e por serem meus grandes incentivadores.

“Se eu vi mais longe, foi por estar sobre ombros de gigantes.”

Isaac Newton

RESUMO

No Brasil, após muitos escândalos e fraudes envolvendo a administração pública e privada, os órgãos regulamentadores e normativos se manifestaram e passaram a exigir das empresas, em de todas as esferas administrativas, uma gestão de risco voltada à conformidade. Esse novo enfoque de gestão tem o intuito de "tratar" possíveis riscos relacionados ao comportamento antiético, os quais ameaçam negligenciar a cultura corporativa, suas regras e condutas. Essa negligência pode acarretar danos à empresa por não respeitar a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência dos Princípios da Administração Pública. Então, com a finalidade de executar um Programa de Integridade, cujos requisitos principais advêm da legislação brasileira aplicável às organizações, é realizado um estudo de caso em uma Companhia a fim de gerar critérios para realizar a análise de riscos de *compliance* e possibilitar a criação e monitoramento de controles que norteiam a conduta dos Colaboradores, auxiliando assim a integridade e a sustentabilidade da empresa objeto de estudo. Como resultado dessa pesquisa tem-se uma proposta de um manual para direcionar o Programa de *Compliance* e suas ações para mitigar riscos de desvio de conduta. Imperioso ressaltar que, o Manual de Riscos de *Compliance* é relevante para fornecer subsídio e transparência à implantação do Programa de Integridade e atender a legislação, uma vez que as organizações que realizam atividades de *Compliance* e possuem experiência, por motivos de estratégia e sigilo acabam não divulgando o processo.

Palavras-chave: Gestão de Riscos. *Compliance*. Manual de Riscos de *Compliance*.

ABSTRACT

At Brazil, after many scandals and frauds involving the public and private administration, the regulatory and normative bodies came out and started to demand from companies, in all administrative spheres, a risk management focused on compliance. This new management approach is intended to "treat" possible risks related to unethical behavior, which threaten to neglect the corporate culture, its rules and conduct. This negligence can cause damage to the company, affronting the legality, impersonality, morality, publicity and efficiency of the Principles of Public Administration. In order to carry out an Integrity Program, whose main requirements come from the Brazilian legislation applicable to organizations, a case study is carried out in a Company in order to generate criteria to carry out the analysis of compliance risks and enable the creation and monitoring of controls that guide the conduct of Employees, thus helping the integrity and sustainability of the Company. As a result of this research, there is a proposal for a manual to guide the Compliance Program and its actions to mitigate risks of misconduct. It is imperative to emphasize that the Compliance Risk Manual is relevant to provide support and transparency to the implementation of the Integrity Program and comply with legislation, since organizations that carry out Compliance activities and have experience, for reasons of strategy and secrecy, end up not publicizing the process

Keywords: Risks Management. Compliance. Compliance Risk Manual.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

É comum, nas mídias sociais, observar escândalos envolvendo casos de corrupção em pequenas e grandes empresas. Assim, notícias com investigações, seguidas de constatações de que ocorreram favorecimentos, fraudes, abuso de poder, nepotismo, conflito de interesses, subornos, uso indevido de informação privilegiada e sigilosa, configuram-se como exemplos de infração de leis e normas, bem como a quebra de conduta dos funcionários.

No âmbito público, atos como esses, relacionados à quebra de integridade, quase sempre dolosos, caracterizam-se por serem praticados por um indivíduo e/ou por um grupo contrários aos Princípios da Administração Pública, ou que afrontam a legalidade, a impessoalidade, a moralidade, a publicidade e a eficiência dos atos da administração (COELHO, 2016). Essa quebra de conduta de integridade prejudica a moralidade das organizações envolvidas, sejam instituições públicas ou privadas.

Seguindo esse pensamento, verifica-se que é oportuno, segundo Castro e Gonçalves (2018) decidir e direcionar ações no caminho da integridade e da ética nas relações da Administração. Assim, temos o processo de *compliance,* relacionado à identificação e ao tratamento dos desvios de conduta nas organizações. Este direcionamento se estrutura norteador para criar e aprimorar procedimentos de gestão e controle em *compliance*.

Para tanto, cita-se aqui a Lei n.º 12.846/13 que amplia e eleva as discussões sobre o tema integridade corporativa, preconizando a adoção de Programa de Integridade como um dos principais fatores de mitigação de riscos na Administração Pública, seja por corrupção ou por fraude. Neste cenário, as empresas de economia mista orientam-se pelos mesmos Princípios da Administração Pública, sendo orientadas pela ética e normatizações, com o fito de buscar o efetivo atendimento da legislação brasileira.

A Lei da Empresa Limpa ou Lei n.º 12.846/13 foi regulamentada pelo Decreto 8.420/15, que tem como objetivo instituir medidas ao combate da corrupção, e a responsabilização das pessoas envolvidas e a recuperação dos danos causados à Administração Pública. Em especial destacamos aqui o artigo 42 do Decreto, que trata do Programa de *Compliance*. Um de seus pilares é a identificação dos riscos de *compliance* que atende à necessidade de registrar e de monitorar as causas, os controles,

os riscos, bem como os planos de ação.

Complementarmente, menciona-se a Lei nº. 13.303/16, que estabelece disposições aplicáveis às empresas públicas e as sociedades de economia mista, a qual preconiza que os riscos devem ser identificados, analisados, tratados e monitorados. Sendo assim, a gestão de riscos aplicada apropriadamente na estrutura de governança das organizações promove o aumento da transparência da prestação de contas, o fortalecimento dos controles internos, bem como o maior comprometimento com a responsabilidade corporativa.

Assim, muitos instrumentos e normatizações vêm sendo implementados nas organizações da administração direta e indireta ligados ao Estado, com a finalidade de executar um Programa de Integridade, cujos requisitos principais advêm da legislação brasileira aplicável às organizações de Economia Mista. Ressalta-se que este programa poderá ser desenvolvido em conformidade com diferentes leis e, ainda assim, incorporar as normatizações já existentes nas instituições (CARVALHO, BEROLCCELLI, ALVIM, VENTURINI, 2018). Convém destacar, ainda, que a implementação necessita do entendimento e do apoio da alta direção na sequência da identificação dos Riscos de Integridade ou *Compliance* (CASTRO, GONÇALVES, 2018). Entende-se aqui, apoio da alta direção, como sendo o comprometimento e o patrocínio das atividades de *compliance*, desde o provimento de recursos, até divulgação de seu apoio aos trabalhos de conformidade.

Sobre o tema *compliance*, seus instrumentos e normatizações aplicado nos setores público e\ou privado no Brasil, Coelho (2017, pg.93) comenta que existe uma convergência entre o tratamento legal regulamentado das empresas, sejam elas estatais ou de direito privadas. Essa convergência ocorre, uma vez que, o objetivo a ser alcançado, nos dois segmentos é o mesmo: evitar os grandes esquemas de corrupção, de suborno e fazer análise ampla, para evitar e mitigar todas as infrações sejam elas administrativas ou penais.

Por conseguinte, infere-se que ao conhecer, analisar e monitorar os riscos de *compliance*, a governança corporativa fica fortalecida. Nesse sentido a gestão de riscos de *compliance* constitui assim um mecanismo estratégico sob o ponto de vista da sensibilização dos usuários internos e partes interessadas do processo. A finalidade do processo é de trabalhar os resultados entregues aos diferentes públicos envolvidos, além de transformar as informações em importantes direcionadores de priorização de ações.

Logo, por meio da gestão de riscos de c*ompliance*, a organização compartilha opiniões e aprimora as tomadas de decisão, uma vez que proporciona o diálogo entre os diferentes *stakeholders*, além de mitigar riscos de c*ompliance*. Segundo Giovanini (2014) está sendo usual encontrar áreas de *compliance* formalizadas, cuja missão é a de proteger organizações contra atos que podem ser mitigados, sendo eles: inibir a corrupção, impedir o suborno e os pagamentos de facilitação; evitar o engajamento em conluio dos funcionários; bloquear as combinações prejudiciais às leis concorrenciais, obstar fraudes contábeis, lavagem de dinheiro, assim como outras práticas do gênero.

Contudo, mesmo havendo a formalização, Andreisová (2016), ressalta que ainda há muito a ser construído na cultura organizacional para que um programa de *compliance* torne-se eficaz. As empresas globais procuram manter seus resultados presentes e futuros e, ainda assim, garantir que os resultados foram atingidos seguindo a ética e integridade, sendo esses princípios, norteadoras peças de sua cultura organizacional. A percepção de que a ética é fundamental na cultura corporativa precisa permear toda empresa, desde o conselho de administração, passando por seus gestores e líderes, chegando a todos os funcionários. Andreisová (2016) ainda comenta que apesar de não ser fácil criar ou mudar cultura organizacional, é importante que todos os colaboradores façam o que é certo e entendem a importância de tal comportamento. Hoje a realidade para qualquer organização que deseja competir com sucesso no mercado global, é manter um forte programa de conformidade, frequentemente visto como essencial exigência de negócio.

Ainda, no entendimento de Melo e Lima (2019), é necessário o fomento da "cultura" de *compliance*, que servirá de base para o fortalecimento ético, sem o qual programas de *compliance* não obterão êxito. A implantação de *compliance* atua como uma estratégia disponível que possibilita o combate e a prevenção dos riscos. À vista disso, a presente pesquisa se fundamenta pela necessidade de conhecer, registrar e monitorar os riscos que afetam as condutas e a integridade da organização, bem como o andamento dos planos de ação elencados para tratar os riscos, conforme priorização do processo.

Em consequência, o presente estudo tem a finalidade de apresentar uma proposta de Manual de *Compliance*, assim como contribuir enquanto referência teórico-prática e metodológica, para ser aplicada em outras organizações. Este estudo aborda os temas gerenciamento de riscos de *compliance*, com a descrição das métricas a serem

utilizadas para realizar a identificação, a análise, a avaliação e o monitoramento dos riscos de *compliance*. Em vista disso, foi realizada pesquisa de caráter descritivo, buscando entendimento necessário com levantamento bibliográfico, com o intuito de adquirir informações para criar conhecimento e apresentar um modelo de Manual para identificar, analisar, avaliar e monitorar os riscos de *compliance.*

Desse modo, após esta breve introdução sobre o tema gestão de riscos de c*ompliance,* bem como sobre a necessidade da elaboração do Manual, são apresentados os objetivos do trabalho. No segundo capítulo deste estudo buscam-se referências bibliográficas para conceituar gestão de riscos de c*ompliance*. No terceiro capítulo, descreve-se o estudo de caso e sua participação na elaboração deste manual, juntamente com um relato de como ocorreram os trâmites para a elaboração do manual. No quarto capítulo é descrita a estruturação do manual, apresentando os detalhes de cada etapa da metodologia utilizada, incluindo a proposição de métricas para a análise da probabilidade e do impacto. Os resultados deste estudo de caso são narrados no quinto capítulo. Por derradeiro, este estudo é concluído no sexto capítulo, etapa em que se atinge o objetivo deste estudo. E, no apêndice, tem-se o produto desta pesquisa - um modelo de Manual de Gerenciamento de Riscos de *Compliance*.

1.1 Objetivos

Este trabalho tem como objetivo geral apresentar uma proposta de Manual de Gerenciamento de Riscos de *Compliance*, a ser aplicado em uma empresa de economia mista.

Os objetivos específicos são:

- Estruturar procedimento de identificação dos riscos de c*ompliance*;
- Estabelecer métricas que permitam analisar a probabilidade e o impacto dos riscos de c*ompliance* identificados; e
- Estruturar procedimento para realizar respostas e monitoramento aos riscos de c*ompliance;* e análise crítica do processo.

2 REFERENCIAL TEÓRICO

O referencial teórico da pesquisa tem por intuito fundamentar e discutir as especificidades dos processos de gestão de riscos de *compliance*, bem como subsidiar as escolhas metodológicas realizadas no estudo. Dessa forma, o referencial teórico foi estruturado em dois blocos: a Gestão de Riscos e de *Compliance*.

2.1 Gestão de Riscos

Todas as Empresas, em todos os segmentos, enfrentam incertezas internas e externas, que fazem com que ocorra dúvida sobre a consecução dos seus objetivos. Assim, a ISO 31000 define Risco como "o efeito que essa incerteza tem sobre os objetivos da organização." Por este ângulo, o Adams (2009, p.237) apresenta seu entendimento sobre risco descrevendo a seguinte situação:

> O modo como as pessoas lidam com algo é influenciado pelo modo como o percebem, e o ato de lidar com esse algo o altera. Esse esquema foi formulado antes, da seguinte maneira: o risco percebido é o risco pelo qual se reage. Ele muda em um piscar de olhos quando os olhos o fixam.

O estudo destes riscos, ou melhor, destas incertezas, é justificado conforme comenta Rinaldi (2010), após surgirem eventos como os acidentes em Flixborough em 1974, Seveso em 1976, Three Mille Island em 1979, Bhopal em 1984 e Chernobyl em 1986; com impactos internacionais gigantescos, por afetarem negativamente a vida das pessoas e do meio ambiente. Centenas de vidas humanas foram ceifadas, e apesar de todos os alertas/sinais que ocorreram antes dos acidentes, nenhuma ação foi realizada para evitar tais tragédias. Em resposta a esses eventos, diferentes atores da sociedade começaram a exigir dos Poderes Públicos, regulamentações pelas quais as empresas apresentassem transparência no processo de monitoramento e gerenciamento dos riscos de negócio.

Como consequência a esse cenário de incerteza e escândalos, no qual ocorreu a desconfiança do público sobre a fidedignidade das informações contábeis publicadas, em 2002, foi sancionada a Lei Sarbanes Oxley (PETERS 2007). A SOX, como ficou conhecida a lei federal dos Estados Unidos, visa estabelecer padrões para todas as companhias abertas norte-americanas.

Já, no Brasil, os escândalos envolvendo grandes organizações, nos anos de 2007

e 2008 evidenciaram uma série de riscos possíveis, desde a crise de liquidez nos mercados financeiros até as preocupações emergentes envolvendo clima, disponibilidade de alimentos, infraestrutura e energia. Observa-se, com isso, a fragilidade sistêmica dos processos estratégicos envolvendo nações e, consequentemente, o mundo.

Na mesma percepção, Coelho (2016) faz uma análise da importância do *compliance* público no Brasil, e comenta sobre a força da edição da Lei n.º 13.303/16 e de outras leis nacionais e internacionais que revestem o tema corrupção no mundo moderno, com destaque para o Brasil. Segundo Coelho (2016) o cenário atual exige mudança de comportamento das empresas, mas também do Poder Público. A experiência brasileira segue fazendo da Lei Sarbanes Oxley sua referência na implantação de controles e na transparência destes, buscando compreender que o risco deve ser a base de suas ações. Ou seja, ao identificar previamente os riscos, pretendem-se mitigá-los, possibilitando assim que as ações aumentem sua credibilidade econômica, financeira e social.

Em especial, no âmbito nacional, iniciou-se um movimento para a estruturação de convergência das melhores práticas de mercado quando em 2009, foi publicada a ISO 31000 (ABNT, 2009), para harmonizar padrões, regulamentos e metodologias utilizadas em gestão de riscos. Para a Comissão Especial, que desenvolveu a norma, o maior desafio para implementar gestão de riscos foi integrar em um único documento diretrizes, que possibilitassem atender a qualquer indivíduo e/ou empresa, independente de tipo, tamanho e da área de atuação. Ainda, segundo Brasiliano (2009, p. 20):

> A ISO 31000 surge também para integrar as diversas metodologias e terminologias, pois hoje, ainda há falta de consenso em relação à terminologia e aos conceitos utilizados para gestão de riscos. O resultado mais comum dessa equação é que a gestão de riscos acaba sendo tratada isolada, fazendo com que vários gestores (saúde, meio ambiente, segurança de TI e empresarial, legal, financeiro, seguros, entre outros) trabalhem em linhas departamentais, o que ocasiona a utilização de terminologias, sistemas, critérios e conceitos diferentes para cada uma das áreas da empresa.

Quatro anos mais tarde, em 2013, a Declaração de Posicionamento do IIA (Instituto dos Auditores Internos do Brasil) foi publicada com o título: As Três Linhas de Defesa no Gerenciamento eficaz de Riscos e Controle. A referida declaração busca esclarecer quais atribuições de cada linha de defesa devem ser conhecidas pelos funcionários, e as responsabilidades devem ser definidas para cada atividade, é o que

descreve o posicionamento:

> Não basta que diferentes atividades de risco e controle existam - o desafio é determinar funções específicas e coordenar com eficácia e eficiência esses grupos, de forma que não haja "lacunas" em controles, nem duplicações desnecessárias na cobertura. Responsabilidades claras devem ser definidas para que cada grupo de profissionais de riscos e controle entenda os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de riscos e controle da Organização (IIA, 2013, p. 01).

A Declaração de Posicionamento do IIA auxilia na definição das atividades desempenhadas, na utilização de conhecimentos trabalhados no COSO ICIF e no COSO ERM. O COSO ICIF constitui um modelo conceitual para sistemas de controles internos, com o intuito de alcançar os objetivos e sustentar o desempenho da Organização, visto que o controle interno é um processo dinâmico e integrado. O *framework* do COSO ICIF apresentado no Anexo C está baseado em três objetivos: operacional, divulgação e conformidade.

O COSO ERM de 2013 também é um modelo conceitual para ser aplicado no Sistema de gestão de riscos, a fim de alcançar os objetivos estratégicos das Organizações. O COSO ERM, demonstrado no Anexo D tem um *framework* baseado em quatro objetivos: operacional, conformidade, comunicação e estratégico.

O COSO ERM pode ser aplicado utilizando As Três Linhas de Defesa, todavia, é bem provável que, na prática, observemos delegações para que as execuções das atividades ocorram. Isso porque o COSO ERM (2017), sugere que as validações dos riscos sejam realizadas pelo Conselho de Administração, que atualmente, consoante a Lei n.º 13.303/16, é o órgão responsável pelos riscos estratégicos.

Tendo em vista que o Conselho de Administração possui disponibilidade limitada em atender as demandas junto às diversas áreas dentro da empresa, sua participação, em específico, para a área de riscos e *compliance* é eventual. Fato esse que implica uma gestão ineficaz e possíveis postergações de resultados.

Em síntese, ao ocorrer a delegação e o acompanhamento por parte do Conselho de Administração, este não será um obstáculo, pois pode ser vencido com os esclarecimentos das responsabilidades de toda a hierarquia e com as capacitações dos membros da Diretoria Executiva, dos Conselhos de Administração e do Comitê de Auditoria Estatutário (Órgão que vai assessorar os Conselheiros nas Empresas de Economia Mista dos Estados, atendendo a Lei n.º 13.303/16).

O COSO ERM apresentou atualização no seu *framework* em 2017 (Anexo E),

integrando estratégia e *performance* e reconhecendo as mudanças quanto às responsabilidades e às atividades dos membros dos Conselhos de Administração e de toda a alta direção das organizações. O *framework* é composto por 20 princípios distribuídos em 05 componentes, e tais princípios abrangem o ciclo de vida dos negócios, desde a Governança Corporativa até o monitoramento das atividades demonstradas no Anexo E.

Por sua vez, a ISO 31000, também apresentou atualização em 2018. As principais alterações foram quanto a determinação da importância de criação e proteção de valor como centro de todos os princípios e, quanto ao *framework* de processo houve a inclusão da etapa de registro e relato. Essas modificações podem ser percebidas no Anexo F.

Em 2020, dois anos após a atualização da ISO, o Instituto dos Auditores Internos também publicou uma atualização do posicionamento da Instituição a respeito dos riscos. A nova publicação iniciou alterando o próprio nome do posicionamento, substituindo a denominação "As Três Linhas de Defesa no Gerenciamento eficaz de Riscos e Controle", para "As Três Linhas". Tal posicionamento resultou em um novo *framework* (Anexo B) que descreve com maior fluidez a interação das atividades, suas responsabilidades e a hierarquia nas Organizações. O posicionamento presente no documento "As Três Linhas" busca agregar valor com mais alinhamento, comunicação, coordenação e colaboração entre as atividades em todos os níveis hierárquicos.

