Gestão de Riscos de Negócio

Política

NEXA
LISTED
NYSE

Summary

1. OBJETIVO

O objetivo desta política é estabelecer diretrizes para o processo de Gestão de Riscos Corporativos (ERM) na Nexa Resources S.A. ("Nexa" ou a "Empresa"). Ela define as responsabilidades de todos os participantes no processo de ERM, incluindo a identificação, avaliação, tratamento, monitoramento e comunicação dos Riscos. Esta política tem como objetivo integrar as considerações de Risco na tomada de decisões estratégicas da Empresa.

2. ABRANGÊNCIA

Esta política se aplica à Nexa, seus contratados e todas as subsidiárias e ativos que são de propriedade, controlados ou operados pela Nexa, direta ou indiretamente, em todo o mundo.

3. REFERENCES

- COSO ERM
- ISO 31000: 2018 Diretrizes de Gestão de Risco
- Estatuto do Comitê de Risco
- Manual de ERM da Nexa
- Regras Internas do Conselho de Administração
- Estatutos do Comitê de Auditoria, Comitê de Finanças, Comitê de
- Remuneração, Nomeação e Governança, e Comitê de Sustentabilidade
- Projetos de Capital
- Regras Internas do Comitê de Gestão (ManCo)
- Política de Riscos Financeiros da Nexa

4. DEFINITIONS

Apetite ao Risco: Os tipos e o nível de Risco que a Empresa está disposta a assumir em busca de valor.

Área de Risco: Área da Nexa responsável por coordenar o processo de ERM da Nexa e garantir o fluxo correto de informações e relatórios de Risco dentro da Empresa.

Categorias de Risco: Taxonomia de Risco utilizada para melhorar a gestão integrada de Riscos, bem como para auxiliar a Empresa na determinação de seu Apetite.

Controle Interno: Processo realizado pelo Conselho de Administração, Diretores Executivos e colaboradores da Empresa, considerando políticas, procedimentos, atividades e mecanismos destinados a proporcionar uma garantia razoável quanto ao alcance dos objetivos empresariais por meio da eficácia e eficiência operacional, confiabilidade dos relatórios financeiros e conformidade com leis, regulamentos e políticas.

Controles: Atividades que fazem parte das operações regulares da organização, realizadas para mitigar o Impacto ou a Probabilidade de um Risco.

Diretores Executivos: Coletivamente, o diretor-presidente e todos os diretores.

Donos de Riscos: Indivíduos responsáveis por gerenciar Riscos específicos em suas unidades / áreas.

Fatores de Risco: Fatores que contribuem para que o Risco eventualmente se materialize. O mesmo Risco pode conter um ou mais fatores relacionados.

Gestão de Riscos Corporativos ("ERM"): Processo que tem o objetivo de identificar eventos potenciais que podem afetar a capacidade da Empresa de alcançar seus objetivos estratégicos e definir e implementar ações para gerenciá-los. A ERM inclui a cultura, capacidades e práticas, integradas com a definição de estratégias e seu desempenho, nas quais as organizações confiam para gerenciar Riscos na criação, preservação e realização de valor.

Impacto: O resultado ou efeito de um Risco. Pode haver uma variedade de Impactos possíveis associados a um Risco. O Impacto do Risco pode ser positivo ou negativo em relação à estratégia ou aos objetivos empresariais da entidade.

Matriz de Riscos: Diagrama elaborado com base na análise geral dos Riscos e na avaliação própria da gestão, considerando o Impacto e a Probabilidade dos Riscos.

Modelo de Governança de Riscos: Processos e atividades que a Nexa segue para gerenciar os Riscos.

Plano de Ação: É uma ação temporária e específica com um prazo definido para sua implementação. Projetado para abordar uma deficiência na gestão de Riscos ou implementar novos Controles. Seu propósito é fechar lacunas, melhorar ou reforçar o controle existente. O Plano de Ação deve ter uma pessoa responsável e uma data de conclusão.

Probabilidade: A possibilidade de que um Risco ocorra.

Registro de Riscos: Registro de informações dos Riscos identificados.

Risco: Qualquer evento potencial que possa afetar a capacidade da Empresa de alcançar seus objetivos e seus planos estratégicos de negócios.

Risco Inerente: Nível intrínseco de Risco para o negócio ou atividade, sem considerar a implementação de Controles mitigadores ou planos de ação.

Risco Residual: Nível remanescente de Risco após considerar todos os Controles e Planos de Ação implementados para mitigar os Riscos Inerentes.

