GIULIA RIBEIRO LIMA MOREIRA

Análise de lacunas e proposta de melhoria para o Sistema de Gestão de *Compliance* de uma empresa de construção civil

São Paulo

2021

GIULIA RIBEIRO LIMA MOREIRA

Análise de lacunas e proposta de melhoria para o Sistema de Gestão de *Compliance* de uma empresa de construção civil

Trabalho de Formatura apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do diploma de Engenheira de Produção.

São Paulo
2021

GIULIA RIBEIRO LIMA MOREIRA

Análise de lacunas e proposta de melhoria para o Sistema de Gestão de *Compliance* de uma empresa de construção civil

Trabalho de Formatura apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do diploma de Engenheira de Produção.

Orientador: Professor Doutor Fernando Tobal Berssaneti

São Paulo

2021

Catalogação-na-publicação

Moreira, Giulia Ribeiro Lima
Análise de lacunas e proposta de melhoria para o Sistema de Gestão de Compliance de uma empresa de construção civil / G. R. L. Moreira -- São Paulo, 2021.
109 p.

Trabalho de Formatura - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Produção.

1.Compliance 2.Avaliação de risco 3.Sistema de gestão da qualidade 4.Certificação ISO I.Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Produção II.t.

Ao meu marido e melhor amigo,
por todo apoio, amor e cuidado de sempre.
Aos meus avós que certamente gostariam
de comemorar o fim dessa etapa comigo: Antônio
(*in memoriam*), Iracy (*in memoriam*) e Iraci (*in*
memoriam); e aos que ainda tenho por perto:
Alceu e Neila.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me criou, me deu vida e dirige todos os meus passos, por me dar a oportunidade de começar e terminar esse curso e por me capacitar para fazer este trabalho até o fim.

Agradeço ao meu marido pelo amor e cuidado, pelo encorajamento ainda maior nos últimos meses, e pela compreensão por tantas horas dedicadas à minha graduação e a este trabalho.

Agradeço à minha mãe e ao meu pai, que nunca mediram esforços para que eu tivesse uma boa educação, pelo apoio e encorajamento, e por estarem presentes e se alegrarem comigo a cada conquista.

Agradeço aos meus familiares, por celebrarem comigo o início dessa etapa, por cada encorajamento e incentivo recebidos ao longo do curso, e especialmente à minha sogra pela ajuda na revisão deste texto.

Agradeço aos professores da graduação, pelo conhecimento e experiência transmitidos, especialmente: ao meu orientador por todo direcionamento nos últimos meses; ao prof. Laerte pelo aprendizado tão enriquecedor para minha vida e formação durante a Iniciação Científica; e à prof. Débora por sua confiança e afeto, e por me proporcionar a experiência de ser monitora.

Agradeço ao time da empresa que estagiei e na qual fiz este trabalho, pela parceria e por todo aprendizado, e principalmente ao Fernando e à Thamires pela ajuda e disposição, sem as quais este trabalho não teria sido possível.

Agradeço aos meus colegas de turma pela amizade, convivência e ajuda durante esses anos, pelas companhias no bandejão, pela parceria em diversos trabalhos, e pelos momentos presenciais e à distância, especialmente a Bárbara, Giulia, Luiza, Gabriel M., Gabriel S., Gabriel V., Flávio, Fábio, Juliana e outros que certamente esqueci de mencionar.

Agradeço aos meus colegas da Aliança Bíblica Universitária por serem uma família dentro da universidade, pela amizade, pelas orações e pelo encorajamento, especialmente a Bianca, Doris, Ian, Arthur, Jhonny, Mathias, Felipe, Silas e tantos outros fazem parte desse grupo incrível dentro e fora da Poli

Entregue o seu caminho ao SENHOR,
confie nele, e o mais ele fará.
Sl 37,5

Quanto melhor é adquirir a sabedoria do
que o ouro! E mais excelente é adquirir o
entendimento do que a prata!
Pv 16,16

RESUMO

É crescente entre as empresas a adequação a práticas de ESG, especialmente as que possuem capital aberto; governança, transparência e *compliance* estão entre os principais aspectos avaliados pelos investidores. Este trabalho objetivou a melhoria do Sistema de Gestão de *Compliance* (SGC) de uma empresa de construção civil com base na NBR ISO 37301:2021, tendo em vista os requisitos já atendidos parcialmente por seus processos e a necessidade de demonstrar boa governança perante seus acionistas. Para isso, foi feita uma análise de lacunas entre a situação da empresa e os requisitos da NBR ISO 37301:2021, seguida pela priorização das oportunidades de melhoria identificadas por meio de uma avaliação de riscos de *compliance* e um critério adicional de esforço; as tarefas priorizadas foram desenvolvidas em maiores detalhes. Os principais resultados obtidos foram uma lista de oportunidades de melhoria, atreladas aos riscos de *compliance* avaliados em uma matriz de riscos, e 27 propostas de melhoria, das quais 15 a empresa pretende adotar integralmente. As maiores contribuições deste estudo para a empresa, além das ações propostas, foram o fornecimento de um panorama de seu SGC e do potencial de integração entre os sistemas da Qualidade e de *Compliance*, a melhoria da gestão de riscos através da consolidação de critérios de avaliação, e a identificação de oportunidades de melhoria para além dos requisitos da NBR ISO 37301:2021.

Palavras-chave: *Compliance*, Avaliação de risco, Sistema de gestão da qualidade, Certificação ISO.

ABSTRACT

The adaptation to ESG practices is growing among companies, specially those that are publicly traded; governance, transparency and compliance are some of the main aspects valued by investors. This study aimed the improvement of a construction company's Compliance Management System (CMS), based on the NBR ISO 37301:2021, in view of the requirements already partially met by its processes and the need to demonstrate good governance before its shareholders. For that, a gap analysis between the company's situation and the requirements of NBR ISO 37301:2021 was carried out, followed by the priorization of the identified improvement opportunities through a compliance risk assessment and an additional effort criterion; the prioritized tasks were developed in greater detail. The main results obtained were a list of improvement opportunities, associated to the compliance risks assessed in a risk matrix, and 27 improvement proposals, of which 15 the company intends to fully adopt. The main contributions of this study to the company, in addition to the proposed actions, were the provision of an overview of its CMS and of the potential for integration between the Quality and Compliance systems, the improvement of the risk management through the consolidation of assessment criteria, and the identification of improvement opportunities beyond the NBR ISO 37301:2021 requirements.

Key words: Compliance, Risk assessment, Quality management system, ISO certification.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ESG	*Environment, Social and Governance*
FMEA	*Failure Modes and Effects Analysis*
GRC	Governança, Riscos e *Compliance*
GUT	Gravidade, Urgência e Tendência
NBR	Norma Brasileira
SGC	Sistema de Gestão de *Compliance*
SGQ	Sistema de Gestão da Qualidade
SSTMA	Saúde, Segurança do Trabalho e Meio-Ambiente

SUMÁRIO

1 INTRODUÇÃO

Publicada oficialmente no Brasil no mês de junho do presente ano, a NBR ISO 37301:2021 – Sistemas de Gestão de *Compliance* (ABNT, 2021) é resultado de uma revisão profunda da NBR ISO 19600:2014 (ISO, 2014), não mais em vigor; a nova norma, diferente da anterior, é certificável. O conceito de "conformidade" é provavelmente o mais próximo em português para *compliance;* uma vez que o termo em inglês é amplamente utilizado no meio corporativo, inclusive pela NBR ISO 37301:2021, também será adotado neste trabalho. O *compliance* é "um processo contínuo e o resultado de uma organização que cumpre suas obrigações" (ABNT, 2021, p. vii), sejam elas mandatórias, como leis e regulamentos aplicáveis, ou voluntárias, como políticas internas e os próprios requisitos das normas nas quais busca certificação. Assim, este será o sentido adotado para o termo *compliance* ao longo deste trabalho; quando empregada inicial maiúscula (*Compliance*), o termo se refere à função de *compliance.*

A empresa escolhida para a realização deste trabalho, tendo em vista o estágio realizado pela autora, foi denominada Empresa A para manter sua confidencialidade, e é certificada na NBR ISO 9001:2015, cuja estrutura de alto nível é a mesma da NBR ISO 37301:2021, por serem ambas normas de sistema de gestão. Além disso, os princípios que dirigem esta última – integridade, boa governança, proporcionalidade, transparência, responsabilização e sustentabilidade (ABNT, 2021, p. viii) – vão ao encontro do que tem buscado a empresa, considerando sua visão de negócio e a recente abertura de capital, com exigências crescentes, não só sobre o *Compliance,* mas sobre toda a organização. Entre essas exigências, está a adequação a práticas de ESG (*Environment, Social and Governance*), o que a empresa tem buscado com auxílio de uma consultoria, no presente ano.

1.1 OBJETIVO

Este trabalho tem como objetivo propor processos e alterações em processos existentes visando a melhoria do Sistema de Gestão de *Compliance* da empresa, tendo como base os itens 4 a 8 da NBR ISO 37301:2021. Este objetivo geral se desenvolve nos seguintes objetivos específicos:

a) Compreender as atividades e processos de *compliance* existentes na empresa;
b) Analisar as lacunas entre a situação atual da organização e os requisitos da NBR ISO 37301:2021;

c) Avaliar os principais riscos de *compliance* e priorizar, dentro da função, os processos a ser elaborados;
d) Propor alterações e novos processos, indicando a necessidade de treinamentos e de elaboração de documentos.

Os itens da NBR ISO 37301:2021 estudados consistem em: 4 – Contexto da organização, 5 – Liderança, 6 – Planejamento, 7 – Apoio e 8 – Operação. Este último envolve o estabelecimento de critérios e controles para todos os processos necessários na organização, mas este trabalho se limitou aos processos de responsabilidade de *Compliance.*

Os itens 9 – Avaliação de desempenho e 10 – Melhoria não fizeram parte do escopo deste trabalho. No entanto, o desenvolvimento dos itens propostos fornece as bases necessárias para a implementação destes, e especialmente o último item pode ser aplicado com base no processo vigente de tratamento de não conformidades, exigência da NBR ISO 9001:2015, fazendo as devidas adequações para que atenda à NBR ISO 37301:2021.

1.2 JUSTIFICATIVA

Uma análise preliminar da NBR ISO 37301:2021 e da realidade da empresa permitiu identificar o atendimento parcial de diversos requisitos, seja devido a processos decorrentes da NBR ISO 9001:2015, seja pelas atividades em andamento por parte da função de *compliance.* A empresa apresenta entendimento do contexto e determinação de seu escopo (4.1, 4.3); possui função de *compliance* estabelecida e pessoal orientado, de forma geral, nas questões de *compliance* (5.3.2, 5.3.4); tem processos de planejamento (6) e estrutura de apoio para *Compliance* (7); possui canal para o levantamento de preocupações de *compliance* (8.3), um conjunto de indicadores de *compliance* (9.1) e procedimento estabelecido para tratamento de não conformidades (10).

Com isso, é possível afirmar que a empresa possui um Sistema de Gestão de *Compliance*, embora não totalmente de acordo com a NBR ISO 37301:2021. No entanto, o fato de ser uma empresa de capital aberto é decisivo para a importância de seu SGC, e a certificação na NBR ISO 37301:2021 é uma excelente forma de comprovar perante seus acionistas seu comprometimento com as boas práticas de Governança (terceiro termo do ESG). Assim, ainda que não busque a certificação no curto prazo, este trabalho é um incentivo nesta direção, fornecendo uma análise do SGC atual e propostas de melhoria baseadas na NBR ISO 37301:2021, permitindo que a empresa tome os próximos passos.

1.3 A EMPRESA

A Empresa A é uma construtora e incorporadora localizada na cidade de São Paulo. A empresa desenvolve empreendimentos de médio e alto padrão, concentrados na Grande São Paulo, com a visão de ser referência em excelência e *expertise* no mercado, bem como líder em satisfação de clientes, colaboradores e acionistas. Com quase 60 anos de existência, começando como empresa familiar, passou por intensa profissionalização desde 2008, com a mudança da alta direção. Hoje, a construtora e incorporadora é apenas uma das empresas do grupo, apresentadas abaixo:

a) Empresa A: Construtora e incorporadora de empreendimentos residenciais de alto e médio padrão;
b) Empresa B: Imobiliária focada em vender produtos da Empresa A;
c) Empresa C: Operadora focada em residência estudantil;
d) Empresa D: Agropecuária com fazendas próprias e arrendadas, focada na integração lavoura/pecuária e cultivos diversos.

O grupo conta com cerca de 350 funcionários na Empresa A, 10 na Empresa B, 50 na Empresa C e 170 na Empresa D. Atualmente a Empresa A possui grande influência nas demais; além de terem o mesmo CEO, as Empresas B, C e D partiram como braços da primeira. No entanto, as empresas caminham para se tornarem independentes, com cada vez mais processos e funções estabelecidos separadamente.

A Empresa A, foco deste trabalho, é certificada em seu Sistema de Gestão da Qualidade pela NBR ISO 9001:2015 – Sistemas de Gestão da Qualidade (ABNT, 2015) e pelo PBQP-H – Sistema de Avaliação de Conformidade de Empresas de Serviços e Obras da Construção Civil (BRASIL, 2018), além de ser auditada pela empresa Ernst & Young em seus processos financeiros. Também passou por abertura de capital recentemente, o que trouxe ainda mais exigências sobre seus processos.

O escopo da empresa abrange desde a incorporação do terreno até a assistência técnica pós-entrega. As atividades que são o núcleo principal dos propósitos de existência da organização (ABNT, 2021), referidas como de processos de negócio, são:

a) Novos negócios: captação e aquisição de terrenos, além de análise de viabilidade técnica e financeira;
b) Produto e Licenciamento: programa de necessidades para a regularização do imóvel, projeto legal, anteprojeto e registro de incorporação;

c) Projeto e desenvolvimento: planejamento e elaboração de projetos, bem como análise crítica, validação e controle de alterações e distribuição de projetos;
d) Comercial: processo de vendas, proposta de compra de imóveis e avaliação de imobiliárias e corretores;
e) Marketing: previsão de lançamento, material de divulgação de vendas e materiais institucionais;
f) Relacionamento com o cliente: processo financeiro, administração de contratos e cobrança, contato com o cliente e pesquisa de satisfação;
g) Planejamento e custo: planejamento e controle de andamento físico e de custos de obra, além de conciliação de custos no sistema;
h) Suprimentos diretos: cadastro e homologação de fornecedores para Obra, acompanhamento da avaliação de fornecedores por outros processos, elaboração de pedidos de compra e contratos;
i) Obras: execução da obra conforme projetos, cronograma físico-financeiro e orçamento, entrega do empreendimento com o padrão de qualidade requerido, além de treinamentos e avaliação de fornecedores. Cada obra conta com um gerente de obra (GO), engenheiros e estagiários, um administrador, um almoxarife, um mestre de obras, além dos trabalhadores terceiros; acima dos GOs estão os gerentes gerais de obra (GGOs), que dividem a responsabilidade por todas as obras em andamento;
j) Assistência técnica pós-entrega: análise de solicitações dos clientes, acompanhamento dos reparos e do processo de entrega de empreendimentos.
k) *Compliance*: garantia da conformidade de todo o processo com leis, normas e procedimentos internos, através de práticas como governança corporativa, gestão de riscos, treinamento e comunicação interna.
l) Sistemas de Gestão da Qualidade (SGQ): garantia da qualidade em Obras e demais processos, através do acompanhamento de objetivos e indicadores, visitas mensais às obras, acompanhamento de auditorias e apoio em diversas atividades.

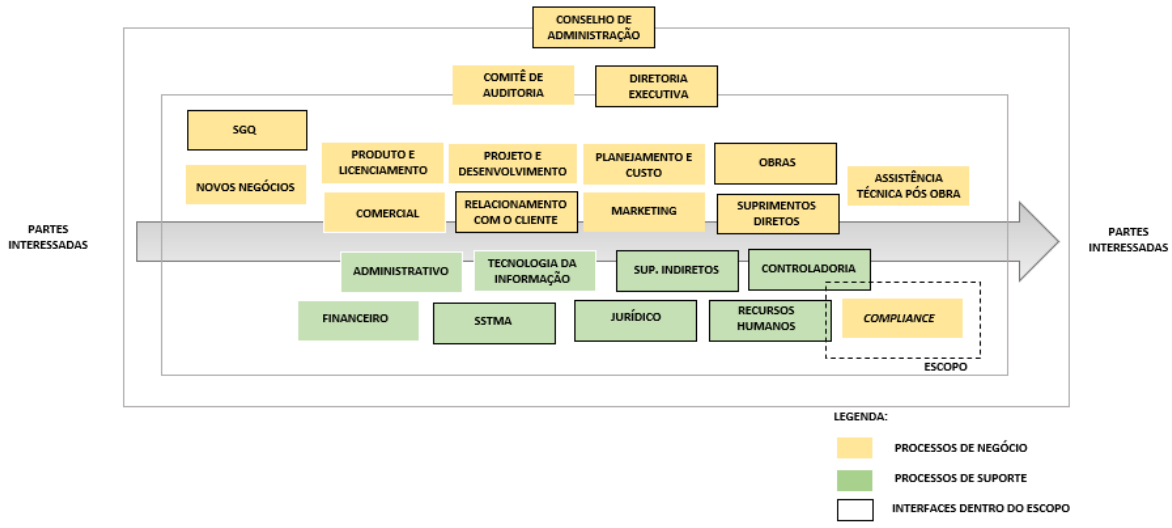
Como processos de suporte, aqueles que criam condições para a execução dos processos de negócio, gerando valor para os clientes internos, temos: Financeiro, Administrativo, Recursos Humanos, Suprimentos indiretos, Jurídico, Tecnologia da Informação, Controladoria e Saúde, Segurança do Trabalho e Meio Ambiente (SSTMA).

Acima dos processos descritos, existe ainda a Diretoria executiva, composta por CEO, CFO e mais seis diretores, e o Comitê de auditoria. Diretoria e Comitê prestam contas ao Conselho de Administração, o nível mais alto da empresa com responsabilidade e autoridade

finais, e formado por membros da empresa e conselheiros independentes. O Conselho define a estratégia da organização e seu apetite ao risco, avalia a eficácia do SGC e define os valores e princípios éticos da empresa. A Diretoria, por sua vez, é responsável por implementar as diretrizes aprovadas pelo Conselho, enquanto o Comitê de auditoria deve supervisionar as atividades de gestão de riscos e *compliance*, bem como auditorias internas, e reportar ao Conselho. A NBR ISO 37301:2021 refere-se frequentemente à Alta Direção, o grupo de pessoas "que dirige e controla a organização em seu nível mais alto" (ABNT, 2021), e ao Órgão Diretivo, o grupo de pessoas "com responsabilidade e autoridade finais na organização, e ao qual a Alta Direção se reporta" (ABNT, 2021). No caso da empresa, estes correspondem respectivamente à Diretoria executiva e ao Conselho de Administração; o Comitê de auditoria mencionado encontra-se no mesmo patamar da Diretoria, mas teve menos relevância no decorrer do trabalho comparado aos dois primeiros.

A relação entre os processos de negócio, processos de suporte e as entidades acima é esquematizada a seguir (Figura 1). O escopo definido para este trabalho é a função de c*ompliance* e seus processos, considerando as interfaces com outras áreas à medida que contribuem para a compreensão destes, sem maiores detalhes. A referência a *Compliance* ao longo deste trabalho utilizou a terminologia de "função", estando de acordo com a NBR ISO 37301:2021; para os demais processos descritos, no entanto, foi adotada a terminologia de "área" por ser o termo utilizado pela empresa.

Figura 1 - Processos da empresa e escopo



Fonte: autora.

2 REVISÃO DA LITERATURA

Este capítulo apresenta a literatura pertinente ao estudo realizado, tendo como principais temas a Qualidade e Melhoria, a Gestão de Riscos, a Governança corporativa, o *Compliance* e a Integração de Sistemas de Gestão. O dois primeiros são centrais para este trabalho tendo em vista a NBR ISO 37301:2021, sua estrutura baseada no ciclo PDCA e sua ênfase na gestão de riscos. Os temas de Governança e *Compliance* são apresentados para contextualização, demonstrando sua importância no ambiente corporativo. O último tema visa pontuar benefícios e boas práticas relacionadas a sistemas integrados, uma vez que a Empresa A é certificada na NBR ISO 9001:2015.

2.1 QUALIDADE E MELHORIA

Tendo em vista o objetivo de melhoria do Sistema de Gestão de *Compliance,* é preciso definir o conceito de melhoria, discussão que se inicia no conceito de Qualidade. Este, no entanto, não tem uma definição simples; trata-se de um conceito que evolui e é incorporado aos conceitos existentes (BERSSANETI; BOUER, 2018). De adequação ao padrão, nos anos 1950, passando por adequação ao uso e adequação ao custo, o conceito de Qualidade agregou ainda a adequação às necessidades latentes e a fidelização dos clientes, a partir dos anos 2000 até os dias atuais. Os cinco conceitos não são conflitantes, mas é recomendado priorizá-los conforme a situação ou a função da empresa, por exemplo.

Destacam-se para o objeto de estudo os conceitos de adequação ao padrão e fidelização dos clientes. Na função de *compliance*, temos a adequação aos padrões estabelecidos interna e externamente, com o princípio de avaliar e corrigir desvios, e também a fidelização dos clientes e satisfação de todas as partes interessadas, com os princípios de atendimento às expectativas e conquista da fidelidade.

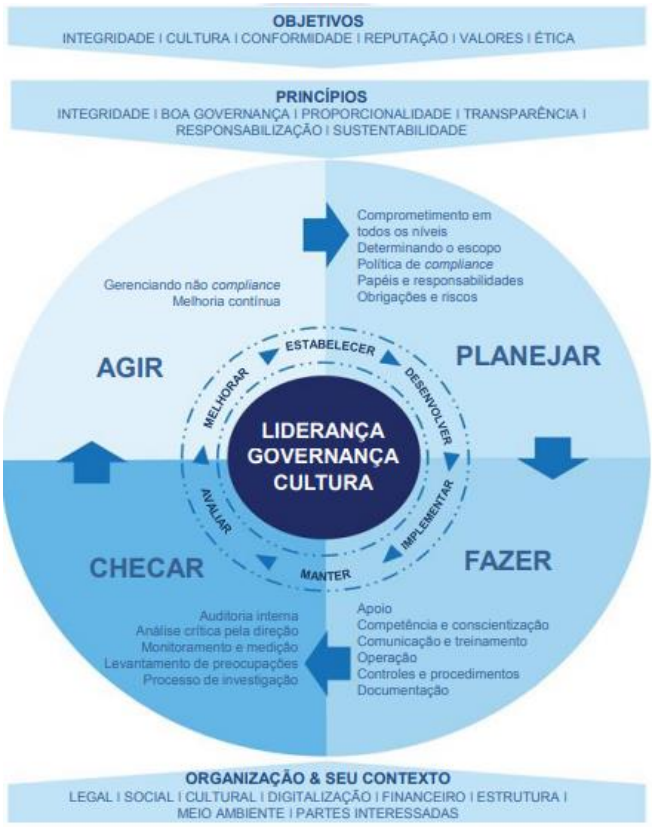
2.1.1 Ciclo PDCA

É de notada importância a contribuição dos gurus da qualidade no conceito de melhoria, em especial o ciclo de Deming, ou ciclo PDCA, difundido no Japão nos anos 1950. O ciclo é parte fundamental do conceito de melhoria (*kaizen*) e trata-se de um método de gestão para garantir a sobrevivência e o crescimento da organização (BERSSANETI; BOUER, 2018), consistindo em: Planejar (P), estabelecendo os objetivos e metas do negócio e os processos e

recursos necessários para alcançá-los, atendendo as expectativas do cliente e da própria organização; Fazer (D), implementando o que foi planejado; Checar (C), monitorando e medindo os processos, produtos e serviços em relação aos objetivos e requisitos da organização, além de reportar os resultados; e Agir (A); executando ações para melhoria do desempenho, conforme a necessidade (BERSSANETI; BOUER, 2018).

O ciclo PDCA possui aplicações para diferentes tipos de negócio, sendo utilizado, por exemplo, na NBR ISO 9001:2015 e na NBR ISO 37301:2021, como direcionador para a sua estrutura de requisitos (Figura 2). O escopo deste trabalho se situa nas duas primeiras etapas do ciclo: os itens 4 – Contexto da organização, 5 – Liderança e 6 – Planejamento integram a etapa de *planejar*, e os itens 7 – Apoio e 8 – Operação, a etapa de *fazer*. Os itens 9 e 10, fora do escopo, consistem nas etapas de *checar* e *agir*.

Figura 2 - Ciclo PDCA aplicado à NBR ISO 37301:2021



Fonte: ABNT (2021).

Além do ciclo PDCA, a melhoria contínua foi um dos principais legados de Deming e Ishikawa, abrangendo também o ciclo SDCA, no qual o planejar (P) é substituído pelo padronizar (S, de *standardize*). Não pode haver melhoria sem padronização; o ciclo PDCA

promove a melhoria e o SDCA, a padronização dessa melhoria até que haja novo padrão (BERSSANETI; BOUER, 2018).

