1. OBJETIVO

Estabelecer as diretrizes e responsabilidades de Gestão de Riscos para a Cosan S.A. (“Cosan” ou “Companhia”), bem como orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos, incorporando a visão de riscos à tomada de decisão estratégica e promovendo a cultura de Gestão de Riscos em todos os níveis organizacionais, em conformidade com as melhores práticas de mercado.

2. APLICAÇÃO E ABRANGÊNCIA

A presente Política de Gerenciamento de Riscos (“Política”) abrange a Cosan e deve servir como referência às suas controladas e/ou co-controladas, a partir da data de sua aprovação e consequente publicação.

3. DEFINIÇÕES

Os termos abaixo listados terão os significados atribuídos a seguir:

Ações Mitigatórias (plano de ação) – Uma ação (ou conjunto de ações) endereçada para a redução das exposições ao risco que deve estar conectada com os fatores que causam as exposições. Deve, ainda, possuir responsáveis por sua implantação e prazo de conclusão.

Apetite a Risco – Nível de exposição à perda, financeira ou não financeira, quantitativo ou qualitativo, que a Companhia está disposta a assumir para atingir seus objetivos estratégicos de curto, médio e longo prazo.

Auditoria Interna – Área responsável por avaliar, conforme seus princípios e diretrizes, a efetividade da Gestão de Riscos e dos processos da Companhia, das ações mitigatórias de risco, dos controles internos e da conformidade às normas e legislações dos mercados em que a Companhia opera.

Capacidade de Risco – Limite máximo de Tolerância ao Risco, superior ao apetite, que a Companhia pode suportar para atingimento de seus objetivos estratégicos, mantendo a continuidade dos seus negócios.

Comissão de Riscos Cosan – Colegiado composto por executivos da Companhia, e pela Gerência de Gestão de Riscos, responsável por identificar, revisar, discutir e acompanhar os riscos que possam afetar o negócio.

Comitê de Auditoria – Órgão de auxílio vinculado e subordinado ao Conselho de Administração da Companhia, de funcionamento permanente, responsável (i) pelo assessoramento ao Conselho de Administração em relação aos processos de controles internos e de administração de riscos; (ii) pela supervisão das atividades da Auditoria Interna; e (iii) pela supervisão das atividades das empresas de auditoria independente do Grupo Cosan, dentre outras funções descritas no Estatuto Social da Companhia.

Conselho de Administração da Companhia – É o órgão de governança mais elevado da Companhia. O Conselho de Administração, entre outras atribuições, é responsável por eleger os administradores, aprovar os planos de trabalho, de investimentos e orçamento da Companhia e suas controladas. As principais diretrizes e políticas da Companhia são aprovadas pelo Conselho de Administração.

Consequência – Efeito da materialização dos Riscos, identificados ou não.

Controles Internos – Área responsável por desenho e implementação de controles para redução do grau de exposição a riscos da Companhia, manutenção da conformidade às normas e legislações dos mercados que a Companhia opera, bem como manter a confiabilidade dos relatórios financeiros e gerenciais.

Criticidade – Classificação do risco de acordo com suas avaliações de impacto e Probabilidade.

Dicionário de riscos – Documento que registra os principais riscos identificados a partir da análise das estratégias e do contexto de negócios. É parte fundamental na definição de uma linguagem comum de riscos, possibilitando melhor entendimento na organização.

Diretoria Executiva (Diretoria) – A Diretoria Executiva da Cosan é o órgão responsável pela organização interna e pelo funcionamento diário das operações, implementando as políticas e diretrizes gerais estabelecidas pelo Conselho de Administração.

Dono do Risco – Gestor responsável pelo gerenciamento de riscos, ou Fatores de Riscos, bem como da implementação de respectivos ações mitigatórias e/ou controles internos.

ESG (*Environment, Social and* Governance) – Conceito que avalia a sustentabilidade de uma empresa considerando aspectos ambientais, sociais e de governança.

Fatores de Risco – Conjunto específico de circunstâncias que contribuem para que eventualmente um risco se materialize. O mesmo risco pode conter um ou mais fatores relacionados.

Ficha de Risco – Documento que formaliza todas as informações relativas ao processo de identificação, avaliação e Tratamento do Risco.