Observa-se que Instituições que ditam as melhores práticas de mercado em Gestão de Riscos Corporativos, como o Instituto dos Auditores Internos, o Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO), a Associação Brasileira de Normas Técnicas) disponibilizando a Norma ISO 31.000, entre outros, vêm buscando a convergência de papéis e conceitos, procurando formas de viabilizar a implantação da Gestão de Riscos nas Organizações.

Diante disso, a Gestão de Riscos não deve ser vista como uma atividade pontual simplesmente para atender a Lei, mas sim como uma melhoria contínua de desempenho, permitindo que atores internos e externos reavaliem as prováveis ocorrências do Risco. Para melhor exemplificar, trazem-se os ensinamentos de Brasiliano (2009, p.10):

> Toda organização existe para gerar valor às partes interessadas. Todas as organizações enfrentam incertezas, e o desafio de seus administradores é determinar até que ponto aceitar essa incerteza, assim como definir como essa incerteza pode interferir no esforço para gerar valor às partes

> interessadas. Incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O Gerenciamento de Riscos Corporativos possibilita aos administradores tratar com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

No mundo corporativo, o termo Gestão está sendo muito utilizado, e de acordo com Rinaldi (2010, p.19):

> O Gerenciamento de Riscos é um termo aplicado ao Processo de Gestão que consiste em um conjunto de medidas e procedimentos internos que incluem a identificação, a estimativa, a avaliação, a redução e o controle dos riscos a serem mantidos em níveis aceitáveis pelos técnicos.

Entende-se que a importância da Gestão de Riscos é, primeiramente, garantir boas práticas gerenciais de Controle dos Riscos, de maneira proativa e não reativa. Sobre o tema, Alexandra Rinaldi (2010, p.23) afirma:

> A gestão de riscos não deve ser encarada como uma prática estanque e de cumprimento de normas, mas como uma reafirmação de melhoria de desempenho e implementação de novas ações, permitindo aos seus atores internos e externos reavaliarem as prováveis ocorrências do risco.

Neste sentido, observa-se que Processo de Gerenciamento de Riscos mantém os riscos em níveis controlados, ou aceitáveis, realizando um papel de prevenção, sendo proativo e não reativo em suas atividades. Essa prevenção é aplicável nas várias disciplinas (tipologias) de riscos que estejam sendo trabalhadas: operacionais, estratégicos, financeiros ou de *compliance*, com o objetivo de garantir a sustentabilidade da empresa.

2.2 *Compliance*

Compliance está ligado ao cumprimento rigoroso das regras e das leis internas e externas das Organizações. Sobre esse tema, afirma Giovanini (2014, p.20),

> No mundo corporativo, *Compliance* é associado ao fato de estar em conformidade com as leis e os regulamentos internos e externos da Organização. E, cada vez mais, o *Compliance* vai além do simples entendimento à legislação, busca consonância com os princípios da empresa, alcançando a ética, a moral, a honestidade e a transparência, não só na condução dos negócios, mas em todas as atitudes das pessoas.

Sob esse aspecto, o desafio do *compliance* é alinhar valores e mitigar riscos relacionados às condutas antiéticas dos profissionais, tendo impactos positivos na

imagem organizacional, no ambiente de trabalho, na motivação dos profissionais e na perenidade das Organizações (SANTOS, HOYOS e AMORIM, 2013).

Compliance é um tema recorrentemente discutido desde a aprovação da Lei Anticorrupção (Lei n.º 12.846 de 2013), e conquistou ainda mais notoriedade com a aprovação da Lei n.º 13.303 de 2016, conforme esclarece Lucas (2020, p.83):

> Em vários países, leis foram criadas, assim como novas regras comerciais entre empresas. No Brasil, a Lei Anticorrupção, Lei n.º 12.846, foi promulgada em 2013 e inseriu o país em um universo de outros países que adotaram medidas semelhantes. Essa soma de fatores, das crises à criação de leis e a crescente conscientização dos consumidores, preocupados com o planeta e com o meio ambiente, contribuiu para criar contexto e cenário propícios ao resgate e à priorização da cultura de valores.

Por conta disso, após os escândalos envolvendo grandes corporações nacionais, a gestão de riscos passou a ser mais exigida e cobrada das organizações, incluindo as empresas de economia mista da administração direta e indireta em todas as esferas administrativas brasileiras (Federal, Estadual e Municipal). Destaca-se aqui, dentro da gestão, a prática de mecanismos que minimizem as fraudes e os desvios de recursos financeiros. Esses mecanismos incluem a identificação e a criação de controles que norteiam a integridade e a conduta dos colaboradores das empresas.

Por se tratar de uma área relativamente nova nas organizações, com metodologias ainda em desenvolvimento, a implantação de um programa de gestão de *compliance* se tornou um desafio. Convém ressaltar que existe uma extensa literatura teórica sobre o assunto, contudo, na prática, a falta de objetividade para a condução das atribuições continua sendo um entrave para a administração.

Todavia, mesmo havendo a formalização Andreisová (2016) lembra que administrar uma empresa ética que coloca seus valores em conformidade é uma excelente ideia, pois proporciona bons resultados para os negócios. Entretanto ela cita que nestes últimos anos, observa-se muita literatura sobre a importância da ética nas organizações, comentários sobre danos causados pelas falhas e escândalos de conformidade e sobre os requisitos e benefícios legais relacionados. Assim, uma cultura de conformidade duradoura e bem-sucedida deve ser alcançada, em conjunto com o programa de conformidade, resultando em mais do que uma simples abordagem de ponto a checar e pronto.

Para tanto, o gestor de *compliance* tem um papel fundamental para que esse processo de implementação ocorra de forma adequada. Nesse viés, Giovanini comenta que o Gestor passa a desempenhar uma gama de funções ou de papéis, quais sejam: Conselheiro, Facilitador, Defensor ou Sensibilizador. Em consonância Giovanini (2014, p.358) descreve:

> Os quatro papéis apresentados não são dissociados. No cotidiano, o especialista do *Compliance* precisará "flutuar" entre eles para ser realmente eficiente e agregar valor à organização. Além do mais, em determinadas situações poderá haver uma "zona cinzenta" e a combinação de atitudes poderá ser necessária.

Na estruturação das áreas de c*ompliance* nas organizações, destacam-se as atividades voltadas para a elaboração e a manutenção do código de conduta, os treinamentos relacionados a este código, como também a estruturação e a manutenção de canais de denúncias. As funções de c*ompliance* buscam privilegiar a integridade da organização e, para isso, é fundamental realizar análise completa de situação, considerando o ambiente interno e externo, os cenários que envolvem o contexto regulatório, político, socioeconômico e, por fim, as normas internas e os procedimentos de cada organização.

Quando se compreende o contexto estratégico no qual estão inseridas as empresas, os gestores aumentam suas chances em ser assertivos nas suas tomadas de decisão. Essa compreensão, somada à avaliação dos riscos norteados pela cultura organizacional, é fundamental para estabelecer um programa de *compliance* nas organizações.

Os autores Azevedo *et. al* (2017) entendem que, o programa de *compliance* traz benefícios diversos para as organizações que o implementa. Esses benefícios propiciam bons resultados os quais podem ser analisados sob os seguintes aspectos: evitar custos por não conformidades e aumentar as habilidades das instituições de satisfazer as necessidades de seus clientes e colaboradores. Dos benefícios encontrados, vale mencionar a diminuição de riscos e de prejuízos financeiros relacionados às condutas antiéticas. Ressalta-se ainda, que os riscos relacionados a comportamento antiético, em regra, são causados por pessoas que, de alguma forma, negligenciaram a cultura corporativa, suas regras e condutas. Essa negligência pode acarretar danos à empresa; em contrapartida, o *compliance* lida com o cumprimento de normas e leis externas, bem como, com o princípio de boa governança e dos padrões éticos, sociais e ambientais.

Para Carvalho *et. al* (2018), é importante que o programa de *compliance* seja incorporado como padrão valorativo e comportamental, refletido em todas as atividades do dia a dia dos colaboradores. Para Carvalho *et. al* (2018, p.41):

> *Compliance* é um sistema materializado por um Programa de *Compliance*, sobre o qual não há sequer que diferenciar a importância de um Programa de *Compliance* de um Programa de *Compliance* "efetivo". Sem efetividade, não há que se falar em Programa - e sim, mera simulação ou ficção jurídica, o que proporciona danos reputacionais ainda mais graves para quem busca se valer de tal artifício.

A Legislação brasileira ressalta inúmeras vezes a importância da correta identificação dos riscos para a efetivação do programa de *compliance* ou de integridade. Acerca dessa temática, escrevem Oliveira e Acocella (2019, p.48):

> É fundamental a correta identificação dos riscos aos quais se sujeita a Organização, de forma a garantir a efetividade do Programa. Vale o registro de que o Manual da CGU, sobre implementação dos Programas de Integridade, estabelece que um dos pilares do Programa é justamente a Gestão de Riscos e Controles. Sem tal premissa bem executada, o Programa ficará fadado ao insucesso, na medida em que não apontará para os reais riscos incidentes sobre a Organização.

Ainda, no Guia Implantação de Programa de Integridade em empresas estatais, disponibilizado em 2015, pela Controladoria Geral da União (CGU), a instituição respalda que a criação do programa de integridade deverá considerar os riscos identificados, juntamente com a criação e as normatizações. Deverá contemplar também, mecanismos que permitam a mitigação de riscos de fraudes, de corrupção, de conflito de interesses, de nepotismo e outros. Registrando que compete a cada organização observar seus ambientes interno e externo.

A Controladoria Geral da União na Portaria CGU n.º 1.089/2018, no art.2, item II define riscos de integridade como "aqueles que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção".

O levantamento e a análise dos reais riscos de *compliance,* realizados previamente para a implementação do Programa de Integridade, ajudarão a organização a identificar suas vulnerabilidades e as áreas mais suscetíveis à corrupção, o que dará à empresa a oportunidade de prevenir, de forma eficiente e eficaz, a ocorrência dos eventos referenciados. Segundo Castro e Gonçalves (2018, p.51),

> O Programa de Integridade, diante dos riscos mapeados, tem por objetivo a criação de mecanismos internos que ofereçam respostas aos riscos de *Compliance*, ou seja, aqueles que versem sobre os desvios de conduta, violações das diretrizes fundamentais da empresa, normas internas, descumprimento de leis e normas regulatórias.

Diante disso, e acompanhando a tendência das melhores práticas de mercado e a

necessidade de atendimento à legislação brasileira, é imposto às organizações conhecer mais sobre os riscos de *compliance* e, por meio deste conhecimento, incorporar cultura e valores nas práticas da empresa.

Neste segmento, Saad-Diniz e Silveira (*apud*, CARVALHO, BEROLCCELLI, ALVIM VENTURINI, 2018, p.39) comentam sobre o termo *Compliance*:

> Orienta-se, em verdade, pela finalidade preventiva, por meio da programação de uma série de condutas (condução de cumprimento) que estimulam a diminuição dos riscos da atividade. Sua estrutura é pensada para incrementar a capacidade comunicativa da pena nas relações econômicas, ao combinar estratégia de defesa da concorrência leal e justa com as estratégias de prevenção de perigos futuros.

A harmonia nas organizações possibilita identificar que a comunicação e a consulta avancem para obter um melhor entendimento de que o processo de *compliance* é estruturado, e que segue os princípios do ciclo da qualidade PDCA (Planejamento, Desenvolvimento, Controle e Análise Crítica) e que precisa ser retroalimentado. Observa-se que Instituições que ditam as melhores práticas de mercado em Governança Corporativa, como o Instituto dos Auditores Internos; COSO; ABNT; com a publicação das normas ISO 31.000 - que trata de Gestão de Riscos; ISO 19.600 - que trata do Sistema de Gestão de *Compliance*; ISO 37.000 - que trata do Sistema de Gestão Antissuborno; e ISO 37301 - apresenta requisitos de Sistemas de Gestão de *Compliance*; o IBGC (Instituto Brasileiro de Governança Corporativa); entre outras, vêm buscando a convergência de papéis e conceitos, procurando formas de viabilizar a implantação de Gestão de Riscos de *Compliance* nas organizações.

3 METODOLOGIA UTILIZADA

A proposta elaborada para o processo de Gestão de Riscos de *Compliance* busca estabelecer linguagem padrão para todas as gerências da organização, normatizando as melhores práticas com foco na aplicabilidade do processo. Assim, diante de todas as metodologias de gestão de riscos e *compliance* apresentadas no capítulo 2, o manual proposto é estruturado com base na metodologia desenvolvida por Brasiliano (2018), que integra várias ferramentas de qualidade interconectadas. Registra-se que a metodologia é citada no capítulo 4.

O método descrito em Brasiliano (2018), para Gestão de Riscos de *Compliance*, possui *framework* adaptado, utilizando fundamentos da ISO 31.000 (ABNT, 2009 e 2018), integrados ao COSO I e COSO II-ERM, também considera ferramentas e técnica da ISO 31010. A ISO 31010 sugere ferramentas de qualidade para a execução das atividades a serem desenvolvidas no Processo de Gestão de Riscos de *Compliance*, o que proporciona um pensamento sistêmico com uma sequência estruturada para uso delas.

Vale destacar, que há o entendimento de que é possível aperfeiçoar recursos internos e integrar a metodologia aos demais *frameworks,* já que os dois outros *frameworks* que a empresa objeto de estudo faz uso, são para as disciplinas dos riscos nos processos (operacionais) e para os riscos estratégicos.

Abaixo, estão expostas as fases do *framework* apresentadas por Brasiliano (2018) para a gestão de riscos de *compliance*:

- Comunicação e Consulta;
- Contexto Estratégico;
- Identificação de Risco de *Compliance*;
- Análise e Avaliação de Riscos de *Compliance* – Inerente;
- Análise e Avaliação de Riscos *Compliance* – Residual;
- Respostas aos Riscos *Compliance*; e
- Monitoramento e Análise crítica – Indicadores.

O processo de coleta de dados foi realizado mediante levantamento de dados documentais, entrevistas não estruturadas, com os facilitadores de riscos e responsáveis pelas gerências na empresa objeto de estudo.

Os documentos consultados na empresa objeto de estudo, foram: Política Interna de Compliance, Política Interna de Gerenciamento de Riscos e Manual de Gerenciamento de Riscos Estratégicos.

Nesta pesquisa, observa-se que a empresa objeto de estudo, em seu processo de gestão de riscos, tem funcionários designados para todas as gerências, denominados de facilitadores de gestão de riscos. Como o próprio nome diz, os Facilitadores visam tornar mais colaborativo o processo de gestão de riscos, auxiliando em reuniões com equipes de trabalho, incentivando a participação individual. Além de colaborar com a aplicação da metodologia para identificação, análise, avaliação e tratamento dos riscos.

No capítulo quatro, deste documento, poderão ser encontradas as fases trabalhadas na empresa objeto de estudo, e no apêndice, o Manual, resultado do trabalho, bem como para uso das demais empresas interessadas.

3.1 Preparação do Manual

Iniciou-se a pesquisa acerca da elaboração de normatizações básicas e norteadoras do processo de c*ompliance,* para a empesa objeto estudo de estudo, em especial, a política de *compliance*.

Observa-se que a política tem a finalidade de estabelecer as diretrizes gerais de c*ompliance*, norteando os demais documentos que compõem o programa de gestão de c*ompliance* da instituição. Para atender a essa política de *compliance*, deu início à elaboração de um Manual de Gerenciamento de Riscos de *Compliance,* em conjunto com a área de gestão de riscos e conformidade da empresa objeto de estudo. Este documento, em conjunto com o Código de Conduta, corroboram a política da empresa objeto de estudo.

Tal Manual de Gerenciamento de Riscos de *Compliance* visa estabelecer a metodologia e os parâmetros do processo de gestão de riscos de c*ompliance* na Organização. No que tange à elaboração da Política, do Manual de *Compliance*, estes foram desenvolvidos (entre os meses de outubro a dezembro de 2020) e compartilhados com gestores e facilitadores das seguintes áreas da empresa objeto de estudo: Gerências de Contabilidade e Controladoria, Gerência de Licitação, Aquisição e Suprimentos, Gerência de Recursos Humanos, Gerência Jurídica, Gerência de Tecnologia da Informação, Secretaria Geral e Auditoria Interna.

Tais documentos foram encaminhados por e-mail, após reunião (virtual) de

alinhamento e discussão sobre o tema. O compartilhamento foi realizado para conhecimento e análise crítica dos documentos, por parte dos facilitadores, após receber as contribuições e críticas das áreas envolvidas. Os documentos foram atualizados e então, apresentados para o Comitê de Conduta e Integridade da Organização (em dezembro de 2020), para também conhecerem os documentos e realizarem suas críticas. Só depois (em fevereiro de 2021), o conjunto dos documentos foram encaminhados para que os assessores realizassem leitura destes, e seguissem, a fim de serem pautados e apresentados para Diretoria Executiva.

Sobre a elaboração do Manual, relata-se que foram consultadas outras empresas do mesmo segmento de negócio, as chamadas empresas coirmãs, para entender como estavam trabalhando o processo de c*ompliance*, mais especificamente, como identificavam e analisavam os riscos de c*ompliance*. Essas consultas foram realizadas por conversas telefônicas e por e-mail, nos meses de outubro e novembro de 2020. Não obtendo respostas satisfatórias, ou que nos possibilitasse um ponto de partida para entender e/ou escrever o processo.

Buscou-se contato então, sobre o tema, por meio de contato telefônico com pessoas que atuam em outras empresas, e que estão familiarizadas com o assunto. Todavia, as organizações que já executam o processo não estão confortáveis em compartilhar o conhecimento, visto que, para elas, trata-se de assunto estratégico e/ou sigiloso.

Ainda que houvesse a falta de subsídio documental por parte das empresas consultadas, identificou-se dentre as conversas como sendo oportuno utilizar o *framework* para riscos de c*ompliance* proposto por Brasiliano (2018) no Livro Inteligência em Riscos - Gestão integrada em riscos corporativos (p. 172). Somado esses conhecimentos teóricos dos livros e da fundamentação teórica desenvolvida a experiência prática vivenciada pela autora no mercado de trabalho e participação em cursos sobre *compliance*, com foco maior em Riscos de *Compliance* em Instituições como LEC *Legal, Ethics & Compliance* os quais dispunham de um corpo docente atuante no mercado. Esses eventos possibilitaram adquirir informações sobre como o mercado está realizando a identificação, a análise e o monitoramento de riscos de *compliance*.

Torna-se imperioso ressaltar, também, que as pesquisas bibliográficas, realizadas, reforçaram o estudo do tema, e dentre os autores pesquisados elencam-se

Antônio Celso Ribeiro Brasiliano e Wagner Giovanini, pela praticidade com que abordam os assuntos, sem deixar, é claro, de aplicarem a teoria. O primeiro, pelo primor nos detalhes, permitindo com isso, trabalhar diversas disciplinas de riscos; já, o segundo, por trazer um material sobre a implementação de um programa de *compliance*.

Traçando um paralelo entre o *framework* proposto por Brasiliano (2018) e a empresa objeto de estudo, foi possível efetuar comparações cuidadosas entre eles, tanto para riscos de processos quanto para riscos estratégicos, realizando com isso, as adequações necessárias para o atendimento da empresa. Em outras palavras, respeitaram-se o apetite aos riscos aprovado na empresa objeto de estudo, como também as premissas da Política de Gestão de Riscos aplicada nesta Empresa no momento de propor um Processo de Gestão de Riscos de *Compliance*.