2.1.2 Gestão de Processos e Qualidade

A obra de Deming (1986) é fundamental na discussão da qualidade, especialmente sobre seus impactos na gestão. O autor aponta como a qualidade do processo gera uma reação em cadeia, reduzindo custos, melhorando a posição competitiva, fazendo pessoas mais felizes em seu trabalho e gerando mais empregos. Deming é reconhecido por seus 14 princípios de gestão, sendo destacados para este trabalho cinco deles:

a) Princípio 3: Eliminar a necessidade de inspeção em massa construindo qualidade no produto. A inspeção total equivale ao planejamento para defeitos, reconhecendo a incapacidade do processo, devendo ser adotado, no lugar desta, o controle estatístico do processo;
b) Princípio 5: Melhorar constantemente e para sempre o sistema de produção e serviço, resultando numa redução constante do custo. Destaca-se a necessidade de rastrear as causas de falhas que aparecem periodicamente, em vez de associá-las à aparente causa imediata;
c) Princípio 7: Instituir liderança, que tem como objetivo melhorar o desempenho dos demais. A liderança não deve apenas encontrar falhas, mas remover sua causa, ajudando as pessoas a fazerem um trabalho melhor com menos esforço;
d) Princípio 9: Quebrar barreiras entre departamentos, para que pessoas de todos eles possam trabalhar em equipe e antever problemas do produto ou serviço;
e) Princípio 12: Remover barreiras que impedem as pessoas de se orgulhar de seu trabalho, tais como a avaliação anual por mérito. O problema dessa avaliação é seu foco no produto final, e não na liderança para ajudar pessoas, visando atingir a qualidade.

Destaca-se também para este estudo a importância de definições operacionais para viabilizar a conformidade, ou seja, o *compliance*. Definições operacionais colocam sentido comunicável em um conceito (DEMING, 1986), que terá o mesmo sentido para todas as partes envolvidas e em todo tempo. O autor salienta que desentendimentos entre empresas e entre departamentos frequentemente têm suas raízes na falha em definir termos e suas especificações de desempenho.

A importância de definições fica mais clara dentro do tema de padrões e regulações, ao qual o autor dedica um capítulo de seu livro (DEMING, 1986, cap. 10). A conformidade só

pode ser julgada com testes e critérios bem definidos em termos estatísticos, não qualitativos. É ressaltada a distinção entre regulações e padrões voluntários como essencialmente as penalidades atreladas à falha em cumprir cada um; apesar de a NBR ISO 37301:2021 ser um padrão voluntário, a penalidade de não a atender cresce à medida que mais empresas a adotam, como ocorre com a NBR ISO 9001:2015 atualmente.

Ainda no mesmo capítulo, Deming (1986) aponta como a violação de regulações causa um estado crescente de desordem, destruindo a consciência pública. As regulações devem ser rigorosas num sistema permanente e organizado, para que a violação seja evitada; por outro lado, autoridades públicas não devem impor obrigações que são incapazes de fazer cumprir (DEMING, 1986), o que de certa forma pode ser aplicado às organizações quanto a seus regulamentos internos.

2.1.3 Ferramentas de Gestão

Dentre as principais ferramentas da qualidade, destaca-se para este trabalho o mapeamento de processos, através de fluxogramas. O mapeamento de processos fornece uma figura completa, permitindo visualizar e estudar as peças em movimento e as transferências envolvidas no processo (MARRIOT, 2018). Isso facilita não só o entendimento do processo atual, mas também sua comparação com o planejado ou desejado, além de possibilitar a realização de análises críticas e auditorias em busca de oportunidades de melhoria (BERSSANETI; BOUER, 2018). Os fluxogramas presentes neste trabalho foram elaborados no *Bizagi Modeler* ® e seguem a simbologia apresentada no Apêndice A.

A implementação de melhorias comumente se dá como um projeto, isto é, “um empreendimento temporário visando obter um resultado específico” (PMI, 2017). Isto posto, destaca-se a contribuição de ferramentas de gestão de projetos para o propósito desde trabalho, como a Matriz RACI (Figura 3). Esta ferramenta é um tipo de matriz de atribuição de responsabilidades, relacionando atividades e membros da equipe de projeto; o formato matricial mostra todas as atividades associadas a uma pessoa, bem como todas as pessoas associadas a uma atividade. A Matriz RACI, em especial, classifica os envolvidos em responsável (R), aprovador (A), consultado (C) e informado (I), permitindo atribuição clara dos papéis e responsabilidades dos envolvidos.

Figura 3 - Exemplo de Matriz RACI.

Matriz RACI	Pessoa				
Atividade	Ana	Bento	Carlos	Dina	Eduardo
Criar contrato	A	R	I	I	I
Coletar requerimentos	I	A	R	C	C
Submeter requisição	I	A	R	R	C
Desenvolver plano de testes	A	C	I	I	R
	R = Responsável, A = Aprovador, C = Consultado, I = Informado				

Adaptado de PMI (2017).

2.2 GESTÃO DE RISCOS

Os conceitos de risco e gestão de riscos são fundamentais na discussão do tema de *compliance.* Risco pode ser definido como o efeito da incerteza nos objetivos, considerando as consequências de um evento e sua probabilidade associada (GREEN, 2015). A gestão de riscos consiste no conjunto de princípios, processos, atividades, papéis, responsabilidades e infraestrutura, combinados num sistema utilizado para controlar as ações da organização, com base nos riscos que ela enfrenta.

James Lam (2003) destaca razões práticas para considerar a gestão de riscos essencial dentro da gestão empresarial, especialmente de organizações de capital aberto como é o caso da Empresa A. Primeiramente, gerir riscos é responsabilidade da gestão, não dos acionistas; estes podem eleger diretores conforme seus interesses e retirar seu dinheiro caso a gestão os desagrade, mas não tratam dos riscos enfrentados internamente pela organização. Em segundo lugar, gerir riscos pode maximizar o valor para os acionistas, uma vez que a organização mostra um capital melhor alocado considerando os riscos, possui métricas e incentivos alinhados aos objetivos de risco, e incorpora o elemento de risco em suas decisões chave. A gestão de riscos ainda promove segurança ao trabalhador e segurança financeira à organização.

2.2.1 Avaliação de Risco

É essencial entender o contexto de risco para compreender os critérios utilizados na avaliação do risco. O contexto de risco é tanto interno, associado à cultura, aos processos, à estrutura, à estratégia e aos objetivos da organização, quanto externo, associado ao mercado, à economia e à política, por exemplo. A avaliação consiste na identificação, análise e priorização dos riscos, gerando como resultado o perfil de risco da organização (GREEN, 2015).

A identificação é uma listagem de eventos que podem ter consequências significativas, tanto os que estão sob controle da empresa quanto os que não estão; deve-se levar em conta a possível dificuldade de definir tais eventos, devido à ocorrência de eventos em cadeia ou às diferentes perspectivas existentes. Os eventos identificados são chamados perigos, e depois de analisados, passam a ser considerados riscos (GREN, 2015).

A análise de risco pode ser qualitativa ou quantitativa, sendo importante estabelecer critérios bem definidos, considerando que consequências são importantes, por que são importantes, quais são as partes interessadas, qual o contexto interno e externo etc. Uma importante ferramenta na análise de riscos é a Matriz de Probabilidade-Impacto, também chamada Matriz de Riscos, que permite dispor os riscos identificados em quadrantes para que sejam priorizados conforme a avaliação (Figura 4). A matriz geralmente é composta por três regiões, representando riscos prioritários (vermelho), pontos de atenção (amarelo) e riscos não urgentes (verde). A priorização deve determinar quais riscos serão tratados e em qual ordem, considerando as diretrizes da organização e os resultados da análise.

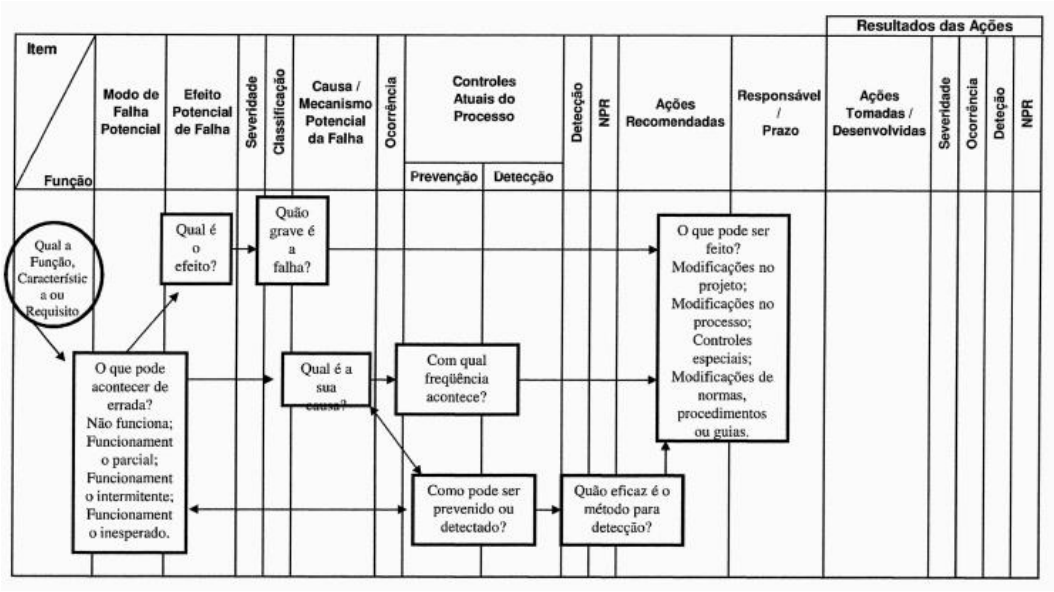
Figura 4 - Exemplo de Matriz Probabilidade-Impacto.

Adaptado de Green (2015) e da matriz de riscos utilizada na Empresa A.

Outra ferramenta de priorização é a FMEA (Análise de Modos e Efeitos de Falha; do inglês, *Failure Modes and Effects Analysis*), cujo objetivo é a prevenção de problemas de produto e processo (BERSSANETI; BOUER, 2018). O modelo permite avaliar a severidade (similar ao impacto da Matriz de Riscos), a ocorrência (similar à Probabilidade) e a detecção da falha, isto é, quão eficaz é o método de detecção atual em relação à falha e à causa

correspondente; estas três dimensões são avaliadas em uma escala de 1 a 10, sendo para detecção a nota 1 se for possível detectar a causa (melhor cenário), e nota 10 se não for detectada a causa nem a falha (pior cenário). O resultado das três dimensões multiplicadas é o NPR (número de prioridade de risco), indicador que varia de 1 a 1000; quanto maior o valor do NPR, maior a prioridade da falha associada. O uso da ferramenta é exemplificado, com instruções, abaixo (Figura 5):

Figura 5 - Exemplo de FMEA.



Fonte: Berssaneti; Bouer (2018).

Ainda outra técnica de priorização é a ferramenta GUT, tendo como base os fatores de Gravidade, Urgência e Tendência. Cada evento ou perigo avaliado deve receber uma nota de 1 a 5 em cada um dos fatores, e a nota final consiste na multiplicação das três, variando, portanto, de 1 a 125. Quanto maior a nota final obtida, maior a prioridade (BERSSANETI; BOUER, 2018).

Priorizados os riscos, temos ainda as etapas de tratamento e monitoramento de riscos. O tratamento consiste em escolher e implementar soluções para modificar o risco e melhorar os controles sobre ele (GREEN, 2015). Após o tratamento, o risco residual torna-se novo risco para a próxima rodada de avaliação. Existem diferentes estratégias para tratar os riscos (BERSSANETI; BOUER, 2018), sendo elas:

a) Transferir o risco (pagando a alguém para gerenciá-lo);
b) Evitar o risco (com ações para reduzir sua probabilidade);
c) Mitigar o risco (com ações para reduzir a consequência depois de ocorrido);

d) Aceitar o risco (não exercendo ação sobre ele, não como negligência, mas como decisão estratégica).

O monitoramento e a revisão de riscos envolvem o constante aprendizado e a investigação dos eventos. Destaca-se aqui o KRI (*key risk indicator*), que é todo indicador útil para monitorar a gestão de riscos da empresa, a efetividade de seus controles de risco, ou mesmo variáveis que indiquem probabilidade ou impacto associados a algum risco (GREEN, 2015).

2.2.2 Risco Operacional e Cultura de Risco

Um dos riscos destacados por Green (2015) é o risco operacional. Nas organizações, muitos riscos são conhecidos e aceitos, por serem inerentes ao negócio, enquanto outros podem criar desvios ao planejamento estratégico da empresa, inviabilizando a entrega consistente de seus objetivos. Riscos operacionais geralmente perturbam o centro da criação de valor: ativos, pessoas e processos de negócio. Se não forem devidamente tratados, tendem a criar volatilidade na organização; a gestão de riscos operacionais, desta forma, contribui para maior resiliência organizacional.

O autor destaca ainda os temas fundamentais para essa gestão, sendo eles: o foco em fatores humanos; a comunicação efetiva sobre riscos acima e abaixo na organização; e a construção de competências de resiliência. A comunicação não efetiva, em especial, é por si só fonte de risco (GREEN, 2015). Potenciais riscos podem ser identificados e informados, mas a falta de efetividade de comunicação com a liderança pode causar consequências severas. É preciso garantir não apenas a identificação, mas a comunicação efetiva para o tratamento dos riscos operacionais.

A cultura de risco é outro ponto destacado por Green (2015), dentro do tema de fatores humanos, com atenção especial à questão dos incentivos. Estes podem encorajar certos comportamentos, mas não necessariamente levarão aos resultados desejados. É fundamental estabelecer, dentro da cultura de risco, uma governança de incentivos, com monitoramento e gestão do plano de incentivos; tais práticas contribuem para que a avaliação por mérito não seja uma barreira ao orgulho do trabalho (DEMING, 1986), mas esteja atrelada à cultura e apoiada pela liderança.

Green (2015) aponta ainda que não se pode pagar por tudo que precisa ser feito, sendo de suma importância o papel dos gestores na definição de metas e objetivos, *feedback*, direcionamento do desempenho e reconhecimento de seus subordinados, reduzindo a dependência de incentivos para que o trabalho aconteça. Além disso, comportamentos que

trazem risco à organização não podem ser tolerados simplesmente para cumprir metas e receber incentivos; a gestão de riscos deve considerar, na própria elaboração de metas e determinação de incentivos, os riscos associados.

2.3 GOVERNANÇA CORPORATIVA

De acordo com Moeller (2011), as três questões de maior impacto nas empresas hoje são: gestão de riscos corporativos, processos de governança corporativa e programas efetivos de *compliance* em toda a organização. Governança, Riscos e *Compliance* resultam na sigla GRC, termo que tem crescido em reconhecimento entre as organizações e reflete uma nova forma de abordagem, integrada, desses aspectos em seus negócios.

Governança trata-se do conjunto de processos, políticas, leis e instituições que afetam a forma como a empresa é dirigida, administrada ou controlada (MOELLER, 2011). Inclui ainda o relacionamento entre as partes envolvidas e os objetivos para os quais a organização é governada, visando a eficiência econômica e a satisfação das partes interessadas. O conselho de diretores é o mecanismo fundamental interno de governança corporativa, sendo a fonte de autoridade de gestão na organização (GRIFFITH, 2016); no caso da empresa estudada, trata-se do Conselho de Administração.

O interesse por governança foi intensificado a partir de 2001 com o colapso de lucrativas empresas norte-americanas, como o caso Enron. A empresa se beneficiou de brechas da legislação constituindo novas empresas e alocando nelas suas dívidas, o que permitiu indicar lucros sempre crescentes, até que os resultados vieram à tona trazendo grande prejuízo, em especial, aos acionistas. O caso contribuiu para a criação da *Sarbanes-Oxley* (conhecida como SOx), lei norte-americana voltada para governança corporativa (UNITED STATES OF AMERICA, 2002).

De fato, empresas de qualquer local e tamanho enfrentam um crescente conjunto de regras e procedimentos, sejam ordens de segurança pública, leis nacionais ou internacionais e amplas regras e padrões de negócio. É preciso cumprir exigências em diversos níveis, sendo necessários processos para assegurar a operação em conformidade – em *compliance* – com tais exigências. Daí a forte relação com a gestão de riscos, tendo em vista o risco de violação de alguma regulação, o risco de as próprias regras de governança não atingirem os resultados desejados, além de riscos fora do controle da organização. O GRC trata-se, portanto, de um paradigma necessário para cuidar da organização e garantir seu crescimento da melhor forma possível (MOELLER, 2011).

2.3.1 ESG – *Environment, Social and Governance*

Na discussão sobre governança, destaca-se o termo ESG, especialmente na relação com investidores. O termo está associado não apenas a práticas sustentáveis, sociais e de governança, mas a "todo fundamento não financeiro que pode impactar o desempenho da organização" (HARPER, 2016 *apud* POLLMAN, 2021). Com a tendência de investimentos sustentáveis, o ESG torna-se tema central tanto para tomadores de políticas e corporações, quanto para investidores corporativos e individuais (BOFINGER *et al*, 2021), e iniciativas regulatórias nacionais aliadas ao movimento mundial de adoção dos princípios de ESG aumentam a demanda por empresas avaliadas neste quesito. A título de exemplo, o estudo de Bofinger *et al* (2021) enfatiza a todos os investidores, independentemente de suas preferências, que levem o critério de ESG em consideração por sua relevância no valor das empresas.

Dentre as abordagens de ESG presentes na literatura, Pollman (2021) aponta as relações com a qualidade da gestão de forma geral, a gestão de riscos e o *compliance*; destaca-se não apenas a importância das práticas de ESG, em si, mas também a forte imagem positiva associada, de forma geral, às empresas que as praticam. Uma das principais exigências relativas ao ESG, segundo a autora, é a transparência; a pressão para que as empresas disponibilizem "informações padronizadas, acuradas e auditadas" (POLLMAN, 2021) é crescente, objetivando a comparação entre elas para decisões de investimento.

2.4 *COMPLIANCE*

O último termo do GRC, o *Compliance,* se caracteriza pelo conjunto de processos internos usados pelas empresas para adaptar seu comportamento às normas aplicáveis, sejam elas legais, regulatórias ou sociais. A função de *compliance* – que é "uma pessoa ou grupo de pessoas com responsabilidade e autoridade para operar o Sistema de Gestão de *Compliance*" (ABNT, 2021) – é o meio pelo qual as empresas se ajustam às restrições necessárias, sendo geralmente responsável pelo risco de reputação e pela conduta do negócio consistente com as normas sociais (GRIFFITH, 2016).

2.4.1 Definições para Sistemas de Gestão de *Compliance*

Ao estabelecer requisitos e diretrizes para um SGC eficaz, a NBR ISO 37301:2021 utiliza definições que serão úteis no decorrer deste trabalho, sendo, por isso, indicadas a seguir:

a) Obrigações de compliance: são os “requisitos que uma organização mandatoriamente tem que cumprir, como também os que uma organização voluntariamente escolhe cumprir” (ABNT, 2021);
b) Não *compliance:* é o não atendimento às obrigações de *compliance*;
c) Riscos de *compliance*: é a “probabilidade de ocorrência e as consequências de não *compliance* com as obrigações de *compliance* da organização” (ABNT, 2021), ou seja, os perigos de não *compliance* depois de avaliados;
d) Requisito: é uma “necessidade ou expectativa que é declarada” (ABNT, 2021), como os requisitos da NBR ISO 37301:2021 referidos neste trabalho;
e) Não conformidade: é o não atendimento de um requisito;
f) Preocupações de *compliance*: são relatos de tentativas, suspeitas ou de violações reais às obrigações de *compliance* da organização;
g) Cultura de *compliance*: são os valores, comportamentos e práticas existentes por toda a organização que interagem com as estruturas e sistemas de controle, produzindo normas de comportamento que contribuem com o *compliance*;
h) Informação documentada: é uma “informação que se requer que seja controlada e mantida por uma organização e o meio no qual está ela está contida” (ABNT, 2021).

2.4.2 *Compliance* na prática

Enquanto a governança está atrelada ao conselho de diretores, interno à organização, a função de *compliance* se apresenta como fonte externa que revoga autoridade sobre o conselho. A função se sobrepõe, de certa forma, à governança como uma “atividade universal de governança corporativa” (GRIFFITH, 2016), o que enfatiza a importância evidente do *Compliance* no ambiente empresarial.

O estudo de Griffith (2016) traz interessantes contribuições sobre um núcleo comum de *compliance*, apesar das diferenças existentes entre os diversos setores que se adequam às regulações necessárias. Em primeiro lugar, temos o aspecto estrutural, que consiste em mais do que regras e regulações, mas na cultura de *compliance* e no pessoal alocado. O autor enfatiza que políticas e procedimentos bem desenhados não são suficientes, devendo ser destinado à função de *compliance* um agente com autoridade específica e um time adequado para as tarefas de *compliance.* A cultura, conforme Cardoni *et al* (2021), contribui para mudanças profundas na organização, e os funcionários podem contribuir efetivamente com a minimização de oportunidades de fraude. O princípio do equilíbrio é que não deve ser necessário escolher entre

resultados e regras, negócios e valores, o que implica também no treinamento de pessoal, ressaltando a importância da transparência de todos os departamentos em relação a seus dados e conhecimentos (CARDONI *et al*, 2020). A combinação de políticas e procedimentos com o pessoal engajado fará do *compliance* uma parte viva da organização, com capacidade de adaptação e mudança (GRIFFITH, 2016).

Em segundo lugar, há o fluxo de informação. Na organização, a informação flui para cima e para baixo, dos funcionários da operação para a alta gestão e vice-versa. *Compliance* deve se engajar com ambos os fluxos, por meio de uma função de reportes, permitindo que os níveis mais baixos possam reportar à alta direção e até ao CEO, e através de treinamentos nas políticas e procedimentos, para que até os mais altos níveis estejam instruídos e engajados (GRIFFITH, 2016).

Por fim, as regras devem ser cumpridas. Recomenda-se que os esforços internos para execução sejam direcionados às áreas com maior risco de *compliance*. Para isso, é necessária avalição de riscos regularmente (seção 2.2.1), envolvendo planejamento e revisão periódica. O processo deve retornar à elaboração de políticas e procedimentos, garantindo assim a atualização e contribuindo para a manutenção da relevância da função de *compliance* (GRIFFITH, 2016).

Sobre modelos de auditoria, vale destacar o estudo de caso de Cardoni *et al* (2020), sobre auditoria continuada como estratégia para controle de riscos e corrupção. A auditoria continuada difere da tradicional por sua frequência, foco em processos automatizados e análise de exceções. A efetividade dos esforços anticorrupção, e a favor do *compliance*, de forma geral, está muito ligada à efetividade do modelo de auditoria. Novas tecnologias levam a novos tipos de fraude, além do elevado volume de dados, o que exige novas formas de detecção. Enquanto na auditoria tradicional o auditor se conecta com o sistema de informação por um tempo determinado, na auditoria continuada, a análise é automatizada e aplicações de TI verificam toda a base de dados. A aplicação do modelo, no entanto, não é simples; no estudo de caso em questão (CARDONI *et al*, 2020), apenas os processos de maior risco utilizam auditoria continuada, enquanto os demais são auditados através de ferramentas tradicionais.

A atuação da função de *compliance* na prática, isto é, com base em relatos de executivos de diferentes empresas, também é explorada no estudo de Griffith (2016). No que diz respeito ao escopo e à organização, o que se observa é que a função de *compliance* tem feito bem mais do que garantir o cumprimento das leis aplicáveis. De acordo com os entrevistados (GRIFFITH, 2016), as principais áreas de foco da função incluem as esperadas, como regulações da indústria específica, corrupção, conflito de interesses, fraudes e discriminação, mas também outras, como

risco estratégico, continuidade do negócio, privacidade de dados e mídias sociais. Além disso, muitas companhias têm conferido ao responsável por *compliance* um cargo de diretoria, como CCO (*Chief Compliance Officer*), destacando a importância crescente da função nas organizações.

Com relação a métricas, o estudo (GRIFFITH, 2016) aponta a dificuldade de se demonstrar a eficácia da função de *compliance*, mesmo com todo o esforço empregado em diferentes ações. Algumas formas de avaliação utilizadas são descobertas de auditorias internas, taxa de treinamentos concluídos, pesquisas com os funcionários, revisões regulatórias de desempenho, entre outros. As métricas, no entanto, trazem resultados mais das próprias atividades do que do impacto trazido por elas à organização. Destaca-se a importância de outras métricas para que a exposição ao risco da organização seja entendida pela gestão, como apontado, por exemplo, com novos modelos de auditoria e uso de tecnologia.

2.5 INTEGRAÇÃO DE SISTEMAS DE GESTÃO

É de central importância para este trabalho a discussão de integração de sistemas de gestão, tendo em vista a adequação da empresa estudada à NBR ISO 37301:2021, sendo que já possui implementada a NBR ISO 9001:2015. O trabalho de Vitoreli e Carpinetti (2013) traz uma perspectiva empírica, proveitosa a este estudo, sobre o processo de integração dos sistemas de gestão da qualidade (ISO 9001) e de segurança e saúde ocupacional (OHSAS 18001); esta última foi substituída posteriormente pela NBR ISO 45001:2018 – Sistemas de Gestão de Saúde e Segurança Ocupacional (ABNT, 2018).

Entre as razões para a adoção de diferentes sistemas de gestão, encontra-se a exigência do ambiente organizacional de um bom relacionamento com as diferentes partes interessadas. O conjunto de processos inter-relacionados que dividem recursos e infraestrutura, visando atingir objetivos relacionados à satisfação dessas partes interessadas, trata-se de um Sistema de Gestão Integrado (SGI). É interessante que as organizações integrem e não separem seus sistemas de gestão, conforme Bernardo *et al.* (2015), que destacam o crescimento dos padrões de sistema de gestão nos últimos anos, apontando que todos esses sistemas podem constituir um SGI. Além disso, é ressaltada facilidade da implementação de outras normas por empresas que já atendem à ISO 9001[1].