Gestão de Riscos – Área, subordinada à Diretoria de Gestão de Riscos, Controles Internos e Auditoria Interna, responsável por conduzir o Processo de Gestão de Riscos dentro da Companhia.

IBGC – Instituto Brasileiro de Governança Corporativa. É uma organização da sociedade civil e uma rede colaborativa de ideias dedicada a explorar temas e questões importantes sobre governança e que impactam positivamente a sociedade.

IIA – *The Institute of Internal Auditors* (Instituto dos Auditores Internos). Associação profissional internacional com sede nos Estados Unidos. Seu objetivo principal é promover e desenvolver a prática da auditoria interna e governança corporativa no mundo inteiro.

Impacto – O impacto diz respeito às Consequências que serão geradas caso o risco se materialize podendo ser medido de forma qualitativa ou quantitativa. Em geral, trata-se da categorização e mensuração das Consequências de materialização do risco.

ISO 31000 - Norma ABNT NBR ISO 31000 de 2018, que é a norma internacional que fornece princípios e diretrizes para a gestão de riscos, sendo aplicável a qualquer tipo de organização, independente do seu tamanho ou setor.

Matriz de Riscos – Representação gráfica da avaliação dos graus de Criticidade da Companhia considerando as análises de impacto e Probabilidade.

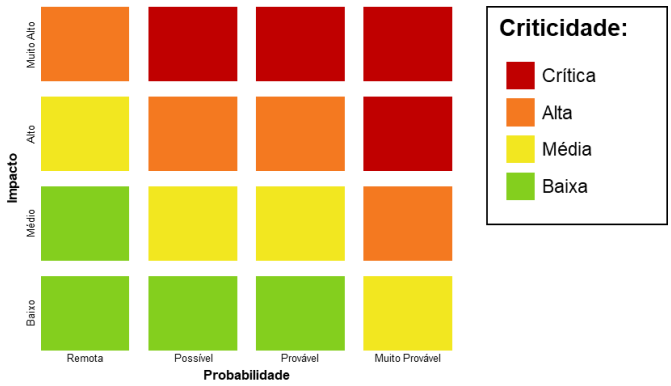

Figura 1 - Matriz de Riscos Cosan

Planejamento Estratégico – Ferramenta de gestão que define metas, ações e recursos para que uma organização alcance seus objetivos. Na Cosan, o planejamento estratégico é executado através da RPA (Reunião de Planejamento Anual).

Probabilidade – Chance de materialização de um risco. Pode ser avaliada de forma qualitativa ou quantitativa.

Processo de gestão de riscos – Conjunto de atividades coordenadas para a identificação, análise, tratamento e revisão dos riscos do negócio, executadas de acordo com política e metodologia aprovadas para avaliação, classificação e reporte de riscos.

Régua de Impacto – Critérios e escalas, definidos de acordo com as especificidades do negócio, de análise de Impacto.

Régua de Probabilidade – Critérios e escalas, definidos de acordo com as especificidades do negócio, de análise de Probabilidade.

Resposta ao Risco – Definição da forma de Tratamento ao Risco.

Risco – Possibilidade de ocorrência de um evento capaz de afetar de maneira adversa o atendimento dos objetivos da organização, impedindo a criação de valor ou até mesmo destruindo valor existente.

Temas Materiais ESG – São os tópicos ESG mais relevantes para a Companhia e seus stakeholders, considerando seu Impacto financeiro e estratégico.

Tolerância ao risco – Trata-se de um limite de risco, inferior ao apetite, em que a alta administração deve ser alertada para tomada de ações mitigatórias e redução da exposição ao risco.

Tratamento dos riscos – Conjunto de iniciativas, que podem ser documentadas a partir de uma Ficha de Riscos juntamente com todas as informações referentes a um determinado risco, dentre elas, mas não limitadas a (i) ações mitigatórias, (ii) controles internos, (iii) execução de projetos, (iv) desenvolvimento/aquisição de sistemas ou (vi) criação de documentos normativos, para endereçar a Resposta aos riscos.