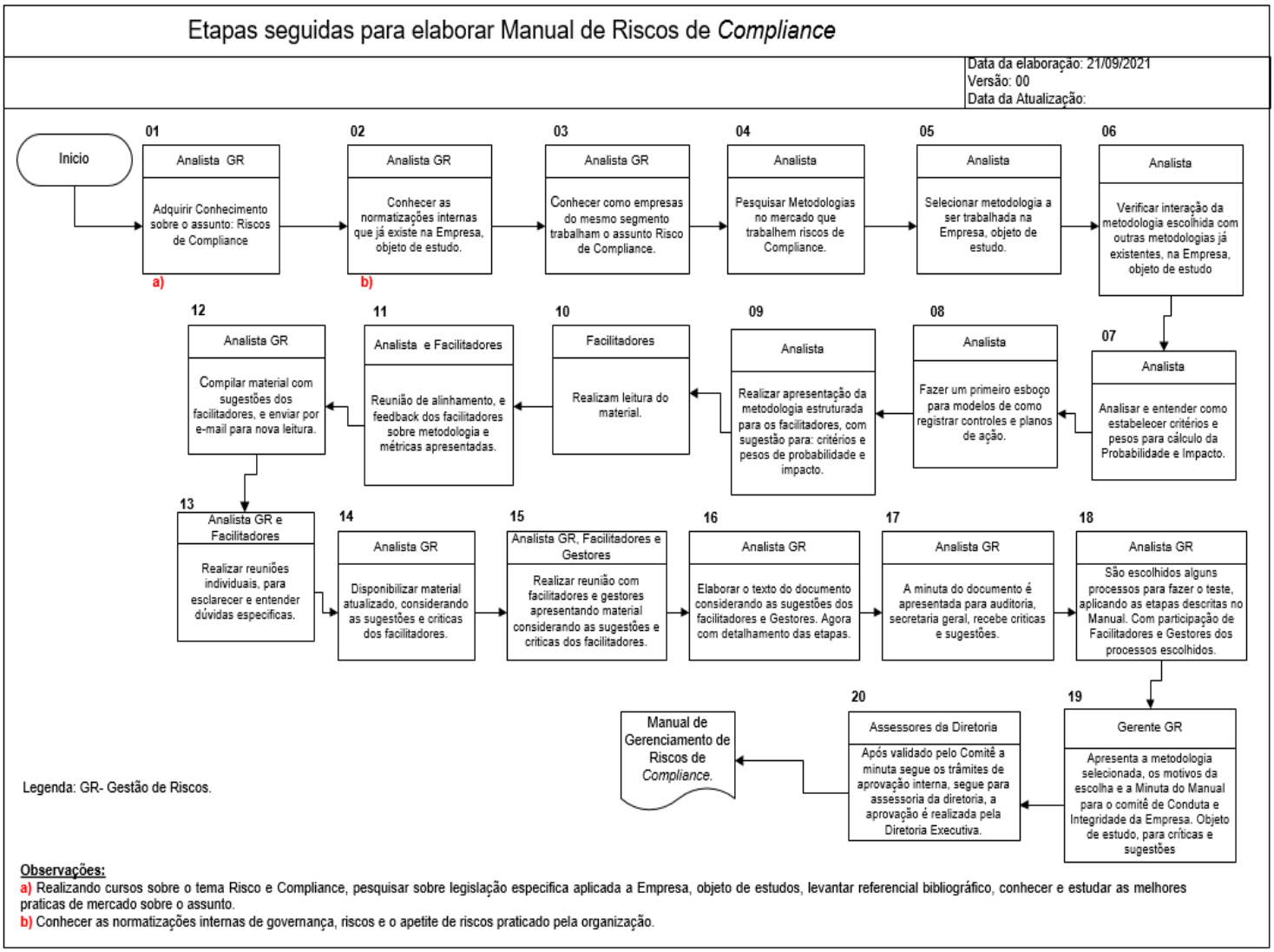
De acordo com o contexto estratégico foram trabalhadas as etapas delineadas no processo de gerenciamento de riscos de *compliance* propostas por Brasiliano (2018), para estabelecer como seriam usadas as métricas de probabilidade e de impacto na avaliação dos riscos identificados. Na sequência do trabalho, no intuito de compartilhar, criar conhecimento e com a finalidade de receber contribuições, foi realizada consulta com os facilitadores da empresa em reuniões virtuais.

Em uma primeira reunião virtual com os facilitadores, foi feita uma apresentação da Metodologia do "Projeto de Manual para Riscos de *Compliance*", cada fase desta, e as métricas propostas para calcular a Probabilidade e o Impacto dos riscos identificados de *compliance*. O material apresentado seguiu por e-mail para ser analisado por eles.

Após receber suas contribuições, em novembro de 2020, por meio de reuniões de alinhamento e de entendimento, foram realizados vários ajustes na proposta apresentada. Depois, seguiu para ser consolidado em dezembro de 2020. O Manual consolidado foi novamente encaminhado aos Facilitadores e ao Gerente de Gerenciamento de Riscos. Na sequência, o documento foi disponibilizado e uma nova apresentação realizada para o Auditor Interno, o Secretário Geral e os Membros do Comitê de Conduta e Integridade da Organização. Após a validação de todos os envolvidos, o Manual de Gerenciamento de Riscos de *Compliance* seguiu para a avaliação da Diretoria Executiva juntamente com a Política e com a Norma de *Compliance*.

A elaboração do Manual de Riscos de *Compliance* na Empresa, objeto de estudos, segue resumidamente no fluxograma da Figura 1.

Figura 1: Etapas seguidas para elaborar Manual de Riscos de *Compliance*.



Fonte: Elaborado pela Autora (2021).

O Manual apresentado no apêndice deste estudo de caso possui diferenças do documento proposto na empresa objeto de estudo. Mas, imperioso dizer que, as adequações foram efetuadas no que tange aos valores, às descrições e aos pesos aqui apresentados para Probabilidade e Impacto. Porém, tais mudanças no material foram necessárias, uma vez que cada Empresa, ao trabalhar o Manual proposto, deverá considerar seus próprios valores e, com base neles, ponderar seus pesos e suas descrições, assim como qual é seu apetite ao risco.

Destaca-se, ainda, que foram feitos ajustes a fim de tornar o Manual adequado para um maior número de empresas, assim como preservar também o sigilo da Empresa, objeto de estudo.

3.2 Estudo de Caso

O presente estudo de caso foi realizado em uma Empresa de Economia Mista, ligada à administração indireta do Estado. A Empresa tem em sua identidade corporativa os seguintes valores: acreditar nas pessoas, praticar segurança, ser transparente, priorizar o cliente, promover inovação e atuar com responsabilidade socioambiental.

Neste estudo foi considerado o que a Lei n.º 13.303/16 dispõe sobre o Estatuto Jurídico da Empresa Pública, da Sociedade de Economia Mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios, é conhecida como a Lei das Estatais. Cita-se também a Lei n.º 12.846/2013, que trata de assuntos de Anticorrupção, conhecida com a Lei da Empresa Limpa. Inclui-se aqui o Decreto n.º 8.420/2015 que regulamenta a Lei n.º 12.846/13, nas questões da responsabilização administrativa de pessoas jurídicas pela prática de atos contra a Administração Pública, nacional ou estrangeira e dá outras providências. E por derradeiro a ISO 31000, e demais referências nas melhores práticas de mercado de gestão de riscos.

Vale ressaltar que o processo de gerenciamento de riscos deve ser aprimorado sempre que identificada a necessidade de atender mudanças ou novidades na legislação, assim como para buscar as melhores práticas de mercado ou quando ocorrerem mudanças significativas no seu negócio ou em sua estrutura organizacional.

Dessa forma, faz-se necessário contextualizar como é realizado o atual processo de Gerenciamento de Riscos da Empresa, objeto de estudo, trazendo o que já é praticado. Em alguns momentos no texto são realizadas referências ao Processo, tendo em vista já existir gestão de riscos corporativos, uma vez que são discutidas na construção das métricas de Probabilidade e de Impacto no Manual de Gerenciamento de Riscos de *Compliance*. Também é importante compreender como será a interconectividade desta disciplina ou tipologia de risco com as já praticadas no processo existente: riscos estratégicos e riscos nos processos.

Com um olhar macro, pode-se afirmar que este novo Manual de Gerenciamento de Riscos de *Compliance* é uma proposta para a melhoria do Processo de Gestão de Riscos Corporativos da Empresa, objeto de estudo.

Assim, esclarecemos que a Empresa, objeto de estudo, já aplica a Metodologia Brasiliano (2018), e está ciente da necessidade de otimizar recursos internos e integrar a

metodologia com critérios e política, aplicada até o momento com um *framework* para riscos estratégicos e outro *framework* para riscos nos processos.

A Empresa, objeto de estudo, tem em seu Processo de Gerenciamento de Riscos um *framework* específico para cada disciplina de risco, e trabalha respeitando a estrutura proposta pela ISO 31000/2018, ou seja, um *framework* com a metodologia para riscos nos Processos (operacionais) e outro para riscos estratégicos. Cada disciplina (tipologia) de risco trabalha com um Manual de Gerenciamento de Riscos próprio, mantendo alinhamento entre estratégia, desempenho e Apetite de Risco.

Figura 2: Fases do Processo de Gestão de Riscos Atual.

Nota: CA = Conselho de Administração.
CPE=Comitê de Planejamento Estratégico.
DE = Diretoria Executiva.
Fonte: Elaborado pela Autora (2019).

Cada *framework* trabalha uma tipologia ou disciplina em toda Instituição, realizando análise e avaliação dentro de sua disciplina. Com isso, os riscos que não estejam dentro do Apetite de Risco declarado pela Empresa, objeto de estudo, são analisados em conjunto com os riscos estratégicos.

A Empresa, objeto de estudo, inicia a análise dos riscos corporativos com a disciplina estratégica, fazendo uso do *framework* para riscos estratégicos, cujas fases são descritas no Manual de Gerenciamento de Riscos Estratégicos. Tal atividade de levantamento dos riscos é realizada juntamente com o Comitê de Planejamento Estratégico (CPE). O Comitê faz uso do Planejamento Estratégico e observa o

orçamento aprovado na Empresa para nortear sua análise. Os riscos estratégicos identificados e analisados são apresentados para a Diretoria Executiva (DE) para aprovação e para o Comitê de Auditoria Estatutária (CAE) conhecer. Em seguida, são apresentados para conhecimento do Conselho de Administração (CAD), e junto com os riscos estratégicos é apresentado cronograma dos processos que deve ser analisado dentro do período de um ano.

Na sequência, conforme descrito no Processo de Gestão de Riscos Corporativos da Empresa, objeto de estudo, são analisados aqueles Processos identificados com maior criticidade para o negócio da Organização, e que possam interferir nos objetivos estratégicos, definidos na fase de análise dos riscos estratégicos.

Aplicando-se *framework* para Processos, serão analisados os riscos nos Processos. Cada Processo será analisado seguindo as premissas descritas no Manual de Gerenciamento de Riscos nos Processos, e todos os Facilitadores e Gestores seguem as mesmas métricas. Assim que concluída a análise de todos os Processos, é realizada a consolidação das informações dos riscos nos Processos, momento em que é elaborado o relatório consolidado de riscos nos Processos. Neste relatório são apontados os riscos residuais que estão fora do Apetite de Risco declarado pela Empresa, objeto de estudo, os riscos enquadrados no quadrante vermelho da matriz de riscos dos Processos.

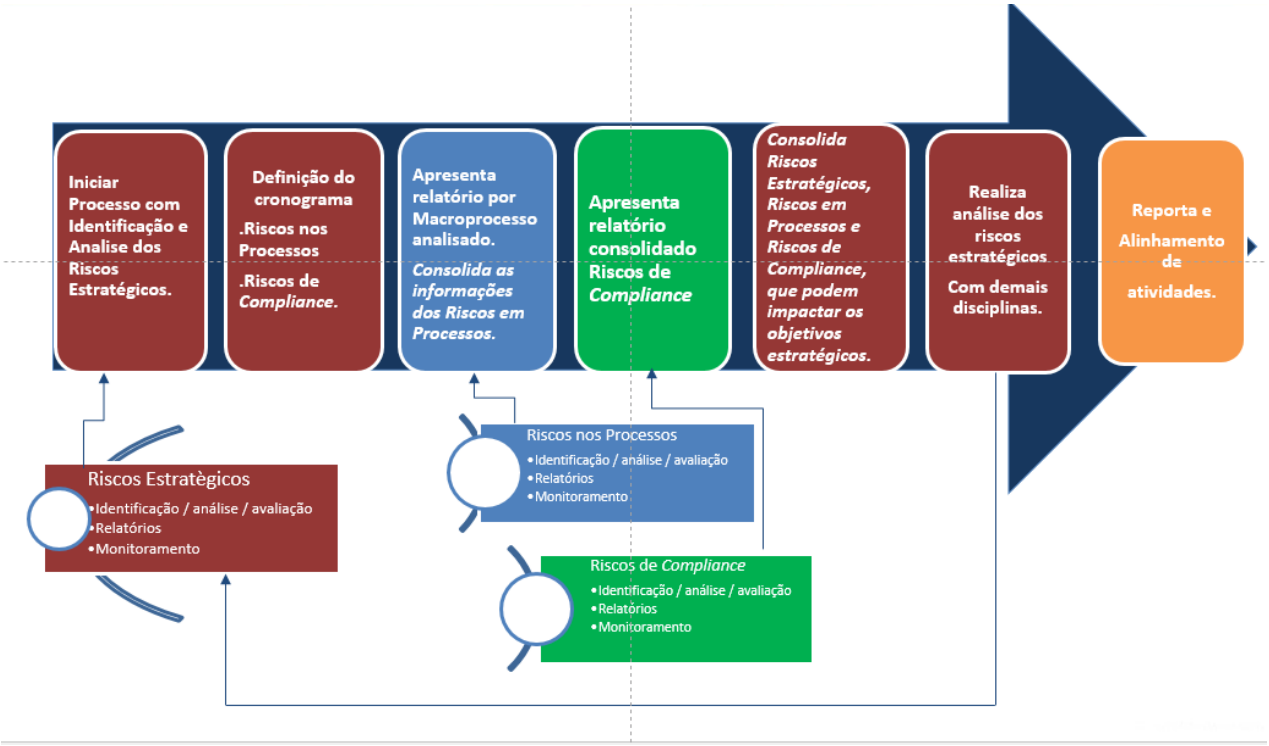
Desta forma, aqueles riscos identificados fora do Apetite da Empresa, objeto de estudo, são acrescentados aos riscos estratégicos, onde se realiza a identificação da interconectividade e se refaz a avaliação deles, juntamente com os riscos nos Processos fora do Apetite da Instituição, fazendo uso do *framework* de riscos estratégicos. Seguindo todas as fases: desde o cruzamento dos fatores dos riscos, a motricidade dos riscos e a criticidade dos riscos, culminando com a priorização do tratamento dos riscos. Lembrando que esta análise é realizada com a participação do Comitê de Planejamento Estratégico, apresentado e validado pela Diretoria Executiva e pelo Comitê de Auditoria Estatutária, seguindo depois para apresentar ao Conselho de Administração.

Este Manual para Riscos de *Compliance* será incorporado ao Processo de Riscos Corporativos da Empresa, objeto de estudo. Dessa forma, teremos mais uma disciplina de riscos a ser analisada com métricas próprias.

Este Manual de Gerenciamento de Riscos de *Compliance* proposto descreve as fases do Processo de Gerenciamento dos Riscos de *Compliance*, e tem a intenção de estabelecer linguagem comum entre todas as Gerências da Empresa, objeto de estudo.

Ademais, propõe alinhamento de linguagem e de procedimento que permite identificar, analisar e monitorar os Riscos de *Compliance*, e apresenta métricas que permitem analisar a Probabilidade e o Impacto dos Riscos de *Compliance* identificados. Com isso, este Processo irá integrar um Processo maior de Gestão de Riscos Corporativos da Empresa, objeto de estudo. Abaixo, Figura 3, seguem as fases descritas resumidamente.

Figura 3: Integração entre os *frameworks* de gestão de riscos- com *Compliance.*



Fonte: Elaborado pela Autora (2020).

4 ESTRUTURAÇÃO DO PROCESSO DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*

Apresenta-se na Figura 04, o *framework* do Processo de Gerenciamento de Riscos de *Compliance* aplicado neste estudo. Este processo é composto por sete (07) fases, interconectadas, sobre as quais serão realizados pontuais comentários, trazendo de que forma foi pensada e estruturada a realização de cada fase deste processo dentro da Empresa, objeto de estudo.

Sob esse enfoque, citamos as fases do Processo do *framework*:

4.1 Comunicação e Consulta;

4.2 Contexto Estratégico;

4.3 Identificação de Risco de *Compliance*;

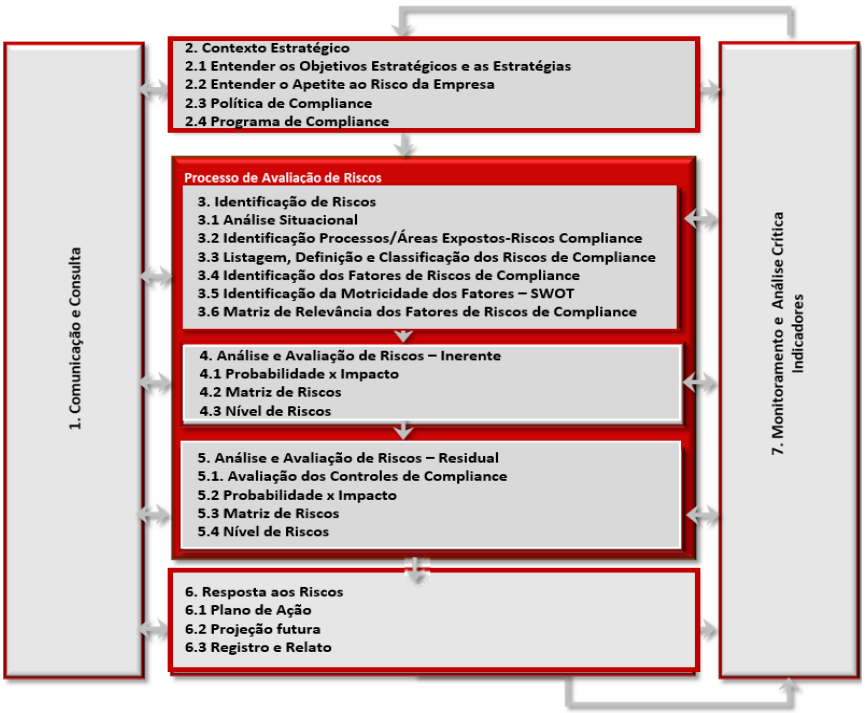
4.4 Análise e Avaliação de Riscos de *Compliance* – Inerente;

4.5 Análise e Avaliação de Riscos de *Compliance* – Residual;

4.6 Respostas aos Riscos de *Compliance*; e

4.7 Monitoramento e Análise Crítica – Indicadores

Figura 4: *Framework* do Processo de Gerenciamento de Riscos de *Compliance*



Fonte: Adaptado de BRASILIANO (2018).

Inicia-se o relato pelos elementos que dão suporte à construção do Manual de Risco de *Compliance.*

4.1 Comunicação e Consulta

Entende-se que a comunicação deve fluir em toda Organização. No caso específico da Empresa, objeto de estudo, a Comunicação e Consulta de Riscos de *Compliance* é responsabilidade conjunta da Gerência de Análise de Riscos e Conformidade, do Comitê de Ética e Integridade e, da Diretoria Executiva.

A fase de Comunicação e Consulta tem como finalidade estabelecer contato e relacionamento com os públicos de interesse da Empresa, de maneira interna, com os Gestores, Funcionários, Contratados Terceirizados e, de forma externa, com os Clientes, Fornecedores, Parceiros, Associações, Governo, Imprensa, Comunidades, entre outros.