[1] A ISO 9001 foi indicada sem a referência do ano de publicação visando manter a coerência com o estudo citado (VITORELI; CARPINETTI, 2013) que a apresenta desta forma; o mesmo se aplica à OHSAS 18001.

Diferentes benefícios são elencados para a integração de sistemas de gestão, entre eles: redução de custos, melhoria no gerenciamento, unificação dos treinamentos, melhor utilização de recursos financeiros, unificação das auditorias internas e externas (VITORELI; CARPINETTI, 2013), melhoria da satisfação do cliente, melhoria da imagem, melhoria na posição competitiva e melhoria na relação com autoridades e partes interessadas (BERNARDO *et al.,* 2015). Comparando a integração de sistemas de qualidade (ISO 9001) e meio-ambiente (ISO 14001), Bernardo *et al* apontam que há mais benefícios internos do que externos, o que é coerente com a própria decisão de integrar, que é mais interna do que a decisão de implementar os padrões em si, muitas vezes conduzida por exigências internas.

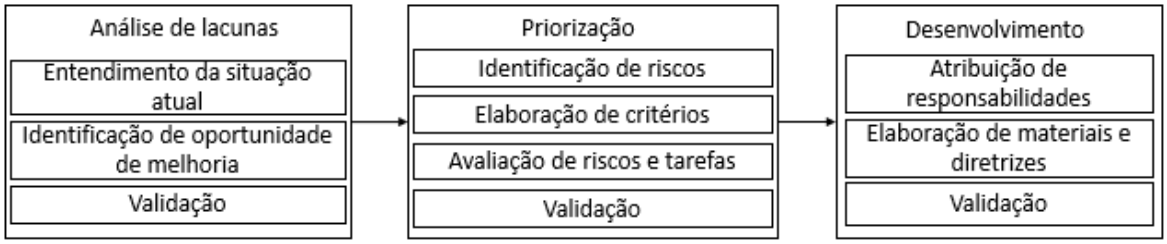
No entanto, conforme Vitoreli e Carpinetti (2013), a integração também apresenta dificuldades. Estas podem ser internas, relacionadas à falta de recursos humanos, colaboração entre os departamentos, auditores especializados, tempo para a integração e motivação dos funcionários, e externas, relacionadas com as normas e seus diferentes modelos e elementos; estas últimas têm maior impacto no nível de integração do que as dificuldades internas O mesmo estudo (VITORELI; CARPINETTI, 2013) aponta que os requisitos integrados com maior frequência e em maior grau são: controle de documentos e registros; política; objetivos e metas; manuais; auditoria interna; análise crítica da direção; e comunicação interna. Além disso, modelos têm sido desenvolvidos para que as empresas integrem os requisitos comuns entre as normas e formem subsistemas para os requisitos específicos de cada uma. Diferentes níveis de integração são possíveis, sendo eles: integração de documentação, integração de ferramentas de gerenciamento, políticas e objetivos comuns, e estrutura organizacional comum (SAMPAIO *et al.,* 2012 *apud* VITORELI; CARPINETTI, 2013).

Cada organização deve avaliar a possibilidade e o nível de integração, conforme suas características e contexto específico. Dependendo da criticidade do sistema de gestão para o negócio, por exemplo, pode-se optar por não integrar. No processo de implementação do SGI, de acordo com Karapetrovic (2013 *apud* VITORELI; CARPINETTI, 2013), cabe à alta direção decidir em que pontos da organização realizar a integração. São escolhidas funções para o SGI, e os requisitos das normas são integrados, permitindo a análise de lacunas para identificar os pontos comuns e os específicos de cada norma. É feita então a integração de documentação, objetivos específicos, recursos e processos dos sistemas. O último passo é a melhoria do sistema do SGI, como acontece nos sistemas de gestão não integrados. Vitoreli e Carpinetti (2013) deixam a sugestão de ampliar o estudo para outros sistemas de gestão além da ISO 9001 e OHSAS 18001, como é o caso deste trabalho.

3 MÉTODO

O estudo foi realizado com base em informação documentada disponível, observações diretas dentro da empresa durante seis meses de estágio, reuniões quinzenais com o gerente e a analista de *compliance* e entrevistas pontuais com outros quatro gerentes, das áreas de Jurídico, Relacionamento com o cliente, Controladoria e Suprimentos diretos. O trabalho foi realizado em três etapas (Figura 6), detalhadas a seguir.

Figura 6 - Etapas do trabalho



Fonte: autora.

3.1 ANÁLISE DE LACUNAS

A primeira etapa consistiu na realização de uma análise de lacunas, comparando as atividades e processos existentes na empresa com os itens 4 a 8 da NBR ISO 37301:2021; os próprios requisitos serviram, de forma geral, como guia para a compreensão dos processos da empresa. Com base na vivência do estágio, foi possível analisar as atividades em andamento e em desenvolvimento, bem como os documentos disponíveis, e a partir disso buscou-se esclarecer dúvidas e aprofundar o entendimento através de entrevistas com o gerente e a analista de *compliance.* A análise foi feita ao longo de seis semanas, sendo realizadas duas reuniões com a analista e quatro com o gerente de *compliance.* Além do esclarecimento de dúvidas, foi apresentada a evolução da análise a cada reunião, para validação das conclusões obtidas. Foram incluídos na "situação atual" da empresa apenas processos em vigor e documentos divulgados até o mês de agosto do presente ano; tomou-se conhecimento dos projetos em andamento, mas estes foram considerados posteriormente na análise.

Para cada item que foi avaliado, dividido por subitens, indicou-se: o status de atendimento ao requisito ("atende", "atende parcialmente" ou "não atende"); se o requisito é comum à NBR ISO 9001:2015; e as evidências de atendimento total ou parcial. Vale destacar que os requisitos da NBR ISO 37301:2021 comuns à NBR ISO 9001:2015 não são necessariamente idênticos; a relação foi feita identificando requisitos similares para promover

a busca por soluções integradas (SGQ e SGC), tendo em vista a facilidade da implementação de outras normas a partir da NBR ISO 9001:2015, conforme Bernardo *et al.* (2015).

As lacunas encontradas – os requisitos atendidos parcialmente ou não atendidos – foram exploradas para a identificação de oportunidades de melhoria para o SGC. Assim, para cada um desses requisitos, foram elaboradas tarefas para possibilitar seu atendimento, considerando novamente o texto da NBR ISO 37301:2021 e a evidências encontradas na empresa. Finalizada a determinação das tarefas, estas foram comparadas aos projetos em andamento da função de *Compliance*, para identificar quais tarefas poderiam ser englobadas por eles; essa informação foi utilizada na etapa de priorização.

3.2 PRIORIZAÇÃO

Para a priorização das tarefas, o primeiro passo foi identificar os principais perigos – pela definição de Green (2015) – de *compliance* da organização, para então agrupar as tarefas em cada um deles; a partir deste ponto, os perigos são apresentados como riscos pois já foram avaliados no decorrer do estudo. Vale destacar que a definição da NBR ISO 37301:2021 para riscos de *compliance* (ver seção 2.4.1, alínea c) considera todas as obrigações de *compliance* da organização, sendo mais abrangente do que os riscos identificados neste trabalho, tendo em vista o escopo delimitado.

Foi utilizada a classificação da empresa para os tipos de risco, como sendo: risco de imagem, ligado a fraudes e corrupção, trazendo danos à reputação da empresa; risco regulatório, envolvendo o não cumprimento tanto da legislação aplicável quando das normas internas; e risco operacional, decorrente de sistemas e controles inadequados, bem como falhas de gerenciamento e operação.

Para o agrupamento das tarefas, a lógica utilizada foi considerar as principais consequências da não realização destas e atribuir essas consequências a um risco. A elaboração dos riscos foi feita concomitantemente ao agrupamento das tarefas, uma vez que a análise destas em maior detalhe permitiu identificar novas consequências possíveis. No caso de mais de um risco aplicável, a decisão coube ao gerente de *compliance*; poderia ter sido associado mais de um risco para cada tarefa, mas optou-se por apenas um para conseguir maior objetividade e menor complexidade na priorização.

3.2.1 Definição de critérios

A ferramenta escolhida para a avaliação dos riscos foi a Matriz de Riscos, e utilizou-se um critério de esforço como dimensão adicional para avaliar cada tarefa; uma vez que possuem diferentes níveis de complexidade e tempo de realização, essa dimensão contribuiu para uma priorização mais coerente com o cotidiano da empresa. Assim, foram definidos os critérios de Impacto, Probabilidade e Esforço para viabilizar a priorização. Apesar de existir uma matriz de riscos da empresa, o processo de avaliação de riscos não foi documentado e, portanto, sua classificação não foi utilizada neste trabalho. O material da empresa foi aproveitado para a definição dos critérios de impacto e probabilidade, em conjunto com um guia de avaliação de riscos (COSO, 2012), adequando os fatores analisados à realidade da organização. Para que os critérios fossem, de fato, úteis à empresa, tanto neste trabalho quanto em aplicações futuras, foram realizadas duas reuniões com o gerente e a analista de *compliance* para sua validação.

O critério de Impacto foi definido considerando três aspectos, relacionados aos tipos de risco mencionados acima: imagem, operacional e legal. Logo, para definir o impacto de determinado risco, este teve de ser avaliado nos três aspectos para obter uma nota final, que foi a média de três notas; no caso de valores finais não inteiros, a nota foi arredondada para o inteiro mais próximo. Vale salientar que, apesar da classificação dos riscos em tipos, o impacto do risco dificilmente se restringe ao tipo classificado, e por isso tal diferenciação no critério foi considerada proveitosa. Para sistematizar a avaliação de cada critério, foi feita uma breve descrição do que deve ser levado em conta para cada nota, como mostra o Quadro 1.

O critério de Probabilidade foi definido em faixas por número de ocorrências no ano (Quadro 2), sendo a maior probabilidade “mais de 12 ocorrências no ano” e a menor, “menos de 1 ocorrência no ano”. Inicialmente, a escala havia sido definida de “1 ocorrência a cada 5 anos ou menos” até “mais de 10 ocorrências no ano”, mas nenhum dos riscos se encaixou nas faixas inferiores, o que levou à revisão da escala. Utilizou-se o número de ocorrências no ano para facilitar a comparação em base mensal, o que foi considerado proveitoso pela equipe de *compliance*. Assim, se todo mês é observada a mesma ocorrência, esta se enquadra no nível “frequente”; se ocorre quase todo mês, mas nem sempre, “provável”, e assim por diante.

Quadro 1 - Critério de Impacto: notas e definições

Nota	Nível	Impacto de imagem	Impacto operacional	Impacto legal
5	Extremo	Imagem nacional negativa no longo prazo com perda decisiva de *market share*[2], credibilidade seriamente prejudicada, grave prejuízo na obtenção de recursos	Muitos problemas morais e de maior gravidade, com alto *turnover*[3] da Diretoria	Multas significativas, ações judiciais, prisão de lideranças
4	Alto	Imagem nacional negativa no longo prazo com perda de *market share*, credibilidade prejudicada, algum prejuízo na obtenção de recursos	Muitos problemas morais, com aumento do *turnover* de cargos de gestão	Necessidade de grande projeto para ação corretiva, multas moderadas
3	Moderado	Imagem nacional negativa no curto prazo, pouco prejuízo na captação de recursos	Muitos problemas morais, com aumento do *turn over* nas posições intermediárias (analistas, coordenadores)	Violação reportada com correção imediata a ser implementada
2	Pequeno	Reputação local prejudicada, sem prejuízo na captação de recursos	Alguns problemas morais, com aumento pontual do *turnover*	Reporte para órgão regulador, sem prosseguimento de ações
1	Incidental	Reputação local rapidamente recuperada, sem perda de credibilidade	Insatisfação pontual de colaboradores, sem impacto significativo no *turnover*	Sem necessidade de reporte para órgão regulador

Fonte: autora.

Quadro 2 - Critério de Probabilidade: notas e definições

Nota	Nível	Definição
5	Frequente	Mais de 12 ocorrências no ano
4	Provável	De 9 a 12 ocorrências no ano
3	Possível	De 5 a 8 ocorrências no ano
2	Improvável	De 1 a 4 ocorrências no ano
1	Raro	Menos de 1 ocorrência no ano

Fonte: autora.

O critério de Esforço foi o que necessitou maior detalhamento, tendo em vista a variedade de tarefas consideradas. Inicialmente, propôs-se uma classificação das tarefas de forma mais abrangente, sendo obtidas sete categorias, da menos para a mais complexa: (1) Alteração em documentos, (2) Elaboração de documento simples, (3) Alteração em processo,

[2] *Market share*: fatia de mercado na indústria em que a empresa atua.
[3] *Turnover*: taxa de rotatividade, de substituição dos funcionários antigos por novos.

(4) Ações para executar processo existente, (5) Tomada de decisão/definições e documentação, (6) Elaboração de documento complexo e (7) Desenho de processo. O quadro 3 indica a descrição de cada categoria e uma estimativa de duração; esta foi baseada na experiência e no conhecimento adquirido da empresa, com as atividades realizadas no último ano, na configuração atual da função de *compliance*. Considerou-se o tempo total para finalização, não apenas o efetivamente empregado na tarefa; por exemplo, ainda que um documento complexo (categoria 2) requeira dez horas de escrita, em geral envolverá reuniões com outras áreas e um prazo para revisão e aprovação, sendo concluído todo o processo em, no máximo, seis semanas. A estimativa também considera, para a determinação do tempo necessário, que a função de *compliance* não estará focada somente na tarefa, tendo outras responsabilidades em paralelo. As sete categorias iniciais foram agrupadas em cinco notas a fim de manter a mesma escala dos critérios anteriores. Destaca-se que o critério de esforço possui a nota inversamente proporcional, isto é, quanto menor o esforço, maior a nota atribuída.

Quadro 3 - Critério de esforço: notas e definições

Nota	Nível	Definição
5	Alterações em documento	Alterações em documento existente, como mudança, atualização, inclusão ou remoção de elementos; duração de até 1 dia
5	Elaboração de documento simples	Elaboração de documento de até duas páginas, como modelos ou formulários; duração até 1 dia
4	Alterações em processo	Alteração na forma como um processo atual é realizado, envolvendo alteração de documento e conscientização dos envolvidos; duração até 1 semana
4	Ações para executar processo existente	Desenvolvimento de ações para colocar em prática processos de *compliance* já existentes formalmente; duração até 1 semana
3	Tomada de decisão/definições e documentação	Definições que envolvem Diretoria e/ou gestão de outras áreas, com a necessidade de reuniões e aprovações; duração de até 4 semanas
2	Elaboração de documento complexo	Elaboração de documento com mais de duas páginas, possivelmente envolvendo diferentes áreas, incluindo período para aprovação; duração até 6 semanas
1	Desenho de processo	Desenho de novo processo, incluindo documentos e treinamentos envolvidos; duração de até 12 semanas

Fonte: autora.

Além das categorias de esforço, foi estabelecido um fator de redução de esforço (e aumento da nota correspondente) quanto a tarefas correlacionadas, redundantes e em andamento. Foram consideradas correlacionadas tarefas que podem ser executadas juntas, ou que apresentam algum tipo de dependência entre si, gerando, desta forma, ganho de escala. Tarefas redundantes são aquelas que, uma vez realizadas, contribuem para o atendimento de mais de um requisito; estas foram repetidas na lista de tarefas geral para evidenciar quais os requisitos atendidos. As tarefas em andamento também exigem menor esforço quando comparadas a tarefas não iniciadas. Para tarefas enquadradas em mais de um fator, foi considerado o de valor maior para a nota final; por exemplo, para tarefas correlacionadas (10%) mas também em andamento (30%), prevalece a redução de 30%.

Os valores definidos para o fator de redução do esforço (Quadro 4) foram baixos (10% e 30%) pois a intenção inicial era avaliar as tarefas com uma espécie de análise GUT, sendo a Gravidade correspondente ao Impacto, a Urgência, à Probabilidade, e a Tendência, substituída pelo critério de Esforço (ou seja, "IPE" no lugar de GUT). Assim, buscou-se um aumento percentual pequeno para minimizar a distorção, uma vez que a nota final seria uma multiplicação das três. No entanto, observou-se grande distorção não pelo percentual de aumento em si, mas pela própria ferramenta escolhida; tarefas com baixo esforço, mesmo que sem grande risco de *compliance*, ficaram à frente daquelas atreladas a riscos prioritários (área vermelha da Matriz de Riscos), mas com maior esforço envolvido.

Quadro 4 - Fator de redução de esforço

Fator	Descrição	Redução do esforço
Tarefas correlacionadas	Ganho de escala	10%
Tarefas redundantes	Mesma tarefa atende 2 requisitos	30%
Tarefa em andamento	Já iniciada antes do estudo	30%

Fonte: autora.

Com isso, optou-se por utilizar a Matriz de Riscos no lugar da análise GUT, sendo utilizado o critério de Esforço somente para refinar as tarefas avaliadas como prioritárias na Matriz; a decisão considerou os critérios de risco mais importantes que o de esforço, e teve a aprovação do gerente de *compliance*. Dessa forma, os riscos foram avaliados de acordo com Impacto e Probabilidade e dispostos na Matriz de Riscos, enquanto as tarefas foram avaliadas, individualmente, de acordo com o Esforço; esta última avaliação foi verificada e aprovada pela analista de *compliance*, por estar habituada às atividades mais operacionais. A nota de Esforço foi utilizada para priorizar as tarefas atreladas aos riscos prioritários (área vermelha da Matriz), e as dez primeiras colocadas seguiram para a etapa de desenvolvimento.

Com a alteração da ferramenta, porém, foi necessário rever o fator de redução de esforço (Quadro 4), uma vez que a baixa porcentagem se devia à ferramenta anterior. Foi realizado um teste substituindo os valores de 10% e 30% por 30% e 50%, respectivamente, para as tarefas enquadradas no fator. O resultado foi que as dez primeiras colocadas se mantiveram as mesmas, havendo apenas alteração na ordem entre elas, como indicado na abaixo (Figura 7); a tarefa 46 ficou à frente das tarefas 26 e 52 no cenário 2. Uma vez que não houve diferença significativa no escopo analisado, os valores de 10% e 30% foram mantidos. Destaca-se, no entanto, que essa porcentagem de redução é apenas uma estimativa para fins de priorização, não devendo ser considerada em termos exatos do tempo necessário para execução das tarefas.

Figura 7 - Teste para o fator de redução de eforço

Ranking	Tarefa	Esforço
1	14	5,2
2	20	5,2
3	40	5,2
4	48	5,2
5	26	5
6	52	5
7	46	4,4
8	39	4
9	44	4
10	51	4
11	23	3,3
12	43	3,3
13	12	3
14	45	2,6
15	16	2,2
16	17	2,2
17	59	1
18	18	1

Cenário 1 (10% e 30%)

Ranking	Tarefa	Esforço
1	14	6
2	20	6
3	40	6
4	48	6
5	46	5,2
6	26	5
7	52	5
8	39	4
9	44	4
10	51	4
11	23	3,9
12	43	3,9
13	12	3
14	45	3
15	16	2,6
16	17	2,6
17	59	1
18	18	1

Cenário 2 (30% e 50%)

Fonte: autora.

3.3 DESENVOLVIMENTO

Antes de prosseguir no desenvolvimento, o texto da NBR ISO 37301:2021 foi retomado para garantir que os requisitos seriam atendidos corretamente com os materiais e diretrizes elaborados. Foi criado um quadro indicando, para cada tarefa priorizada, o texto integral relacionado; no caso de tarefas redundantes (conforme descrição do Quadro 4), foi indicado o texto de ambos os requisitos a serem atendidos.

As dez tarefas foram, então, divididas em subtarefas de menor complexidade, sendo separado o que seria feito pela autora e o que ficaria a cargo da analista de *compliance*, seja pelo tempo disponível ou pela autoridade necessária para realizar a atividade. Para a atribuição de responsabilidades, foi elaborada uma Matriz RACI tendo como agentes não só a autora, a

analista e o gerente de *compliance*, mas também outros agentes considerados importantes dentro da organização.

Para facilitar o desenvolvimento e a elaboração de materiais associados entre si, as subtarefas foram agrupadas em cinco assuntos, de acordo com as correlações já identificadas e relações feitas posteriormente. Para cada assunto, foi retomada a situação atual com maior aprofundamento, e então elaborados materiais e diretrizes, conforme indicado na Matriz RACI. A elaboração ocorreu ao longo de cinco semanas, com duas reuniões com o gerente e uma com a analista de *compliance* para esclarecimento de dúvidas, solicitação de materiais da empresa e validação final. Dos assuntos tratados, dois requerem maior detalhamento do método utilizado: "Ações de *compliance* dos gestores" (seção 4.3.3) e "Política de *compliance*" (seção 4.3.5).

O primeiro diz respeito à tarefa 26 e envolveu a consulta a gerentes de outras áreas para enriquecimento da solução. Quatro gerentes, indicados pelo gerente de *compliance,* foram consultados a respeito: de seu entendimento das próprias responsabilidades de *compliance;* de ações de encorajamento em relação à sua equipe; da conscientização de sua equipe em assuntos de *compliance*; e de como a área de *compliance* pode ajudar e facilitar suas ações diárias nesse sentido. Foram entrevistados os gerentes das áreas de Jurídico, Relacionamento com o cliente, Controladoria e Suprimentos diretos. As entrevistas foram de grande contribuição para o trabalho, e a proposta de solução, que seria inicialmente restrita à uma especificação de como evidenciar as ações diárias dos gestores, passou a incluir uma relação de propostas de melhoria para as próprias ações.

O segundo inclui quatro tarefas, mas será detalhada especialmente a tarefa 16, que consiste na elaboração completa da política de *compliance*. Uma vez que isso exigiria mais tempo e envolvimento de outras áreas da empresa do que seria possível neste trabalho, ficou acordado com o gerente de *compliance* a criação de uma estrutura para auxiliar a posterior elaboração em detalhes. Para tal, foi utilizado o texto integral da NBR ISO 37301:2021, bem como as orientações de uso referentes ao requisito 5.2 (ABNT, 2021, p. 31-32). Para cada item requerido, foi relacionado o processo ou documento da empresa que o atende ou o que deve ser feito para atendê-lo; no caso de o requisito estar relacionado a alguma das tarefas não priorizadas, estas foram também indicadas.

4 RESULTADOS E DISCUSSÃO

Este capítulo apresenta os resultados obtidos com a aplicação do método descrito, bem como a discussão pertinente a cada etapa. Os principais resultados da análise de lacunas são o resumo da situação atual e uma lista de oportunidades de melhoria baseadas nas lacunas encontradas. A priorização, por sua vez, tem como principais resultados a avaliação de riscos e de esforço das tarefas, e uma discussão que levou à inclusão de duas tarefas não priorizadas. Por fim, os resultados da etapa de desenvolvimento são 27 propostas de melhoria, incluindo alterações em processos e documentos existentes, novos processos e documentos, e recomendações diversas.

4.1 ANÁLISE DE LACUNAS

O resultado resumido da análise de lacunas é apresentado abaixo (Quadro 5A e 5B), seguido pela descrição em maiores detalhes de como a empresa atende a cada um dos requisitos com as evidências apresentadas.

Quadro 5A - Resumo da análise de lacunas: Situação atual

Item	Subitem	Status	ISO9001	Evidência
4	4.1	Atende parcialmente	Sim	Planejamento estratégico Documentos de Relacionamento com o cliente, Suprimentos, Incorporação, Comercial, Novos negócios Demonstrações financeiras (site de relação com investidores) Programa de *Compliance* (apresentação de slides)
4	4.2	Atende parcialmente	Sim	Partes interessadas
4	4.3	Não atende	Sim	-
4	4.4	Atende parcialmente	Não	Programa de *Compliance* (apresentação de slides) Documentos associados (treinamentos, políticas etc.) Política de gerenciamento de riscos
4	4.5	Atende parcialmente	Não	Partes interessadas Grupo de monitoramento de leis (evidência fraca)
4	4.6	Atende parcialmente	Não	Política de gerenciamento de riscos Plano de abordagem
5	5.1.1	Atende parcialmente	Não	Política de gerenciamento de riscos Código de Ética e Conduta; Site Institucional
5	5.1.2	Atende parcialmente	Não	Código de Ética e Conduta; Site Institucional Plano de comunicações de *compliance* Treinamentos de *compliance* e atividades obrigatórias Pesquisa de clima com questões de *compliance*
5	5.1.3	Atende parcialmente	Não	Estrutura organizacional Sistemas de apoio e orçamento específico

Quadro 5B - Resumo da análise de lacunas: Situação atual

Item	Subitem	Status	ISO9001	Evidência
5	5.2	Não atende	Não	-
5	5.3.1	Atende parcialmente	Sim	Orçamento para a função de *compliance* Política de Medidas disciplinares
5	5.3.2	Atende parcialmente	Não	Programa de *Compliance* (apresentação de slides) (evidência fraca) Política de gerenciamento de riscos Indicadores de *compliance* Políticas e código de *compliance* documentados Treinamento de conflito de interesses Plano de comunicações de *compliance*
5	5.3.3	Atende parcialmente	Sim	Código de Ética e Conduta Política de gerenciamento de riscos
5	5.3.4	Atende parcialmente	Sim	Treinamentos de compliance e Código de Ética e Conduta Indicador do canal de ética
6	6.1	Atende parcialmente	Sim	Programa de *Compliance* (apresentação de slides) (evidência fraca) Indicadores de *compliance*
6	6.2	Atende parcialmente	Sim	Programa de *Compliance* (apresentação de slides) (evidência fraca)
6	6.3	Não atende	Sim	-
7	7.1	Atende parcialmente	Sim	Orçamento para a função de *compliance* Sistemas de software de apoio
7	7.2.1	Atende parcialmente	Sim	Modelo de Descrição de cargos Comprovação de competências (evidência fraca)
7	7.2.2	Atende parcialmente	Sim	Treinamentos de *Compliance* e atividades obrigatórias Política de Medidas disciplinares
7	7.2.3	Atende parcialmente	Sim	Procedimento de Recursos Humanos Registros de treinamento no sistema
7	7.3	Atende parcialmente	Sim	Pesquisa de clima
7	7.4	Atende parcialmente	Sim	Plano de comunicações de *compliance* E-mails de comunicados salvos na rede
7	7.5	Atende parcialmente	Sim	Procedimento de Informação documentada Registros de treinamento e evidências de comunicação
8	8.1	Atende parcialmente	Sim	Indicadores de *compliance* Norma de Gestão de fornecedores Procedimento de Compras Quadros e planilhas de avaliação de fornecedores
8	8.2	Não atende	Não	-
8	8.3	Atende	Não	Canal de ética
8	8.4	Não atende	Não	-

Fonte: autora.