4. DIRETRIZES GERAIS

A Gestão de Riscos corporativos é parte integrante da governança corporativa da Companhia e deve ser utilizada como fonte de informação relevante para tomada de decisão estratégica e definição dos objetivos estratégicos, além de estar presente nos ciclos de gestão da Companhia como gestão orçamentária e Planejamento Estratégico. Deve ser executada de modo a manter a exposição ao risco em níveis compatíveis com o Apetite a Risco da Companhia, possibilitando a garantia de seus objetivos e metas.

O gerenciamento dos riscos da Companhia obedece ao Modelo de Três Linhas de Atuação, previsto no parecer do IIA de setembro de 2024, representado conforme abaixo:

- **1ª Linha de Atuação:** é composta pelas áreas de negócios da Companhia, incluindo suas controladas e co-controlada, responsáveis pelos riscos que gerenciam, assim como pela execução e eficácia de suas respectivas Ações Mitigatórias e de seus controles internos associados.
- **2ª. Linha de Atuação:** é composta pelas estruturas que devem instrumentalizar os gestores da primeira linha para o correto gerenciamento dos riscos através da organização e estruturação dos processos, definição de metodologias, desenvolvimento de treinamentos e orientação, além de reportar as informações aos órgãos de governança competentes. A 2ª Linha pode ser composta pelas (i) áreas de Gestão de Riscos, Controles Internos, Compliance e afins; e também por (ii) órgãos internos de governança como comitês executivos, comissões, fóruns e/ou grupos de trabalho.

- **3ª. Linha de Atuação:** é composta pela Auditoria Interna da Companhia, atuando com um olhar independente para verificar a eficácia e conformidade do modelo e reportar suas recomendações aos órgãos de governança competentes.

  Papéis e responsabilidades mais abrangentes de cada linha de atuação em relação ao gerenciamento de riscos estão detalhados no item 4.3. (Papéis e Responsabilidades) abaixo.

Para definição dos critérios constantes dessa Política, a área de Gestão de Riscos da Companhia se utiliza das seguintes definições para os riscos em seus diferentes estágios da identificação.

- **Risco Inerente –** Risco associado ao negócio antes do efeito de qualquer ação, controle ou contramedida. É a exposição bruta da Companhia ao risco;
- **Risco Residual (Real) –** Risco remanescente após a implantação de algumas ações mitigatórias e atividades de controle no atual momento de identificação e avaliação do risco; e
- **Risco Projetado –** Risco, em sua forma futura, após a implementação total de ações mitigatórias e atividades de controle. O risco projetado determina o mínimo grau de Criticidade do risco de acordo com o tratamento que a Companhia está disposta a realizar.

4.1. Processo de Gestão de Riscos

A estrutura organizacional proposta para Gestão de Riscos é baseada em parâmetros e diretrizes estabelecidas pelo IBGC e a ISO 31000, especialmente no que diz respeito às etapas da gestão dos riscos, as quais possuem os seguintes objetivos:

- Garantir que a Gestão de Riscos seja integrada em todas as atividades organizacionais da Companhia;
- Definir papéis e responsabilidades para o gerenciamento de riscos;
- Padronizar conceitos e práticas;
- Influenciar na tomada de decisão;
- Proporcionar uma rotina dinâmica e eficiente de informação;

- Assegurar que a governança corporativa da Companhia seja seguida e criticamente analisada; e
- Proporcionar maior transparência da Companhia para os diversos stakeholders: acionistas, analistas de mercado, agências de crédito, órgãos reguladores, entre outros.

Abaixo as etapas do processo de Gestão de Riscos, baseado na ISO 31000:

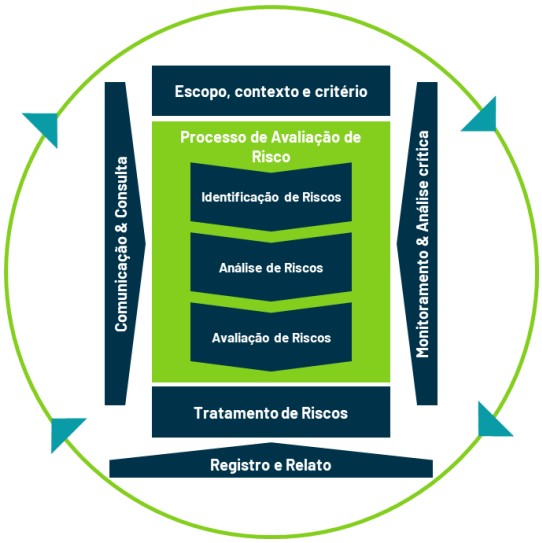

Figura 2 - Processo de Gestão de Riscos

4.1.1. Escopo, Contexto e Critério

Na fase de planejamento de qualquer atividade, objetivos realistas e mensuráveis são definidos no contexto do ambiente de negócios. Na primeira etapa do processo de gerenciamento de riscos, são capturados o entendimento dos objetivos estratégicos, levando em consideração os contextos interno e externo em que a Companhia está inserida.

4.1.2. Identificação de Riscos

A identificação dos riscos é um processo contínuo de gestão e possuí maior valor quando diretamente vinculada aos objetivos estratégicos do negócio. Diferentes abordagens são adotadas para identificar os riscos e a abordagem adotada dependerá do tamanho e complexidade do negócio, da oportunidade/projeto e da volatilidade do ambiente de risco. A identificação dos riscos envolverá reuniões, entrevistas ou

workshops dedicados a riscos ou poderá ocorrer, também, por meio da materialização de um evento significativo com possibilidade de novas ocorrências.

Nesta etapa deve-se criar uma relação e descrição de riscos, e seus respectivos fatores, que possam desviar a Companhia do atingimento de seus objetivos estratégicos ou da desconformidade de normas e regulamentos, inclusive internos.

Por se tratar de uma *holding*, a Companhia deve também buscar identificar Riscos Sistêmicos através das matrizes de riscos de suas investidas ou de eventuais processos, eventos ou fatores que pertençam a estruturas transversais nas empresas. Riscos desta natureza podem gerar descontinuidade, total ou parcial, de uma ou mais operações das investidas ao mesmo tempo.

4.1.3. Análise de Riscos

Na etapa de análise de riscos, deve-se levar em consideração o Impacto e Probabilidade de materialização do risco assim como de seus respectivos fatores.

O Impacto não apenas deve levar em consideração as Consequências imediatas da materialização de um risco, mas também os efeitos indiretos. Nem todos os riscos poderão ser quantificados em termos financeiros, e, para alguns riscos, critérios qualitativos são mais adequados para a análise. Critérios qualitativos podem ser, mas não se limitam a, de meio ambiente, sociais, de conformidade, de saúde e segurança, de imagem institucional, de qualidade do produto ou de tecnologia.

A análise de Probabilidade deve levar em consideração o histórico de materialização do risco, os controles existentes que endereçam o tema, a existência e efetividade de Ações Mitigatórias e a opinião técnica dos especialistas do tema, incluindo os donos do risco.

4.1.4. Avaliação de Riscos

Nesta etapa, comparamos o nível de risco classificado durante a etapa de análise, levando em consideração os critérios estabelecidos na etapa anterior. Na avaliação, classificamos o risco na Matriz de Riscos da Companhia.

A Matriz de Riscos se torna então uma ferramenta de priorização, de acordo com a avaliação dos riscos em comparação ao determinado Apetite ao Risco, para

direcionamento dos esforços e mitigação dos riscos mais relevantes de acordo com o contexto de negócio. Conforme apresentado na Figura 2, os riscos são avaliados em 4 graus de Criticidade, de acordo o vetor composto das notas de Probabilidade e impacto em ordem decrescente:

- Muito Alta - maior Criticidade ao valor do negócio;
- Alta;
- Média; e
- Baixa – Menor Criticidade ao valor do negócio.