A comunicação perpassa todas as demais fases do processo, conforme exposto na Figura 3. Ela é importante, também, porque tem a função de informar e sensibilizar cada um dos envolvidos no Processo para que o plano de comunicação alcance os melhores resultados.

As informações adquiridas nas Consultas realizadas embasam e orientam as partes no processo de tomada de decisão, de definição da alta direção a respeito de questões específicas.

4.2 Contexto Estratégico

Destaca-se no Contexto Estratégico a necessidade de conhecer o cenário de risco na qual a Empresa está inserida, para que as ações e tratativas reflitam o quanto de risco ela está disposta a aceitar, sendo indispensável ter conhecimento dos objetivos estratégicos, e saber quais os fatores críticos de sucesso.

Essa fase é de suma importância, pois possibilita um alinhamento entre o apetite ao risco com a estratégia da Empresa. Lembrando que a Empresa considera o apetite ao risco para avaliar as opções estratégicas e definir seus objetivos, a fim de que estes estejam alinhados com as estratégias definidas.

Na Matriz de Riscos são enquadrados os riscos segundo sua Capacidade de Risco, de Tolerância e do Apetite ao Risco, Brasiliano (2016, p.87).

Figura 5: Matriz de Riscos com Níveis de Apetite, de Tolerância e de Capacidade aos Riscos.

Fonte: Adaptado de Documento Interno da Empresa, objeto de estudo (2020).

Na Figura 05 é apresentada a Matriz de Riscos utilizada pela Empresa, objeto de estudo, e seus respectivos níveis de Apetite, de Tolerância e de Capacidade aos Riscos, com suas definições:

a) **Capacidade de risco** – são os quadrantes cuja criticidade é extrema, necessitando de ações imediatas. Para a Organização pesquisada, a Capacidade de Risco (representada pelo número "5" na Matriz) foi definida considerando os riscos cuja Probabilidade de concretização é elevada; já, o Impacto, é considerado massivo ou severo. Desta forma, são riscos que devem ser tratados prioritariamente, porquanto possuem elevado potencial de gerar danos à Instituição.

b) **Tolerância ao Risco** – elenca os quadrantes cuja criticidade está superior ao Apetite ao Risco; entretanto, seu tratamento poderá ser em período mais longo. Para a Companhia estudada, a Tolerância (representada pelo número "4" na Matriz) foi determinada considerando riscos com probabilidade considerável de se concretizar, e cujo impacto acarretará danos significativos à Organização. Assim sendo, estes riscos serão tratados em Regime de Urgência.

c) **Apetite ao Risco** – são os quadrantes cuja criticidade a Organização aceita, temporariamente, para atingir seus objetivos. Para a Instituição estudada, o Apetite ao Risco (representado pelo número "3" na Matriz) foi definido

considerando-se duas premissas: riscos com alta probabilidade de concretização, com impacto de possível gerenciamento; e riscos de baixa probabilidade de concretização, com impacto severo ou massivo, necessitando realizações de ações em médio prazo.

Quanto aos demais quadrantes -1 e 2 (na cor amarelo e verde da Matriz acima) tratam-se dos riscos cuja Probabilidade e Impacto podem ser aceitos pela Empresa, objeto de estudo, precisando de constante monitoramento.

Como uma recomendação para Gestão, está a definição do Apetite ao Risco na Política de Riscos das Empresas, representado na Matriz de Risco (Probabilidade e Impacto), sugere-se o descrito na Figura 4, seguindo definições da Matriz de Riscos com os Níveis de Apetite, de Tolerância e de Capacidade aos Riscos, definidos no Quadro 1.

Quadro 1: Apetite ao Risco X Tratamento X Atribuições

NÍVEL DO APETITE AO RISCO	**QUADRANTE**	**TRATAMENTO**	ATRIBUIÇÕES
1	**Monitoramento e Gestão**	Riscos com baixa criticidade, que apresentam consequências administráveis. Monitoramento de forma rotineira ou sistemática. **Ponto de monitoramento a cada 90 dias.** **Plano de Ação de acordo com a decisão do Gestor**	Dono do Processo (Gerência)
2	**Monitoramento e Gestão**	Riscos com alguma criticidade, mas que apresentam consequências administráveis. Monitoramento de forma rotineira ou sistemática. **Ponto de monitoramento a cada 60 dias.** **Plano de Ação de acordo com a decisão do Gestor**	Dono do Processo (Gerência)
3	**Apetite ao Risco**	**Riscos que podem ser assumidos desde que o custo não seja maior do que o benefício gerado.** A tomada de decisão deve ser registrada pelo Dono do Processo e pela Diretoria Responsável, com base em relatório. **Ponto de monitoramento a cada 30 dias.** **Plano de Ação de acordo com a decisão do Gestor.**	Dono do Processo (Gerência e Diretoria Responsável)
4	**Tolerância ao Risco**	Riscos críticos. Necessita tratamento a curto prazo com ações preventivas e/ou contingenciais. Podem ser assumidos somente em circunstâncias excepcionais, por meio do registro em formulário de risco assumido, assinado pela Diretoria e com a anuência dos acionistas. **As ações de prevenção e/ou mitigação devem ser propostas, aprovadas e iniciadas em até 20 dias.**	Diretoria Executiva juntamente com os acionistas

NÍVEL DO APETITE AO RISCO	QUADRANTE	TRATAMENTO	ATRIBUIÇÕES
5	**Capacidade de Risco**	Riscos não aceitáveis. Precisam de tratamento imediato com ações preventivas e contingenciais. Não podem ser assumidos em nenhuma circunstância. **As ações de prevenção e/ou mitigação devem ser propostas, aprovadas e iniciadas em até 14 dias.**	N/A

Fonte: Adaptado de Documento Interno da Empresa, objeto de estudo (2020).

Após conhecer os objetivos estratégicos da Empresa, objeto de estudo e entender sobre o Apetite ao Risco da Organização, é importante verificar como foi elaborada a Política de Gestão de Riscos e a Política de *Compliance.* A Empresa, objeto de estudo, administrava a Política de Gerenciamento de Riscos Corporativos, mas ainda não possuía a Política de *Compliance*.

Por conta disso, juntamente com a elaboração deste Manual foi elaborada a Política Interna de *Compliance*, a qual foi desenvolvida com a finalidade de estabelecer as diretrizes gerais de *Compliance*, norteando os demais documentos que compõem o Sistema de Gestão de *Compliance*; e, por sua vez, a Norma Interna de *Compliance*, tem o objetivo de instituir diretrizes específicas para a implementação, a manutenção, a análise crítica e a melhoria de um Programa de *Compliance*, auxiliando na Governança Corporativa, buscando mecanismos para prevenir, detectar e responder a eventuais desvios de conduta - incluindo atos de corrupção -, além de cumprir com as leis aplicáveis, de igual forma com a Lei Anticorrupção Brasileira n.º 12.846/13.

De posse das informações norteadoras do Processo, quais sejam: as Políticas de Riscos e de *Compliance*, as Normas Internas, os Objetivos Estratégicos conhecedores do Apetite ao Risco da Empresa, objeto de estudo, assim como da existência de outros *frameworks* já trabalhados, iniciaram-se os testes para a construção da Avaliação de Riscos de *Compliance*.

4.3 Identificação de Risco de *Compliance*

Na etapa de identificação de riscos é necessária a análise de todas as áreas da Empresa, objeto de estudo, propiciando a identificação de todos os fatores de riscos (causas) e os controles associados. Na Empresa, objeto de estudo, a análise é realizada por macroprocesso, em reuniões de tempestades de ideias, com participação dos colaboradores do macroprocesso analisado e de seus gestores.

Na fase de identificação, devem-se aplicar as ferramentas e técnicas mais adequadas em todos os Riscos de *Compliance*. Segundo Brasiliano (2018) esta fase é constituída por seis subetapas que visam subsidiar a identificação dos riscos de *Compliance:*

4.3.1 Análise Situacional

4.3.2 Identificação de Processos e áreas expostos aos Riscos de *Compliance*

4.3.3 Listagem, definição dos Riscos de *Compliance*

4.3.4 Identificação dos fatores de Riscos de *Compliance*

4.3.5 Identificação da motricidade dos fatores– SWOT

4.3.6 Matriz de relevância dos fatores

As seis subetapas estão detalhadas no Manual de Gerenciamento de Riscos de *Compliance*, disponível no apêndice, mais especificamente no item 4.3 do documento.

4.4 Análise e Avaliação de Riscos

A Análise e a Avaliação de Riscos serão calculadas utilizando a Probabilidade e o Impacto de cada evento, sem considerar os controles realizados pela Organização. Seguindo o disposto no item 5.3 da NBR ISO/IEC 31010, nas generalidades da avaliação dos riscos.

4.4.1 Probabilidade

Propomos que seja calculada neste modelo de Manual a aplicação com dois fatores. Cada fator de Probabilidade terá um peso diferenciado, tendo em vista seu grau de importância, a saber:

a) **Segurança/Controle:** serão avaliadas questões que tratam dos fatores de riscos e controles identificados. Quanto maior a nota, pior é a condição de segurança e dos controles (no risco inerente esse critério automaticamente é pontuado com nota 5); pois nele não avaliamos os controles realizados para prevenir e/ou mitigar os fatores de riscos.

b) **Frequência/Exposição:** diz respeito a, com que frequência o risco costuma se manifestar, podendo-se levar em consideração históricos internos ou externos

(empresas similares), além da exposição que a Empresa está a determinado risco, considerando o contexto.

Figura 6: Métricas para cálculo da Probabilidade

Fonte: Adaptado de BRASILIANO (2018).

As descrições para auxiliar na análise da nota a ser atribuída encontram-se no Descritivo de Escalas, no Apêndice deste documento - Manual de Gerenciamento de Riscos e de *Compliance*, item. 4.4.1.

O Descritivo de Escalas se faz necessário para tentar equalizar a interpretação dos critérios escolhidos, uma vez que estes são subjetivos, mas quantificados e, dessa forma, carecem de interpretação. Os pesos foram definidos após as reuniões com os Facilitadores e os Gestores; e os valores dos pesos aceitos na proposta apresentada para a empresa objeto de estudo, são diferentes dos apresentados no Estudo de Caso e no Manual do Apêndice. Ainda sobre a definição dos pesos, os mesmos foram validados pelo Comitê de Conduta e Integridade da Organização e serão aprovados pela Diretoria Executiva.

Para as futuras avaliações de riscos de *Compliance* é proposta a inclusão de mais uma métrica: Intervalo de validação, pelo qual serão consideradas as Auditorias Internas realizadas na Organização. Esta métrica foi proposta na Empresa, objeto de estudo, mas não foi aceita, embora tenha sido admitida como uma excelente opção, porém, constatou-se que, para efetuar a Probabilidade com as três métricas, será necessário maior alinhamento entre Auditoria Interna e Gestão de Riscos. No Quadro

02, apresenta-se sugestão de descrição para a métrica que sugerimos chamar Intervalo de validação.

Quadro 2: Descrição para Métrica de Intervalo de Validação

Intervalo de Validação (peso 3)		
Conceito	**Descritivo da Escala**	**Pontuação**
Anual	Apresenta registro de fiscalizações/auditorias anualmente	5
Mensal	Apresenta registro de fiscalizações/auditorias mensalmente	4
Quinzenal	Apresenta registro de fiscalizações/auditorias quinzenalmente	3
Semanal	Apresenta registro de fiscalizações/auditorias diariamente	2
Diário	Apresenta registro de fiscalizações/auditorias em todos os casos	1

Fonte: Elaborado pela Autora (2020).

O Nível de Probabilidade (PB) no Estudo de Caso é o resultado da média ponderada dos dois critérios de Probabilidade (multiplicação do peso, X a nota, dividida pela soma dos pesos), conforme demonstrado na Figura 03.
No Quadro 03 está descrita a classificação do nível de Probabilidade.

Quadro 3: Classificação para nível de Probabilidade.

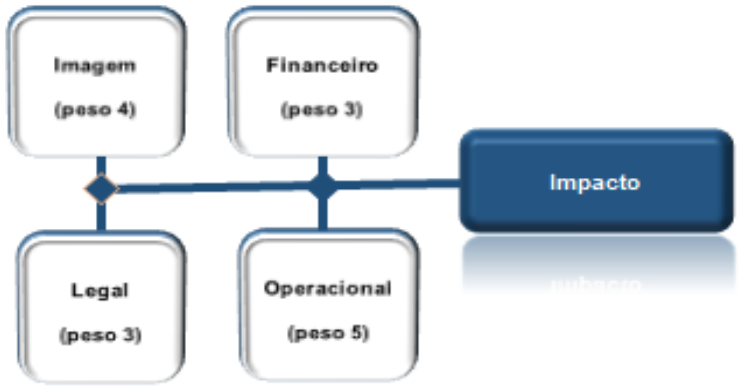
Grau de Probabilidade	Escala	Nível de Probabilidade
4,51 - 5,00	5	Muito provável
3,51 - 4,50	4	Provável
2,51 - 3,50	3	Possível
1,51 - 2,50	2	Improvável
1,00 - 1,50	1	Muito improvável

Fonte: Dados da Pesquisa (2020).

4.4.2 Impacto

Com o objetivo de se obter uma visão holística do Impacto, há a necessidade de se projetar todas as consequências que os riscos causam. Na Figura 07, apresenta-se a graduação para os critérios de avaliação do Impacto da ocorrência dos riscos:

Figura 7: Métricas para cálculo de Impacto



Fonte**:** Dados da Pesquisa (2020)

As descrições para auxiliar na análise da nota a ser atribuída encontram-se no Descritivo de Escalas, no Apêndice deste documento - Manual de Gerenciamento de Riscos de *Compliance*, item. 4.4.1. No Quadro 04, consta o Descritivo do Grau de Impacto.

Quadro 4: Descritivo do Grau de Impacto.

Grau de Impacto	Escala	Nível de Impacto	Interpretação
4,51 – 5,00	5	Catastrófico	Eventos que causam impactos nas operações, de maneira a paralisar os processos críticos da EMPRESA, atingindo o fluxo de caixa, a imagem, e com consequências gravíssimas para os Órgãos Reguladores.
3,51 – 4,50	4	Severo	Eventos que também causam impactos extremos nas operações, atingindo o fluxo de caixa e a imagem da EMPRESA.
2,51 – 3,50	3	Moderado	Eventos que causam impactos significantes, não atingindo as operações.
1,51 – 2,50	2	Leve	Eventos que causam impactos leves.
1,00 – 1,50	1	Insignificante	Eventos que causam pouco ou nenhum impacto.

Fonte: Dados da Pesquisa (2020).

4.4.3 Matriz de riscos - Inerente

A avaliação de riscos visa comparar os níveis de riscos em relação aos critérios pré-estabelecidos. A relevância dos riscos possui como parâmetro a Matriz de Riscos, e o seu resultado é o grau de criticidade do risco, ou seja, é a priorização que a Empresa deve utilizar para tratar cada risco frente ao seu Apetite ao Risco. A Matriz é dividida em quadrantes, e para cada quadrante existe uma estratégia de tratamento e priorização.

A Matriz de Riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Quanto maior for a probabilidade e o impacto de um risco, maior será o nível do risco. O detalhamento sobre os quadrantes da Matriz de Riscos e suas tratativas esperadas, pode ser visualizado no Quadro 01.

4.4.4 Nível de risco - Inerente

O Nível de Risco é um índice calculado com base na média ponderada das probabilidades e média ponderada dos impactos dos riscos identificados.

Para identificar o nível de risco é necessário utilizar critérios descritos no Quadro 05. Ainda, é importante ressaltar que quanto maior o nível do risco, maior sua criticidade.

Quadro 5: Descritivo do Grau de Impacto

NÍVEL DE RISCO			TRATAMENTO
1 a 5	**1**	**Verde**	Existe grau de riscos consideráveis, mas que causam consequências gerenciáveis. Devem ser monitorados de forma rotineira ou sistemática.
5,1 a 10	**2**	**Amarelo**	Devem ser monitorados de forma rotineira ou sistemática.
10,1 a 15	**3**	**Laranja**	Deve-se receber tratamento em médio e curto prazo. Possui riscos com probabilidades e/ou impactos consideráveis. Devem ser constantemente monitorados.
15,1 a 25	**4**	**Vermelho**	Alto grau de risco, podendo resultar em impacto extremamente severo. Exige implementação imediata de estratégias de prevenção e/ou continuidade.

Fonte: Dados da Pesquisa (2020).

4.5 Análise e Avaliação de Riscos – Residual

Risco residual considera em sua a avaliação os controles existentes. Esses conceitos permitem que os controles sejam verificados e avaliados, como também a sua efetividade seja comprovada durante os testes das Auditorias.

4.6 Avaliação dos controles - Residual

Com o objetivo de verificar a eficácia dos controles identificados no Processo em estudo, é necessário realizar a avaliação dos controles. No final desta etapa, a informação disponível permitirá ao executante conhecer a eficácia, a ineficácia ou a inexistência dos controles, bem como sua relação com os fatores de risco ou riscos, possibilitando, com isso, a análise de riscos residuais.

Para registro da avaliação dos controles, deve-se preencher formulário com descrição do Resultado e do Parecer, conforme Quadro 16, apresentado no item 4.4.3, do Apêndice.

Os controles identificados necessitam ser associados a um ou mais riscos ou fatores/causas de riscos. Conceitualmente, os controles preventivos atuam "bloqueando" fatores de risco; enquanto os controles detectivos atuam como alertas a possível concretização do risco. Esta associação permitirá identificar na análise de risco residual o quão exposto o risco está, norteando, inclusive, a atribuição da nota de "Segurança e Controle".

4.6.1 Probabilidade X Impacto - Residual

Para realizar a análise de riscos residuais, deve-se utilizar a metodologia e os critérios abordados na Subfase "4.5.1 Probabilidade x Impacto – Inerente", porém, há que se considerar os controles existentes e sua relação com os fatores de risco, como também, os riscos, atribuindo nota aos critérios "Segurança e Controle".

Todavia, se a Empresa apresentar controles que agem mitigando os impactos, é possível reavaliar as notas atribuídas aos critérios de Impacto.

4.6.2 Matriz de riscos - Residual

Para elaborar a Matriz de Riscos Residuais, utilizar a metodologia descrita na Subfase "4.5.2 Matriz de Riscos – Inerentes". Cabe destacar que devem ser utilizadas as notas de Probabilidade e Impacto residuais, considerando os controles identificados e avaliados para cada risco analisado.

A Matriz de Riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e o impacto. Desta forma, pela divisão da Matriz, em quatro quadrantes, podemos avaliar o nível de vulnerabilidade do Processo estudado ou do departamento. Quanto maior for a Probabilidade e o Impacto de um risco, maior será o nível do risco.