O documento de Planejamento Estratégico atende parcialmente ao requisito 4.1, apresentando o modelo de negócio (incluindo a estratégia e a natureza do negócio) e as

estruturas internas da empresa. Normas e procedimentos de diferentes áreas, como Relacionamento com o cliente, Suprimentos, Incorporação, Comercial e Novos negócios, atendem ao mesmo requisito, apresentando a natureza e o escopo dos negócios na relação com terceiras partes, sendo elas: clientes, fornecedores, governo e proprietários de terreno. Outras partes como comunidade, sindicato e mídias sociais possuem comitês ou ações pontuais, não documentados. O mesmo requisito é atendido também pelas demonstrações financeiras da empresa, que apontam sua situação econômica, disponíveis no site de relação com investidores da organização.

O Programa de *Compliance*, documentado em uma apresentação de slides, atende a cinco requisitos da NBR ISO 37301:2021, apesar de ser uma evidência fraca; a apresentação indica as atividades em andamento da função de *compliance*, mas faltam processos documentados evidenciando como são realizadas. Destaca-se aqui a importância da padronização com pré-requisito à melhoria (BERSSANETI; BOUER, 2018). Os requisitos 4.1 e 4.4 são atendidos parcialmente pelo Programa; o 4.1 pela disseminação da cultura de *compliance* na organização, e o 4.4 pela comprovação da existência de um Sistema de Gestão de *Compliance*, ainda que este não esteja de acordo com todos os requisitos da NBR ISO 37301:2021.

Documentos associados ao Programa, como treinamentos e políticas, contribuem para o atendimento parcial ao requisito 4.4. O Programa atende parcialmente ao requisito 5.3.2, de modo que, com melhores evidências do que é realizado e algumas poucas alterações, é possível atender ao requisito totalmente; isso porque o Programa aborda a identificação de obrigações de *compliance*, o alinhamento do sistema com os objetivos de *compliance*, um sistema de documentação e reporte de *compliance*, entre outros. O Programa também evidencia a existência da função de *compliance*, com acesso a todos os níveis da organização e a todo o pessoal, informação documentada e dados necessários. Os requisitos 6.1 e 6.2 também são parcialmente atendidos pelo Programa de *Compliance.* O primeiro é atendido pelo planejamento de ações para abordar riscos e oportunidades, mas este planejamento não é atrelado à análise de riscos vigente. O requisito 6.2 é atendido pelas metas apresentas no Programa, mas falta uma descrição detalhada dos objetivos, como métricas, monitoramento e planejamento para alcançá-los; além de exigido pela NBR ISO 37301:2021, a importância de definições operacionais como essas é ressaltada por Deming (1986), para que a conformidade seja realmente atingida.

O documento de Partes Interessadas atende parcialmente aos requisitos 4.2 e 4.5. Uma vez que foi elaborado para o SGQ, o documento considera partes interessadas e requisitos

voltados para a Qualidade. Para atendimento total ao requisito 4.2, é preciso reconsiderar as partes interessadas pertinentes para o Sistema de Gestão de *Compliance,* seus requisitos relacionados, e quais destes serão abordados pelo SGC (uma vez que podem ser abordados também por outras áreas da empresa). O requisito 4.5 é atendido apenas parcialmente, pois a identificação das obrigações de *compliance* não é sistemática, como exige a NBR ISO 37301:2021. Além do documento citado, é feito um monitoramento manual (sem auxílio de sistema específico) da legislação pertinente, sem periodicidade estabelecida, por um grupo de monitoramento. As mudanças necessárias decorrentes de novas obrigações são realizadas conforme a demanda, sem processo implementado.

A Política de Gerenciamento de Riscos estabelece diretrizes e responsabilidades para a gestão de riscos da organização, contribuindo para o atendimento parcial de cinco requisitos. O documento atende parcialmente ao requisito 4.4, como informação documentada do SGC, e ao requisito 4.6, indicando o processo de avaliação de riscos das diferentes áreas da empresa, incluindo aqueles relacionados a terceiras partes. No entanto, nem todos os riscos levantados são riscos de *compliance*; há também riscos de forma geral (por exemplo: risco de acidente nas obras). Não há um processo de avaliação periódica de riscos específicos de *compliance.* Os riscos e as ações para abordá-los são documentados no Plano de abordagem (documento desenvolvido pelo SGQ que é preenchido para cada área), o que também contribui para o atendimento parcial ao requisito 4.6; ainda falta rastreabilidade entre os riscos levantados na Política de Gerenciamento de Riscos e os tratados no Plano de abordagem, mas este é um exemplo de adaptação a ser feita para integrar os sistemas, permitindo a melhoria no gerenciamento (VITORELI; CARPINETTI, 2013). A Política ainda atende parcialmente ao requisito 5.1.1, determinando as responsabilidades da diretoria e do conselho de administração quanto ao gerenciamento de riscos, ao 5.3.2, documentando a avaliação de riscos de *compliance,* e ao 5.3.3, uma vez que o mapeamento de riscos realizado conta com a participação dos gestores das diferentes áreas.

Um documento fundamental para o *compliance* da empresa é o Código de Ética e Conduta, que apresenta seus valores e princípios, reforça a responsabilidade de todos os colaboradores pelo *compliance* e inclui diretrizes para diversos assuntos, entre eles: privacidade, conflito de interesses, lavagem de dinheiro, contratação de fornecedores e setor público. Com isso, o documento atende parcialmente aos requisitos 5.1.1, 5.1.2 e 5.3.3. As informações divulgadas no Site Institucional também contribuem para o atendimento dos requisitos 5.1.1 e 5.1.2.

O Plano de Comunicações de *Compliance* contém as datas e os assuntos dos comunicados de *compliance* ao longo ano. O documento atende parcialmente aos requisitos 5.1.2 e 5.3.2, fomentando a cultura de *compliance* e aconselhando a organização sobre assuntos relacionados, e ao 7.4, determinando as comunicações pertinentes; a informação documentada requerida por este último requisito é atendida pelos e-mails dos comunicados salvos na rede[4] da organização.

Um e-mail é enviado a todos os novos colaboradores com atividades obrigatórias a serem realizadas, incluindo treinamentos de *compliance* e do SGQ (com procedimentos das diferentes áreas da empresa para conhecimento de todos, conforme pertinente), leitura e adesão ao Código de Ética de Conduta e preenchimento de questionário sobre conflito de interesses. Isso contribui para o atendimento parcial aos requisitos 4.4, integrando o SGC vigente, 5.1.2, fomentando a cultura de *compliance*, 5.3.2, com o treinamento de todas as pessoas pertinentes, 5.3.4, incentivando o cumprimento dos procedimentos e políticas da organização, e 7.2.2, como treinamento obrigatório para novos contratados. A unificação de treinamentos, um dos benefícios da integração de sistemas (VITORELI; CARPINETTI, 2013), não foi observada; ainda que não seja um requisito, é um ponto a ser considerado pela organização.

É realizada também, anualmente, uma Pesquisa de Clima com toda a organização, abordando, entre outras questões, o tema de *compliance*; a pesquisa inclui perguntas sobre a ética da empresa em seus negócios, as diretrizes de comportamento da empresa, a imagem da empresa na relação com os colaboradores e a disposição destes em utilizar o Canal de Ética. Em 2021, conforme informado pela analista de *compliance*, 92% dos colaboradores responderam à pesquisa e, destes, 75% apresentaram resultado favorável em relação às perguntas de *compliance.* Assim, a Pesquisa contribui para o atendimento parcial aos requisitos 5.1.2, como avaliação da cultura de *compliance*, e 7.3, indicando a conscientização sobre a importância desta cultura. Este último requisito, no entanto, tem a maior parte das exigências não atendidas, o que indica baixa conscientização.

A posição da função de *compliance* na estrutura organizacional vigente, de forma não conflitante, o orçamento específico para a função e os sistemas de apoio disponíveis atendem parcialmente ao requisito 5.1.3. Para que o atendimento seja total, é necessário evidenciar a realização de apresentações periódicas ao CFO; estas já ocorrem, porém não há documentação. O contato direto da função com os níveis mais altos da organização (Diretoria e Conselho) contribui na instrução e engajamento destes com o *Compliance*, conforme recomenda Griffith

[4] *VPN: rede privada virtual.*

(2016). O orçamento destinado à função de *compliance* ainda atende parcialmente aos requisitos 5.3.1, e 7.1, comprovando a alocação de recursos. Os sistemas de apoio citados anteriormente também contribuem para o atendimento ao requisito 7.1, sendo somente parcial devido aos relatos sobre a necessidade de outros sistemas e maior conscientização da Diretoria sobre recursos para a função de *compliance.*

A empresa conta ainda com uma Política de Medidas Disciplinares, que estabelece diretrizes para a aplicação destas medidas aos colaboradores que pratiquem atos em violação à legislação, ao Código de Ética e Conduta ou a outras políticas e procedimentos internos. A política contribui para o atendimento parcial aos itens 5.3.1, estabelecendo mecanismo de responsabilização, e 7.2.2, como informação a todo o pessoal após a contratação. Destaca-se a necessidade de conscientização e fortalecimento da cultura de *compliance* nesse aspecto, uma vez que, mesmo com a política estabelecida e divulgada, ainda há resistência na organização em fazer cumpri-la.

Os indicadores de *compliance* existentes abrangem: monitoramento de riscos (avaliados anualmente); elaboração e aprovação de normativos; aderência à legislação de *compliance*; documentos assinados; adesão ao Código de Ética; comunicações efetuadas; treinamentos realizados; fornecedores homologados e solicitações no Canal de Ética. Esses indicadores atendem parcialmente aos requisitos 5.3.2, como forma de monitorar o desempenho de *compliance* e como sistema de documentação, 6.1, como meio para avaliação da eficácia das ações realizadas, e 8.1, como controle dos processos de *compliance* vigentes. Especialmente o indicador sobre o Canal de Ética evidencia o não atendimento ao requisito 5.3.4, indicando a baixa adesão dos colaboradores em reportar questões de *compliance,* além de reportes sobre assuntos diversos, inadequados ao propósito do Canal. Foi relatada a existência de reportes feitos pessoalmente, mas que não são registrados e, consequentemente, não considerados no indicador. Ademais, apesar da existência dos indicadores, a baixa rastreabilidade entre riscos e ações realizadas (referida acima) dificulta a identificação dos KRIs (*key risk indicators*), que seriam de grande utilidade para a gestão de riscos da organização (GREEN, 2015).

Dois documentos de responsabilidade de Recursos Humanos são agregados ao SGC. O Modelo de Descrição de Cargos, que determina as competências necessárias para os cargos da empresa, atende parcialmente ao requisito 7.2.1, juntamente com a comprovação de competências recolhida dos colaboradores. O atendimento é parcial pois as competências foram definidas conforme as necessidades do SGQ, ou seja, não consideram os riscos e o desempenho de *compliance,* e não há procedimento padrão para a coleta das comprovações de competência. O Procedimento principal de Recursos Humanos atende parcialmente ao requisito 7.2.3,

definindo treinamentos necessários, avaliação de eficácia e condições para treinamento. O registro dos treinamentos realizados é feito no sistema de gestão de documentos da organização, o que atende parcialmente aos requisitos 7.2.3 e 7.5.

O Procedimento de Informação Documentada, desenvolvido pelo SGQ, contém diretrizes para a criação, atualização e controle da informação documentada, atendendo parcialmente ao requisito 7.5. O documento pode ser adaptado para que atenda também ao SGC, uma vez que o controle de documentos e registros está entre os requisitos integrados com maior frequência e grau (VITORELI; CARPINETTI, 2013), além de não serem necessárias grandes alterações. O SGC também atende à informação documentada requerida nos requisitos 7.2.3 e 7.4, e parcialmente nos requisitos 4.6 e 7.2.1. A informação documentada requerida nos requisitos 4.3, 4.5, 5.2, 6.2 e 8.4 não é atendida pela empresa.

Dois documentos de responsabilidade de Suprimentos contribuem para o atendimento parcial ao requisito 8.1. A Norma de Gestão de Fornecedores descreve o processo de homologação destes, servindo como controle do que é provido externamente com base em categorias da análise de riscos de Suprimentos. O Procedimento de Compras, por sua vez, determina que os fornecedores sejam avaliados periodicamente quanto ao serviço prestado; no entanto, não é monitorado o desempenho de *compliance*. Os quadros de avaliação, presentes nas obras, e as planilhas de avaliação de cada área, salvas no sistema de gestão de documentos, também atendem parcialmente ao requisito.

O Canal de Ética, disponibilizado para toda a organização e também para o público externo, no Site Institucional, atende totalmente ao requisito 8.3. O Canal permite o levantamento de preocupações de *compliance* (ver seção 2.4.1, alínea f) de forma anônima e o tratamento os relatos de forma confidencial, e sua existência é divulgada no Código de Ética e Conduta e nas comunicações de *compliance*. O Canal é fundamental para que os reportes de todos os níveis cheguem à Diretoria, como recomendado por Griffith (2016).

Por fim, no que diz respeito à integração de sistemas, é notável a quantidade de requisitos da NBR ISO 37301:2021 similares à NBR ISO 9001:2015 (conforme descrito no Método, seção 3.1). No entanto, pelas evidências encontradas, pode-se dizer que o SGC e o SGQ da empresa possuem um nível inicial de integração, essencialmente de documentação, conforme a classificação de Sampaio *et al.* (2016 *apud* VITORELI; CARPINETTI, 2013). Assim, observa-se o potencial de integração dos sistemas a ser explorado nas próximas etapas deste trabalho e, posteriormente, pela organização.

4.1.1 Oportunidades de melhoria

O Quadro 6 (A, B e C), a seguir, apresenta as tarefas elaboradas com base nos requisitos atendidos parcialmente ou não atendidos, sendo oportunidades de melhoria para o SGC. A coluna "#" à esquerda indica o número associado a cada tarefa; a numeração foi mantida ao longo de todo o trabalho, permitindo a rastreabilidade com essa identificação inicial. A coluna à direita indica se a tarefa se encaixa nos projetos em andamento do SGC, isto é, em elaboração ou ainda não implementados totalmente na empresa; as evidências são apresentadas abaixo.

Quadro 6A - Tarefas necessárias para atendimento aos requisitos

#	Item	Subitem	Tarefa	Em andamento?
1	4	4.1	definições da organização: porte e escala de complexidade e sustentabilidade	
2	4	4.1	entendimento do contexto: sistematizar informações + contexto ambiental, cultural e social	
3	4	4.2	revisar partes interessadas do SGC + definir requisitos específicos	
4	4	4.3	determinar escopo do SGC	
5	4	4.3	informação documentada do escopo do SGQ	
6	4	4.4	atender todos os requisitos	Sim
7	4	4.5	processo para sistematizar a identificação de obrigações	
8	4	4.5	processo para avaliar e implementar mudanças	
9	4	4.5	informação documentada das obrigações de *compliance*	
10	4	4.6	processo para avaliar riscos de *compliance* periodicamente	
11	4	4.6	informação documentada sobre processo de avaliação de riscos e ações	
12	5	5.1.1	evidenciar comprometimento da liderança	
13	5	5.1.1	revisar descrição de cargos considerando desempenho esperado de *compliance*	
14	5	5.1.2	inserir níveis da organização sem e-mail nas comunicações de *compliance*	
15	5	5.1.3	evidenciar apresentações periódicas ao CFO	
16	5	5.2	elaborar política de *compliance*	
17	5	5.2	informação documentada sobre política de *compliance*	
18	5	5.3.1	avaliação e supervisão da Diretoria por parte do Conselho de Administração	
19	5	5.3.1	alinhar metas e estratégias às obrigações de *compliance*	
20	5	5.3.1	integrar compliance na avaliação de desempenho	
21	5	5.3.2	avaliar desempenho do SGC e identificar necessidades de ação corretiva	
22	5	5.3.2	evidenciar análise crítica e definição do escopo feita anualmente	
23	5	5.3.2	alocar responsabilidades ao longo da organização	
24	5	5.3.2	evidenciar envolvimento do gerente de *compliance* nas tomadas de decisão	
25	5	5.3.3	integrar obrigações de *compliance* às áreas responsáveis	
26	5	5.3.3	evidenciar ações diárias de *compliance* dos gestores	

Quadro 6B - Tarefas necessárias para atendimento aos requisitos

#	Item	Subitem	Tarefa	Em andamento?
27	5	5.3.4	melhorar adesão ao canal de ética e registrar (ou eliminar) reporte informal	Sim
28	6	6.1	planejar ações atreladas à análise de riscos	
29	6	6.1	planejar integração e implementação de ações nos processos do SGC	
30	6	6.1	planejar criação de controles e testes de efetividade	
31	6	6.2	estabelecer requisitos de *compliance* com detalhamento necessário	
32	6	6.2	detalhar como objetivos de *compliance* serão alcançados	
33	6	6.2	informação documentada sobre objetivos de *compliance*	
34	6	6.3	estabelecer planejamento de mudanças	
35	7	7.1	determinar e prover sistemas de apoio necessários	
36	7	7.2.1	revisar descrição de cargos considerando desempenho esperado de *compliance*	
37	7	7.2.1	estabelecer processo para comprovação e aquisição de competências	
38	7	7.2.1	informação documentada sobre comprovação de competência	
39	7	7.2.2	incluir treinamento na política de *compliance* nas atividades obrigatórias	
40	7	7.2.2	implementar processo de medidas disciplinares	Sim
41	7	7.2.2	incluir *due dilligence* dos candidatos no processo de contratação	
42	7	7.2.2	integrar *compliance* na avaliação de desempenho	
43	7	7.2.3	considerar responsabilidades e riscos de *compliance* nos treinamentos	
44	7	7.2.3	incluir análise crítica no processo de treinamentos	
45	7	7.2.3	procedimento de conscientização e treinamento de terceiras partes	Sim
46	7	7.3	assegurar conscientização da política de *compliance* e da relação com os papéis individuais	
47	7	7.3	assegurar conscientização das contribuições para a eficácia do SGC	
48	7	7.3	assegurar conscientização das implicações de não *compliance*	Sim
49	7	7.3	assegurar conscientização das formas de levantamento de preocupações de *compliance*	Sim
50	7	7.4	inserir níveis da organização sem e-mail nas comunicações de *compliance*	
51	7	7.4	comunicar sobre obrigações e objetivos de *compliance*	
52	7	7.4	esclarecer "com quem" e "como" no plano de comunicações	
53	7	7.4	comunicar externamente sobre cultura, objetivos e obrigações de *compliance*	Sim
54	7	7.5	adequar procedimento para atender o sistema integrado	
55	7	7.5	elaborar informação documentada requerida em 4.6, 7.2.1, 4.3, 4.5, 5.2, 6.2, 8.4	
56	8	8.1	estabelecer critérios para os processos pertinentes	
57	8	8.1	implementar controles conforme os critérios	
58	8	8.1	controlar mudanças planejadas e analisar criticamente	
59	8	8.1	monitorar desempenho de *compliance* de terceiras partes	
60	8	8.2	estabelecer controles e testes para gerenciar obrigações e riscos de *compliance*	

Quadro 6C - Tarefas necessárias para atendimento aos requisitos

#	Item	Subitem	Tarefa	Em andamento?
61	8	8.4	estabelecer processo de investigação de relatos, de forma independente e sem conflito de interesses	Sim
62	8	8.4	realizar regularmente reportes sobre as investigações à Diretoria	Sim
63	8	8.4	informação documentada sobre investigações	Sim

Fonte: autora.

As tarefas 40, 48, 61, 62 e 63 são consideradas em andamento pela criação de um Comitê de Ética na empresa. O Regimento Interno do Comitê de Ética, que define a composição do comitê, com representantes das funções de *Compliance,* Recursos Humanos e Jurídico, bem como diretrizes para o processo de investigação de relatos, está atualmente em fase de aprovação. O Regimento inclui a realização de um relatório para cada tomada de decisão, como informação documentada das investigações, e estabelece reportes para a Diretoria e o Comitê de Auditoria, contemplando assim as tarefas 61, 62 e 63. Além disso, o Comitê de Ética, uma vez estabelecido, contribui para a implementação do processo de medidas disciplinares e, consequentemente, para a conscientização a respeito destas, o que envolve também as tarefas 40 e 48.

Contribuindo para o atendimento aos requisitos 5.3.4 e 7.3 (tarefas 27 e 49, respectivamente), há um treinamento no formato *e-learning*[5] sobre o Código de Ética e Conduta, que inclui orientação específica sobre o Canal de Ética. O treinamento foi lançado no mês de setembro, não sendo considerado na análise de lacunas, e possui prazo até dezembro para que 100% dos colaboradores sejam treinados. Um comunicado interativo, a ser lançado de forma conjunta, também contribui para o esclarecimento dos assuntos que devem ser relatados no Canal. Resta, para atendimento ao requisito, avaliar se essas ações, de fato, trarão melhor adesão dos colaboradores ao Canal de Ética.

Para conscientização e treinamento de terceiras partes (tarefa 45), conforme especifica o requisito 7.2.3, destaca-se o Código de Ética e Conduta para corretores associados à empresa, em fase de aprovação, bem como treinamentos realizados na LGPD (Lei Geral de Proteção de Dados Pessoais) para o mesmo público. Falta, porém, um procedimento para que conscientização e treinamento sejam sistematizados e periódicos. Está em fase de elaboração o novo Site Institucional da empresa, que contará com uma página destinada a *Compliance* para

[5] *E-Learning*: modalidade de ensino *online* que possibilita autoaprendizagem, com conteúdo apresentado de forma sistematizada, didática e interativa.

comunicação externa de questões pertinentes, contribuindo para atendimento ao requisito 7.4 (tarefa 53).

Todas as tarefas, inclusive as em andamento, seguiram para a fase de priorização, com exceção das tarefas 6 e 55. A primeira é considerada “em andamento” tendo em vista todas as evidências até aqui apresentadas, uma vez que requisito 4.4 consiste na existência de um Sistema de Gestão de *Compliance* que atenda todos os demais requisitos da NBR ISO 37301:2021; assim, seu atendimento ocorre em consequência ao atendimento destes, o que torna redundante sua inclusão na priorização. Já a tarefa 55 depende de outras tarefas (5, 9, 11, 17, 33, 38), não fazendo sentido sua priorização de forma isolada; ela foi mantida no quadro para enfatizar que o atendimento às outras também atende ao requisito 7.5.

4.2 PRIORIZAÇÃO

O Quadro 7 a seguir apresenta os riscos identificados e sua classificação; dentre os riscos de *compliance* já mapeados pela organização, foram aproveitados dois (CPL.1 e CPL.5) e elaborados outros cinco, sendo dois deles adaptados de riscos existentes (CPL.3 e CPL.4). Destacam-se quatro riscos classificados como operacionais, cuja gestão é essencial para maior resiliência organizacional (GREEN, 2015). Os riscos CPL.1 e CPL.2 foram classificados como de imagem por sua repercussão externa, e operacionais, pela interna; especialmente esta última se relaciona à resiliência organizacional, ressaltando a importância de um ambiente interno ético, transparente e confiável para que a atividade da empresa se sustente. O risco CPL.6 tem impacto semelhante no ambiente interno, enquanto o CPL.5 foi considerado operacional no sentido mais específico, por sua evidente repercussão nas atividades diárias reguladas por normas internas.

A associação entre tarefas e riscos, conforme descrito no Método (seção 3.2), consta no Quadro 8. Para ilustrar a elaboração deste quadro, consideremos a tarefa 1 (primeira linha): caso as “definições de porte e escala de complexidade e sustentabilidade da organização” não sejam realizadas, a principal consequência é a dificuldade de identificar seus riscos e obrigações de *compliance* relacionados, o que corresponde ao risco CPL.3 (Quadro 7); e assim por diante. A descrição das tarefas foi incluída novamente no Quadro 8 (A e B) para facilitar sua identificação.

Quadro 7 - Riscos de *compliance* identificados

Código	Risco	Tipo
CPL.1	Conduta não *compliant* [6] dos colaboradores	Imagem/Operacional
CPL.2	Conduta não *compliant* especificamente da Diretoria	Imagem/Operacional
CPL.3	Falha na identificação de riscos e obrigações de *compliance*	Regulatório
CPL.4	Falha na gestão de riscos e obrigações de *compliance*	Regulatório
CPL.5	Atividades executadas em desacordo com políticas, normas e procedimentos da organização	Regulatório/Operacional
CPL.6	Falha na identificação e tratamento de denúncias de não *compliance*	Regulatório/Operacional
CPL.7	Conduta não *compliant* de terceiros	Imagem

Fonte: autora.