Riscos Aceitos: Riscos que a Empresa opta por não abordar ativamente com novas medidas porque os Controles existentes são considerados suficientes e, com base na avaliação, não é possível nem razoável implementar ações adicionais. Esses Riscos serão aceitos em seu nível atual de exposição, com monitoramento contínuo para garantir que não se transformem em Riscos que exijam mitigação ou intervenção adicional.

Riscos Emergentes: Riscos que ainda não se manifestaram totalmente, mas que podem ter um Impacto significativo na realização dos objetivos estratégicos da organização e potencialmente alterar seu perfil de Risco no futuro. Esses Riscos podem surgir de mudanças tecnológicas, sociais, regulatórias e outras no contexto empresarial.

Riscos Priorizados: Riscos relacionados à estratégia que são relevantes para a Empresa, seja para alcançar objetivos específicos, que estão fora do Apetite de Risco definido, classificados como “Alto” ou “Crítico”.

5. RESPONSABILIDADES

5.1 Conselho de Administração

As principais responsabilidades de supervisão em relação a ERM da Nexa são:

- Aprovar a orientação geral dos negócios da Empresa, sua missão, seus objetivos estratégicos e diretrizes, e garantir que os Diretores Executivos cumpram essa missão, objetivos estratégicos e diretrizes, levando em conta os Riscos e o Apetite da Empresa e de acordo com a recomendação dos Comitês do Conselho de Administração.
- Revisar e aprovar a declaração de Apetite de Risco da Empresa e alterações a ela quando aplicável.
- Aprovar o orçamento e o plano estratégico que levam em conta os Riscos e o Apetite da Empresa.
- Aprovar a política de ERM da Nexa e monitorar a conformidade com essa política.
- Supervisionar os Riscos Priorizados e a exposição ao Risco da Empresa.

5.2 Comitês do Conselho

As principais responsabilidades de supervisão dos Comitês de Auditoria; Finanças; Remuneração, Nomeação e Governança; e Sustentabilidade e Projetos de Capital em relação ao ERM da Nexa são:

- Apoiar o Conselho na supervisão de ERM da Nexa em questões relacionadas às responsabilidades de cada Comitê, de acordo com os estatutos de cada comitê.
- Discutir os Riscos que serão classificados como Riscos Aceitos e submetê-los para aprovação do Conselho.
- Discutir os Riscos Priorizados e como eles são tratados e monitorados, acompanhando seus Planos de Ação.
- Monitorar os processos ou Controles da Empresa, incluindo as Ações de Mitigação que estão sendo tomadas.
- Reportar regularmente ao Conselho de Administração sua supervisão do processo de ERM.

Além das responsabilidades listadas acima, o **Comitê de Auditoria também assume as seguintes atribuições**:

- Monitorar os Controles e processos de gestão de Riscos da Empresa, de acordo com a Política de ERM.
- Compreender a estrutura de avaliação de Risco da Empresa, incluindo diretrizes e políticas adequadas para governar o processo
- Avaliar a estrutura organizacional e as atividades do processo de gestão de Riscos da Empresa.
- Avaliar a implementação e manutenção das estruturas e políticas de gestão de Riscos pela administração.

5.3 Comitê de Gestão

As principais atribuições em relação a ERM da Nexa são:

- Adotar um processo de planejamento estratégico e, anualmente, propor ao Conselho o orçamento e o plano estratégico da Empresa que considerem os Riscos do negócio.
- Promover e assegurar a conformidade com as políticas da Empresa, bem como com a política de ERM da Empresa.
- Propor o Apetite de Risco e apresentar ao Conselho para revisão e aprovação, conforme a recomendação dos comitês, quando aplicável.
- Recomendar os Riscos que serão classificados como Riscos Aceitos e submetê-los para a aprovação dos Comitês do Conselho.
- Recomendar os Riscos que serão classificados como Riscos Priorizados e submetê-los para a aprovação dos Comitês do Conselho.

- Executar e coordenar o processo de gestão de Riscos, assegurando a aplicação da metodologia definida, auxiliando na supervisão dos Riscos, no monitoramento do Plano de Ação e dos Riscos Priorizados.
- Individualmente, cada Diretor Executivo deve realizar periodicamente reuniões com suas respectivas equipes para monitorar os Riscos identificados e os Planos de Ação para responder a esses Riscos e aos Controles associados.