4.6.3 Nível de riscos – Residual

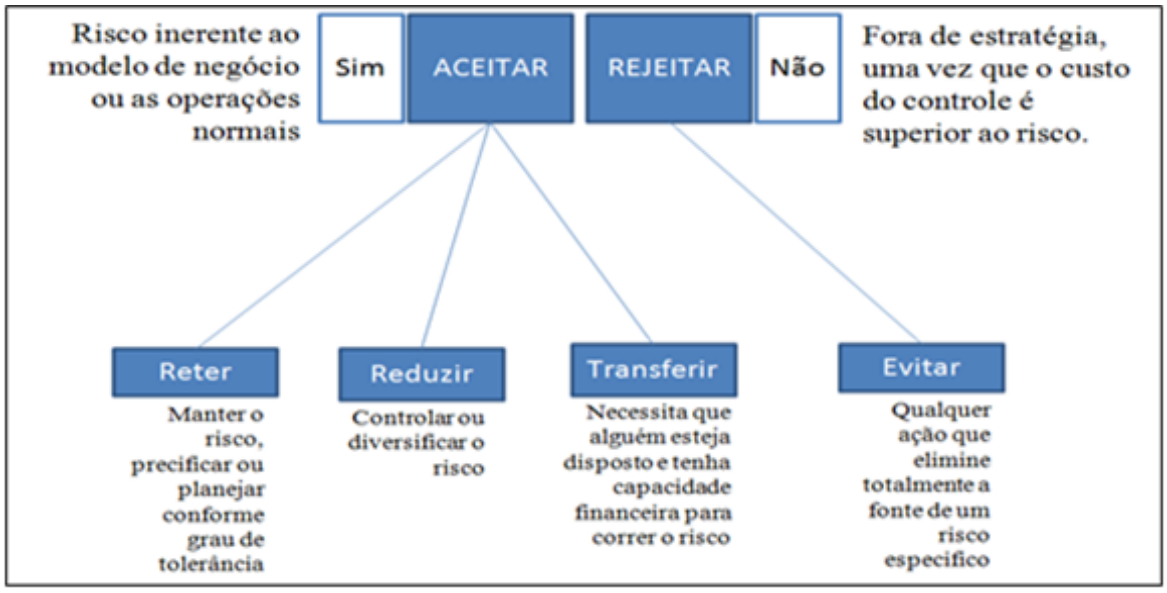
O Nível de Riscos residual reflete, por intermédio da média das probabilidades e dos impactos, o cenário de risco de uma forma geral. Trata-se de um indicador cuja descrição complementar consta no item 4.4.3, deste documento.

4.7 Respostas aos Riscos

Realizadas a identificação, a análise e a avaliação dos riscos, levando-se em consideração a Matriz de Riscos Residuais, e respeitando o Apetite ao Risco, é necessário determinar como será a Resposta aos Riscos.

Nesse contexto, os tomadores de decisão são os responsáveis por essa Gestão, ou seja, mediante a Matriz de Riscos deve-se identificar qual a resposta a ser adotada para o tratamento do risco, conforme figura 8. Na figura original, encontrada em Brasiliano (2009, Pg.112), consta mais uma categoria para tratar o ACEITAR, trata-se do EXPLORAR**,** o qual foi retirado das possibilidades, pois a Empresa, objeto de estudo ainda não realiza análise de riscos positivos.

Figura 8: Respostas aos Riscos



Fonte: Adaptado de BRASILIANO (2009).

As estratégias para tratamento de riscos estão descritas no Apêndice, item 4.6, do Manual. Neste item, constam as descrições de ferramenta para a realização e o registro dos Planos de Ação, além das informações para a realização do cálculo da Projeção futura dos riscos e dos seus registros.

4.8 Monitoramento e Análise Crítica

No que tange ao Monitoramento e a Análise Crítica percebe-se que ambos precisam ser planejados como parte do Processo e devem envolver a checagem e a vigilância regular. Eles podem ser periódicos ou acontecer em resposta a um fato específico. Para tanto, faz-se necessária a elaboração do relatório contendo os itens de monitoramento e os indicadores apurados, constando as justificativas essenciais para o entendimento. Assim, citam-se os seguintes tipos de indicadores, os quais estão detalhados no Apêndice:

a) Criticidade dos riscos residuais
b) Planos de Ação
c) Registros de Ocorrências (Materialização de riscos)

Ressalta-se a importância de as informações serem registradas com os dados organizados, permitindo a consolidação de indicadores que podem ser representados em um “painel de controle”, efetivando sua visualização de forma separada (por tipo) e de forma integrada.

5 RESULTADO

Como resultado obtido acerca da realização desta pesquisa, apresenta-se no apêndice uma Proposta de Manual de Gerenciamento de Riscos de *Compliance,* para o atendimento à Lei n.º 13.303 e ao Decreto n.º 8.420.

A Empresa, objeto de estudo, fazendo uso da metodologia proposta pelo Manual, apresentou sucesso em estruturar um procedimento de identificação dos riscos de *compliance* quando o processo de gerenciamento de riscos de *compliance* passa a integrar o processo de riscos corporativos. Assim, o processo torna possível identificar e analisar os riscos de *compliance*, pela construção de um Dicionário de Riscos de *Compliance*, realizando os registros das ações necessárias para "tratar" os fatores/causas dos riscos identificados.

Como este documento propõe um conjunto de ferramentas estruturadas e interconectadas, ele permite suporte de realização e de registro do processo de identificação e de análise dos riscos de *compliance*. Assim, essas ferramentas auxiliam no mapeamento e controle das ações para a mitigação de causas determinadas, com o objetivo de baixar as probabilidades. O conhecimento das causas dos riscos de *compliance* é basilar na criação de planos de ação, com foco na sustentabilidade e na continuidade de negócios, com o intuito de garantir a resposta aos impactos bem como em atendimento as normatizações de conformidade existentes no mercado.

Destaca-se que as métricas sugeridas promovem a realização da análise da probabilidade e dos impactos dos riscos de *compliance* identificados. Então, para o cálculo da probabilidade medida é composta por Segurança dos Controles e Frequência (exposição aos riscos); e para cálculo de Impacto os aspectos relacionados à Imagem, Legal, Financeiro e Operacional.

Para o cálculo da Probabilidade, apresentam-se neste primeiro momento duas métricas: Segurança dos Controles e Frequência (exposição aos riscos). Para as próximas rodadas, quando o processo de gerenciamento dos riscos *de compliance* estiver ultrapassado o momento de seu aculturamento e de aceite, sugere-se a inclusão de outra métrica: o Intervalo de validação. Para essa sugestão a probabilidade será assim calculada: Segurança dos Controles, Frequência (exposição aos riscos) e Intervalo de validação. Na métrica Intervalo de validação serão considerados os períodos em que ocorreu Auditoria e/ou Fiscalização.

Ao aplicar a metodologia apresentada no Manual, é possível identificar e

analisar os riscos de *Compliance*, pela construção de um Dicionário de Riscos de *Compliance*, realizando os registros das ações necessárias para “tratar” os fatores/causas dos riscos identificados.

Nessa linha de raciocínio, infere-se que o Manual proposto seja aplicável, assim como suas métricas sugeridas para cálculo de Probabilidade e de Impacto, para oferecer resposta aos riscos, monitorar e analisar criticamente o processo de *compliance*.

6 CONCLUSÃO

Esta pesquisa é pautada na necessidade de que a empresa objeto de estudo, precisar conhecer registrar e monitorar os riscos que afetam as condutas e a integridade da Organização, para, desta forma, servir de subsídio ao Programa de *Compliance*, também denominado Programa de Integridade.

A legislação brasileira, atendendo aos anseios dos cidadãos e investidores, passou a exigir processos de conformidade das empresas quanto à necessidade de conhecer, registrar e monitorar os riscos que afetam a integridade das organizações. Diante disso, a implantação do Programa de *Compliance* é um novo passo perante as atuais regras de mercado, onde a legislação exige maior transparência das intuições públicas e privadas, demonstrando a integridade das mesmas.

Nesse viés, constata-se imprescindível criar e aprimorar normatizações e procedimentos de Gestão nas Organizações, a fim de priorizar e garantir recursos que atendam às necessidades existentes e à efetividade dos registros do Gerenciamento de Riscos, fornecendo assim, fundamentos da melhoria contínua do Processo.

Nessa linha de raciocínio, objetivo geral deste trabalho que consiste em apresentar uma proposta de Manual de gerenciamento de riscos de *compliance* foi atingido, com a apresentação e estruturação do manual constante no apêndice deste documento. Uma vez que essa proposta passou por diversas validações internas na empresa objeto de estudo infere-se que a execução do processo de gerenciamento de riscos de *compliance*, seja aplicável, assim como as métricas sugeridas para cálculo de Probabilidade e de Impacto.

Ressalta-se, também, que é importante conhecer as Organizações para que o Manual, ao ser aplicado em outras Instituições, considere os ajustes necessários quanto a pesos e descrições de métricas, os quais espelhem os valores e o negócio de cada pessoa jurídica.

O Manual ainda traz informações sobre critérios para realizar a análise de riscos de c*ompliance,* tais critérios são incipientes tanto no mercado quanto na literatura. Com a estrutura proposta pelo Manual, o programa de *compliance* direcionará suas ações para mitigar riscos de desvio de conduta.

Destaca-se que na realização dos testes de aplicação do Manual, junto aos facilitadores, constatou-se que a área de Gerenciamento de Riscos e Conformidade terá melhores resultados na aplicação deste Manual ao ter o apoio e patrocínio da alta

administração. Pois sem esse comprometimento da alta administração, poderá existir a falta de recursos para área de gestão de risco e conformidade, dificultando ou impedindo o desempenho de suas atividades com eficácia. O patrocínio da alta administração nas Organizações fortalece a conscientização de todos os colaboradores, deixando clara a responsabilidade que cabe a cada um, no que tange a conduta no desempenho de suas funções e o respeito a normatizações existentes.

No que diz respeito à cultura interna dos Colaboradores, esta deve refletir os valores da Organização, e cada líder deverá executar suas tarefas em sincronia, pois as ações de todos resultarão no resultado esperado.

Por derradeiro, para trabalhos futuros sugere-se como tema, averiguação do alinhamento entre as atividades de gestão de riscos, conformidade e auditoria interna, com fito de esclarecer as definições das atividades das linhas de defesa das organizações.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 37.301: Sistemas de Gestão de Compliance. Rio de Janeiro: ABNT, 2021.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 31000: Gestão de riscos, princípios e diretrizes. Rio de Janeiro: ABNT, 2018.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO 31000: Gestão de riscos, princípios e diretrizes. Rio de Janeiro: ABNT, 2009.

ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 31010: Gestão de riscos, técnicas para o processo de avaliação de riscos. Rio de Janeiro: ABNT, 2012.

ADAMS, John. Risco. São Paulo: Editora SENAC, 2009.

ANDREISOVÁ, *Ing*. Lucie. *Building and Maintaining an Effective Compliance Program. International Journal of Organizational Leadership, University of Economics in Prague, Czech Republic*, pg. 24-39, 2016.

ASSIS, Marcos. Governança, Riscos e *Compliance*: mudando a conduta nos negócios. São Paulo: Editora Saint Paul, 2017.

AZEVEDO, Mateus Miranda de; CARDOSO, Antônio Almeida; DARTE, Jairo Gonçalves; FEDERICO, Bianca Ellen; LIMA, Marco Antônio Ferreira. O Compliance e a Gestão de Riscos nos Processos Organizacionais. Revista de Pós-Graduação Multidisciplinar, São Paulo, v. 1, n. 1, pg. 179-196, março-junho, 2017.

BRASIL. DECRETO n.º 8.420, DE 18 DE MARÇO DE 2015. Regulamenta a Lei n.º 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências, Brasília, DF, mar 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm. Acesso em: 16 out. 2020.

BRASIL, LEI n.º 12.846, DE 01 DE AGOSTO DE 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências, Brasília, DF, 01 ago 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 16 out. 2020.

BRASIL, LEI n.º 13.303, DE 30 DE JUNHO DE 2016. Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios, Brasília, DF, 30 jun 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-

2018/2016/lei/l13303.htm. Acesso em: 16 out. 2020.

BRASILIANO, Antônio Celso Ribeiro. Gestão e Análise de Riscos Corporativos: Método Brasiliano Avançado - Editora Sicurezza, 2009.

BRASILIANO, Antônio Celso Ribeiro. Cenários Prospectivos em Gestão de Riscos Corporativos, um estudo de caso brasileiro - Editora Sicurezza, 2010.

BRASILIANO, Antônio Celso Ribeiro. Inteligência em Riscos - Gestão Integrada em Riscos Corporativos. Editora Sicurezza, 2016.

BRASILIANO, Antônio Celso Ribeiro. Inteligência em Riscos [livro eletrônico] - Gestão Integrada em Riscos Corporativos, 2ª edição revisada e ampliada com o COSO 2017 e ISO 31000:2018. São Paulo: Editora Sicurezza, 2018.

CARVALHO, André Castro; BEROLCCELLI, Rodrigo de Pinho; ALVIM, Tiago Cripa e VENTURINI, Otávio. Manual de *Compliance*. Rio de Janeiro: Editora Forense Ltda, 2018.

CASTRO, Rodrigo Pironti Aguirre de; GONÇALVES, Francine Silva Pacheco. *Compliance* e Gestão de Riscos nas Empresas Estatais. Belo Horizonte: Editora Fórum, 2018.

CHARAN, Ran; tradução Cristina Yamagami. Reinventando a Governança Corporativa. São Paulo: Editora Campus, 2010.

COELHO, Cláudio Carneiro Bezerra Pinto. Compliance na Administração Pública: Uma necessidade para o Brasil. RDFG – Revista de Direito da Faculdade, Guanambi, v. 3, n. 1, pg.75-95, julho-dezembro, 2016.

COSO - Gerenciamento de Riscos Corporativos - estrutura integrada. PricewaterhouseCoopers, 2017. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf. Acesso em: 16 out. 2020.

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Manual de Gerenciamento de Riscos Estratégicos da Empresa Pesquisada. Florianópolis, 2019.

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Política Interna de *Compliance* da Empresa Pesquisada. Florianópolis, 2021.

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Política Interna de Gerenciamento de Riscos da Empresa Pesquisada. Florianópolis, 2019.

GARETH, Morgan; tradução Geni G. Golldschmidt. Imagens da Organização. São Paulo: Editora Atlas SA, 2007.

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

GUIDE, F. C. P. A. A Resource Guide to the US Foreign Corrupt Practices Act. By the Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, 2012.

Instituto Brasileiro de Governança Corporativa. Gerenciamento de Riscos Corporativos: evolução em governança e estratégia. São Paulo: IBGC, 2017. (Série Cadernos de Governança Corporativa, 19). Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21794/Riscos%20cad19.pdf. Acesso em: 17 nov. 2020.

Instituto Brasileiro de Governança Corporativa. *Compliance* à Luz da Governança Corporativa. São Paulo: IBGC, 2017.(Série: IBGC Orienta). Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/23486/Publicacao-IBGCOrienta-*Compliance*SobaLuzDaGC-2017.pdf. Acesso em: 17 nov. 2020.

Instituto Brasileiro de Governança Corporativa. Código das Melhores Práticas de Governança Corporativa. 5.ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21138/Publicacao-IBGCCodigo-CodigodasMelhoresPraticasdeGC-5aEdicao.pdf. Acesso em: 17 nov. 2020.

Instituto dos Auditores Internos do Brasil – Modelo das Três linhas do IIA, Uma atualização das três linhas de defesa, 2020. Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf. Acesso em: 17 nov. 2020.

La Fabrica de Pensamiento – Instituto de Auditores Internos de Espanã, Definición e Implantición de Apetito de Riesgo, 2013. Disponível em: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf. Acesso em: 29 ago. 2021.

LUCAS, Luiz Fernando. A Era da Integridade: Homo conscious - A próxima evolução. São Paulo: Gente Editora, 2020.

MELO, Hildegardo Pedro Araujo de; LIMA, Adilson Celestino de. Instituto Compliance no Brasil e a Eficácia na Mitigação ao Risco Corporativo. Revista Evidenciação Contábil & Finanças, ISSN 2318-1001, João Pessoa, v. 7, n.3, p.60-82, Set./Dez. 2019.

OLIVEIRA, Rafael Carvalho Rezende; ACOCELLA, Jéssica. Governança Corporativa e *Compliance*. São Paulo: JusPodivm, 2019.

PADOVEZE, Clóvis Luís. Gerenciamento do Risco Corporativo em Controladoria. São Paulo: Cengage Learning, 2008.

PETERS, Marcos. Implantando e Gerenciando a Lei Sarbanes Oxley. São Paulo: Atlas, 2007.

VERÍSSIMO, Carla. *Compliance*: Incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.

RINALDI, Alexandra. A Importância da Comunicação de Risco para as Organizações. São Paulo: Sicurezza, 2010.

APÊNDICE

MANUAL DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*

MANUAL DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*

Florianópolis

2021

ELABORADO POR:

VALDETE APARECIDA ANDRETT

MANUAL DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*

Florianópolis

2021

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

APRESENTAÇÃO

A Gestão de Riscos nas Organizações deve ser responsabilidade presente em todos os níveis hierárquicos, não só dos Gestores, mas também de todos os Colaboradores, fato esse que contribui para agregar vantagens competitivas e criar valores, sendo eles: de preservação de sustentabilidade, de tutela da sua imagem corporativa e de prevenção dos atos de fraude.

Além disso, o Gerenciamento de Riscos também proporciona superação aos efeitos das incertezas, com maior capacidade para alcançar seus objetivos, com isso, o simples fato de uma atividade existir, abre a possibilidade da ocorrência de eventos ou de uma combinação de eventos; e suas consequências promovem oportunidades para obter vantagens, ou, por vezes, para ameaçar o sucesso da atividade.

Nesse viés, o presente trabalho se fundamenta na necessidade de conhecer, registrar e monitorar os riscos que afetam as condutas e a integridade das Organizações. Então, por meio da Gestão de Riscos de *Compliance*, a Instituição compartilha opiniões e aprimora as tomadas de decisão, uma vez que, além de mitigar Riscos de *Compliance,* proporciona o diálogo entre os diferentes *stakeholders*. Dentre os riscos de *Compliance,* elencam-se: a corrupção, o suborno, o assédio (moral e sexual), a discriminação, o conflito de interesses, os roubos, as fraudes contábeis, a evasão fiscal, o desrespeito aos direitos humanos e trabalhistas, bem como as vulnerabilidades cibernéticas.

Assim, partindo-se da afirmação acima, verificamos oportuno, segundo Castro e Gonçalves (2018), decidir e direcionar ações nas relações da Administração, mantendo o caminho da integridade, com o intuito de criar e aprimorar procedimentos de Gestão e Controle, além de priorizar e garantir recursos que atendam às necessidades existentes e à efetividade dos registros da Gestão de Riscos de *Compliance*, fornecendo, portanto, fundamentos para a melhoria contínua do Processo.

Então, apresentamos este Manual como um direcionador do Processo de Gerenciamento de Riscos de *Compliance.*

1. OBJETIVO DO DOCUMENTO

Este documento tem por objetivo estruturar uma metodologia e propor parâmetros ao Processo de Gestão de Riscos de *Compliance* à Empresa XYZ.

Didaticamente neste Manual estaremos denominando a empresa como XYZ.