Quadro 8A - Tarefas e riscos de *compliance* associados

#	Tarefa	Risco
1	definições da organização: porte e escala de complexidade e sustentabilidade	CPL.3
2	entendimento do contexto: sistematizar informações + contexto ambiental, cultural e social	CPL.3
3	revisar partes interessadas do SGC + definir requisitos específicos	CPL.3
4	determinar escopo do SGC	CPL.3
5	informação documentada do escopo do SGQ	CPL.3
7	processo para sistematizar a identificação de obrigações	CPL.3
8	processo para avaliar e implementar mudanças	CPL.4
9	informação documentada das obrigações de *compliance*	CPL.3
10	processo para avaliar riscos de compliance periodicamente	CPL.4
11	informação documentada sobre processo de avaliação de riscos e ações	CPL.4
12	evidenciar comprometimento da liderança	CPL.2
13	revisar descrição de cargos considerando desempenho esperado de compliance	CPL.5
14	inserir níveis da organização sem e-mail nas comunicações de compliance	CPL.1
15	evidenciar apresentações periódicas ao CFO	CPL.4
16	elaborar política de *compliance*	CPL.1
17	informação documentada sobre política de *compliance*	CPL.1
18	avaliação e supervisão da Diretoria por parte do Conselho de Administração	CPL.2
19	alinhar metas e estratégias às obrigações de *compliance*	CPL.4
20	integrar compliance na avaliação de desempenho	CPL.1
21	avaliar desempenho do SGC e identificar necessidades de ação corretiva	CPL.4
22	evidenciar análise crítica e definição do escopo feita anualmente	CPL.3
23	alocar responsabilidades ao longo da organização	CPL.1
24	evidenciar envolvimento do gerente de compliance nas tomadas de decisão	CPL.4
25	integrar obrigações de compliance às áreas responsáveis	CPL.4
26	evidenciar ações diárias de compliance dos gestores	CPL.1
27	melhorar adesão ao canal de ética e registrar (ou eliminar) reporte informal	CPL.6

[6] Conjugação do verbo equivalente a "não *compliance*" (ver seção 2.4.1, alínea b).

Quadro 8B - Tarefas e riscos de *compliance* associados

#	Tarefa	Risco
28	planejar ações atreladas à análise de riscos	CPL.4
29	planejar integração e implementação das ações nos processos do SGC	CPL.4
30	planejar criação de controles e testes de efetividade	CPL.4
31	estabelecer requisitos de compliance com detalhamento necessário	CPL.4
32	detalhar como objetivos de compliance serão alcançados	CPL.4
33	informação documentada sobre objetivos de *compliance*	CPL.4
34	estabelecer planejamento de mudanças	CPL.5
35	determinar e prover sistemas de apoio necessários	CPL.4
36	revisar descrição de cargos considerando desempenho esperado de compliance	CPL.5
37	estabelecer processo para comprovação e aquisição de competências	CPL.5
38	informação documentada sobre comprovação de competência	CPL.5
39	incluir treinamento na política de compliance nas atividades obrigatórias	CPL.1
40	implementar processo de medidas disciplinares	CPL.1
41	incluir *due dilligence* dos candidatos no processo de contratação	CPL.3
42	integrar compliance na avaliação de desempenho	CPL.1
43	considerar responsabilidades e riscos de compliance nos treinamentos	CPL.1
44	incluir análise crítica no processo de treinamentos	CPL.1
45	procedimento de conscientização e treinamento de terceiras partes	CPL.7
46	assegurar conscientização da política de compliance e da relação com os papéis individuais	CPL.1
47	assegurar conscientização das contribuições para a eficácia do SGC	CPL.5
48	assegurar conscientização das implicações de não compliance	CPL.1
49	assegurar conscientização das formas de levantamento de preocupações de *compliance*	CPL.6
50	inserir níveis da organização sem e-mail nas comunicações de compliance	CPL.1
51	comunicar sobre obrigações e objetivos de compliance	CPL.1
52	esclarecer "com quem" e "como" no plano de comunicações	CPL.1
53	comunicar externamente sobre cultura, objetivos e obrigações de compliance	CPL.4
54	adequar procedimento para atender o sistema integrado	CPL.5
56	estabelecer critérios para os processos pertinentes	CPL.5
57	implementar controles conforme os critérios	CPL.5
58	controlar mudanças planejadas e analisar criticamente	CPL.5
59	monitorar desempenho de compliance de terceiras partes	CPL.7
60	estabelecer controles e testes para gerenciar obrigações e riscos de compliance	CPL.4
61	estabelecer processo de investigação de relatos, de forma independente e sem conflito de interesses	CPL.6
62	realizar regularmente reportes sobre as investigações à Diretoria	CPL.6
63	informação documentada sobre investigações	CPL.6

Fonte: autora.

Algumas considerações adicionais devem ser feitas. Primeiro, a lista de riscos de *compliance* (Quadro 7) não é exaustiva; certamente há mais riscos, especialmente relacionados

ao Jurídico, Recursos Humanos e Tecnologia da Informação. No entanto, os sete riscos identificados estão de acordo com o escopo do trabalho, tendo sido definidos em conjunto com o gerente de *compliance*, que considerou suficientes para o agrupamento das tarefas levantadas. Outro ponto é que a análise de riscos feita anteriormente pela empresa considera riscos de cada área de forma geral, sem identificar riscos específicos de *compliance* em cada uma delas. É recomendável que a organização reveja sua análise de riscos em momento oportuno e realize nova priorização, se necessário, considerando outros fatores. Novamente, considera-se o que foi feito adequado ao escopo proposto.

As tarefas enquadradas no fator de redução de esforço, conforme descrito no Método (seção 3.2) são indicadas no Quadro 9 (para conferir o assunto de cada tarefa, vide Quadro 6).

Quadro 9 - Tarefas com fator de redução de esforço

Correlacionadas	Redundantes	Em andamento
1 e 2	5 e 55	27
4 e 5	9 e 55	40
7 e 9	11 e 55	45
8 e 34	17 e 55	48
10, 11, 28, 43 e 60	33 e 55	49
16, 17 e 46	38 e 55	53
23 e 25	13 e 36	61
27 e 49	14 e 50	62
28, 29, 30 e 60	20 e 42	63
32 e 33		
37 e 38		
40 e 48		
61, 62 e 63		

Fonte: autora.

O resultado da avaliação de riscos quanto ao seu impacto e probabilidade (conforme Quadros 1 e 2) é indicado na Matriz de Riscos a seguir (Figura 8). Para direcionar as ações de tratamento dos riscos, é preciso considerar as diferentes estratégias existentes (BERSSANETI; BOUER, 2018). Para os riscos da região vermelha, a estratégia adotada foi evitar (reduzir probabilidade); considerando o impacto destes, a melhor opção é impedir que se concretizem. Já para a região amarela, pode-se considerar ações tanto para evitar quanto para mitigar (reduzir impacto); a transferência do risco também é uma opção, e a empresa têm considerado essa possibilidade avaliando uma nova plataforma para o Canal de Ética (relacionado ao risco CPL.6), que conta com suporte terceirizado no tratamento de denúncias. Finalmente, para a região verde, é indicado também tomar ações para evitar o risco (CPL.3), pois apesar de

classificado como não urgente, está próximo da região amarela, não sendo recomendada a estratégia de aceitar.

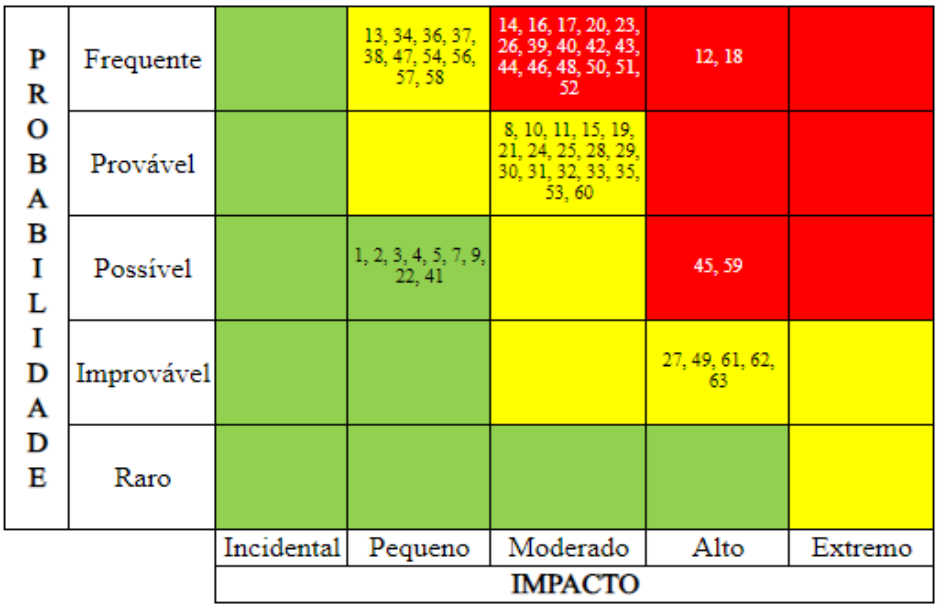
Figura 8 - Matriz de riscos de *compliance*

PROBABILIDADE						
	Frequente		CPL.5 - Ativ. exec. em desacordo com pol., normas e proc. da org.	CPL.1 - Conduta não compliant de colaboradores	CPL.2 - Conduta não compliant especificamente da Diretoria	
	Provável			CPL.4 - Falha na gestão de riscos e obrigações de compliance		
	Possível		CPL.3 - Falha na identificação de riscos e obrig. de compliance		CPL.7 - Conduta não compliant de terceiros	
	Improvável				CPL.6 - Falha na ident. e tratam. de denúncias de não compliance	
	Raro					
		Incidental	Pequeno	Moderado	Alto	Extremo
		IMPACTO				

Fonte: autora.

Para facilitar a visualização das tarefas associadas a cada risco, conforme a Quadro 8 (A e B), foi elaborada nova matriz de riscos, substituindo os riscos pela numeração das tarefas em si (Figura 9). Com isso, é possível observar a concentração de tarefas por região da matriz: 20 tarefas prioritárias, 32 como ponto de atenção e apenas 9 tarefas não urgentes. Dentre as 20 tarefas prioritárias (Figura 9), nota-se quatro tarefas redundantes: 14 e 50, e 20 e 42 (conforme Quadro 9); uma vez que a seleção de uma obrigatoriamente implica a seleção da outra, apenas uma de cada par (14 e 20) foram incluídas no último passo da priorização. Ordenando as 18 tarefas restantes conforme a nota de esforço, obteve-se a colocação apresentada no Quadro 10. Para que a análise completa fique disponível, seja para simples verificação ou para a continuidade do processo de melhoria pela organização, a classificação e as notas de esforço de cada tarefa (conforme Quadros 3 e 4) encontram-se no Apêndice B.

Figura 9 - Matriz de riscos com tarefas associadas



Fonte: autora.

Quadro 10 - Classificação pelo critério de Esforço

Ranking	**Tarefa**	**Esforço**	**Descrição**
1	14	5,2	inserir níveis da organização sem e-mail nas comunicações de compliance
2	20	5,2	integrar compliance na avaliação de desempenho
3	40	5,2	implementar processo de medidas disciplinares
4	48	5,2	assegurar conscientização das implicações de não *compliance*
5	26	5	evidenciar ações diárias de compliance dos gestores
6	52	5	esclarecer "com quem" e "como" no plano de comunicações
7	46	4,4	assegurar conscientização da política de compliance e da relação com os papéis individuais
8	39	4	incluir treinamento na política de compliance nas atividades obrigatórias
9	44	4	incluir análise crítica no processo de treinamentos
10	51	4	comunicar sobre obrigações e objetivos de *compliance*
11	23	3,3	alocar responsabilidades ao longo da organização
12	43	3,3	considerar responsabilidades e riscos de compliance nos treinamentos
13	12	3	evidenciar comprometimento da liderança
14	45	2,6	procedimento de conscientização e treinamento de terceiras partes
15	16	2,2	elaborar política de *compliance*
16	17	2,2	informação documentada sobre política de *compliance*
17	59	1	monitorar desempenho de compliance de terceiras partes
18	18	1	avaliação e supervisão da Diretoria por parte do Conselho de Administração

Fonte: autora.

As correlações (Quadro 9) indicam, no entanto, que a tarefa 46 depende de duas tarefas não priorizadas, 16 e 17, uma vez que a conscientização sobre a política de *compliance* requer a existência deste documento. A política de *compliance* é descrita no requisito 5.2 da NBR ISO 37301:2021 e trata-se de um documento central para o SGC. Nas reuniões com a equipe de *compliance*, também foi frisada a importância do documento, não somente para atendimento ao requisito, mas para a consolidação das informações concernentes ao *compliance* na organização. Além de evidenciar o comprometimento da empresa com o *compliance*, a política permite sistematizar os diversos documentos e processos já existentes, facilitando a compreensão, tanto da empresa quanto das demais partes interessadas, do que abrange o SGC. Tal sistematização segue a orientação para uso da NBR ISO 37301:2021, de que "não convém que a política de *compliance* seja um documento único, mas convém que ela seja apoiada por outros documentos, incluindo processos e políticas operacionais" (ABNT, 2021, p. 32).

Assim, apesar do resultado da priorização, considerou-se adequado adaptá-lo para o que poderia servir melhor à organização na situação atual; a decisão foi incluir as tarefas 16 e 17, substituindo a 9ª e 10ª posições (tarefas 44 e 51). A relação definitiva das tarefas que seguiram para desenvolvimento encontra-se no Quadro 11.

Quadro 11 - Tarefas priorizadas para elaboração

Tarefa	Descrição
14	inserir níveis da organização sem e-mail nas comunicações de *compliance*
20	integrar *compliance* na avaliação de desempenho
26	evidenciar ações diárias de *compliance* dos gestores
52	esclarecer "com quem" e "como" no plano de comunicações
40	implementar processo de medidas disciplinares
46	assegurar conscientização da política de *compliance* e da relação com os papéis individuais
48	assegurar conscientização das implicações de não *compliance*
39	incluir treinamento na política de *compliance* nas atividades obrigatórias
16	elaborar política de *compliance*
17	informação documentada sobre política de *compliance*

Fonte: autora.

A etapa de priorização tornou clara a importância de se estabelecer critérios e avaliar os riscos antes de tomar ações na organização. Tarefas destacadas como essenciais nas primeiras reuniões, e mesmo tarefas em andamento (conforme Quadro 2), acabaram não sendo priorizadas pelos critérios adotados, com exceção de duas (40 e 48), enquanto tarefas mais simples associadas a riscos prioritários puderam ser identificadas, permitindo melhor alocação de tempo

e esforço. Por outro lado, conforme a discussão acima sobre a Política de *Compliance*, destaca-se a relevância de considerar, junto à avaliação de riscos, aquilo que melhor se adequa ao momento em que está a organização.

4.3 DESENVOLVIMENTO

O Quadro 12 (A e B), a seguir, indica o item da NBR ISO 37301:2021 relacionado a cada tarefa e seu respectivo texto de referência. As tarefas 50 e 42, omitidas na classificação final (Quadro 11) foram incluídas novamente para que o texto correspondente também fosse considerado na elaboração. A Matriz RACI elaborada é apresentada na Figura 10; as subtarefas de responsabilidade da analista de *compliance* foram destacadas em itálico, indicando que estão fora do escopo deste trabalho. A inclusão de outros agentes na Matriz levou em conta o texto da NBR ISO 37301:2021 e ideias preliminares de solução.

Quadro 12A - Texto da NBR ISO 37301:2021 referente a cada tarefa

Tarefa	**Item**	**Texto da NBR ISO 37301:2021**
14	5.1.2	*A organização deve desenvolver, manter e promover uma cultura de compliance em todos os níveis dentro da organização.* (p. 8)
50	7.4	*A organização deve:* *considerar os aspectos de diversidade e de barreiras potenciais ao considerar suas necessidades de comunicação (...) reter informação documentada, como evidência da sua comunicação, conforme apropriado.* (p. 15-16)
20	5.3.1	*A alta direção deve (...) assegurar a integração do desempenho do compliance nas avaliações de desempenho do pessoal.* (p. 10)
42	7.2.2	*A organização deve implementar um processo que permita realizar uma análise crítica periódica das metas de desempenho, dos bônus por desempenho e de outros incentivos, para verificar se existem medidas apropriadas em vigor para prevenir o encorajamento ao não compliance.* (p. 14)
26	5.3.3	*A direção deve ser responsável pelo compliance dentro da sua área de responsabilidade:* *— cooperando e apoiando a função de compliance e encorajando o pessoal a fazer o mesmo;* *— assegurando que todo o pessoal dentro de seu controle esteja cumprindo os procedimentos, os processos, as políticas e as obrigações de compliance da organização; (...)* *— apoiando e atendendo as atividades de treinamento de compliance;* *— desenvolvendo a conscientização junto ao pessoal sobre as obrigações de compliance, e orientando-os a cumprir os requisitos de competência e treinamento;* *— encorajando seu pessoal a levantar preocupações de compliance e apoiando-os e impedindo de quaisquer formas de retaliação;* (p. 11-12)
52	7.4	*A organização deve determinar as comunicações internas e externas pertinentes para o sistema de gestão de compliance, incluindo: (...) c) com quem se comunicar; d) como se comunicar.* (p. 15)

Quadro 12B - Texto da NBR ISO 37301:2021 referente a cada tarefa

Tarefa	Item	Texto da NBR ISO 37301:2021
40	7.2.2	*Em relação a todo o seu pessoal, a organização deve desenvolver, estabelecer, implementar e manter processos: (...)* *c) ações disciplinares apropriadas devem ser tomadas contra o pessoal que viole os processos e os procedimentos e as políticas e as obrigações de compliance da organização* (p. 14)
48	7.3	*As pessoas que realizam trabalho sob o controle da organização devem estar conscientes: (...)* *— das implicações de estarem em não conformidade com os requisitos do sistema de gestão de compliance.* (p. 15)
46	7.3	*As pessoas que realizam trabalho sob o controle da organização devem estar conscientes: (...)* *— da política de compliance;* *— das suas contribuições para a eficácia do sistema de gestão de compliance, incluindo os benefícios da melhoria do desempenho de compliance;*(p. 15)
39	7.2.2	*Em relação a todo o seu pessoal, a organização deve desenvolver, estabelecer, implementar e manter processos: (...)* *b) que dentro de um período razoável do início da sua contratação, o pessoal receba uma cópia da política de compliance e treinamento em relação a essa política, ou tenha acesso a ela;*(p. 14)
16	5.2	*O Órgão Diretivo e a Alta Direção devem estabelecer uma política de compliance que:* *a) seja apropriada ao propósito da organização;* *b) proveja uma estrutura para estabelecer os objetivos de compliance;* *c) inclua um comprometimento para atender aos requisitos aplicáveis;* *d) inclua um comprometimento para a melhoria contínua do sistema de gestão de compliance.* *A política de compliance deve:* *— estar alinhada com os valores, os objetivos e a estratégia da organização;* *— requerer o compliance com as obrigações de compliance da organização;* *— apoiar os princípios de governança de compliance de acordo com 5.1.3;* *— fazer referência e descrever a função de compliance;* *— definir as consequências de estar em não compliance com os procedimentos, processos, políticas e obrigações de compliance da organização;* *— encorajar o levantamento de preocupações e proibir quaisquer formas de retaliação;* *— estar escrita em uma linguagem clara de modo que todo o pessoal possa entender facilmente os propósitos e princípios;* *— ser adequadamente implementada e aplicada (...)*(p. 9)
17	5.2	*A política de compliance deve: (...)* *— estar disponível como informação documentada;* *— ser comunicada dentro da organização;* *— estar disponível para as partes interessadas, conforme apropriado* (p. 9-10)

Fonte: autora.

Figura 10 - Matriz RACI

#	Tarefa	Subtarefa	Autora	Analista de compliance	Gerente de compliance	Gerentes do escritório	Gerentes de obra	Responsável de SSTMA	Diretoria
14	inserir níveis da organização sem e-mail nas comunicações de compliance	desenhar fluxograma	R	C	A		I	I	
		implementar mudanças		R	A		I	I	I
20	integrar compliance na avaliação de desempenho	desenhar fluxograma	R	C	C/A	I			I
26	evidenciar ações diárias de compliance dos gestores	especificar como serão evidenciadas	R	C	C/A	C			
		implementar e orientar gestores		R/A	I	I	I		I
52	esclarecer "com quem" e "como" no plano de comunicações	fazer alterações no documento	R	C/A	I			I	
40	implementar processo de medidas disciplinares	propor iniciativas conforme documento existente	R	C	C/A				
		implementar ações		R	A	I	I		
46	assegurar conscientização da política de compliance e da relação com os papéis individuais	desenhar fluxograma	R	C	A	I			
		implementar ações		R	R/A	I	I		
48	assegurar conscientização das implicações de não compliance	propor iniciativas conforme documento existente	R	C	C/A				
		implementar ações		R	A	I	I		
39	incluir treinamento na política de compliance nas atividades obrigatórias	desenhar fluxograma	R	C	A				
		implementar mudanças		R	A	I			
16	elaborar política de compliance	elaborar estrutura do documento	R	C	C/A				I
		redigir documento		R	A	I	I		I
17	informação documentada sobre política de compliance	especificiar disponibilização da informação documentada	R	C	A				I
		publicar documento		R	A	I	I		I

Fonte: autora

Os assuntos nos quais foram agrupadas as subtarefas (conforme descrito no Método, seção 3.3) são: 1. Comunicações de *compliance*; 2. *Compliance* na avaliação de desempenho; 3. Ações de *compliance* dos gestores; 4. Implicações do não *compliance*; e 5. Política de *compliance.* Um resumo das propostas consta no Quadro 13, e os resultados da elaboração são apresentados a seguir.

Quadro 13 - Resumo das propostas de melhoria

Assunto	Propostas
1. Comunicações de *Compliance*	1. Inclusão de SSTMA e GOs/GGOS no planejamento anual de comunicação 2. Inclusão do SSTMA e SGQ no processo mensal de comunicação 3. Inclusão de visita mensal de *compliance* nas obras 4. Alteração do plano de comunicações de *compliance* 5. Criação do plano de comunicações de obra
2. *Compliance* na avaliação de desempenho	6. Inclusão de metas de *compliance* nas metas individuais 7. Inclusão dos gestores na validação de metas 8. Inclusão de avaliação de conduta na avaliação de competências 9. Utilização do FMEA na análise crítica
3. Ações de *compliance* dos gestores	10. Criação de checklist para auxílio dos gestores 11. Realização de reunião periódica do *Compliance* com os gestores para conscientização e orientação 12. Aumento da função de *compliance* e revisão das tarefas operacionais 13. Criação de treinamentos interativos pelos gestores 14. Inclusão das responsabilidades de *compliance* na descrição de cargos dos gestores
4. Implicações de não *compliance*	15. Inclusão de avaliação periódica no Regimento do Comitê de Ética 16. Estabelecimento de prazo para avaliação da mudança de cultura 17. Inclusão de novos formatos de divulgação das medidas disciplinares 18. Inclusão de questionário de medidas disciplinares nas atividades obrigatórias 19. Inclusão do SGQ na avaliação de conscientização da obra
5. Política de *compliance*	20. Criação da política de *compliance* com base na estrutura elaborada 21. Inclusão dos gestores na criação da política 22. Inclusão da política de *compliance* na integração e nas atividades obrigatórias 23. Criação de treinamento interativo sobre a política de *compliance* 24. Inclusão de questões sobre a política de *compliance* na pesquisa de clima 25. Revisão da comunicação de obra após elaboração da política de *compliance* 26. Disponibilização da política de *compliance* em meio físico e digital 27. Revisão das partes interessadas para garantir seu acesso à política de *compliance*

Fonte: autora.

4.3.1 Comunicações de *compliance*

O primeiro assunto trata das tarefas 14 e 52. Atualmente, as comunicações são feitas somente por e-mail, não abrangendo todos os níveis da organização; os mestres de obra e os operários terceirizados, que não possuem e-mail corporativo, não recebem as comunicações, fazendo-se necessário envolvê-los efetivamente na cultura de *compliance.* Isso está alinhado à importância da comunicação efetiva acima e abaixo na organização, sendo a falta desta, por si só, fonte de risco (GREEN, 2015); neste caso, especialmente o risco de conduta não *compliant* dos colaboradores (conforme Quadro 8A).

A solução proposta é adicionar ao plano de comunicações de *compliance* existente um plano de comunicação para a obra. Tendo em vista que a duração média das obras é de dois anos e que os trabalhadores são rotativos (podendo estar na obra por todo o período, por meses ou apenas dias), o plano de comunicação da obra poderia ocorrer em ciclos mais curtos do que as comunicações por e-mail. Enquanto estas são distribuídas ao longo do ano, o recomendado para a obra seria uma distribuição cíclica trimestral (ou semestral); assim, por exemplo, a cada três meses, todos os assuntos necessários à obra seriam comunicados.