5.4 Comitê de Risco

O Comitê de Risco ("RiskCo") é um comitê permanente do Comitê de Gestão, com a principal finalidade de auxiliá-los no cumprimento de suas responsabilidades de implementação e execução em relação a:

- Monitorar e gerenciar os Riscos da Empresa que podem afetar a realização dos objetivos da Empresa.
- Fornecer supervisão em todas as Categorias de Risco e aprimorar a cultura de Risco.
- Aprovar e supervisionar os processos utilizados para identificar, avaliar e gerenciar Riscos.
- Emitir recomendações ao Comitê de Gestão relacionadas a) ao desempenho dos Controles de Risco, b) ao cumprimento dos planos de ação e c) às estratégias de resposta a Riscos, entre outras.

5.5 Área de Auditoria Interna, Controles Internos, Compliance e Linha Ética

As principais atribuições em relação ao ERM da Nexa são:

- Auditoria Interna: A equipe de Auditoria Interna incorpora a Matriz de Riscos de ERM como insumo para seu planejamento anual de auditoria, garantindo uma abordagem baseada em Riscos. Eles identificam Riscos durante os processos de auditoria e comunicam observações significativas para a área de ERM. Além disso, avaliam a eficácia dos processos de gestão de Riscos, garantindo a conformidade com as políticas estabelecidas, e fornecem recomendações para melhorar a mitigação de Riscos.

- Controles Internos: A equipe de Controles Internos aprimora o ambiente de controle para garantir que os Controles mitiguem efetivamente os Riscos identificados e colabora com a área de ERM para compartilhar o status da eficácia dos Controles implementados.

- Compliance: A equipe de Compliance integra a Matriz de Riscos de ERM em seu planejamento anual para abordar os principais Riscos, garantindo a aderência a todos os requisitos de compliance relevantes. Eles também investigam possíveis violações de compliance e comunicam quaisquer Riscos identificados à área de ERM.

- Linha Ética: A equipe de Linha Ética fornece um mecanismo confidencial e seguro para os funcionários relatarem preocupações éticas, má conduta ou Riscos potenciais. Eles monitoram e investigam os relatos recebidos através da linha ética, comunicam quaisquer Riscos identificados ou questões éticas à área de ERM para inclusão no processo de avaliação de Risco, e promovem a conscientização sobre padrões éticos e a importância de relatar dentro da organização.

5.6 Donos de Riscos

As principais atribuições em relação ao ERM da Nexa são:

- Liderar os esforços de gestão de Riscos, garantindo monitoramento contínuo e atualizações.
- Promover a participação efetiva e uma abordagem multidisciplinar nas avaliações de Riscos.

- Garantir a definição e implementação de medidas de resposta em coordenação com os Responsáveis pelos Controles e Responsáveis pelos Planos de Ação.
- Monitorar a evolução dos Riscos e o status das medidas de resposta, reportando o progresso à Equipe de Riscos e outros principais interessados.
- Garantir que as ações implementadas sejam eficazes e alinhadas com os objetivos estratégicos da Nexa.
- Comunicar os Riscos Emergentes à Área de Riscos para incluí-los na Matriz de Riscos.

5.7 Pontos Focais

As principais atribuições em relação ao ERM da Nexa são:

- Auxiliar a área de ERM no Processo de Avaliação de Risco em sua unidade ou área corporativa.
- Ajudar a área de ERM a entrar em contato com os Responsáveis por Riscos e especialistas.
- Apoiar o monitoramento do cumprimento dos Controles e planos de ação.
- Participar de reuniões de acompanhamento e monitoramento.
- Promover a comunicação com a equipe de ERM.
- Incentivar a participação em sessões de treinamento de ERM.

5.8 Área de Riscos

As principais atribuições em relação a ERM da Nexa são:

- Desenvolver a estratégia, aplicar a metodologia e promover a cultura de ERM, de acordo com as regulamentações vigentes e as melhores práticas de mercado.
- Monitorar os Riscos reportados pelas unidades e áreas corporativas.
- Monitorar a implementação dos Planos de Ação desenvolvidos para mitigar os Impactos dos Riscos identificados.
- Reportar o nível de exposição da Nexa aos Riscos identificados aos Diretores Executivos, ao respectivo Comitê, ao Comitê de Auditoria e ao Conselho de Administração, quando aplicáve.
- Monitorar tendências de mercado e sua conexão com o negócio e possíveis Impactos para a Nexa.
- Ministrar treinamentos para disseminar a cultura e a metodologia de ERM.
- Discutir a Matriz de Riscos com as áreas de Auditoria Interna, Controles Internos, Compliance e Linha Ética.