2. ABRANGÊNCIA/APLICAÇÃO

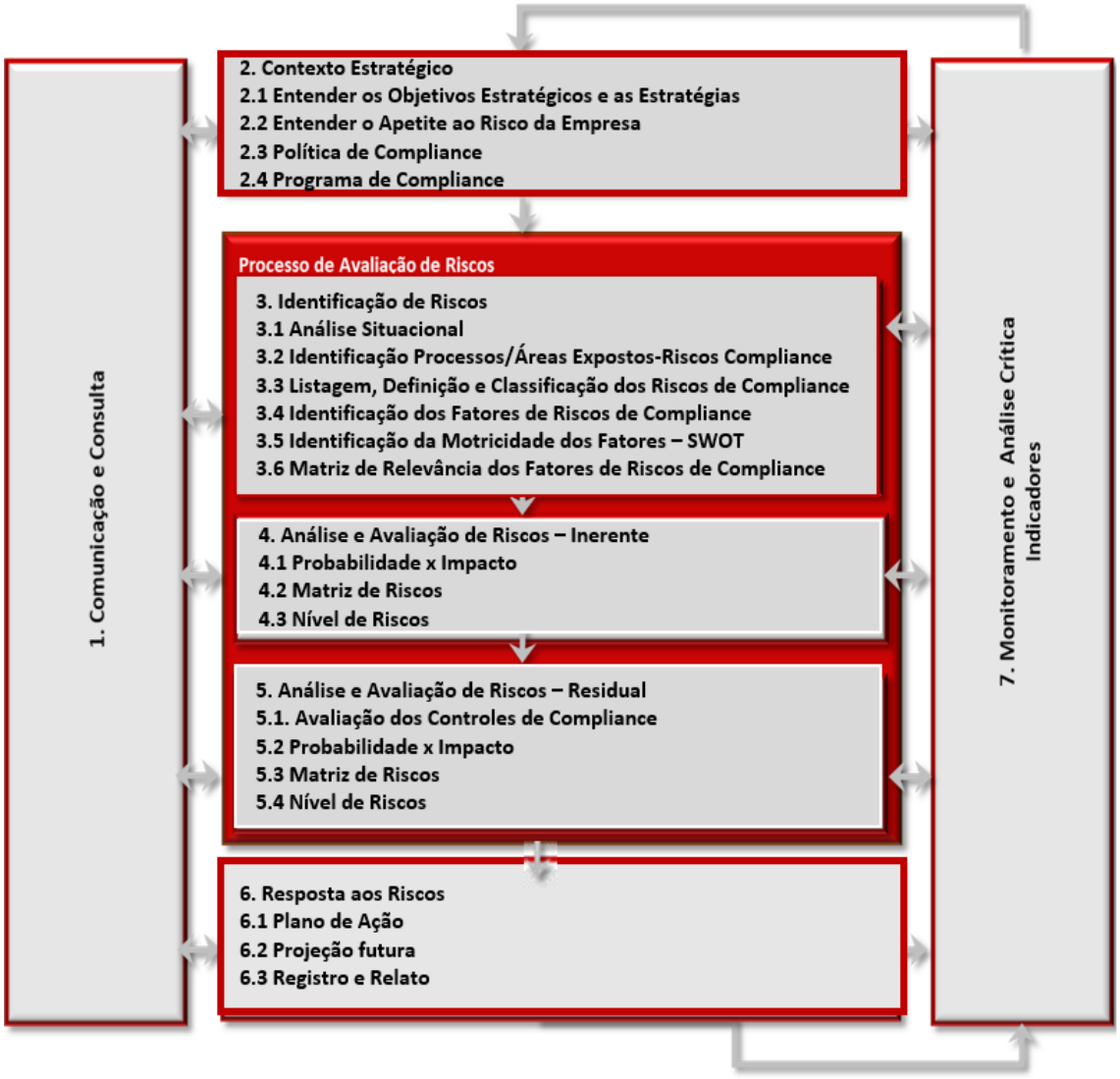
Este documento é aplicado aos Colaboradores e a todas as partes interessadas que se relacionam com a Empresa, independentemente do nível hierárquico.

3. DESCRIÇÃO DA METODOLOGIA

O Processo de Gerenciamento de Riscos de *Compliance* da Empresa XYZ compreende sete (07) fases, interconectadas, conforme os itens abaixo, e a Figura 01 a seguir:

1. Comunicação e Consulta;
2. Contexto Estratégico;
3. Identificação de Risco de *Compliance*;
4. Análise e Avaliação de Riscos de *Compliance* - Inerente;
5. Análise e Avaliação de Riscos de *Compliance* - Residual;
6. Respostas aos Riscos de *Compliance*; e
7. Monitoramento e Análise Crítica - Indicadores.

Figura 01: Framework do Processo de Gerenciamento de Riscos de *Compliance*



Fonte: Adaptado de BRASILIANO (2018)

O Framework acima apresenta a Metodologia Brasiliano (2018), com pequenas adaptações organizadas pela Autora.

A seguir, detalharemos as fases do Processo de Gerenciamento de Riscos de *Compliance* da Empresa XYZ.

4. FASES DO PROCESSO DE GERENCIAMENTO DE RISCOS DE *COMPLIANCE*

4.1 COMUNICAÇÃO E CONSULTA

Comunicação e Consulta é a forma de executar o processo e estabelecer a estratégia de comunicação com as partes interessadas. Esta fase permeia todo o Processo de Gestão de Riscos, até porque sem a comunicação, não existe esse Processo, tendo em vista a necessidade de sensibilizar aqueles que dele fazem parte.

4.2 CONTEXTO ESTRATÉGICO

4.2.1 Entender os objetivos estratégicos

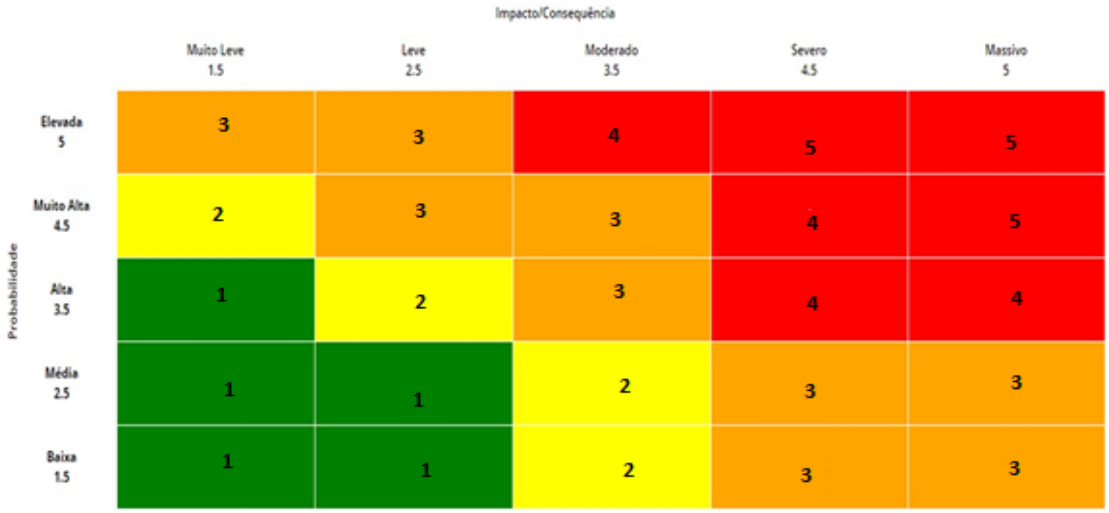
Para o desenvolvimento do Processo de Gerenciamento de Riscos, é essencial conhecer os contextos interno e externo da Empresa XYZ, além de seus potenciais impactos para o Programa de *Compliance*.

4.2.2 Entender o Apetite ao Risco da Empresa

Conhecer o cenário de risco em que a Empresa está inserida é importante para que as ações e tratativas reflitam o quanto de risco ela está disposta a aceitar, sendo fundamental, também, estar a par dos objetivos estratégicos, e identificar quais são os fatores críticos de sucesso.

A Política Interna de Gerenciamento de Riscos deverá ser aprovada pelos Órgãos competentes, definidos conforme a Estrutura Organizacional e normatizações internas de cada Organização. Assim, na Empresa, objeto de estudo, a aprovação das normatizações internas é realizada pela Diretoria Executiva, e posteriormente apresentada ao Conselho de Administração. Por conseguinte, após ser conhecida a instância que aprova, e definido qual o Apetite ao Risco a Organização tem, este apetite pode ser representado na Matriz de Risco (probabilidade e impacto), exposta, neste caso, no Manual de Riscos Estratégicos da Empresa, objeto de estudo, conforme estratificação na Figura 2, abaixo:

Figura 02: Matriz de Riscos com os Níveis de Apetite, Tolerância e Capacidade aos Riscos.



Fonte: Adaptado de Documento Interno da Empresa, objeto de estudo (2020).

O Apetite ao Risco de cada Organização pode ser estruturado a partir de quadrantes, de níveis e de atribuições. No contexto apresentado pela Empresa, objeto de estudo, observamos o Apetite ao Risco, os tratamentos para as causas dos riscos enquadrados em cada quadrante, e as atribuições que definem, hierarquicamente, quem é o "dono do risco" analisado, descritas no Quadro 01.

Quadro 01: Apetite ao Risco x Tratamento x Atribuições

NÍVEL DO APETITE AO RISCO	**QUADRANTE**	**TRATAMENTO**	ATRIBUIÇÕES
1	**Monitoramento e Gestão**	Riscos com baixa criticidade, que apresentam consequências administráveis. Monitoramento de forma rotineira ou sistemática. **Ponto de monitoramento a cada 120 dias.** **Plano de Ação de acordo com a decisão do Gestor**	Dono do Processo (Gerência)
2	**Monitoramento e Gestão**	Riscos com alguma criticidade, mas que apresentam consequências administráveis. Monitoramento de forma rotineira ou sistemática. **Ponto de monitoramento a cada 90 dias.** **Plano de Ação de acordo com a decisão do Gestor**	Dono do Processo (Gerência)
3	**Apetite ao Risco**	**Riscos que podem ser assumidos desde que o custo não seja maior do que o benefício gerado.** A tomada de decisão deve ser registrada pelo Dono do Processo e pela Diretoria Responsável, com base em relatório. **Ponto de monitoramento a cada 60 dias.**	Dono do Processo (Gerência e Diretoria Responsável)

NÍVEL DO APETITE AO RISCO	QUADRANTE	TRATAMENTO	ATRIBUIÇÕES
		Plano de Ação de acordo com a decisão do Gestor.	
4	**Tolerância ao Risco**	Riscos críticos. Necessita tratamento a curto prazo com ações preventivas e/ou contingenciais. Podem ser assumidos somente em circunstâncias excepcionais, por meio do registro em formulário de risco assumido, assinado pela Diretoria e com a anuência dos acionistas. **As ações de prevenção e/ou mitigação devem ser propostas, aprovadas e iniciadas em até 30 dias.**	Diretoria Executiva juntamente com os acionistas
5	**Capacidade de Risco**	Riscos não aceitáveis. Precisam de tratamento imediato com ações preventivas e contingenciais. Não podem ser assumidos em nenhuma circunstância. **As ações de prevenção e/ou mitigação devem ser propostas, aprovadas e iniciadas em até 20 dias.**	N/A

Fonte: Adaptado de Documento Interno da Empresa, objeto de estudo (2020).

4.2.3 Política de *Compliance*

O presente Processo de Gestão de Riscos de *Compliance* está ligado às diretrizes corporativas da Empresa XYZ, em especial, à Política de Gestão de Riscos e à Política de *Compliance*. Tais Políticas visam estabelecer as diretrizes vinculadas às normatizações internas de *Compliance* de Riscos, e devem ser observadas e, criteriosamente, seguidas por todos os funcionários, que são também responsáveis por orientar e conscientizar todas as partes interessadas.

Especificamente, nessa realidade, a Política de *Compliance* busca atender às políticas da Organização, aos requisitos legais aplicáveis ao seu negócio, à Lei Anticorrupção brasileira n.º 12.846/13 e o Decreto n.º 8.420/2015, e a qualquer outra lei aplicável à Empresa XYZ e às boas práticas de *Compliance* adotadas pela sociedade.

Registramos ainda, que as referidas Políticas prezam pelo relacionamento ético e íntegro, e não toleram, pois, atos de corrupção, suborno, fraude, lavagem de dinheiro ou sonegação fiscal, assim como quaisquer outros desvios de conduta que sejam praticados, diretamente ou indiretamente, contra as Organizações Públicas ou Empresas Privadas.

Assim sendo, para atingir seus objetivos, faz-se imprescindível a adoção de um Programa de *Compliance*, baseado na identificação, na análise, bem como na avaliação

dos riscos de *Compliance*, propondo ações para manter o estudo dos riscos atualizado, com o intuito de considerar as mudanças de cenários internos e externos, estimulando assim, o combate à corrupção e a outros desvios de conduta.

4.2.4 Programa de *Compliance*

O Programa de *Compliance* tem a finalidade de prevenir, detectar e corrigir atos não condizentes com os valores da Organização, de acordo com a legislação vigente. E ainda, deve ser incluído como padrão de valorização comportamental, refletido em todas as atividades e integrado ao negócio da Empresa XYZ.

4.3 IDENTIFICAÇÃO DE RISCOS

Na fase de Identificação de Riscos, é necessária a análise de todas as áreas da Empresa XYZ, propiciando, com isso, a identificação de todos os fatores de riscos (causas) e os controles associados. Destacamos, aqui, que a análise na Empresa XYZ pode ser realizada por macroprocesso, por processo ou por área de negócio.

Na identificação, todos os riscos de *Compliance* devem ser listados. Para tanto, importante que sejam aplicadas as ferramentas e as técnicas mais adequadas, as quais são compostas por seis (06) subetapas da identificação de riscos de *Compliance.*

4.3.1 Análise situacional

A fim de que tenhamos uma visão holística e bem acurada dos riscos, identificam-se os fatores de riscos (causas) e os controles dos diversos macroprocessos, desenvolvendo-se as seguintes atividades:

a) **Análise situacional:** a primeira linha de defesa (Gestores das áreas) deve avaliar criticamente seus processos, com o objetivo de identificar pontos fortes (controles) e pontos fracos (fatores de riscos), que sirvam para mitigar ou potencializar a concretização dos riscos relacionados à *Compliance*.

b) **Identificação de histórico:** mapear o histórico de ocorrências de risco de *Compliance*.

Os controles, após identificados, são registrados com os seguintes dados:

- Código: identificação alfa numérica do controle (Exemplo: C001);
- Controle: nome do controle (Exemplo: Aprovação segregada);
- Definição: descrição detalhada do controle;

- Objetivo: refere-se à finalidade do controle;
- Tipo: se o controle é “Manual”, fica a cargo da intervenção humana; se é “Automático”, independe da intervenção humana;
- Categoria: se o controle é “Preventivo”, previne a concretização do risco; se é “Detectivo”, alerta sobre a iminência de concretização do risco; e
- Periodicidade: refere-se ao intervalo de execução do controle, podendo ser “Sob demanda”, “Diário”, “Semanal”, “Mensal”, “Trimestral”, “Semestral” e “Anual”.

A seguir, no Quadro 02, segue sugestão para registro dos contoles:

Quadro 02: Modelo de Tabela de Registro de Controle

Código	Controle	Definição	Tipo	Categoria	Periodicidade	Objetivo

Fonte: Dados da Pesquisa (2020).

Os fatores de risco, após identificados, são registrados com os dados abaixo:

- Código: identificação alfa numérica do controle (Exemplo: FR 01);
- Fator de Risco: nome do fator de risco;
- Definição: descrição detalhada do fator de risco; e
- Macrofator: refere-se à categoria do fator de risco, sendo eles: Processos, Pessoal, Tecnologia, Infraestrutura e Ambiente Externo.

Sugestão para registro dos fatores/causas de riscos no Quadro 03, abaixo:

Quadro 03: Modelo de Tabela de Registro de Fatores de Risco

Código	Fator de Risco	Definição	Macro fator

Fonte: Dados da Pesquisa (2020).

4.3.2 Identificação de Processos e áreas expostas aos riscos de *Compliance*

Averiguar e ranquear os macroprocessos ou as áreas de negócio, a fim de saber quais deles têm propensão a sofrer desvio de condutas e quais têm maior contato com o público externo, podendo, com isso, mapear as áreas mais propensas a ocorrência de suborno, de fraude e de conflitos de interesse.

4.3.3 Listagem, definição e classificação dos riscos de *Compliance*

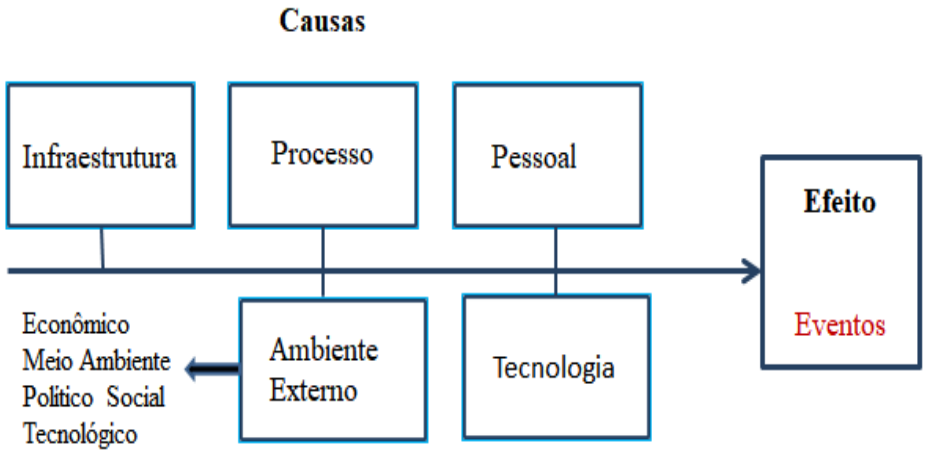
Riscos de *Compliance* são eventos relacionados ao descumprimento de legislações, de normas e de compromissos por parte dos Colaboradores ou de terceiros, agindo em interesse próprio ou da Empresa XYZ, independente da anuência ou do conhecimento de seus Gestores.

A listagem dos riscos pode ser realizada mediante reuniões do tipo *brainstorming,* levantando-se tanto os riscos já identificados quanto aqueles que nunca aconteceram no contexto da Empresa XYZ, mas que poderão surgir.

4.3.4 Identificação dos fatores de riscos de *Compliance*

Os fatores de risco são, na realidade, a origem, melhor dizendo, a causa de cada evento identificado. Para compreender efetivamente o risco, é necessário se aprofundar em suas causas, utilizando, para isso, a técnica do Diagrama de Causa e Efeito, também conhecido como Diagrama de Ishikawa. Trata-se de uma técnica simples para identificar fatores que podem causar o evento analisado.

Figura 03: Diagrama de Causa e Efeito - Macro causas.



Fonte: BRASILIANO (2009).

Apresentamos abaixo o detalhamento das macro causas do Diagrama sugerido por Brasiliano (2009, p.69), na Figura 03, de acordo com o Quadro 04.

Quadro 04: Detalhamento do Diagrama de Causa e Efeito

Macro Causa	Definição
Processo	Influência da existência de processos, políticas, normas e procedimentos para a materialização do risco.
Pessoal	Influência do nível da equipe envolvida, considerando-se perfil e qualificação para a materialização do risco, bem como do nível de relacionamento dos Colaboradores.
Infraestrutura	Influência da existência de recursos físicos e sistemas eletrônicos para a materialização do risco.
Tecnologia	Influência dos sistemas de informação utilizados pela Companhia para a materialização do risco.
Ambiente Externo	Influência das variáveis externas incontroláveis para a materialização do risco.

Fonte: Dados da Pesquisa (2020).

Para cada risco identificado, será elaborado um Diagrama de Causa e Efeito específico. Se estivermos estudando quatro (04) riscos, teremos que elaborar quatro (04) Diagramas.

4.3.5 Identificação da motricidade dos fatores – SWOT

Concluída a identificação dos fatores de riscos, passaremos para a identificação dos fatores comuns nos riscos mapeados. Assim, para reconhecer a relevância dos fatores de riscos, utiliza-se a Matriz SWOT ou "FOFA" - técnica conhecida por identificar os pontos fracos, os pontos fortes, as oportunidades e as ameaças do contexto da Empresa.

A avaliação das forças e fraquezas diz respeito ao ambiente interno, ou seja, às condicionantes que a Empresa possui no que tange ao domínio de ação e à decisão - os chamados fatores de riscos internos ou variáveis internas, podendo ser negativas (fraquezas) ou positivas (forças). Já, os fatores de riscos considerados incontroláveis dizem respeito à ambiência externa, podendo ser negativa (ameaças) ou positiva (oportunidades).

Para identificar a relevância dos fatores de riscos são utilizados dois critérios de avaliação, a saber: Magnitude e Importância.

a) **Magnitude:** representa o número de vezes que o fator de risco é identificado nos Diagramas de Causa e Efeito dos Riscos mapeados e, por consequência, seu potencial grau de influência perante o rol de riscos em estudo. A Magnitude é ranqueada utilizando-se uma pontuação que varia de

1 a 3, sendo positiva (forças e oportunidades) ou negativa (fraquezas e ameaças).

- -1 (baixo);
- -2 (médio); e
- -3 (alto) para cada variável negativa (fraqueza e ameaça).