Duas ocasiões possíveis para as comunicações são o Diálogo Diário de Segurança (DDS) e o treinamento de Integração em Segurança do Trabalho, conforme a NR-18 (BRASIL, 1978). O DDS é uma conversa semanal da equipe de SSTMA, na qual são reforçados os assuntos de segurança do trabalho, com todos os trabalhadores da obra; estes podem compartilhar suas dificuldades, problemas e sugestões. Os treinamentos de Integração são obrigatórios para todos que entram na obra, sendo controlados rigorosamente pelas equipe de SSTMA e do SGQ.

Para levar as comunicações de *compliance* a essas ocasiões, contudo, é preciso repensar os assuntos e a forma de comunicação adotados, uma vez que o público e formato são outros. Os assuntos podem ser baseados no Código de Ética e Conduta da empresa, conforme aplicável para os trabalhadores terceiros e mestres de obra. Alguns exemplos são:

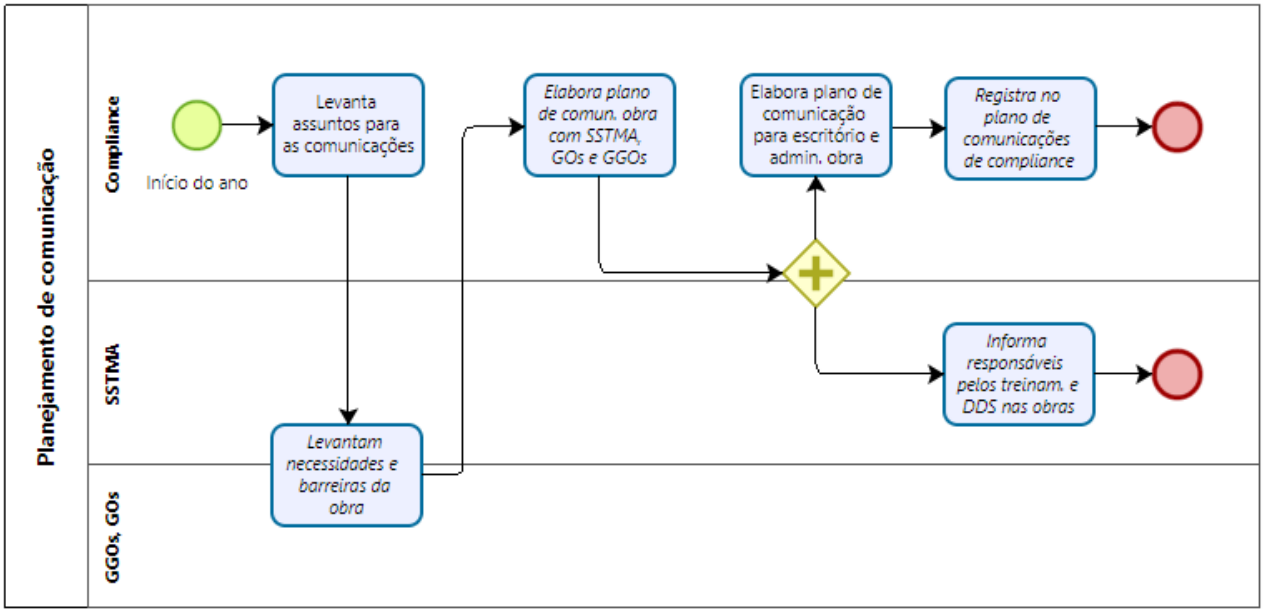
a) Definição de ética;
b) Relação de respeito entre os operários;
c) Uso adequado dos bens e recursos da empresa;
d) Implicações do não *compliance*;
e) Canal de Ética.

Destaca-se a importância de enfatizar, sobre o Canal de Ética, a possibilidade de acesso pelo telefone celular, uma vez que este público não possui acesso aos computadores

corporativos e há pouca conscientização sobre este item. O Canal é a principal forma de comunicação acima na organização (GREEN, 2015), podendo ser apoiada pelas visitas de *compliance* (descritas a seguir).

Os fluxogramas a seguir mostram a proposta para o planejamento anual da comunicação (Figura 11) e a realização da comunicação, em base mensal (Figura 12). Uma vez que a proposta envolve alterações em um processo existente, as atividades inseridas foram destacadas em itálico.

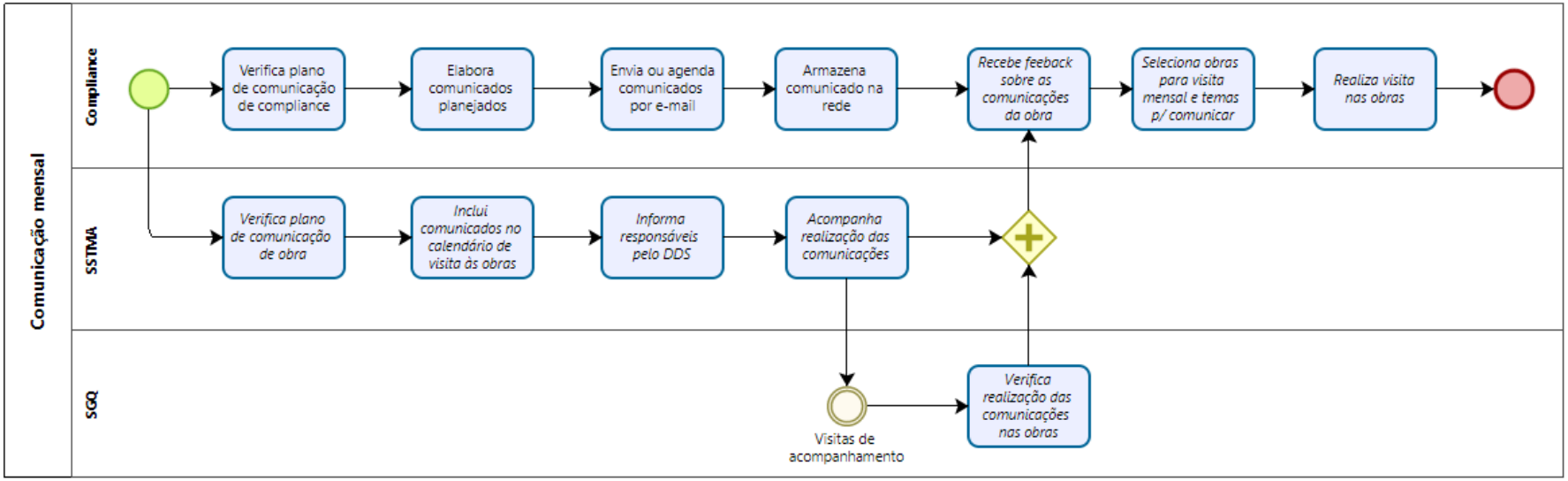
Figura 11 - Fluxograma: Planejamento de comunicação



Fonte: autora.

O planejamento de comunicações de *compliance* (Figura 11) já ocorre no início do ano, mas a proposta é que seja feito em conjunto com o SSTMA e os gerentes gerais de obra (GGOs) e/ou os gerentes de obra (GOs), para que necessidades e barreiras de comunicação existentes na obra sejam levantadas e consideradas no planejamento. No plano de comunicação de obra resultante deve constar tanto o plano trimestral a ser abordado no DDS, quanto o conteúdo de *compliance* a ser tratado no treinamento de Integração de Segurança do Trabalho; este último deve ser mais suscinto, focando em questões essenciais à cultura de *compliance*, deixando para o plano cíclico o maior aprofundamento dos temas. Vale notar que mesmo colaboradores da obra que possuem e-mail corporativo (como almoxarife, administrador, e ocasionalmente analistas e engenheiros) participam do DDS, podendo ser atingidos por essas comunicações, mas o foco deve estar nos mestres de obra e terceiros.

Figura 12 - Fluxograma: Comunicação mensal



Fonte: autora.

As comunicações de obra devem estar registradas no plano de comunicações de *compliance* como forma de informação documentada, e o programa com conteúdo do treinamento de Integração também pode ser armazenado na rede para este fim. Outras formas de informação documentada, como os e-mails armazenados na rede, não são adequadas aqui tendo em vista a comunicação realizada oralmente.

Na comunicação mensal (Figura 12), a função de *compliance* segue o que já tem feito em relação aos comunicados por e-mail: verifica o plano de comunicação, elabora os comunicados necessários, envia ou agenda os comunicados e armazena na rede como evidência. Os elementos novos são o recebimento de *feedback* tanto de SSTMA quanto do SGQ, e a visita de um representante de *compliance* nas obras. A inclusão de pequenas tarefas de *compliance* dentro do que o SGQ já realiza, eliminando a necessidade de criar novos processos, é um exemplo de melhoria no gerenciamento viabilizada pela integração de sistemas (VITORELI; CARPINETTI, 2013).

Um responsável do SSTMA deve verificar, mensalmente, o plano de comunicação de obra e incluir os temas pertinentes no calendário de visitas às obras; esse calendário já é feito atualmente, mas informa apenas a obra e o responsável pela visita. Com essa proposta, o técnico de SSTMA designado para conduzir o DDS em determinada obra saberá qual assunto de *compliance* deve tratar na visita. O responsável do SSTMA deve acompanhar a realização das comunicações e dar um *feedback* mensal para *Compliance.* Com relação ao SGQ, a área já realiza visitas de acompanhamento para orientar as obras e verificar o atendimento aos requisitos da NBR ISO 9001:2015. A proposta é que seja incluída nessas visitas uma verificação acerca das comunicações de *compliance* (por meio de conversas e perguntas aos terceiros, por exemplo), a fim de que o SGQ possa fornecer o devido *feedback* para *Compliance.*

A visita de um representante de *compliance* nas obras parte de uma necessidade identificada pela própria equipe*;* mesmo com o assunto de *compliance* sendo tratado por técnicos de SSTMA, por exemplo, considera-se importante a presença da função de *compliance* nas obras, ainda que pontualmente, visando transmitir confiança e proximidade aos colaboradores e terceiros. No entanto, considerando o volume de tarefas da função (mais detalhes na seção 4.3.3) e o provável aumento no número de canteiros de obra da empresa no próximo ano, tal visita deve ser planejada dentro do contexto de comunicações de *compliance*, e não feita de forma isolada ou "quando possível". A proposta é que, partindo do *feedback* vindo do SSTMA e do SGQ, a função de *compliance* escolha mensalmente algumas obras, numa quantidade possível de ser mantida todos os meses, para serem visitadas, bem como temas a ser

comunicados. É importante variar as obras ao longo dos meses para que todos tenham contato com a função de *compliance* de alguma forma. A ocorrência dessas visitas também pode ser comunicada em outras obras pelo SSTMA, enquanto não são visitadas, reforçando o comprometimento da função e a importância do *compliance* em todos os níveis da organização

Além disso, o plano de comunicações deve indicar "com quem" e "como" cada assunto deve ser comunicado (Quadro 12A, tarefa 52). O plano de comunicações de *compliance* existente consiste em um calendário com indicações de cada assunto e a data de sua comunicação; uma vez que todos os comunicados são feitos por e-mail, tem-se o "como" e, portanto, o "com quem" são todos os colaboradores que possuem e-mail corporativo. Contudo, com as alterações descritas acima, é necessária nova especificação.

A solução proposta é adicionar uma nova guia ao arquivo do plano de comunicações de *compliance* (planilha em Microsoft Excel®) com o plano de comunicações de obra. A guia principal (Figura 13) deve conter a especificação dos destinatários (no caso, todas as áreas do escritório, engenheiros de obra, administradores de obra e almoxarifes) e indicar o e-mail corporativo como forma de comunicação.

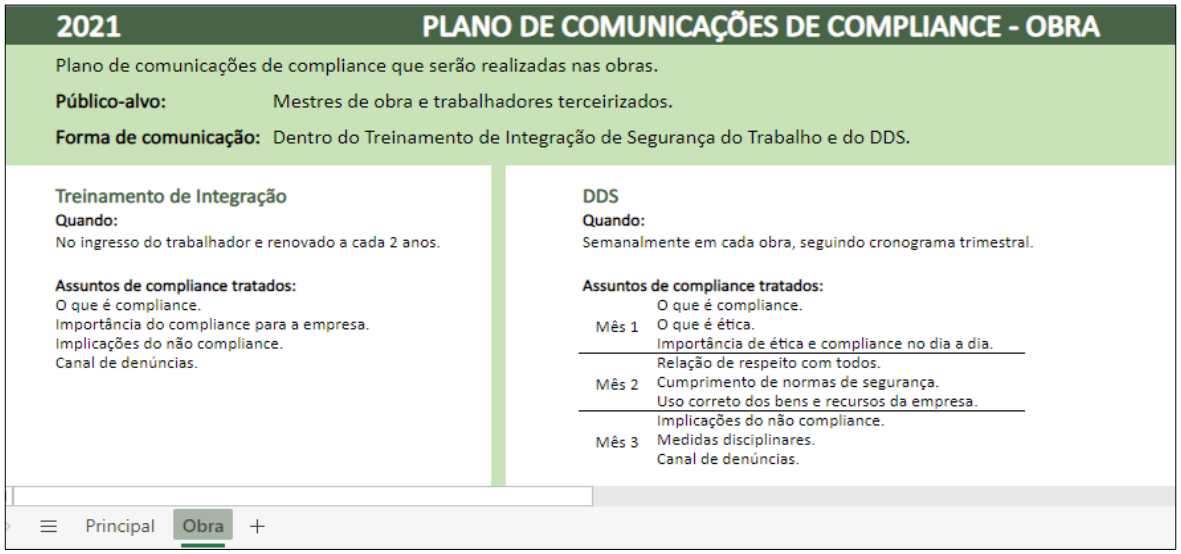
Figura 13 - Exemplo de Plano de comunicações de *compliance*: Guia Principal

Fonte: autora.

A segunda guia (Figura 14), relativa à obra, deve conter a especificação de quem será atingido pelas comunicações de obra (no caso, mestres de obra e terceiros) e como serão realizadas (por exemplo, no DDS e no Treinamento de Integração, e mais detalhes conforme necessário). O plano de comunicações de obra deve indicar claramente "o que" e "quando" cada assunto será comunicado, requisito da NBR ISO 37301:2021 já atendido no plano de comunicações de *compliance* atual. Uma possível melhoria, ainda, é incluir na planilha, ou em

documento relacionado, maiores detalhes sobre os comunicados (conteúdo tratado, relação com objetivos e obrigações de *compliance,* conteúdo interativo utilizado etc.).

Figura 14 - Exemplo de Plano de comunicações de *compliance*: Guia Obra



Fonte: autora.

4.3.2 *Compliance* na avaliação de desempenho

A integração do *Compliance* na avaliação de desempenho é assunto da tarefa 20. Atualmente, a avaliação de desempenho tem como principais atores a área de Recursos Humanos, os gestores de toda a empresa e o Comitê de metas. Este é formado por seis pessoas, das áreas de RH, Jurídico, Engenharia e *Compliance*, e realiza a validação das metas individuais definidas por todos os colaboradores; o principal responsável pela revisão e validação é o gerente de *compliance.* Tal validação consiste na verificação de critérios definidos, como peso adequado entre as metas e se as estas são objetivas, isto é, passíveis de medição e comprovação documental ou numérica. As metas são definidas após a orientação do RH sobre as metas da empresa como um todo, devendo estar alinhadas a elas.

A ação dos gestores está ligada especialmente ao *feedback* contínuo e à avaliação de competência de cada membro do seu time, baseada nos valores da organização; esta avaliação e o atendimento às metas individuais compõem a nota de desempenho do colaborador. Pode-se afirmar que o papel dos gestores no processo contribui para que a medição de desempenho não seja uma barreira ao orgulho do trabalho, como indica o princípio 12 de Deming (1986); uma vez que os gestores participam da construção das metas e fornecem *feedback* continuamente, as metas não focam apenas no resultado final, mas visam atingir a qualidade.

Nas reuniões realizadas com o gerente e a analista de *compliance*, ficou evidente a falta: de metas específicas de *compliance*; de uma análise crítica de *compliance*, para que o desempenho seja avaliado de forma integrada; de medidas para prevenir o encorajamento ao não *compliance*; e de uma maior participação dos gestores na validação de metas, como auxílio ao Comitê de metas e especialmente à função de *compliance*. A governança de incentivos, voltada para a gestão de riscos, e o papel dos gestores na elaboração de metas são aspectos relacionados à construção de uma cultura de risco (GREEN, 2015), sendo especialmente importantes ao SGC.

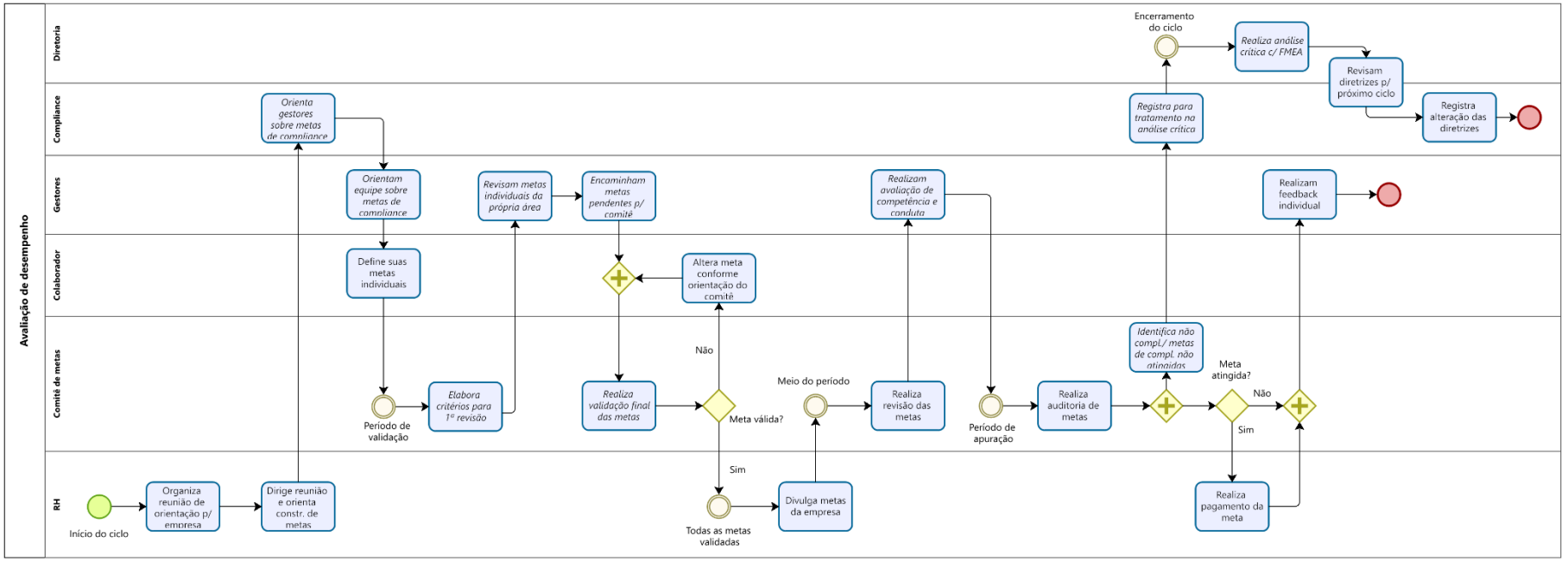
A proposta de solução é indicada no fluxograma a seguir (Figura 15); novamente, os itens incluídos no processo existente foram destacados em itálico. No início do ciclo anual de metas, o RH organiza e dirige uma reunião de abertura com todos os colaboradores, orientando sobre a construção das metas e informando como serão avaliadas. A primeira proposta é que, na mesma reunião, a função de *compliance* oriente os gestores sobre a necessidade de metas específicas de *compliance,* como:

a) Participação total do time nos treinamentos de *compliance;*
b) 100% das compras da área realizadas conforme procedimento interno;
c) Leitura e engajamento em todas as comunicações de *compliance* por e-mail.

Da mesma forma que as metas individuais devem contribuir para o atendimento às metas da empresa, é recomendável que a Diretoria e o Conselho de Administração estabeleçam metas de *compliance* para toda a organização, e estas sejam informadas na reunião de abertura. As metas individuais de *compliance* devem também atender às necessidades de cada área; os gestores são responsáveis por repassar e reforçar essa orientação para suas equipes, bem como definir metas de *compliance* para a área como um todo.

A segunda alteração proposta também envolve os gestores, e consiste na delegação de parte da validação das metas individuais. Hoje, já acontece uma validação prévia dos gestores, mas não é formalizada; o Comitê continua conferindo 100% das metas individuais para validação. A proposta é que o Comitê elabore critérios objetivos para que os gestores façam uma primeira revisão das metas da sua área, e então encaminhem ao Comitê apenas os casos não abordados pelos critérios, exigindo análise mais detalhada para validação; no caso de áreas com muitos colaboradores, outros cargos, como coordenadores e analistas sêniores, podem auxiliar os gestores. O Quadro 14, abaixo, indica exemplos de critérios objetivos para a primeira revisão e casos a ser tratados pelo Comitê.

Figura 15 - Fluxograma: Avaliação de desempenho



Fonte: autora.

Quadro 14 - Exemplo de critérios para validação de metas

Primeira revisão	**Comitê de metas**
A quantidade de metas é adequada? (ex.: 3 a 5)	As metas são atingíveis? (financeiramente, dentro do prazo, considerando histórico etc.)
O peso de cada meta é adequado? (ex.: de 10% a 30%)	As metas são desafiadoras? (nem fáceis demais, nem difíceis demais)
Foi incluída a meta de *compliance* da área?	A metas estão alinhadas à meta geral da empresa?
A meta é objetiva? (cumprimento pode ser evidenciado)	É possível identificar alguma forma de encorajamento ao não *compliance*?
A meta está descrita de forma completa? (ex.: o que, como, quando etc.)	

Fonte: autora.

As metas com pendências devem ser revisadas pelo colaborador e, então, validadas pelo Comitê após as devidas correções. Uma vez validadas todas as metas, estas são divulgadas pelo RH. Na metade do ciclo, é feita uma revisão das metas para acompanhar seu andamento e os gestores realizam a avaliação de competência de cada membro. Atualmente, a avaliação consiste em uma régua que vai de "não atende às expectativas" até "excede significativamente as expectativas", comparando o comportamento do colaborador à cultura da empresa, resumida em sete valores. A terceira alteração proposta é que uma avaliação de conduta seja associada mais intencionalmente à avaliação de comportamento, como outra forma de integrar o *compliance* na avaliação de desempenho. A "ética" como um dos sete valores considerados na avaliação é o mais próximo de uma avaliação de conduta hoje. Recomenda-se que o RH enfatize, na orientação aos gestores sobre essa avaliação, o Código de Ética e Conduta e, posteriormente, a Política de *Compliance* (ver seção 4.3.5), para uma diretriz objetiva do que se deve considerar ao avaliar o comportamento "ético" do colaborador.

Terminado o período para cumprimento das metas, ocorre a auditoria de metas para apuração das evidências. Já ocorre uma análise crítica do desempenho por parte da Diretoria ao final do período, mas a proposta de alteração é que seja adotada a ferramenta FMEA, especialmente como auxílio à elaboração de medidas para prevenir o encorajamento ao não *compliance*. Sendo uma ferramenta de avaliação de riscos, porém mais detalhada que a Matriz de Riscos, ela pode agregar à análise crítica não apenas um olhar sobre o não *compliance* do período analisado, mas sobre o potencial não *compliance*, conduzindo à elaboração de medidas de prevenção e detecção. O FMEA permite ainda considerar, na própria elaboração de metas e

determinação de incentivos, os riscos associados, como recomenda Green (2015). Um guia para a utilização do FMEA para este fim consta no Apêndice B. Este material pode ser adaptado pela empresa e aplicado a diferentes situações; para o SGQ, por exemplo, a ferramenta é de grande valia, tendo em vista a ênfase na mentalidade de risco por parte da NBR ISO 9001:2015, bem como a exigência de ações para abordar riscos e oportunidades (ABNT, 2015, item 6.1).

Como entrada para a análise crítica, é proposto que o Comitê de metas forneça informações pertinentes à função de *compliance* – especialmente ocorrências de não *compliance* relacionadas às metas e metas de *compliance* não atingidas – para que esta leve as informações à Diretoria. Como resultado desta, as diretrizes para o próximo ciclo devem ser revistas e as alterações necessárias, registradas.

4.3.3 Ações de *compliance* dos gestores

Em relação ao terceiro assunto, referente à tarefa 26, as entrevistas realizadas (conforme indicado no Método, seção 3.3) comprovaram a responsabilidade de *compliance* dos gestores dentro de suas respectivas áreas (Quadro 12A, tarefa 26); a forma como exercem essa responsabilidade, no entanto, varia. No Jurídico, por exemplo, o alinhamento com a função de *Compliance* é intenso, não somente na realização dos treinamentos requeridos e uso do Canal de Ética, mas também na cooperação em atividades diárias, como adequação de normas e contratos e apoio à resolução de conflitos internos. As demais gerentes entrevistadas, por sua vez, mostram reconhecer a importância do *compliance* para a empresa e para suas áreas de responsabilidade, mas a relação é mais de dependência da função de *compliance* do que de apoio a ela; em reunião posterior com a analista de *compliance*, destacou-se que essa dependência é a realidade da maior parte das áreas. Isso não significa que as áreas não estejam em *compliance*; pelo contrário, as gerentes se mostraram atuantes no incentivo à realização de treinamentos, cumprimento de normas internas e utilização do Canal de Ética quando necessário. No entanto, a função de *compliance* tem sido associada a atividades fora de seu escopo.