6. ESTRUTURA DE GOVERNANÇA DE RISCOS

O Modelo de Estrutura de Governança de Riscos da Nexa compreende três níveis: (i) um **nível executivo**, que inclui uma visão executiva clara na consolidação de informações de Risco para monitoramento pelo Conselho de Administração; (ii) um **nível tático**, onde os líderes têm fóruns formais de discussão; e, (iii) um **nível transacional**, onde há uma integração metodológica para que as informações estejam alinhadas. Através desse modelo, há discussões estruturadas sobre Riscos e suas priorizações, juntamente com relatórios periódicos disponibilizados pelos Donos de Riscos com o apoio da área de ERM. Esses três níveis são detalhados abaixo:

- ***Nível Executivo***, O nível executivo aborda os Riscos estratégicos e priorizados que podem impactar significativamente os objetivos de longo prazo e a viabilidade da empresa. Os principais objetivos deste nível são fornecer à alta administração uma visão consolidada dos Riscos mais significativos e estabelecer alinhamento entre a gestão de Riscos e os objetivos estratégicos da organização.

Este nível abrange o Conselho de Administração, o Comitê de Gestão, o Comitê de Risco e os Vice-Presidentes Corporativos e Diretores Executivos (quando aplicável), que são responsáveis por supervisionar a política de Gestão de Riscos Corporativos (ERM), definir o apetite de Risco e garantir a eficácia dos processos de gestão de Riscos.

- ***Nível Tático,*** O nível tático aborda os Riscos identificados pelas áreas de negócios e unidades operacionais, tendo discussões estruturadas sobre Riscos Priorizados e quais devem ser escalados para o nível Executivo. Os principais objetivos deste nível são traduzir as políticas estratégicas em ações concretas e garantir que as estratégias definidas pela alta administração sejam executadas corretamente.

  Este nível inclui Vice-Presidentes Corporativos, Gerentes Gerais de Unidades Operacionais e Gerentes Gerais de Áreas Corporativas, que supervisionam a implementação de estratégias de mitigação, monitoram os planos de ação e tomam decisões informadas sobre quais Riscos escalar.

- ***Nível Transacional,*** Nível operacional aborda os Riscos que surgem nos processos operacionais diários, incluindo a saúde e segurança do pessoal. O principal objetivo deste nível é gerenciar os Riscos que surgem das atividades diárias e processos operacionais, impedindo que eles escalem para níveis superiores da organização. Este nível está focado em lidar com eventos que podem comprometer os processos de produção, bem como a saúde e segurança dos envolvidos. Este nível é composto por todos os funcionários relacionados com a primeira fase do processo de ERM e é uma atividade recorrente.

  Este nível envolve Gerentes Gerais de Unidades Operacionais, Gerentes de Área dentro das Unidades e Líderes de Processo que participam da fase inicial do processo de ERM, focando na identificação e relato de Riscos operacionais e de segurança de forma recorrente.

7. PROCESSOS DE GESTÃO DE RISCOS

Nosso processo geral para avaliar e gerenciar Riscos é consistente com as estruturas COSO ERM e ISO 31000. Ele inclui práticas sistemáticas e comuns dentro da Nexa e suas subsidiárias para estabelecer o contexto de Risco e comunicar, discutir, identificar, avaliar, tratar, monitorar, registrar e relatar os Riscos.

O processo de ERM na Nexa inclui Riscos de diferentes naturezas: Estratégicos, Financeiros, Operacionais e de Compliance

ERM também deve se relacionar com outros processos de gestão. ERM se torna mais efetivo ao integrar práticas de ERM com atividades de negócios e entender como o Risco potencialmente afeta a entidade como um todo. Dessa forma, como parte do processo de ERM, juntamente com todas as áreas e unidades de negócio, mais Riscos operacionais e relacionados aos projetos são identificados para ajudar a Empresa a manter seus Riscos dentro de seu Apetite de Risco.

Todos os Riscos identificados são, no mínimo, revisados anualmente e atualizados, se necessário. Além disso, as áreas de negócios e unidades da Nexa têm a autonomia para incluir Riscos Emergentes a qualquer momento, fora da fase anual de identificação do processo de ERM, conforme novas situações possam surgir ou mudanças possam ocorrer.