4.1.5. Tratamento de Riscos

A avaliação de risco auxilia na distribuição de recursos e priorização de ações, com base em um panorama abrangente de todos os riscos significativos no contexto dos objetivos da Companhia. Nesta etapa haverá a definição e implementação de Ações Mitigatórias e/ou controles internos de forma a responder cada respectivo risco ou fator de risco. Vale reforçar que, a decisão sobre o devido tratamento ao risco, ou seu respectivo fator, depende de sua avaliação em comparação ao apetite de risco da Companhia. Podemos tratar riscos da seguinte forma:

- **Mitigar –** Reduzir a exposição de Probabilidade e/ou Impacto utilizando de controles internos ou Ações Mitigatórias;
- **Assumir –** Aceitar os Impactos do risco em sua forma residual e todas as Consequências de uma eventual materialização. Devemos manter os controles existentes, caso existam, para que o risco não tenha aumento de Criticidade e se mantenha gerenciado;
- **Transferir –** Requer que uma terceira parte esteja disposta para assumir parte do risco juntamente com a Companhia. Por exemplo, contratação de seguros, formação de joint ventures, entre outros; ou
- **Evitar –** Eliminar totalmente a fonte de um risco. Por exemplo, interrupção de uma atividade, retirada de operação de uma região/ mercado, ou a venda/desinvestimento de ativos.

4.1.6. Comunicação & Consulta

É necessária a comunicação, de forma ágil e contínua, com os diferentes stakeholders sobre os riscos do negócio, a fim de manter alinhados o processo de gerenciamento de riscos e a implementação da estratégia da Companhia. Desta forma, pode-se identificar informações relevantes que permitam a melhoria contínua das informações sobre os riscos identificados.

Também é recomendada uma comunicação transparente a respeito dos riscos, para que as decisões sejam tomadas com um pleno entendimento e ponderação dos riscos e oportunidades envolvidos, e como eles serão gerenciados.

Os reportes periódicos sobre os riscos devem ocorrer de forma integrada e consolidada para a Diretoria e demais fóruns de governança da Companhia.

4.1.7. Monitoramento & Análise Crítica

Durante o processo de monitoramento dos riscos, deve-se detectar mudanças no contexto interno e externo, identificando riscos emergentes e mudanças nos riscos já formalizados, além de monitorar a execução de Ações Mitigatórias/controles internos definidos pelos Donos dos Riscos e pelas respectivas áreas da Companhia, atualizando a classificação dos riscos na matriz e reportar à Diretoria e demais fóruns de Governança da Companhia.

4.1.8. Registro e Relato

Os Donos de Riscos devem reportar eventuais materializações de riscos e suas reais Consequências para a Companhia. Desta forma, podemos medir a real aderência do risco identificado e a eficiência das Ações Mitigatórias e controles internos. As lições aprendidas devem ser registradas a fim de manter a melhoria contínua dos processos envolvidos e mitigar as Consequências de uma nova materialização. Em casos significativos, deve-se envolver na discussão a Diretoria e/ou o Comitê de Auditoria da Companhia.

4.2. Dicionário de Riscos

A Companhia está sujeita a diversos riscos que podem impactar adversamente seus negócios. Dessa forma, para definição de uma linguagem comum e possibilitar melhor

entendimento na organização, os riscos podem ser classificados de acordo com as seguintes categorias:

- **Riscos Estratégicos** são aqueles associados à tomada de decisão da alta Administração e podem gerar perda substancial no valor econômico da Companhia ou causar efeito negativo a sua reputação, credibilidade ou a marca perante o mercado e as comunidades onde atua.
- **Riscos Financeiros** são aqueles associados:
  i. A exposição das operações financeiras da organização;
  ii. A emissão de relatórios financeiros, gerenciais, regulatórios, fiscais, estatutários e de sustentabilidade incompletos, inadequados, inexatos ou intempestivos;
  iii. As contrapartes da Companhia que podem, eventualmente, deixar de honrar seus compromissos e obrigações (risco de crédito);
  iv. A alteração ou extinção de incentivos fiscais regionais e/ou setoriais;
  v. a possibilidade de que os fluxos de caixa não sejam administrados efetivamente para maximizar a geração de caixa operacional, gerenciar os riscos e retornos específicos das transações financeiras (risco de liquidez);
  vi. À desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador;
  vii. A redução dos resultados financeiros;
  viii. A volatilidade de taxas de juros, câmbio e outros indicadores macroeconômicos; e
  ix. A captar e aplicar recursos financeiros em desacordo com as políticas estabelecidas.
- **Riscos de Conformidade, Legais ou Regulatórios** são aqueles associados ao não cumprimento de leis e regulamentos emitidos pelos governos centrais e locais assim como regulamentos emitidos por entidades reguladoras ou mesmo de natureza interna. Estão associados também a prevenção de lavagem de dinheiro, a questões antissuborno ou à ocorrência de modificações nas regulamentações e ações de órgãos reguladores que podem afetar

significativamente a habilidade da Companhia em administrar seus negócios de maneira íntegra.