A causa mais evidente para isso, identificada nas entrevistas e reuniões, está relacionada à atuação do gerente de *compliance*. De forma geral, tudo que existe de *compliance* na organização hoje foi por sua iniciativa nos últimos quatro anos, com maior ênfase em consolidação de processos no último ano. Com isso, observa-se nos gestores, de forma geral, uma associação intensa entre o *compliance* e a pessoa do gerente da função. Se de um lado é positivo que as áreas saibam a quem recorrer, de outro há uma busca por ajuda na função de

compliance sobre assuntos não relacionados, como atividades rotineiras de cada área. Tendo em vista, ainda, a pequena equipe de *compliance* e o aumento da organização e da complexidade de seus processos, tal dependência mostra-se insustentável a médio (e até curto) prazo, sendo incompatível com a resiliência organizacional (GREEN, 2015). Vale ressaltar o papel positivo que a liderança já tem exercido na empresa de forma geral, conforme o princípio 7 de Deming (1986); as questões identificadas, no entanto, têm como objetivo a melhoria contínua do sistema, como indica o princípio 5 (DEMING, 1986).

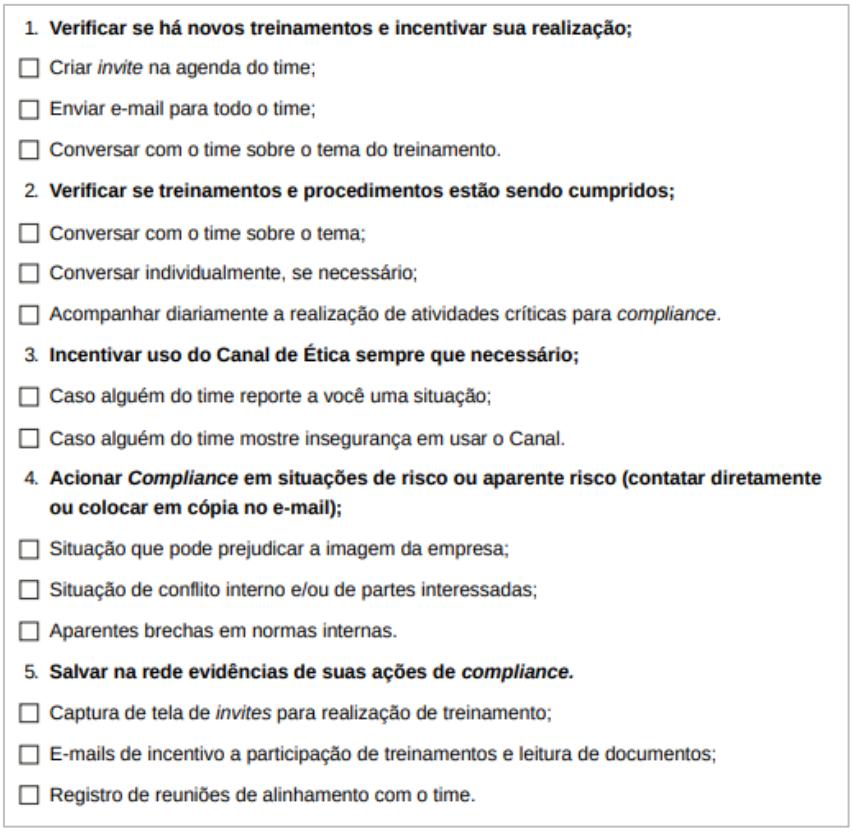
É fundamental esclarecer aos gestores, e a toda a organização, o papel específico da função de *compliance*. De forma mais restrita, o papel consiste em ajustar a empresa às restrições aplicáveis e lidar com riscos de reputação perante a sociedade; de forma mais abrangente, pode incluir também questões de privacidade, risco estratégico e continuidade do negócio (GRIFFITH, 2016). De qualquer forma, recomenda-se adotar uma definição operacional para o *Compliance*, garantindo que seu papel seja claro e reconhecido por todas as áreas (DEMING, 1986).

Dito isso, a tarefa prevista (Quadro 11, tarefa 26) foi ampliada para abordar também propostas de solução sobre o problema descrito acima e outras sugestões, levantadas pelos gestores entrevistados. Iniciando pela tarefa em si, a proposta é a elaboração de um *checklist* semanal para os gestores, auxiliando suas atividades rotineiras relacionadas ao *compliance*, conforme o exemplo na Figura 16. O documento não foi elaborado em detalhes pois recomenda-se fortemente que seja enriquecido com relatos e necessidades dos demais gestores que não foram entrevistados; contudo, considera-se proveitosa a inclusão dos itens dados como exemplo (Figura 16). Tanto o *checklist* preenchido quanto as evidências armazenadas na rede (item 5 da Figura 16) servem ao propósito de evidenciar as ações em andamento.

As demais propostas de melhoria são descritas a seguir, porém seu desenvolvimento em maiores detalhes está fora do escopo deste trabalho, não só pelo tempo disponível, mas pela necessidade de envolver outros membros da organização. A primeira proposta, levantada por um dos entrevistados, é a realização de uma reunião mensal (ou bimestral) da função de *compliance* com os gestores, visando conhecer suas necessidades e direcionar esforços para que possam apoiar e ser apoiados na manutenção do *compliance* em suas áreas. É importante que a reunião seja direcionada pelo papel de *compliance*, descrito acima, contribuindo para a conscientização dos gestores quanto a isso. A título de exemplo, atualmente há uma reunião de *Compliance* com Suprimentos diretos que ocorre de forma quinzenal; ainda que seja de grande auxílio a esta área, a reunião não tem foco em assuntos de *compliance*, mas em questões do dia a dia da área, ou seja, fora do escopo da função de *compliance*, favorecendo sua sobrecarga,

como mencionado. A reunião proposta, por sua vez, visa orientar sobre questões específicas de *compliance* em cada uma das áreas. Relacionamento com cliente, por exemplo, precisa de mais ajuda de *Compliance* com questões de LGPD, reclamações de clientes; Controladoria, por sua vez, com questões de reembolso, compras fora da norma interna, e assim por diante. Assim, a reunião conduzirá à maior autonomia dos gestores, além de contribuir para o *compliance* de toda a organização.

Figura 16 - Exemplo de *checklist*: Ações de *compliance* dos gestores



Fonte: autora.

A segunda proposta de melhoria é que se considere aumentar a função de *compliance*; sendo uma empresa de capital aberto e em processo de adequação ao ESG, as exigências sobre *Compliance*, que já são altas, tendem apenas a aumentar. Bons procedimentos não são suficientes se não há um time adequado para as tarefas de *compliance*, como aponta Griffith (2016). Essa proposta considera especialmente a atual sobrecarga, observada na convivência diária e nas reuniões realizadas, tanto do gerente quanto da analista, não apenas com o apoio às áreas, mas especialmente com as atividades da operação de *compliance.* A revisão das tarefas operacionais pode ocorrer paralelamente à ampliação da equipe; da mesma forma que os gestores devem ser conscientizados sobre o papel de *compliance*, as tarefas realizadas pela

função de *compliance* devem estar de acordo, disponibilizando o tempo necessário para que esta possa operar efetivamente o SGC (ABNT, 2021). A título de exemplo, consideremos a tarefa operacional de assinatura de contratos, que hoje toma a maior parte do tempo da analista de *compliance*. Ainda que os contratos sejam lidos e assinados por outras partes previamente, a função de *compliance* verifica tudo novamente antes de assiná-los, para garantir que não há erros. Trata-se de uma forma de inspeção em massa, indo de encontro ao princípio 3 de Deming (1986); essa forma de inspeção reconhece a incapacidade do processo, sendo necessário construir qualidade no produto (no caso, os contratos como produto interno). Está em discussão na empresa a criação de uma área de auditoria interna, mas, enquanto não ocorre, a função de *compliance* pode, por exemplo, realizar uma inspeção por amostragem dos contratos e, paralelamente, tratar com as demais partes responsáveis pelas assinaturas os erros mais frequentes.

Outro ponto levantado nas entrevistas foi em relação à forma dos treinamentos atuais. Alguns treinamentos são interativos ou em vídeo, mas a maior parte deles consiste na leitura dos documentos da empresa, como o Código de Ética e Conduta e diversos procedimentos e normas de outras áreas. O SGQ define, conforme a área de cada colaborador, o que deve ser lido; após a leitura, o colaborador registra no sistema a realização do treinamento, que deve ser renovada anualmente. Com isso, os gestores podem incentivar a leitura, mas é difícil verificar sua realização (além, é claro, da observação do comportamento diário do seu time). A proposta de melhoria é o envolvimento dos próprios gestores na elaboração de treinamentos mais dinâmicos e interativos, em formato de vídeo ou *e-learning;* o SGQ pode ficar responsável pelo apoio e orientação de forma geral, como já acontece na elaboração e revisão de documentos, mas a responsabilidade principal seria de cada área para desenvolver esse treinamento sobre seus procedimentos principais. Dado que esse processo tomaria algum tempo, podem ser realizadas ações simples no curto prazo, como:

a) Incluir um resumo ilustrativo no início de cada documento (como a Figura 17, seção 4.3.4), facilitando o entendimento e engajamento do leitor;
b) Relacionar documentos nos diagramas de processos[7], facilitando ao leitor identificar onde o procedimento se encaixa no processo da empresa e qual sua importância.

Uma última recomendação, que vai além do requisito, mas que é contemplada como sugestão nas orientações de uso da NBR ISO 37301:2021, é que “as suas respectivas responsabilidades [dos gestores] estejam claramente definidas e incluídas nas descrições de

[7] Diagrama de processos: documento que informa as entradas, saídas e principais interações de cada área com o restante da empresa.

suas funções" (ABNT, 2021, p. 34). A revisão da descrição de cargos existente, não só dos gestores, mas de todos os cargos da organização, é assunto da tarefa 13 (Quadro 2); esta ficou fora da priorização com os critérios adotados, mas a inclusão das responsabilidades de *compliance* dos gestores pode ser considerada prioritária em relação aos demais cargos. Assim, recomenda-se que essa ação seja tomada em conjunto com a solução de *checklist* proposta acima.

4.3.4 Implicações do não *compliance*

A conscientização das implicações do não *compliance* e a implementação do processo de medidas disciplinares estão profundamente relacionados (tarefas 40 e 48). A falta de conscientização na empresa resulta, entre outros fatores, de um processo de medidas disciplinares documentado e existente, mas pouco aplicado; isso vai ao encontro do que escreveu Deming (1986) sobre como a violação de regulações destrói a consciência pública, e como autoridades não devem impor obrigações se não puderem fazer cumpri-las. O que se observa na organização é uma cultura de "tentar outra solução", por vezes mais branda do que o requerido no procedimento, mesmo por parte dos níveis mais altos da gestão. A conscientização existente se baseia na leitura do procedimento de medidas disciplinares e no *e-learning* sobre o Código de Ética e Conduta, que aborda o assunto de forma suscinta. Há também o Comitê de Ética, com Regimento Interno em fase de aprovação (vide seção 4.1), que contribui para essa questão da cultura, além de garantir uma segunda avaliação dos relatos, que hoje é feita apenas por *Compliance.*

O procedimento citado evidencia que há um processo desenvolvido e estabelecido acerca de ações disciplinares a serem tomadas, enquanto o Comitê de Ética visa garantir que este seja implementado, com diretrizes para investigação de relatos e informação documentada. Seguindo o que é requerido pela NBR ISO 37301:2021 (Quadro 12B, tarefa 40), resta assegurar que o processo seja mantido.

A proposta de solução é que o processo de medidas disciplinares e o próprio Comitê de Ética sejam submetidos a avaliação periódica, podendo esta ser realizada junto da análise crítica do SGQ pela Diretoria, que ocorre anualmente; isso vai na direção do que apontam Vitoreli e Carpinetti (2013) sobre a análise crítica como um dos requisitos integrados com maior frequência e grau. Recomenda-se que a necessidade dessa avaliação, bem como diretrizes para ela, seja incluída no Regimento do Comitê. Nota-se que a análise crítica é um aspecto da melhoria contínua, assunto do item 9 da NBR ISO 37301:2021 (ABNT, 2021, p. 20-21), fora

do escopo deste trabalho. Ainda assim, está fortemente relacionada à manutenção do processo; mesmo que a empresa não adote, a princípio, a análise crítica de todo o SGC, é benéfico que especialmente esse processo seja analisado.

Outra proposta é que seja estabelecido um prazo para a mudança de cultura, isto é, para se avaliar a eficácia do Comitê de Ética e verificar se foi suficiente para a implementação do processo ou se são necessárias novas medidas. Essa avaliação pode considerar, entre outras questões:

a) Quantidade de denúncias no Canal de Ética no período;
b) Relação entre denúncias e medidas disciplinares efetivamente aplicadas;
c) Conscientização dos colaboradores sobre as medidas disciplinares.

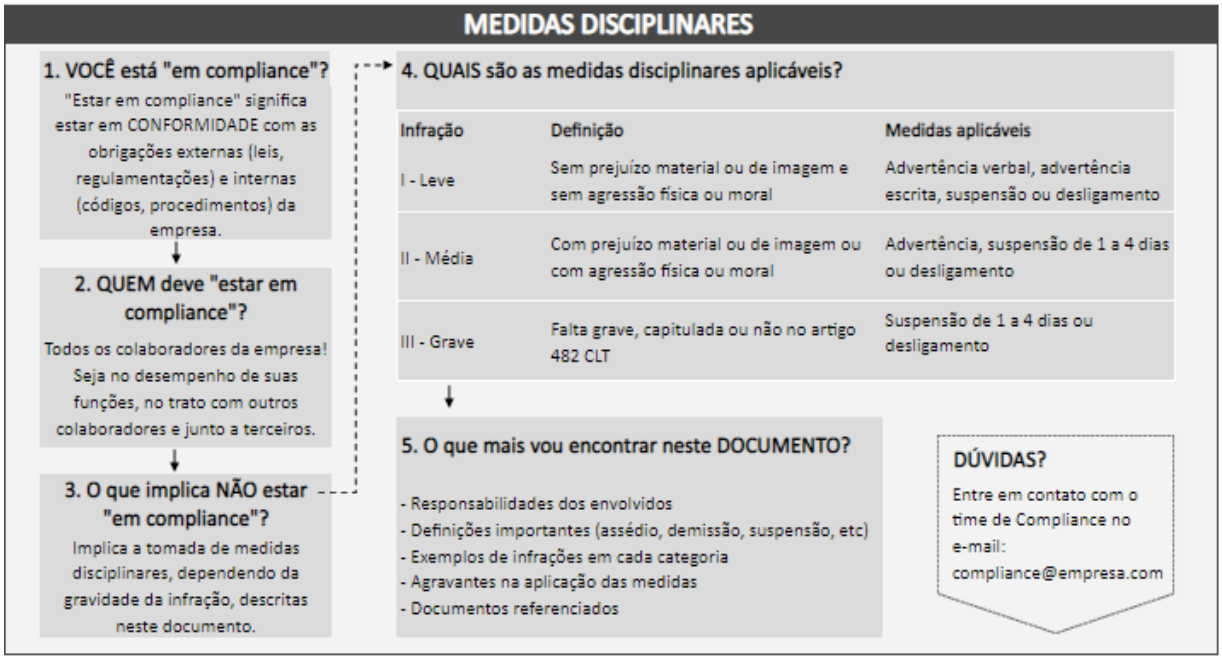
A conscientização sobre as implicações do não *compliance*, em especial, também é requisito da NBR ISO 37301:2021 (Quadro 12B, tarefa 48). Como apontado acima, espera-se que a implementação do processo de medidas disciplinares pelo Comitê de Ética contribua para a maior conscientização, além da política e do *e-learning* disponibilizados. Nas reuniões realizadas com o time de *compliance*, ficou claro que o principal problema da implementação é a cultura que ainda não assimilou a necessidade de aplicação das medidas; não se deve, por exemplo, à rigidez das medidas, o que poderia levar a uma revisão do documento. A NBR ISO 37301:2021 exige, ainda, a conscientização de todas as "pessoas que realizam trabalho sob o controle da organização" (ABNT, 2021, p. 15), o que não é atendido hoje especialmente nos níveis da empresa sem e-mail corporativo (vide seção 4.3.1). Assim, a proposta de solução é melhorar a conscientização em sua eficácia e em sua abrangência.

No que diz respeito à eficácia, a proposta é mudar a forma de divulgação do processo de medidas disciplinares e das medidas em si. Atualmente, trata-se de um documento de dez páginas disponibilizado no sistema de gestão de documentos da empresa, e sua leitura é exigida junto a diversos outros documentos (a dificuldade em relação aos treinamentos de forma geral foi tratada na seção 4.3.3). Para que a leitura se torne mais atrativa e didática, as implicações do não *compliance* poderiam ser disponibilizadas em outros formatos, como:

a) Quadro-resumo do processo e das diferentes medidas disciplinares aplicáveis;
b) Vídeo de treinamento (como já existe tratando do tema de conflito de interesses);
c) Comunicações específicas por e-mail.

Com base na política citada, foi elaborado um modelo de quadro-resumo, apresentado na Figura 17, a seguir.

Figura 17 - Exemplo de quadro-resumo da política de Medidas Disciplinares



Fonte: autora.

Este pode ser colocado na primeira página do documento, como uma visão geral, além de ser utilizado em treinamentos e nas comunicações por e-mail. Esse tipo de comunicação deve ser mais curto, visando lembrar os colaboradores das medidas e encorajá-los a permanecer em *compliance*. Alguns títulos para as comunicações poderiam ser:

a) “Você está em *compliance*?”;
b) “O que é uma infração leve/média/grave?”;
c) “Definições importantes: assédio moral e sexual”;
d) “Presenciei uma ação de não *compliance*, e agora?”;
e) “Conheça algumas obrigações da empresa e saiba como ajudar a cumpri-las!”.

A abrangência da conscientização, por sua vez, está relacionada às pessoas sem acesso ao e-mail e aos sistemas corporativos (mestres de obra e terceiros). Para estes, faz-se necessário ainda outro esforço de conscientização, como a proposta de comunicação na seção 4.3.1 (Figura 14). Além de comunicar as implicações do não *compliance* no Treinamento de Integração e no DDS, é importante disponibilizar para essas pessoas algo por escrito para consulta; algumas opções de local são aqueles de maior circulação na obra, como a portaria, o refeitório e o almoxarifado. Deve ser preferencialmente algo simples, visual, mas que não deixe dúvidas

sobre as medidas aplicáveis e a importância de seguir as normas internas; o quadro-resumo acima (Figura 17) pode ser adaptado para essa finalidade.

Por fim, faz-se necessário avaliar a efetividade dessas medidas. Para o público com acesso a e-mail e sistemas corporativos, a proposta é que seja feito um questionário periódico sobre as medidas disciplinares aplicáveis, encorajando o destinatário a revisitar o documento, ou outros materiais desenvolvidos pelo SGC, em caso de dúvidas; o questionário pode ser incluído no e-mail de atividades obrigatórias (ver seção 4.3.5), o que garante seu envio anual. No caso dos mestres e terceiros, a avaliação mais efetiva é a que foi proposta na seção 4.3.1, isto é, integrando às visitas de acompanhamento do SGQ perguntas sobre as implicações do não *compliance*.

É preciso destacar a limitação das métricas de conscientização, propostas nesta seção e na próxima (4.3.5). Conforme aponta Griffith (2016), é difícil demonstrar a eficácia da função de *compliance*, pois as métricas avaliam mais as próprias atividades do que seu impacto na organização. Assim, além das medidas de avaliação propostas, a observação do comportamento e conduta diários é essencial para verificar a efetividade da conscientização.

4.3.5 Política de *compliance*

Finalmente, o último tópico de desenvolvimento trata-se da política de *Compliance*, documento central para o SGC e de reconhecida importância pela empresa, porém ainda não elaborado. Além da estrutura para a política (conforme descrito no Método, seção 3.3), foram desenvolvidas diretrizes para sua disponibilização como informação documentada (tarefa 17) e um fluxograma ilustrando o processo de conscientização e treinamento (tarefas 39 e 46). A estrutura completa da Política de *Compliance* consta no Apêndice C; recomendações baseadas nas orientações de uso, sendo, portanto, opcionais, foram precedidas pelo termo “convém”, sublinhado. Destaca-se ainda, para atendimento ao requisito (Quadro 12B, tarefa 16) que a Política:

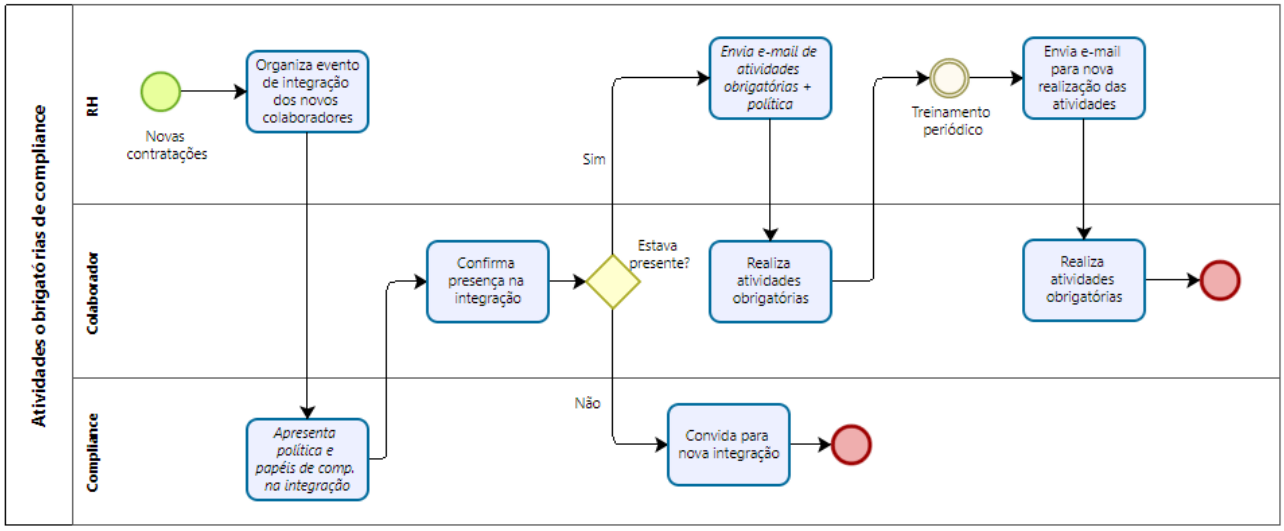
a) Seja escrita em linguagem clara, permitindo o entendimento de todo o pessoal;
b) Seja adequadamente implementada e aplicada, após sua elaboração.

Recomenda-se que o desenvolvimento da Política, seguindo a estrutura (Apêndice C), seja feito de forma colaborativa com os gestores das principais áreas de interface com *Compliance* (como Jurídico, Suprimentos diretos, Controladoria) e de todos os interessados em contribuir; tal colaboração pode ocorrer através da criação de um comitê ou de reuniões pontuais, conforme a necessidade. Além de enriquecer o documento com as atividades e a

percepção das diferentes áreas, a Política feita de forma colaborativa favorece a conscientização sobre o documento (tarefa 46) e a quebra de barreiras entre departamentos, conforme o princípio 9 de Deming (1986).

A proposta de solução para as tarefas 39 e 46 é apresentada na Figura 18; tratando-se de uma alteração de processo, as atividades modificadas foram destacadas em itálico. Atualmente, todos os novos colaboradores passam por um evento de integração, organizado semanalmente pelo RH (e mensalmente nas obras), no qual são apresentadas as áreas da empresa e uma visão geral de suas atividades. A função de *compliance* sempre participa deste evento, e envia a todos que estiveram presentes um e-mail com as atividades obrigatórias de *compliance* (leitura e adesão ao Código de Ética e Conduta, treinamento e formulário de conflito de interesses, acesso ao sistema de gestão de documentos). Anualmente, *Compliance* envia novo e-mail aos colaboradores, para que renovem as atividades.

Figura 18 - Fluxograma: atividades obrigatórias de *compliance*



Fonte: autora.

A proposta é que a política de *compliance* seja incluída na apresentação da área, dentro da integração, e enviada juntamente com o e-mail de atividades obrigatórias. Na integração, além de apresentar a política, recomenda-se destacar também a importância dos papéis individuais para o desempenho de *compliance* (conferir Apêndice C), contribuindo para a conscientização no tema. Vale destacar que a garantia de participação de novos colaboradores na integração é responsabilidade do RH; a área deve estar alinhada com *Compliance* para que todos tenham contato com a política "dentro de um período razoável do início da sua contratação" (ABNT, 2021, p. 14).

Ainda com respeito à conscientização da Política de *Compliance* (tarefa 46), a proposta é desenvolver um treinamento específico nos moldes do *e-learning* do Código de Ética e Conduta, ou seja, que viabilize o autoaprendizado, de modo interativo e dinâmico. Novamente, destaca-se a necessidade de avaliar a eficácia da conscientização, podendo ser feita através de um questionário ao final do treinamento (para o pessoal com acesso aos sistemas corporativos) e pela inclusão de questões sobre a Política de *Compliance* na Pesquisa de Clima feita anualmente (conforme seção 4.1). Em relação às obras, é importante revisar os tópicos de comunicação (seção 4.3.1) depois de elaborada a política; mestres e terceiros devem ser informados sobre o documento e a avaliação da conscientização pode ser feita de forma integrada ao SGQ (conforme descrito nas seções 4.3.1 e 4.3.4 e ilustrado na Figura 12).