Exemplo de cálculo para a nota de Magnitude:

Caso um fator de risco apareça cinco (05) vezes em seis (06) riscos identificados, significa que esta variável possui "alta" Magnitude, e a nota será -3, conforme tabela de cálculo exemplificada no Quadro 05, a seguir:

Quadro 05: Exemplo de Cálculo para nota de Magnitude

Total de Riscos (6) / 3 = 2 (Frequência)

Quantidade de Riscos	6
Frequência	2,0

NOTAS	ESCALA		
-1	1	a	2
-2	3	a	4
-3	5	a	6

Fonte: Dados da Pesquisa (2020).

Nota: A frequência e a tabela de pontuação vão variar sempre que a quantidade de riscos for alterada.

b) **Importância:** trata-se da importância que o fator de risco tem para a concretização dos riscos no contexto em análise. Ainda, é uma nota subjetiva, com base na percepção dos envolvidos na avaliação do contexto. A valoração da importância situa-se em 3 níveis de pontuação:

- 3 (muito importante);
- 2 (média importância); e
- 1 (pouca importância).

Para criar um *ranking* dos itens em cada célula da Matriz SWOT, multiplica-se a avaliação da Magnitude e da Importância. Os fatores de riscos com maior pontuação negativa são considerados motrizes, pois podem influenciar diretamente os riscos identificados.

A Matriz SWOT (Figura 4), adaptada para a Gestão de Riscos, permite visualizar o todo; enquanto o Diagrama de Causa e Efeito visualiza somente o risco analisado. Com esta "fotografia", o Gestor verificará seus pontos de maior fragilidade, podendo, com isso, utilizar as informações da Matriz SWOT como balizadoras para analisar os riscos.

Figura 04: Matriz SWOT

Fonte: BRASILIANO (2018).

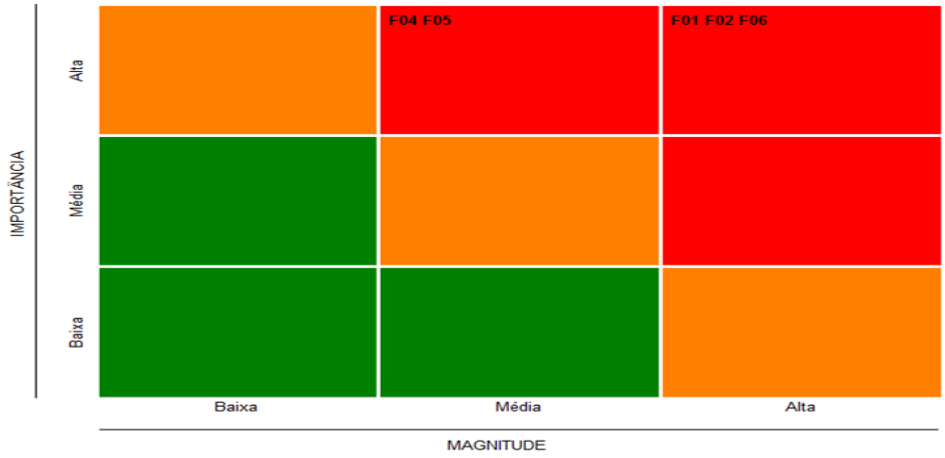
Cabe destacar que as variáveis negativas (fraquezas e ameaças) da Matriz SWOT são a base para a elaboração do Plano de Ação.

4.3.6 Matriz de relevância dos fatores de risco

O resultado do cruzamento da "Importância x Magnitude" define o nível de motricidade do fator de risco, isto é, se estará alocado no quadrante vermelho, laranja ou verde. Com base nesta alocação, o Gestor poderá determinar a prioridade de tratamento do fator de risco, sempre considerando como primeiro nível, o vermelho; segundo nível, o laranja; e o terceiro nível, o verde.

A Matriz auxilia na visualização do enquadramento dos fatores de riscos, conforme exemplificado na Figura 05.

Figura 05: Matriz de Magnitude x Importância



Fonte*:* BRASILIANO (2018).

4.4 ANÁLISE E AVALAÇÃO DE RISCOS - INERENTES

Nos riscos identificados, serão realizadas as análises e as avaliações consoante a metodologia aqui proposta para a avaliação dos riscos. Esta metodologia segue os dois parâmetros para a avaliação, que são definidos na ISO31000, quais sejam: conhecer a **probabilidade** dos eventos, quando ocorrerem, e calcular o **impacto,** quando vierem a acontecer.

A análise e a avaliação serão averiguadas sem considerar os controles nas causas identificadas.

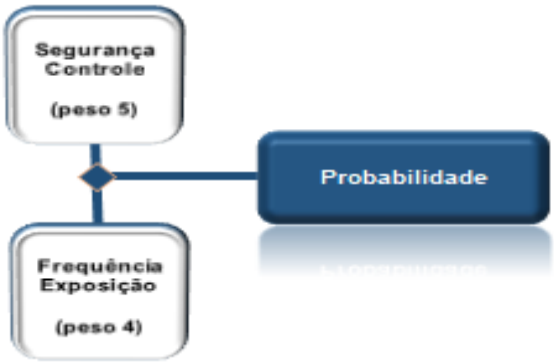
4.4.1 Probabilidade x Impacto - Inerente

Probabilidade - calculada por dois fatores, sendo que cada um terá um peso diferenciado em virtude do seu grau de importância:

Segurança/Controle: é avaliada a questão dos fatores de riscos e controles identificados. Quanto maior a nota, pior é a condição de segurança e dos controles *(no Risco Inerente, esse critério automaticamente é pontuado com nota 5)*;

Frequência/Exposição: é a frequência com que o risco costuma se manifestar, podendo levar em consideração históricos internos ou externos (empresas similares), além da exposição que a empresa se encontra a determinado risco, considerando assim, o contexto.

Figura 06: Probabilidade



Fonte: Adaptado de BRASILIANO (2018).

Quadro 06: Descritivo de Escala - Segurança de Controle

Segurança e Controle (peso 5)		
Conceito	**Descritivo da Escala**	**Pontuação**
Muito ruim	Sem Controle nenhum, atuando nos Fatores de Riscos e/ou no Risco.	5
Ruim	Os Controles que atuam nos Fatores de Riscos e/ou no Risco não previnem ou detectam a concretização do Risco.	4
Média	Os Controles que atuam nos Fatores de Riscos e/ou no Risco previnem ou detectam parcialmente a concretização do Risco.	3
Bom	Os Controles que atuam nos Fatores de Riscos e/ou no Risco previnem ou detectam satisfatoriamente a concretização do Risco.	2
Muito bom	Os Controles que atuam nos Fatores de Riscos e/ou no Risco previnem ou detectam plenamente a concretização do Risco.	1

Fonte: Dados da Pesquisa (2020).

Quadro 07: Descritivo de Frequência / Exposição

Frequência / Exposição (peso 4)		
Escala	**Descritivo da Escala**	**Frequência Observada / Esperada**
5 - Quase certo	Evento esperado que ocorra na maioria das circunstâncias	Maior ou igual a 90%
4 - Provável	Evento previsível que ocorra na maioria das circunstâncias	Maior ou igual a 50% Menor que 90%
3 - Possível	Evento presumível que deve ocorrer em algum momento	Maior ou igual a 20% Menor que 50%
2 - Improvável	Evento incerto que pode ocorrer em algum momento	Maior ou igual a 10% Menor que 20%
1 - Raro	Evento que pode ocorrer em circunstâncias excepcionais	Menor que 10%

Fonte: Dados da Pesquisa (2020).

O Nível de Probabilidade (PB) é o resultado da média ponderada dos dois critérios de probabilidade (multiplicação do peso (x) a nota, dividida pela soma dos pesos), conforme demonstrado no Quadro 08. Ressaltamos que o peso pode ser definido de Empresa para Empresa; todavia, para a Empresa - objeto de estudo, entendemos que os pesos apropriados são 5 e 4, conforme o exemplo.

Quadro 08: Cálculo do nível de probabilidade

$$\textbf{Nível de Probabilidade} = \frac{(\text{Segurança/Controles} * \text{peso}) + (\text{Frequência/Exposição} * \text{peso})}{\text{Soma dos pesos}}$$

Fonte: Dados da Pesquisa (2020).

O nível de probabilidade possui a seguinte classificação, descrita no Quadro 09:

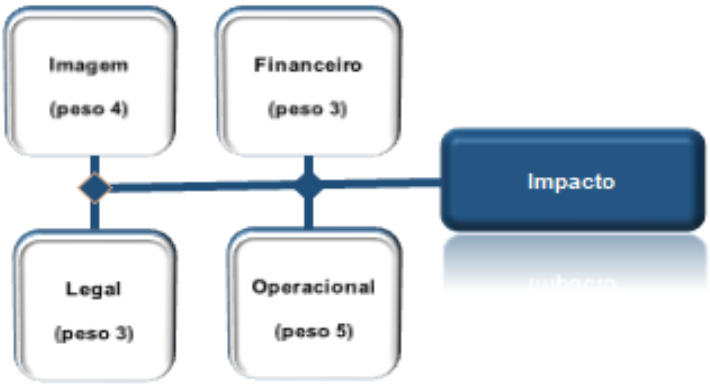
Quadro 09: Classificação para nível de probabilidade

Grau de Probabilidade	Escala	Nível de Probabilidade
4,51 - 5,00	5	Muito provável
3,51 - 4,50	4	Provável
2,51 - 3,50	3	Possível
1,51 - 2,50	2	Improvável
1,00 - 1,50	1	Muito improvável

Fonte: Dados da Pesquisa (2020).

Com o objetivo de obtermos uma visão holística do impacto, há a necessidade de se projetarem todas as consequências que os riscos causam. A seguir, segue a representação do critério de avaliação do **IMPACTO**. Nesse sentido, apresentamos na Figura 07, a graduação para os critérios de avaliação do impacto da ocorrência dos riscos:

Figura 07: Impacto



Fonte: Dados da Pesquisa (2020)

Quadro 10: Descritivo para avaliar Impacto - Imagem

Imagem – Peso 4	
Escala	**Pontuação**
Repercussão nacional: preocupação pública/ da mídia/ política nacional. Situação de alto impacto por envolver interesse público nacional, cobertura de mídia nacional, repercussões junto a autoridades governamentais e representantes de nível nacional e/ou regional; medidas restritivas à empresa. Também tende a mobilizar grupos de ação. Atenção para possíveis reações de redes sociais.	05
Repercussão regional: preocupação pública/ da mídia / política regional. Situação de impacto médio com risco iminente de envolvimento das autoridades regionais e da mídia. É comum existir interesse público regional, ampla repercussão na mídia regional. Atenção para possíveis reações de redes sociais.	04
Repercussão local: envolve algum interesse público local, alguma atenção política local e/ou mídia local, com possíveis aspectos adversos para as operações.	03
Repercussão de caráter interno - dentro da Empresa estudada (acionistas, inclusive). A ocorrência não ultrapassa os limites internos da Empresa e/ou de suas unidades.	02
De caráter Interno – dentro dá Área.	01

Fonte: Dados da Pesquisa (2020).

Quadro 11: Descritivo para avaliar Impacto - Financeiro

Financeiro – Peso 3	
Escala	**Pontuação**
Massivo - acima de R$ 500.000,00	05
Severo - até R$ 500.000,00	04
Moderado - até R$ 350.000,00	03
Leve - até R$ 80.000,00	02
Insignificante - até 20.000,00	01

Fonte: Dados da Pesquisa (2020).

Quadro 12: Descritivo para avaliar Impacto - Legal

Legal – Peso 3	
Escala	**Pontuação**
Perturbação Muito Grave: imposição de restrições por Órgãos governamentais, tais como suspensão total das atividades em algum processo crítico, prisão de Colaboradores-chave e outros.	05
Grave: imposição de restrições por Órgãos governamentais, tais como suspensão total das atividades em algum processo que não seja crítico, prisão de Colaboradores operacionais e outros.	04
Limitada: aplicação de multa por Órgãos governamentais e/ou imposição de restrições que não afetem processos críticos.	03
Leve: questões legais em que há a possibilidade de abertura de fiscalização/investigação/processo contra a Empresa, porém existem argumentos e provas contundentes para inibir a aplicação de multas ou pagamento de indenizações. Existência de precedente favorável para a Companhia.	02
Muito leve: questões legais, sem impacto para o negócio da Empresa ou aplicação de multa/ não há consequências.	01

Fonte: Dados da Pesquisa (2020).

Quadro 13: Descritivo para avaliar Impacto - Operacional

Operacional – Peso 5	
Escala	**Pontuação**
Perturbações Muito Graves: impacta outros processos muito fortemente	05
Graves: impacta outros processos de forma direta	04
Limitadas: impacta outros processos - (processos de outras áreas)	03
Leves: impacta somente o próprio processo levemente	02
Muito Leves: não impacta nenhum processo (apenas é necessário refazer as atividades)	01

Fonte: Dados da Pesquisa (2020).

Nível de Impacto é o resultado da média ponderada dos quatro critérios de impacto (multiplicação do peso, (x) a nota, dividida pela soma dos pesos) demonstrado no Quadro 14, conforme demonstrado na sequência; e o resultado do nível de impacto é descrito no Quadro 14.

Quadro 14: Nível de Impacto

$$\textbf{Nível de Impacto} = \frac{\text{Imagem} + \text{Financeiro} + \text{Operacional} + \text{Legal}}{15 \text{ (soma dos pesos } 4+3+3+5)}$$

Fonte: Dados da Pesquisa (2020).

Quadro 15: Descritivo Grau de Impacto

Grau de Impacto	Escala	Nível de Impacto	Interpretação
4,51 – 5,00	5	Catastrófico	Eventos que causam impactos nas operações, de maneira a paralisar os processos críticos da EMPRESA, atingindo o fluxo de caixa e imagem, com consequências gravíssimas para os Órgãos Reguladores.
3,51 – 4,50	4	Severo	Eventos que também causam impactos extremos nas operações, atingindo o fluxo de caixa e imagem da EMPRESA.
2,51 – 3,50	3	Moderado	Eventos que causam impactos significantes, não atingindo as operações.
1,51 – 2,50	2	Leve	Eventos que causam impactos leves.
1,00 – 1,50	1	Insignificante	Eventos que causam pouco ou nenhum impacto.

Fonte: Dados da Pesquisa (2020).

4.4.2 Matriz de Riscos - Inerente

A avaliação de riscos visa comparar os níveis de riscos em relação aos critérios pré-estabelecidos. A relevância dos riscos possui como parâmetro a matriz de riscos; e o seu resultado é o grau de criticidade do risco, ou seja, é a priorização que a Empresa estudada deve utilizar para tratar cada risco frente ao seu Apetite de Riscos. A Matriz é dividida em quadrantes, e para cada quadrante existe uma estratégia de tratamento e priorização.

A Matriz de Riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e do impacto. Posto isto, verificamos que quanto maior a probabilidade e o impacto de um risco, maior será o nível do risco. Dessa forma, o detalhamento sobre os quadrantes da Matriz de Riscos e suas tratativas esperadas podem ser visualizados no Quadro 02.

4.4.3 Nível de Risco - Inerente

Após a finalização da etapa para determinar a criticidade de cada risco, isto é, sua probabilidade e impacto, deve ser elaborado o nível de risco. O Nível de Risco é

um índice calculado com base na média ponderada das probabilidades, e média ponderada dos impactos dos riscos identificados, conforme cálculo a seguir:

Nível de Risco = Média das Probabilidades x Média dos Impactos

Figura 08: Nível de Risco

Fonte: BRASILIANO (2018).

A Empresa, objeto de estudo, não suporta riscos plotados no quadrante Vermelho. Estes riscos terão ação e tratamento imediatos por parte dos Gestores (Gerente e Diretoria).

Para identificarmos o nível de risco, é necessário utilizar critérios descritos no Quadro 16. Também é importante ressaltar, que quanto maior o nível do risco, maior sua criticidade:

Quadro 16: Descritivo Grau de Impacto x Tratamento

NÍVEL DE RISCO			TRATAMENTO
1 a 5	**1**	**Verde**	Existe grau de riscos consideráveis, mas que causam consequências gerenciáveis. Devem ser monitorados de forma rotineira ou sistemática.
5,1 a 10	**2**	**Amarelo**	Devem ser monitorados de forma rotineira ou sistemática.
10,1 a 15	**3**	**Laranja**	Deve-se receber tratamento em médio e curto prazo. Possui riscos com probabilidades e/ou impactos consideráveis. Devem ser constantemente monitorados.
15,1 a 25	**4**	**Vermelho**	Alto grau de risco, podendo resultar em impacto extremamente severo. Exigem implementação imediata de estratégias de prevenção e/ou continuidade.

Fonte: Dados da Pesquisa (2020).

4.5 ANÁLISE E AVALIAÇÃO DE RISCOS - RESIDUAL

Entendemos por risco residual a avaliação dos riscos após a consideração dos controles. Esses conceitos permitem que os controles sejam avaliados, bem como que sua efetividade seja comprovada durante os testes das Auditorias.

4.5.1 Avaliação dos controles - Residual

Com o objetivo de verificar a eficácia dos controles identificados no processo em estudo, é necessário realizar a avaliação dos controles. No final desta etapa, a informação disponível permitirá ao executante conhecer a eficácia, a ineficácia ou a inexistência dos controles, bem como sua relação com os fatores de risco ou riscos.

Para registro da avaliação dos controles, deve-se preencher formulário com descrição do Resultado e do Parecer, conforme Quadro 17:

- **Resultado:** Descrever como o controle analisado atua, embasando o Parecer final;
- **Parecer:** Com base no resultado obtido, ao averiguar os controles, indicar se o controle é eficaz ou ineficaz.

Quadro 17: Descritivo - Avaliação dos Controles

Cód.do Risco:								
Nome do Risco:								
Cód. do controle	**Controle**	**Definição**	**Objetivo**	**Tipo**	**Categoria**	**Periodicidade**	**Resultado**	**Parecer**

Fonte: Dados da Pesquisa (2020).

Todos os controles devem ser associados a um ou mais riscos ou fatores de riscos. Conceitualmente, controles preventivos atuam “bloqueando” fatores de risco; enquanto controles detectivos atuam “alertando” a possível concretização do risco. Esta associação permitirá identificar, na análise de risco residual, o quão exposto o risco está. Desta forma, nortear-se-á a atribuição da nota de “Segurança e Controle”.

4.5.2 Probabilidade x Impacto - Residual

Para realizarmos a Análise de Riscos Residuais, devemos utilizar a metodologia e os critérios abordados na Subfase “4.4.1 Probabilidade x Impacto - Inerente”, todavia, neste caso, é preciso que se leve em consideração os controles existentes e sua relação com os fatores de risco, como também, os riscos, atribuindo notas específicas aos critérios “Segurança e Controle”.

Caso a Organização conte com controles que atuem mitigando os impactos, pode-se reavaliar as notas atribuídas no critério de impacto. Exemplos de controles

mitigatórios: Plano Estruturado de Gestão de Continuidade de Negócios (Emergência, Crise e Contingência) e Apólice de Seguro.

4.5.3 Matriz de riscos - Residual

Para elaborar a Matriz de Riscos Residuais, vamos utilizar a metodologia descrita na Subfase "4.4.2 Matriz de Riscos - Inerentes". Cabe destacar que devem ser utilizadas as notas de Probabilidade e Impacto residuais.

A Matriz de Riscos demonstra os pontos de cruzamento (horizontal e vertical) da probabilidade de ocorrência e o impacto. Assim sendo, pela divisão da Matriz SWOT em quatro quadrantes, podemos avaliar o nível de vulnerabilidade do processo estudado ou do departamento. Assim, quanto maior for a probabilidade e o impacto de um risco, maior será o nível do risco.

4.5.4 Nível de riscos - Residual

O nível de risco residual reflete, por meio da média das probabilidades e dos impactos, o cenário de risco de uma forma geral. Trata-se de um indicador cuja descrição complementar consta no item 4.4.3.