- **Riscos Operacionais** são aqueles associados à possibilidade de perdas resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e atos terroristas.
- **Riscos Tecnológicos e da Informação** são aqueles associados a ataques cibernéticos, tentativas de comprometer a confidencialidade, integridade ou disponibilidade de dados ou sistemas computacionais, assim como falhas, indisponibilidade ou obsolescência de equipamentos e instalações, de sistemas informatizados de controle, comunicação, logística e gestão operacional, que prejudiquem ou impossibilitem a continuidade das atividades regulares da organização. Também podem estar associados à perda, uso indevido, acesso ou divulgação não autorizada de informações ou dados pessoais de partes interessadas, internas ou externas, podendo ameaçar os negócios ou prejudicar a imagem da Companhia.

Além disso, os riscos podem também ser classificados, não de forma obrigatória, aos Temas Materiais ESG da Companhia. As classificações desta natureza podem ser:

- **Riscos de Transição** são aqueles relacionados às mudanças regulatórias, tecnológicas, de mercado e reputacionais decorrentes da transição para uma economia de baixo carbono. Inclui fatores como precificação de carbono, novas legislações ambientais e mudanças nas preferências dos consumidores e investidores.
- **Riscos Emergentes** são aqueles recém-identificados que podem impactar os negócios da Companhia no longo prazo e, em alguns casos, já apresentam efeitos iniciais. Diferentemente de outros riscos, eles são inéditos e sem precedentes, o que implica uma maior incerteza e falta de preparo para sua gestão.
- **Riscos Físicos** são aqueles relacionados aos Impactos diretos das mudanças climáticas nas operações, ativos e cadeias produtivas. Pode ser agudo (eventos extremos como tempestades e secas) ou crônico (mudanças

graduais como aumento da temperatura e alteração nos padrões de precipitação).

4.3. Papéis e responsabilidades

A Companhia possui uma área específica de Gestão de Riscos e atua juntamente com a Diretoria de Gestão de Riscos, Controles Internos e Auditoria Interna com apoio da Vice-Presidência Financeira e de Relações com o Investidor e do Comitê de Auditoria conforme imagem abaixo:

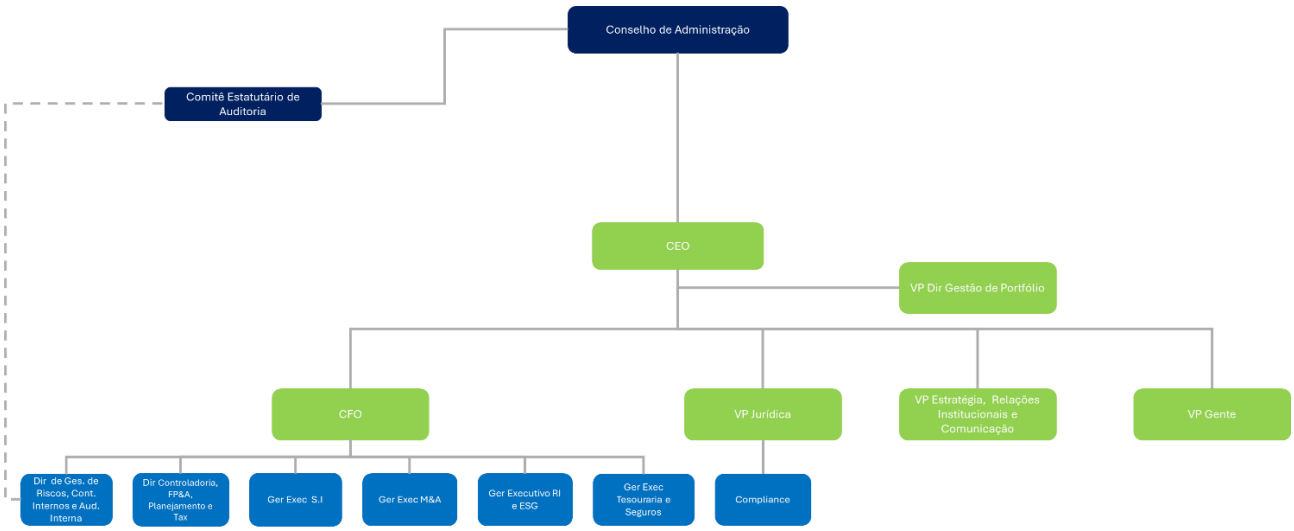

Figura 3 - Estrutura Cosan

4.3.1. Conselho de Administração

- Aprovar a estratégia adotada para a Gestão de Riscos da Companhia;
- Aprovar a Política de Gerenciamento de Riscos e acompanhar sua implementação;
- Aprovar, a cada 3 (três) ciclos de gestão ou a partir da ocorrência de eventos significativos, o Apetite aos Riscos da Companhia proposto pela Diretoria;
- Validar os riscos identificados da Companhia, assim como as suas respectivas Respostas, Ações Mitigatórias e controles, quando aplicável;
- Supervisionar o Processo de Gestão de Riscos a partir das informações apresentadas pela Diretoria e demais órgãos da governança; e

- Garantir a avaliação periódica do processo, políticas e sistemas de Gestão de Riscos.

4.3.2. Comitê de Auditoria

- Avaliar a Política de Gerenciamento de Riscos, sua metodologia e os procedimentos estabelecidos pela Companhia para esse processo e recomendar sua aprovação ao Conselho de Administração;
- Acompanhar e avaliar de forma periódica a gestão dos riscos bem como a execução de seu processo e seus resultados;
- Avaliar, anualmente, a efetividade e a suficiência dos sistemas de gestão dos riscos de negócios conforme esta Política e reportar estes resultados ao Conselho de Administração;
- Assessorar o Conselho de Administração na supervisão do Processo de Gestão de Riscos da Companhia; e
- Analisar e recomendar a aprovação do apetite a riscos e do Processo de Gestão dos Riscos ao Conselho de Administração.

4.3.3. Diretoria Executiva

- Recomendar, ao menos a cada 3 (três) ciclos de gestão ou a partir da ocorrência de eventos significativos, o grau de Apetite aos Riscos para aprovação do Conselho de Administração;
- Apontar ao Conselho de Administração os riscos envolvidos na implementação da estratégia da Companhia a cada ciclo de Planejamento Estratégico ou a partir da ocorrência de eventos significativos;
- Validar a Resposta e as Ações Mitigatórias respectivas a cada risco a partir da recomendação dos Donos de Riscos e da Gerência de Gestão de Riscos;
- Garantir a implantação da Gestão de Riscos em todas as áreas de negócio;
- Definir diretrizes, recursos e metas que garantam o bom funcionamento da Gestão de Riscos e promover a integração da Gestão de Riscos com os ciclos de gestão e planejamento;
- Avaliar, anualmente, a efetividade e a suficiência dos sistemas de gestão dos riscos de negócios conforme esta Política;

- Aprovar o Regimento Interno da Comissão de Riscos da Companhia, se aplicável; e
- Informar à área de Riscos e Controles Internos sobre a identificação de novos riscos ou eventos que sejam relevantes, e suas respectivas evoluções.

4.3.4. Comissão de Riscos Cosan (CRC)

- Identificar, revisar e gerir os riscos que possam afetar o negócio;
- Discutir com as lideranças o nível de exposição aos principais riscos e as ações tomadas para monitorar e controlar tais exposições; e
- Atuar na gestão e monitoramento do Apetite ao Risco.