A disponibilização da Política como informação documentada (tarefa 17) também contribui para a conscientização; a proposta é que a Política seja disponibilizada em meio físico (no escritório e nas obras) e em meio digital (na página de *Compliance* a ser incluída no Site Institucional, na Intranet e em seu sistema de gestão de documentos). Sendo a Política um documento extenso, a proposta é manter, para consulta, uma cópia por andar do escritório e uma cópia em cada obra; o material deve estar disponível para qualquer um que deseje consultá-lo. Ademais, para que a Política seja "comunicada dentro da organização" e esteja "disponível para as partes interessadas, conforme apropriado" (ABNT, 2021, p. 10), são propostas as seguintes ações:

a) Divulgar a Política na Intranet e em comunicado por e-mail, após sua elaboração (não apenas para novos colaboradores);
b) Disponibilizar a Política nos sistemas citados de forma clara e de fácil acesso;
c) Revisar documento de partes interessadas, conforme tarefa 3, não priorizada (Quadro 2) para garantir que todas as partes tenham acesso à Política.

5 CONSIDERAÇÕES FINAIS

Este trabalho atingiu o objetivo proposto, incluindo os objetivos específicos de compreender os processos existentes da Empresa A, analisar as lacunas entre o SGC e a NBR ISO 37301:2021, avaliar riscos e priorizar ações, e propor processos e alterações para a melhoria do sistema. A equipe de *compliance* sinalizou que pretende adotar as propostas acerca das comunicações de *compliance*, das ações de *compliance* dos gestores e da Política de *compliance*, além de uma das propostas sobre as implicações de não *compliance* (vide Quadro 13, propostas 1 a 4, 10 a 12, 16, 20 a 23, 25 a 27). A equipe pretende levar as demais propostas em consideração no planejamento de novas ações, ainda que não venha a adotá-las neste momento. A contribuição deste trabalho à empresa, no entanto, vai muito além das ações propostas. A etapa de análise de lacunas forneceu à organização um panorama de seu Sistema de Gestão de *Compliance* e do que pode ser melhorado visando o atendimento à NBR ISO 37301:2021, além de evidenciar o potencial de integração entre os sistemas de Qualidade e *Compliance* a ser explorado pela organização. A etapa de priorização promoveu a melhoria na gestão de riscos, por meio da definição de critérios objetivos e documentação de todo o processo de avaliação; com isso, os critérios poderão ser utilizados na avaliação de riscos anual, que considera os riscos das diferentes áreas da empresa, não apenas de *Compliance*. Esta etapa deixou, ainda, uma Matriz de Riscos com sete riscos de *compliance* avaliados e uma lista de mais de 50 tarefas atreladas aos riscos e classificadas quanto ao esforço necessário para sua realização, resultados que podem ser usados pela função de *compliance* em seu planejamento anual. Finalmente, a etapa de desenvolvimento possibilitou não só a documentação e alteração de processos e a recomendação de diversas melhorias para *Compliance,* mas também a identificação de outras demandas – para além da NBR ISO 37301:2021 – relacionadas aos gestores de diferentes áreas e às particularidades da empresa e de sua função de *compliance.*

O método adotado foi proveitoso para alcançar os objetivos desejados. A análise de lacunas foi fundamental para identificar as oportunidades de melhoria no SGC, partindo dos requisitos da NBR ISO 37301:2021 e comparando com os processos da organização; a qualidade da análise e as reuniões de validação foram fundamentais para as etapas seguintes, para que não fossem priorizadas e desenvolvidas ações já existentes na empresa ou distantes de sua realidade. Como dificuldades enfrentadas, destaca-se a natureza qualitativa do trabalho, que exigiu diversas revisões para que informações importantes não fossem perdidas, mesmo com a numeração das tarefas e requisitos visando sua rastreabilidade ao longo do estudo. A

interpretação da NBR ISO 37301:2021 também foi dispendiosa, sendo de grande valia a releitura frequente dos requisitos e o auxílio do gerente de *compliance,* mais familiarizado com a natureza do texto pelo atendimento à NBR ISO 9001:2015.

Futuros estudos relacionados a este trabalho incluem: a análise de lacunas dos itens da NBR ISO 37301:2021 não abordados neste estudo (9 – Avaliação de desempenho e 10 – Melhoria); a utilização do método apresentado para propor melhorias ao SGC de outras empresas em diferentes setores; e ainda estudos voltados para a integração de sistemas de gestão, como análises de lacunas da NBR ISO 37301:2021 em relação a outras normas como a NBR ISO 9001:2015 e a NBR ISO 45001:2018.

5.1 PRÓXIMOS PASSOS

Com os resultados apresentados neste trabalho, a Empresa A pode tomar as seguintes ações visando dar continuidade à melhoria do seu Sistema de Gestão de *Compliance:*

a) Implementar as propostas que decidiu adotar, seguindo a atribuição de responsabilidades da Matriz RACI;
b) Considerar no planejamento para o próximo ano as demais propostas de melhoria, bem como a classificação dos riscos na Matriz de Riscos e as notas de esforço disponibilizadas;
c) Aprofundar a análise apresentada através de uma investigação de causas para questões recorrentes, utilizando um Diagrama de Ishikawa, por exemplo;
d) Utilizar os critérios da avaliação de riscos no planejamento estratégico anual, incluindo outros riscos de *compliance* da organização.

Recomenda-se também que a Empresa A considere seriamente buscar a certificação na NBR ISO 37301:2021, tendo em vista os benefícios apontados, mas, principalmente, a necessidade trazida pela relação com investidores e seu comprometimento com o ESG. Para isso, além da análise aqui apresentada, a empresa deve avaliar os três últimos itens da NBR ISO 37301:2021 e aplicá-los à sua realidade; a análise do item 8 (Operação) deve ser desenvolvida para as demais áreas da organização, além de *Compliance*. Recomenda-se, ainda, considerar, no processo de adaptação aos requisitos, a integração dos Sistemas de Gestão da Qualidade e de *Compliance*; como mostrado neste estudo, muito do SGQ pode ser aproveitado no SGC, trazendo principalmente melhoria no gerenciamento, redução de custos e melhor utilização de recursos.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS–ABNT. **NBR ISO 37301**: Sistemas de Gestão de *Compliance* – Requisitos com orientações para uso. Rio de Janeiro: ABNT, 2021. 57 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS–ABNT. **NBR ISO 45001**: Sistemas de Gestão de Saúde e Segurança Ocupacional – Requisitos com orientação para uso. Rio de Janeiro: ABNT, 2015. 41 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS–ABNT. **NBR ISO 9001**: Sistemas de Gestão da Qualidade – Requisitos. Rio de Janeiro: ABNT, 2015. 32 p.

BERSSANETI, Fernando T.; BOUER, Gregório. **Qualidade**: conceitos e aplicações em produtos, projetos e processos. 1. ed. digital. São Paulo: Edgard Blücher, 2018. 192 p.

BERNARDO, Merce *et al.* **Benefits of management systems integration**: a literature review. Journal of Cleaner Production, Elsevier, v. 94, p. 260-267, 2015.

BOFINGER, Yannik *et al.* **Corporate social responsibility and market efficiency:** Evidence from ESG and misvaluation measures. Journal of Banking & Finance, Elsevier, v. 134, 2021.

BRASIL. Ministério das Cidades. Secretaria Nacional de Habitação. **Sistema de Avaliação de Conformidade de Empresas de Serviços e Obras da Construção Civil – SiAC.** Brasília, 2018.

BRASIL. Ministério do Trabalho e Previdência. **Portaria MTb nº 3.214, de 8 de junho de 1978**. Norma Regulamentadora nº 18 – Condições e Meio Ambiente de Trabalho na Indústria da Construção Civil. Brasília, 1978.

CARDONI, Andrea *et al*. **Continuous auditing and data mining for strategic risk control and anticorruption**: Creating “fair” value in the digital age. ERP Environment and John Wieley & Sons Ltd. Itália, v. 29, p. 3072-3085, jun. 2020.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Thought Leadership in ERM**: Risk Assessment in Practice. 2012. Disponível em: <https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf >. Acesso em: 08 set. 2021.

DEMING, W. Edwards. **Out of the crisis**: quality, productivity and competitive position. Cambridge: Cambridge University Press, 1986.

GREEN, Philip. E.J. **Enterprise Risk Management**: A Common Framework for the Entire Organization. 1. ed. Reino Unido: Elsevier Inc., 2016. 260 p.

GRIFFITH, Sean J. **Corporate Governance in na Era of Compliance.** 2016. Disponível em: <https://ir.lawnet.fordham.edu/faculty_scholarship/873>/. Acesso em: 1 jul. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION–ISO. **ISO 19600:2014 –** Compliance management systems – Guidelines. 2014. Disponível em: <https://www.iso.org/standard/62342.html>. Acesso em: 5 nov. 2021.

LAM, James. **Enterprise Risk Management**: From Incentives to Control. 1. ed. Reino Unido: Willey, 2003. 319 p.

MARRIOTT, Robert D. **Process Mapping:** The Foundation for Effective Quality Improvement. Current Problems in Pediatric and Adolescent Heath Care, v. 48, n. 7, p. 177-181, 2018.

MOELLER, Robert R. **COSO Enterprise Risk Management**: Establishing Effective Governance, Risk, and Compliance Processes. 2. ed. Nova Jersey: John Wiley & Sons Inc, jul. 2011. 384 p.

POLLMAN, Elizabeth. **Corporate Social Responsibility, ESG, and Compliance.** In: ROOIJ, Benjamin van; SOKOL, D. Daniel. The Cambridge Handbook of Compliance. Cambridge: Cambridge University Press, 2021.

PROJECT MANAGEMENT INSTITUTE–PMI. **A Guide to the Project Management Body of Knowledge**, 6. ed. Newtown Square: Project Management Institute, 2017. 579 p.

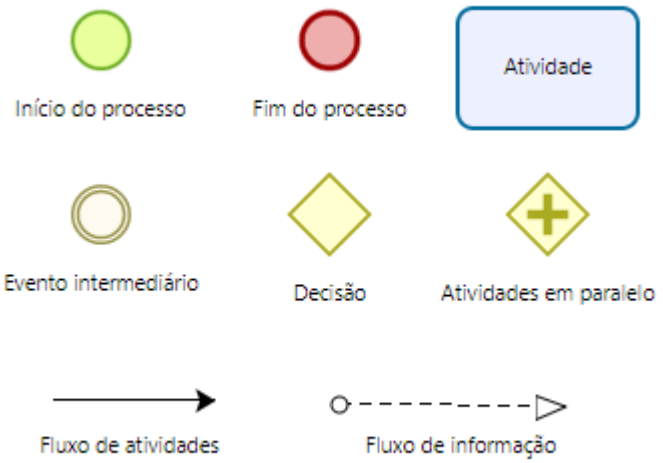
UNITED STATES OF AMERICA. H.R.3763 – 107th Congress (2001-2002): **Sarbanes-Oxley Act of 2002**. 30 jul. 2002. Disponível em: <https://www.congress.gov/bill/107th-congress/house-bill/3763>. Acesso em: 12 nov. 2021.

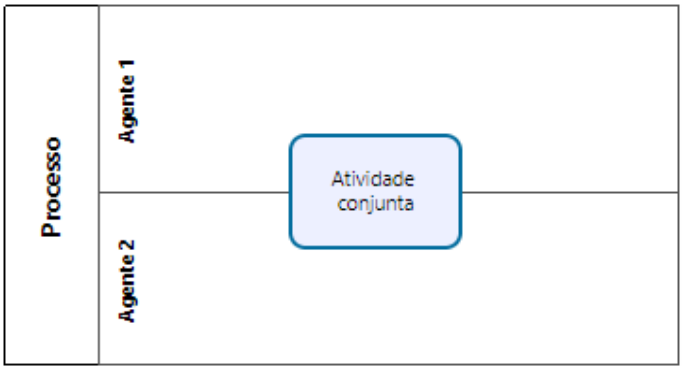
VITORELI, Gislaine A., CARPINETTI, Luiz C. R. **Análise da integração dos sistemas de gestão normalizados ISO 9001 e OHSAS 18001**: Estudo de casos múltiplos. Gest. Prod. São Carlos, v. 20, n. 1, p. 204-217, 2013.

7 APÊNDICES

7.1 APÊNDICE A – SIMBOLOGIA DOS FLUXOGRAMAS

Simbologia utilizada nos fluxogramas elaborados, utilizando o *Bizagi Modeler* ®:





7.2 APÊNDICE B – CLASSIFICAÇÃO E NOTAS DE ESFORÇO

Classificação de cada tarefa[8] quanto ao critério de Esforço e nota final, considerando o fator de redução de esforço conforme os Quadros 4 e 9:

Tarefa	Esforço	Nota
1	Tomada de decisão/definições e documentação	3,9
2	Alterações em documento	5,5
3	Tomada de decisão/definições e documentação	3
4	Tomada de decisão/definições e documentação	3,3
5	Elaboração de documento simples	5,5
7	Desenho de processo	1,1
8	Desenho de processo	1,1
9	Elaboração de documento simples	5,5
10	Desenho de processo	1,1
11	Elaboração de documento complexo	2,2
12	Tomada de decisão/definições e documentação	3
13	Alterações em documento	6,5
14	Alterações em processo	5,2
15	Elaboração de documento simples	5
16	Elaboração de documento complexo	2,2
17	Elaboração de documento complexo	2,2
18	Desenho de processo	1
19	Tomada de decisão/definições e documentação	3
20	Alterações em processo	5,2
21	Desenho de processo	1
22	Elaboração de documento simples	5
23	Tomada de decisão/definições e documentação	3,3
24	Elaboração de documento simples	5
25	Tomada de decisão/definições e documentação	3,3
26	Elaboração de documento simples	5
27	Alterações em processo	5,2
28	Desenho de processo	1,1
29	Alterações em processo	4,4
30	Tomada de decisão/definições e documentação	3,3
31	Elaboração de documento complexo	2
32	Tomada de decisão/definições e documentação	3,3
33	Elaboração de documento complexo	2,2
34	Tomada de decisão/definições e documentação	3,3
35	Tomada de decisão/definições e documentação	3
36	Alterações em documento	6,5
37	Desenho de processo	1,1

[8] As tarefas 6 e 55 estão fora da avaliação conforme explicado na seção 4.1.1.

Tarefa	Esforço	Nota
38	Alterações em processo	4,4
39	Alterações em processo	4
40	Ações para executar processo existente	5,2
41	Alterações em processo	4
42	Alterações em processo	5,2
43	Tomada de decisão/definições e documentação	3,3
44	Alterações em processo	4
45	Elaboração de documento complexo	2,6
46	Alterações em processo	4,4
47	Alterações em processo	4
48	Ações para executar processo existente	5,2
49	Ações para executar processo existente	5,2
50	Alterações em processo	5,2
51	Alterações em processo	4
52	Alterações em documento	5
53	Tomada de decisão/definições e documentação	3,9
54	Alterações em documento	5
56	Tomada de decisão/definições e documentação	3
57	Desenho de processo	1
58	Tomada de decisão/definições e documentação	3
59	Desenho de processo	1
60	Tomada de decisão/definições e documentação	3,3
61	Desenho de processo	1,3
62	Alterações em processo	5,2
63	Elaboração de documento simples	6

7.3 APÊNDICE C – GUIA PARA USO DO FMEA

Para utilizar a ferramenta FMEA na análise crítica de desempenho de *compliance*, a função de *Compliance* e a Diretoria podem fazer uso do quadro guiado abaixo (adaptado de BERSSANETI; BOUER, 2018). A primeira linha, em itálico, indica o que deve ser preenchido em cada coluna; a segunda apresenta um exemplo meramente ilustrativo de preenchimento. O passo a passo com maior detalhamento é descrito a seguir.

FMEA para análise crítica de desempenho

	Função	Modo de falha potencial	Efeito potencial de falha	Severidade	Causa potencial da falha	Ocorrência	Controles atuais		Detecção	NPR	Ações recomendadas	Responsável/ prazo	Resuldados das ações				
							Prevenção	Detecção					Ações tomadas	Severidade	Ocorrência	Detecção	NPR
	Qual a meta analisada e área relacionada?	*O que pode dar errado? Ela gera/ encoraja uma ação de não compliance?*	*Qual o não compliance gerado? Relacionado a leis, normas internas, dano de imagem?*	*Quão grave é a falha? (nota de 1 a 10)*	*Por que/ como é gerado/ encorajado o não compliance?*	*Qual a chance de que isso ocorra? (nota de 1 a 10)*	*O que existe hoje para prevenir essa ocorrência?*	*O que existe hoje para detectar essa ocorrência?*	*Quão eficazes são os controles atuais? (nota de 10 a 1)*	*Nota final: SxOxD*	*O que pode ser feito para reduzir essa nota? Atacar efeito, causa, controles?*	*Quem fará? Até quando?*	*O que foi realmente feito?*	*Qual a nova severidade? (nota de 1 a 10)*	*Qual a nova chance de ocorrência? (nota de 1 a 10)*	*Qual a nova eficácia dos controles? (nota de 10 a 1)*	*Nova nota final: SxOxD*
EXEMPLO	"Satisfação dos clientes acima de 90%" (área: Relacionamento com o cliente)	Encoraja ação de não compliance: não registrar reclamações de clientes	Desacordo com as normas internas e ISO 9001	8	Não registrar as reclamações para aumentar a % de satisfação e bater a meta	4	Orientação para leitura e cumprimento do procedimento	Verificação mensal do gestor da área	6	192	Registro da reclamação permitindo alteração da nota depois de resolvida; Mecanismos no sistema para prevenir alteração de dados	Analista da área. Prazo: 1 mês	Alteração do processo, permitindo alterar nota depois de resolver problema, sem perder informação do cliente	5	2	6	60

Passo a passo:

1. Listar na coluna **Função** as metas e/ou situações que se deseja analisar.
2. Para cada item listado, preencher:
    - **Modo de falha potencial**: O que pode dar errado com essa meta ou situação? Ela gera ou encoraja uma ação de não *compliance*? Como se dá essa ação?
    - **Efeito potencial de falha:** Qual o não *compliance* gerado? O que essa ação infringe? (Leis, normas internas, imagem da empresa)
        - **Severidade:** Quão grave é a falha, considerando seu efeito? Dar uma nota de 1 a 10, sendo 1 – pouco severa e 10 – extremamente severa.
    - **Causa potencial de falha:** Por que se dá a falha ou como ela ocorre? Qual sua causa? Deve-se à elaboração da meta, à má conduta ou má fé do colaborador, ao encorajamento financeiro inadequado etc.
        - **Ocorrência:** Qual a chance de que a falha ocorra? Dar uma nota de 1 a 10, sendo 1 – pouquíssimo provável e 10 – extremamente provável.
    - **Controles atuais:** O que existe hoje tanto para prevenir que a falha ocorra, quanto para detectar sua ocorrência?
        - **Detecção:** Quão eficazes são os controles atuais? Dar uma nota de 10 a 1, sendo 10 – pouquíssimo eficazes e 1 – extremamente eficazes (escala inversa).
3. Calcular o **NPR** (número de prioridade de risco) de cada item, multiplicando os valores de Severidade, Ocorrência e Detecção (S*O*D); os itens com maior valor de NPR devem ser priorizados para a tomada de ações.
4. Identificar **Ações recomendadas** para reduzir o NPR, isto é, reduzir a Severidade do efeito, a Ocorrência da causa e/ou aumentar a eficácia da Detecção.
5. Identificar pelo menos um **Responsável** pelas ações e um **Prazo** para sua realização.
6. Terminado o prazo, verificar e preencher as **Ações tomadas** de fato; não necessariamente todas as ações recomendadas serão realizadas.

7. Avaliar, para a nova situação, a **Severidade,** a **Ocorrência** e a **Detecção,** calculando assim o novo **NPR.** A nota só deve mudar quando as ações tomadas afetam o aspecto em questão; se a ação tomada apenas melhora a Detecção, esta nota deve ser alterada, sendo as demais mantidas, e assim por diante (como no exemplo acima, apenas Severidade e Ocorrência foram alteradas).

8. Manter a lista de itens para análises posteriores. Trata-se de um processo de melhoria contínua; uma vez atacado um item, seu NPR é reduzido e outro toma o lugar de prioridade, até que todos sejam tratados por ações de melhoria.

O modelo acima pode ser utilizado em diferentes situações, sem que seja necessário alterar a linha de títulos. Basta adaptar a instrução de preenchimento (em itálico) para as colunas **Função**, **Modo de falha potencial, Efeito de falha potencial** e **Causa potencial da falha**; as demais colunas são genéricas e não requerem adequação.

Uma das formas de aplicação do FMEA para o SGQ, por exemplo, poderia ser analisar e melhorar a forma como os requisitos da NBR ISO 9001:2015 estão sendo atendidos. A instrução de preenchimento seria, então: em Função, “Qual o requisito analisado?”; em Modo de falha potencial, “O que pode dar errado? Como ele pode não ser cumprido?”; em Efeito de falha potencial, “Qual o efeito gerado? Afeta apenas a operação interna ou traz risco de perda da certificação?”; e em Causa potencial de falha, “O que leva ao não cumprimento do requisito? Por que isso acontece?”.

7.4 APÊNDICE D – ESTRUTURA DA POLÍTICA DE *COMPLIANCE*

Título: "Política de *Compliance* – Empresa A"

Contexto: Destacar o propósito da organização e considerá-lo na elaboração: utilizar Planejamento Estratégico, especialmente itens 2, 6, 10 e 11.

Convém incluir:

- Uma declaração da missão: utilizar Planejamento Estratégico, item 6;
- Uma declaração geral da Política: utilizar como exemplo a introdução do Código de Ética e Conduta.

Convém especificar:

- Contexto e aplicação do SGC: considerar realização das tarefas 1 e 2 (Quadro 2);
- Abrangência da integração do sistema com outras funções da organização: relacionar principais áreas e interfaces com *Compliance;*
- Princípios que regem a relação com as partes interessadas: utilizar documento de Partes interessadas e seus requisitos e considerar realização da tarefa 3 (Quadro 2);
- A importância dos papéis individuais (tarefa 46, Quadro 2) para o *compliance*, conforme exemplificado a seguir:
    - Papel de cada área (*Compliance* – adequação da empresa às suas obrigações; Jurídico – validação de contratos; Suprimentos – contato com fornecedores etc.);
    - Papel de cada cargo (Gestores – encorajar e monitorar; Analistas Sêniores – engajar e contribuir; Analistas Júniores – buscar aprender e seguir instruções etc.);
    - Papel de cada colaborador – comprometimento individual com o *compliance.*
- Os benefícios da melhoria de desempenho de *compliance*, decorrentes do exercício dos papéis individuais.

Incluir no documento toda informação necessária para que este seja uma base para a elaboração e revisão dos objetivos de *compliance.*

Comprometimento: Incluir mensagem da Diretoria e Conselho de Administração, firmando o compromisso da empresa:

- Para atender aos requisitos aplicáveis da NBR ISO 37301:2021;
- Para a melhoria contínua do Sistema de Gestão de *Compliance*.

Componentes: Os seguintes itens devem estar presentes no corpo do documento:

1. Indicar valores, objetivos e estratégia da organização e garantir alinhamento da Política com estes fatores: utilizar Planejamento Estratégico, especialmente itens 7, 8, 10, 11 e 15.
    - Convém indicar estratégias da gestão e alocação de recursos e responsabilidades: utilizar Planejamento Estratégico (item 17) e Política de gerenciamento de riscos (item 6), e considerar elaboração de Diagrama de processos para a função de *compliance.*
2. Referenciar documento contendo todas as obrigações de *compliance* da organização (tarefa 9, Quadro 2), requerendo o *compliance* com estas.
3. Apoiar a governança de *compliance,* estabelecendo que a função de *compliance* deve:
    - Ter acesso direto ao Conselho de Administração;
    - Ser independente, sem quaisquer interferências ou pressão em sua operação;
    - Ter autoridade e competência apropriada.
4. Fazer referência e descrever a função de *compliance*: utilizar material do programa de *compliance*.
    - Convém apontar os procedimentos padrão de *Compliance* e práticas de auditoria e *due dilligence;*
    - Convém relacionar demais documentos de *Compliance* na Política, indicando sua utilização, como exemplo a seguir:
        - Todas as questões relacionadas à ética de nossos colaboradores estão relacionadas no Código de Ética e Conduta[9].
        - A Política de conflito de interesses instrui sobre a existência de conflito de interesses na organização e sobre como proceder.

[9] A empresa pode considerar a substituição do Código de Ética e Conduta pela Política de *Compliance*, visando a centralização em um único documento.

- Sobre recebimento de brindes e afins, a organização dispõe dos documentos: Norma de brindes, presentes e cortesias; Política de brindes, presentes e cortesias – fornecedor; e Carta de recusa de brindes, presentes e cortesias.
- Sobre doações e patrocínios, a organização dispõe dos documentos: Política de doações e patrocínios; Formulário de doação e Formulário de patrocínio.
- Para sistematização do relacionamento com fornecedores, a organização dispõe dos documentos: Planilha de avaliação de fornecedores e Formulário de aprovação de contratação de serviços críticos.
- Sobre a aplicação de medidas disciplinares, a organização dispõe dos documentos: Política de medidas disciplinares; Termo de advertência; Termo de suspensão e Termo de desligamento.

5. Fazer referência à política de Medidas Disciplinares, como definição das consequências de não estar em *compliance*; caso sejam incluídas mais obrigações de *compliance* (tarefa 9, Quadro 2), as implicações correspondentes devem ser abordadas no documento.
6. Encorajar o levantamento de preocupações e denúncias de *compliance*, indicando como acessar o Canal de Ética, e proibir expressamente quaisquer formas de retaliação.