4.6 RESPOSTAS AOS RISCOS

Após realizadas a identificação, a análise e a avaliação dos riscos, levando-se em consideração a Matriz de Riscos Residuais, e respeitando o Apetite ao Risco, o executante e o responsável devem determinar como será a resposta aos riscos residuais.

É importante que existam a conscientização e o comprometimento com o Gerenciamento de Riscos por parte da alta administração da Instituição.

Nesse contexto, os tomadores de decisão são os responsáveis por esse gerenciamento, ou seja, mediante a matriz de riscos devemos identificar qual a resposta a ser adotada para o tratamento do risco.

Abaixo, as estratégias que podem ser adotadas para o tratamento dos riscos:

- **Evitar o Risco -** descontinuação das atividades que geram os riscos. Evitar riscos pode, por exemplo, implicar a descontinuação de um processo.
- **Reduzir o Risco -** são adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos. As medidas devem ser pautadas nos fatores de riscos e no aprimoramento de controles.

- **Compartilhar -** redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro e a "terceirização" de uma atividade (levando-se em consideração a corresponsabilidade).
- **Aceitar -** nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. Tratando-se de riscos, além do Apetite ao Risco, é necessária a formalização pelo Gestor do Risco e a aprovação pela Diretoria Responsável.

O risco é assumido quando, o Gestor, com alçada competente, decide assumir riscos (sem realizar plano de ação) no quadrante laranja ou vermelho, tendo em vista relação custo-benefício ou por questões estratégicas. A assunção deverá ser validada pela Diretoria Executiva.

4.6.1 Plano de ação

Depois de identificados, avaliados e mensurados, devemos definir qual o tratamento será dado aos riscos. A priorização deve estar embasada na Matriz de Riscos Residual, no Diagrama de Causa e Efeito, na Matriz SWOT e na Avaliação dos Controles.

Para a elaboração do plano de ação é utilizada a técnica adaptada das perguntas 5W e 2H.

- "O que ocasiona o risco?" Qual o motivo para a realização da ação? (fator de risco);
- "Criticidade": Refere-se à relevância do fator de risco (Magnitude x Importância);
- "Quem faz parte neste processo?": Nome do responsável pela implementação da ação;
- "Quando será implementado?": Data limite para implementação da ação;
- "O que pode ser implementado?": Medida em relação à causa prioritária (ação corretiva);
- "Como deve ser realizado para melhoria?": Descrever como será executada a ação proposta; e
- "Quanto custa?": Qual o valor do custeio / investimento.

Os donos dos riscos são integralmente responsáveis pelo seu tratamento e/ou monitoramento. Nesse sentido, deve acompanhar o *status* dos planos de ação, bem como informar quando vislumbrar mudanças nos ambientes interno e/ou externo que podem afetar o risco.

Caso não ocorra o planejamento e a aprovação de resposta ao risco, bem como a execução do plano dentro do prazo estipulado, a pendência existente será encaminhada para conhecimento e providências.

4.6.2 Projeção Futura

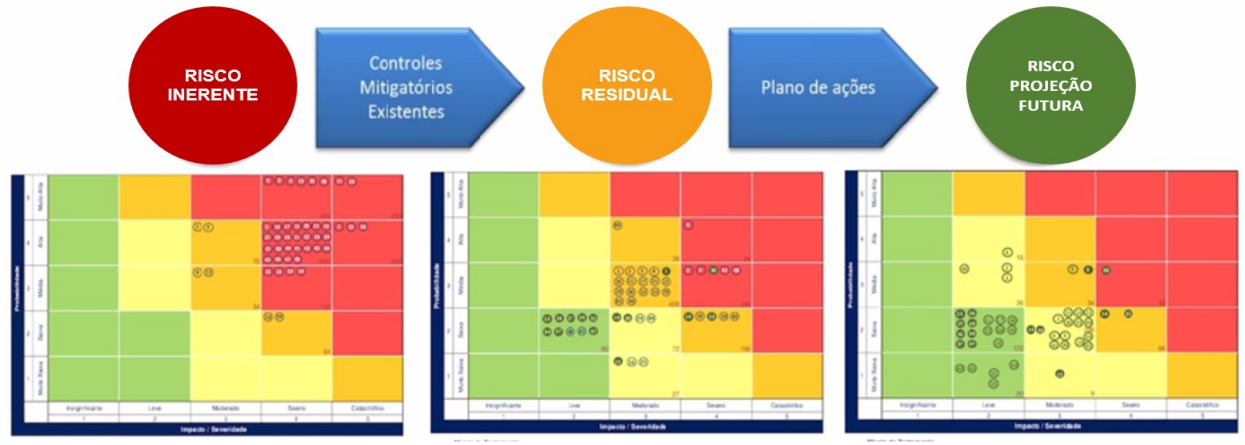
Para que possamos elaborar a Matriz de Riscos com Projeção Futura é necessário reavaliar a Análise de Riscos Residuais, partindo da premissa que o plano de ação previsto está, ou será implementado, em sua totalidade. Desta forma, a análise será realizada reavaliando e considerando a Probabilidade e o Impacto.

- Probabilidade
    - Frequência/Exposição: caso julgarmos prudente, podemos, de forma prospectiva, baixar a pontuação à medida que o Gestor se sentir confortável em afirmar que a ação diminuirá a ocorrência do risco no âmbito da Empresa estudada; e
    - Segurança/Controle: levando-se em consideração o plano de ação previsto, pontuar conforme qualidade futura dos controles no processo, após a conclusão de todas as ações.
- Impacto
    - Devemos repontuar os critérios caso existam melhorias nas estruturas de contingência, como a elaboração efetiva de um Plano de Gestão de Continuidade de Negócios e contratação de Seguro.

4.6.2.1 Matriz de Riscos – Projeção Futura

Apresentar comparativo entre as Matrizes de Riscos Residuais x Projeção Futura, após conhecermos os planos de ação, conforme demonstrado na Figura 09.

Figura 09: Projeção Futura



Fonte: Adaptado de BRUNO PIRES BANDAROVISK.(2020).
Curso Anticorrupção LEC- Legal, Ethics & *Compliance* – WWW.LECNEWS.COM

4.6.2.2 Nível de Riscos - Projeção Futura

Apresentar comparativo entre os níveis de Riscos Residuais x Projeção Futura, após conhecer os planos de ação e validar com os gestores, mediante sempre registro das reuniões: quem participou, o que foi apresentado, o que se pretende realizar, como, e quem vai realizar os planos de ação, e em quais são os prazos.

4.6.3 Registro e Relato

O Processo de Gestão de Riscos e seus resultados devem ser documentados e relatados por meio de mecanismos apropriados, tais como pastas digitais e documentos físicos - todos guardados seguindo regras da Empresa para registro e guarda de documentos. No mínimo, anualmente, será emitido um relatório servindo de parâmetro para a tomada de decisão, bem como em inspeções e verificações futuras.

4.7 MONITORAMENTO E ANÁLISE CRÍTICA

O monitoramento e a análise crítica devem ser planejados como parte do Processo e devem envolver a checagem e vigilância regular. Podem ser periódicos, ou acontecer em resposta a um fato específico. Deve ser elaborado relatório contendo os itens de monitoramento e os indicadores apurados, constando as justificativas necessárias para o entendimento. Podemos citar os seguintes tipos de indicadores:

a) **Criticidade dos riscos residuais**

Diz respeito à evolução das condições dos riscos identificados e analisados na Matriz de Riscos - Residual. Neste caso, devemos montar um processo de acompanhamento para verificar se as condições listadas no Diagrama de Causa e Efeito sofrem mudanças, abrangendo os ambientes interno e o externo.

Objetivo: Apresentar a evolução da criticidade dos riscos residuais (Matriz de Riscos - Residual).

b) **Planos de ação**

Visa verificar se os planos de ação estão sendo executados conforme cronograma estabelecido e aprovado. Para isso, devemos utilizar um farol com os indicadores de: Concluído; Em Andamento; Previsto; Atrasado; e Cancelado.

Devem ser acompanhados para saber se seus objetivos foram atingidos e, se não foram, quais as dificuldades encontradas e as ações corretivas, para assim medir a evolução da implementação dos planos de ação.

c) **Registros de Ocorrências (Materialização de riscos)**

Os eventos que ocorrem devem ser formalmente registrados, indepedentemente de sua classificação/ criticidade, para que os Gestores de todos os níveis possam tomar decisões que sirvam de suporte ao Processo de Análise de Risco (retroalimentação).

As ocorrências devem ser registradas destacando:

- tipo de ocorrência;
- localização (externa e interna - quanto maior o detalhamento, melhor);
- relação dos envolvidos;
- descrição da ocorrência;
- breve registro fotográfico;
- pessoas e/ou Órgãos envolvidos; e
- ações imediatas tomadas.

Os dados fundamentais devem ser tabulados, permitindo a consolidação de indicadores, tais como:

- Riscos concretizados no período;
- Horário de maior ocorrência de riscos;

- Localização de maior ocorrência de riscos;
- Pessoas envolvidas em eventos danosos; e
- Demais aplicáveis.

Todos os indicadores a seguir, devem ser representados por intermédio de um *dashboard* (painel de controle), devendo ser visualizados de forma separada (por tipo) e de forma integrada.

5. HISTÓRICO DE VERSÕES

Sugerimos realizar registro de cada alteração no presente Manual, bem como os registros de suas aprovações.

Os registros das versões e aprovações devem seguir a norma de controle de documentos de sua organização. Seja em sistema específico para controles de versionamento, em separado deste documento ou nas versões futuras deste manual (físico ou digital).

Importante entender que o versionamento é uma metodologia de classificação realizada para acompanhar e controlar históricos das alterações de documentos. O versionamento tem o objetivo de registrar e diferenciar as mudanças efetuadas no documento, facilitando a identificação de cada uma delas. Na prática o registro das versões faz uso de controles numéricos, com o propósito de catalogar as versões de um documento. Conforme são necessárias novas versões, a fim de atualizar o documento, essas são compartilhadas com seus pares, e a numeração é alterada (aumenta sua numeração), demonstrando alterações.

Quadro 18: Histórico de Versões

Versão Nº	Data	Alteração Efetuada	Responsável	Aprovação
		Criação da primeira versão		
		Atualização		

Fonte: Elaborado pela Autora (2020).

REFERÊNCIAS

ABNT. Gestão de Riscos - Princípios e Diretrizes. NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2018.

ABNT. Gestão de Riscos - Técnicas para o Processo de Avaliação de Riscos. NBR ISO/IEC 31010. Associação Brasileira de Normas Técnicas. 2012.

BRASILIANO, Antônio Celso Ribeiro. GESTÃO E ANÁLISE DE RISCOS CORPORATIVOS - Método Brasiliano Avançado. São Paulo: Editora Sicurezza, 2009.

BRASILIANO, Antônio Celso Ribeiro. INTELIGÊNCIA EM RISCOS - Gestão Integrada em Riscos Corporativos. São Paulo: Editora Sicurezza, 2016.

BRASILIANO, Antônio Celso Ribeiro. Inteligência em Riscos [livro eletrônico] - Gestão Integrada em Riscos Corporativos, 2ª edição revisada e ampliada com o COSO 2017 e ISO 31000:2018. São Paulo: Editora Sicurezza, 2018.

CASTRO, Rodrigo Pironti Aguirre de Castro; GONÇALVES, Francine Silva Pacheco. *COMPLIANCE* E GESTÃO DE RISCOS NAS EMPRESAS ESTATAIS. Belo Horizonte: Editora Fórum, 2018.

COSO ERM 2017 - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management. Integrating with Strategy and Performance (Integrado com Estratégia e Perfomance).

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Manual de Gerenciamento de Riscos Estratégicos da Empresa Pesquisada. Florianópolis, 2019.

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Política Interna de *Compliance* da Empresa Pesquisada. Florianópolis, 2021.

DOCUMENTO INTERNO DA EMPRESA - OBJETO DE ESTUDO - Política Interna de Gerenciamento de Riscos da Empresa Pesquisada. Florianópolis, 2019.

IIA - Instituto dos Auditores Internos - As Três Linhas**,** 2020.

7 GLOSSÁRIO

- **Análise de riscos:** processo sistemático para compreender a natureza do risco e deduzir o nível de risco. Fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.
- **Apetite ao risco:** quantidade e tipo de riscos que a Organização está disposta a assumir para atingir seus objetivos.
- **Avaliação de riscos:** processo global de estimar a magnitude dos riscos, e decidir se um risco é ou não tolerável, bem como propor formas de mitigação dos riscos constatados.
- **Comunicação e consulta:** Consulta - processos contínuos e interativos que uma Organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos.
- ***Compliance*:** vem do inglês *to comply with*, significando estar de acordo, cumprir com as normas, as leis e os regulamentos.
- **Consequência:** resultado de um evento que afeta determinados objetivos.
- **Contexto externo:** ambiente externo pelo qual a Organização busca atingir seus objetivos.
- **Contexto interno:** ambiente interno pelo qual a Organização busca atingir seus objetivos.
- **Controle:** medida que está modificando o risco.
- **Critérios de riscos:** termos de referência pela qual o significado de um risco é avaliado.
- **Estrutura da gestão de riscos:** conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, a implementação, o monitoramento, a análise crítica e a melhoria contínua da gestão de riscos por toda a Organização.
- **Fator de risco:** elemento ou ocorrências que, individualmente ou combinado, podem desencadear a materialização de um risco.
- ***Framework* ou arcabouço conceitual:** conjunto de conceitos usados para resolver um problema de domínio específico.

- **Gerenciamento de riscos:** aplicação da arquitetura implantada internamente na Empresa, de modo a identificar, em todos os níveis e unidades da Organização, quais são os eventos capazes de impactar seus objetivos, a fim de adotar medidas de tratamento de riscos, mantendo-os em conformidade com o nível definido como tolerável pela Organização.
- **Gestão de riscos:** conjunto de atividades coordenadas para dirigir e controlar riscos em uma Organização.
- **Identificação de riscos:** processos de busca, de reconhecimento e de descrição de riscos.
- **Incerteza:** deficiência de informações relacionadas a um evento, à sua compreensão, ao seu conhecimento, à sua probabilidade, e à sua consequência ou impacto.
- **Monitoramento:** verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.
- **Nível de risco:** magnitude de um risco, expressa em termos da combinação das probabilidades e dos impactos dos riscos.
- **Probabilidade:** chance de um evento acontecer.
- **Processo:** conjunto de atividades com uma ordenação específica, com uma ou mais entradas, que cria saída de valor para o cliente, e possui começo e fim claramente identificados, podendo subdividir-se em subprocessos.
- **Processo de avaliação de riscos:** processo global de identificação de riscos, análise de riscos e avaliação de riscos.
- **Proprietário do risco:** empregado ou unidade organizacional com a responsabilidade e a autoridade para gerenciamento do risco.
- **Risco inerente:** risco que não leva em consideração controles existentes no ambiente em estudo.
- **Risco residual:** risco que considera todos os controles já existentes no ambiente em estudo.
- **Risco:** efeito que a incerteza tem sobre os objetivos de uma Organização, constituindo-se em um desvio positivo ou negativo em relação ao resultado esperado.

- **Tolerância aos riscos:** limiar de risco a partir do qual certos resultados das operações da empresa podem ser comprometidos. É um indicativo da sensibilidade da empresa em relação aos riscos.
- **Tratamento de riscos:** processo para modificar os riscos.

Anexo A

Figura do Modelo de Três Linhas de Defesa (2013)

Fonte: IIA (2013)

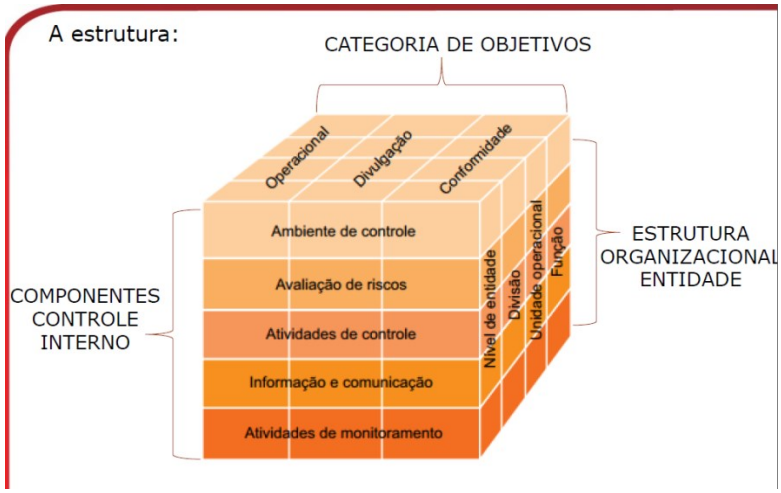
Anexo B

Figura do Modelo de Três Linhas (2020)

Fonte: IIA (2021)

Anexo C

Figura da Estrutura COSO ICIF- Controles internos



Fonte: COSO (2013)

Anexo D

Figura da Estrutura COSO ERM

Fonte: COSO (2013)

Anexo E

Figura do COSO ERM 2017

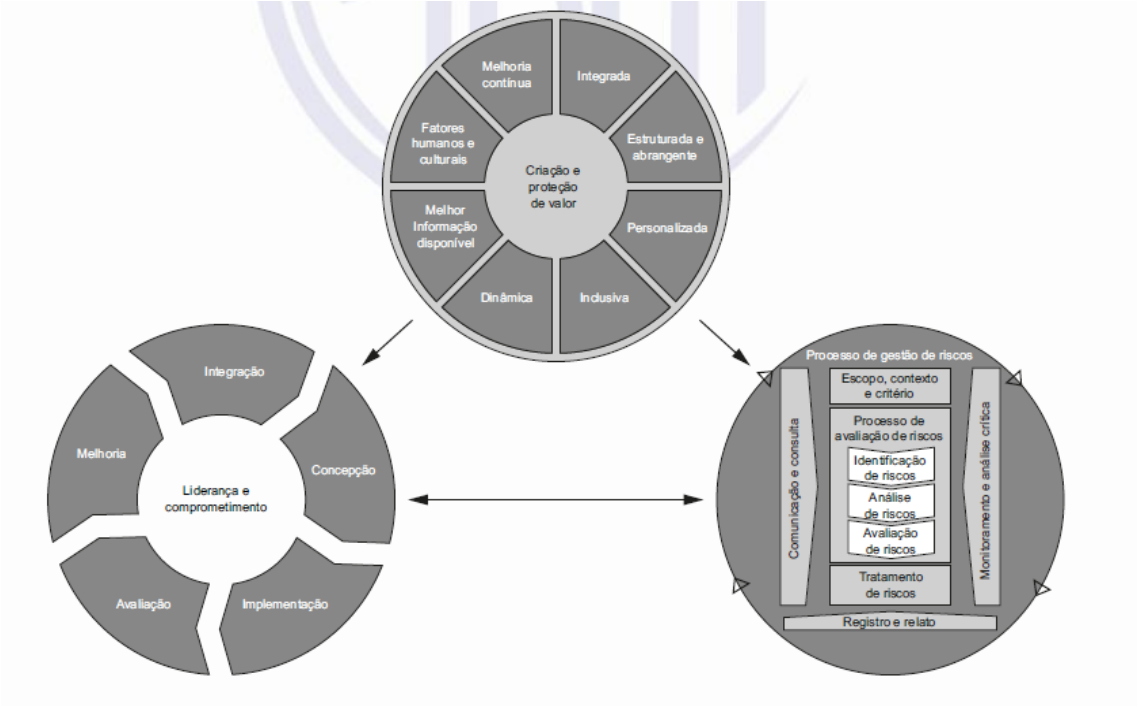
Fonte: https://www.coso.org

Figura do *Framework* COSO ERM 2017

Fonte: COSO (2017)

Anexo F

Figura dos Princípios, Estrutura e Processo de Gestão de Riscos ISO 31000 de 2018



Fonte: ABNT - ISO 31000 (2018)