4.3.5. Gerência de Gestão de Riscos

- Aplicar e gerenciar o processo de Gestão de Riscos, conforme Política de Gerenciamento de Riscos e aprovado pelo Conselho de Administração, bem como atender às recomendações e determinações do Comitê de Auditoria, Comissão de Riscos e/ou da Diretoria;
- Propor o Regimento Interno da Comissão de Riscos e garantir seu cumprimento e atualização, se aplicável;
- Desenvolver e aplicar a estratégia, a metodologia e a cultura de Gestão de Riscos, em conformidade com regulamentações vigentes e melhores práticas do mercado;
- Acompanhar e monitorar os riscos reportados pelas áreas, alocando-os na Matriz de Riscos e o status de implementação de suas respectivas Ações Mitigatórias;
- Apresentar e reportar à Diretoria, à Comissão de Riscos, ao Comitê de Auditoria e ao Conselho de Administração os riscos e o nível de exposição a riscos;
- Buscar as melhores práticas de mercado e realizar a conexão com os negócios;
- Ministrar treinamentos para disseminar a cultura e a metodologia utilizada na Gestão de Riscos;
- Assessorar as áreas na identificação, análise e avaliação do Impacto e Probabilidade dos riscos e suas respectivas Ações Mitigatórias;

- Submeter, anualmente, ao Comitê de Auditoria e à Diretoria Executiva uma avaliação sobre a efetividade e a suficiência dos sistemas de gestão dos riscos de negócios conforme esta Política;
- Identificar novos riscos ou eventos que sejam relevantes, e suas respectivas evoluções.

4.3.6. Áreas de Negócio (Donos de Risco)

- Identificar e gerir os riscos que possam afetar a Companhia e recomendar a Resposta/Tratamento;
- Informar à Diretoria de Gestão de Riscos, Controles Internos e Auditoria Interna sobre a identificação de um risco materializado ou potencial, seja de sua área ou de outras que venha a observar, bem como sugerir sua alocação na Matriz de Riscos;
- Sugerir alterações no mapeamento de riscos e validar todas as informações disponibilizadas, ao menos trimestralmente;
- Reportar, periodicamente, para a Gerência de Gestão de Riscos, o status das Ações Mitigatórias; e
- Quando solicitado, reportar e responder aos órgãos de governança (Diretoria, Comissão de Riscos, Comitê de Auditoria, Conselho de Administração etc.) os riscos sobre sua responsabilidade.

4.3.7. Gerência de Controles Internos

- Desenvolver e manter a metodologia e as boas práticas para avaliação dos riscos e do ambiente de controles internos dos processos de negócio, relacionados aos riscos de negócio;
- Assessorar a Diretoria e Áreas de Negócio na identificação preventiva de riscos, e sugerir medidas para sua prevenção e minimização;
- Gerir o processo de identificação e avaliação dos controles e os riscos inerentes aos seus respectivos processos a partir de critérios qualitativos e/ou quantitativos das Réguas de Impacto e de Probabilidade dos riscos;
- Estruturar o sistema de controles internos de forma compatível com as atividades da Companhia, garantindo as segregações e controles necessários para mitigar eventuais conflitos na condução de seus negócios;

- Reportar os resultados obtidos na avaliação do ambiente de controles internos aos donos dos processos, à Diretoria e ao Comitê de Auditoria e demais fóruns, quando aplicável.
- Alinhar a estrutura de controles internos aos objetivos dos processos da Companhia, aos normativos internos, às estratégias do negócio, à complexidade e aos riscos das operações;
- Apoiar gestores e colaboradores na elaboração de planos de ação necessários para a implementação do adequado ambiente de controles internos e mitigação dos riscos; e
- Conscientizar os gestores sobre a importância da gestão integrada de riscos e suas responsabilidades com a manutenção e preservação do ambiente de controles internos.

4.3.8. Auditoria Interna

- Fornecer opiniões independentes ao Comitê de Auditoria que avaliará a materialidade e reportará ao Conselho de Administração, sobre o Processo de Gestão de Riscos, a efetividade dos controles internos e a governança corporativa, recomendando ações de melhorias, quando aplicáveis; e
- Verificar a conformidade do Processo de Gestão de Riscos com as políticas e normas adotadas pela Companhia.

4.3.9. REFERÊNCIAS

- Estatuto Social - Cosan;
- Regimento Interno do Conselho de Administração - Cosan;
- Regimento Interno do Comitê de Auditoria - Cosan;
- Regimento Interno da Diretoria – Cosan.

HISTÓRICO DE REVISÃO E APROVAÇÃO

Esta Política foi aprovada pelo Conselho de Administração em 23 de maio de 2025 após avaliação do Comitê de Auditoria Estatutário conforme previsto.