As principais etapas do processo de gestão de Riscos são as seguintes:

7.1 Identificação do Risco

A etapa de identificação de Riscos envolve reconhecer e documentar sistematicamente os Riscos que podem potencialmente afetar a realização dos objetivos da organização. Isso inclui identificar Riscos,

Fatores de Risco e seus Impactos potenciais. Os Riscos são classificados de acordo com a taxonomia de Risco definida, o que ajuda na categorização e organização deles para uma análise posterior.

7.2 Análise de Risco

Durante a fase de análise de Risco, os Controles existentes são mapeados e os responsáveis por Riscos são designados. Esta etapa é crucial para entender o ambiente de Risco atual e identificar onde Controles ou intervenções adicionais podem ser necessários.

7.3 Avaliação de Risco

Avaliar os Riscos com base em seu Impacto e Probabilidade.

- *Impacto:* considera as consequências de sua materialização, que são avaliadas em sete (7) dimensões: financeira, ambiental, saúde e segurança, social e direitos humanos, legal e compliance, reputacional e cibernética e segurança da informação. O Impacto é classificado em cinco (5) níveis: mínimo, menor, moderado, maior e extremo.

- *Probalidade*: é a possibilidade de sua ocorrência determinada e avaliada em cinco (5) níveis: remoto, improvável, ocasional, provável e muito provável.

Como resultado da avaliação, os Riscos são classificados entre cinco (5) níveis: Muito Baixo, Baixo, Médio, Alto ou Crítico.

7.4 Apetite de Risco

O Apetite de Risco é o grau de Risco que a Empresa está disposta a assumir na busca de valor ou para alcançar um nível desejado de retorno ou crescimento – resultado. Ele busca um equilíbrio entre Risco e recompensa e pode variar ao longo do tempo e da área de trabalho. O Apetite de Risco deve ser proposto pelo Comitê de Gestão e aprovado pelo Conselho de Administração, sendo comunicado para toda a organização.

O Apetite de Risco da Nexa faz parte do seu processo geral de Riscos, e seus principais objetivos são descritos da seguinte forma:

- Criar transparência e consistência para o tipo e nível de Riscos que a Empresa está disposta a assumir para alcançar objetivos estratégicos e operacionais.
- Promover o comportamento em relação aos Riscos e definir o tom para a cultura de Riscos na Empresa.
- Fornecer um ponto de referência para análise comparativa da tomada de Riscos e das estratégias de resposta necessárias.
- Eliminar a aversão excessiva ao Risco, articulando a preferência pela tomada de Riscos.
- Definir limiares para a tomada de Riscos que otimizem Risco e recompensa.
- Ajudar a integrar a tomada de Riscos e a gestão de desempenho.
- Auxiliar na definição de métricas de Risco que apoiem as operações diárias de negócios.

7.5 Priorização de Riscos

Com base na avaliação e no apetite, os Riscos são priorizados para definir as opções de tratamento apropriadas.

7.6 Tratamento de Riscos

Riscos classificados como "Altos" ou "Críticos" e Riscos "Fora do Apetite" devem ser priorizados para mitigar seu Impacto e/ou Probabilidade. O desenvolvimento de planos de ação para reduzir os níveis de Risco é obrigatório.

O propósito do tratamento de Riscos é selecionar e implementar opções para abordar os Riscos, envolvendo a seleção, formalização e implementação de planos de ação. Essas opções podem incluir eliminar a fonte do Risco, alterar sua Probabilidade, aproveitar oportunidades, modificar suas consequências, compartilhar o Risco ou reter o Risco. O tratamento mais adequado envolve equilibrar os benefícios potenciais contra os custos, esforços ou desvantagens da implementação.

Donos de Riscos desempenham um papel fundamental no desenvolvimento de planos de ação, especificando recursos necessários, indivíduos responsáveis e cronogramas. A Área de Riscos fornece orientação e suporte metodológico aos Donos de Riscos. Os Riscos que não podem ser mitigados para reduzir a exposição da Nexa devem ser discutidos no nível apropriado para aprovação como Riscos Aceitos, considerando o Apetite de Risco da Nexa.

7.7 Monitoramento de Risco

O monitoramento dos planos de ação, a avaliação de mudanças no nível de Impacto ou Probabilidade do Risco, devido a fatores internos ou externos, deve ser realizado regularmente.

7.8 Relatórios

A Área de Riscos é responsável por estruturar as ações necessárias e os materiais relevantes ao que deve ser apresentado em cada nível de governança, considerando a hierarquia da informação. Esses materiais devem ser atualizados de acordo com a frequência dos fóruns aplicáveis.