POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

Vibra Energia S.A.

Índice

1 ATA DE APROVAÇÃO

ATA CA 879, de 15-08-2022 - Pauta nº 33.

2 ABRANGÊNCIA

Aplica-se à Companhia e recomenda-se a sua adoção pelas subsidiárias integrais e sociedades controladas.

No caso das sociedades coligadas e das controladas em conjunto, a norma tem caráter indicativo e contribui para o alinhamento da gestão de riscos nas empresas vinculadas.

3 PRINCÍPIOS

3.1. A vida deve ser respeitada em toda sua diversidade e os direitos, as obrigações, as instalações, os processos, as informações, a reputação e a imagem da Companhia resguardados contra ameaças decorrentes de ações intencionais ou não.

3.2. A gestão de riscos insere-se no compromisso da Companhia de atuar com integridade, conforme seus próprios princípios e de acordo com as normas vigentes.

3.3. A gestão de riscos deve estar alinhada e coerente com o Plano de Negócios e, sobretudo, com os objetivos estratégicos da Companhia.

3.4. Os riscos devem ser considerados na tomada de decisões e a sua gestão deve ser realizada de maneira integrada, permeando todas as áreas da companhia.

3.5. As ações de resposta devem considerar as possíveis consequências cumulativas de longo prazo e de longo alcance dos riscos e devem ser priorizadas para preservar valor aos acionistas e para a continuidade dos negócios

4 DIRETRIZES

4.1. Fortalecer o gerenciamento de riscos como base do Sistema de Gestão da Integridade da Companhia.

4.2. Aproveitar as oportunidades e antecipar-se às ameaças que afetam nossos objetivos estratégicos, econômico-financeiros, operacionais ou de conformidade.

4.3. Promover a uniformidade de conceitos e a integração metodológica na identificação, na análise, na avaliação e no tratamento dos riscos como forma de melhorar a confiabilidade das informações e a transparência de todo o processo.

4.4. Gerenciar, de forma proativa e abrangente, os riscos associados aos processos de negócio, de gestão e de suporte de forma a mantê-los em um nível aceitável de exposição.

4.5. Alinhar as ações de gerenciamento de riscos com as ações das unidades organizacionais responsáveis por controles internos e pela auditoria interna da Companhia, nos termos do Modelo das 3 Linhas.

4.6. Fortalecer a autonomia no processo de gerenciamento dos riscos e a segregação de funções entre os tomadores de riscos e os responsáveis pelo seu monitoramento.

4.7. Permitir a administradores, investidores e demais públicos de interesse, um fluxo contínuo e transparente de informações associadas aos principais riscos e seu processo de gestão na Companhia, respeitado o grau de sigilo das informações, políticas e demais normas internas de segurança empresarial.

4.8. Possibilitar aos empregados e às empresas prestadoras de serviços (através de contratos) a capacitação para o gerenciamento de riscos de forma contínua e adequada às suas atribuições.

4.9. Aprimorar o monitoramento e a análise crítica do próprio gerenciamento de riscos como parte integrante de um processo contínuo de melhoria da governança corporativa.

4.10. Monitorar os riscos considerados de impacto Muito Alto, cuja materialização possa ocasionar a interrupção significativa do negócio, independentemente da probabilidade.

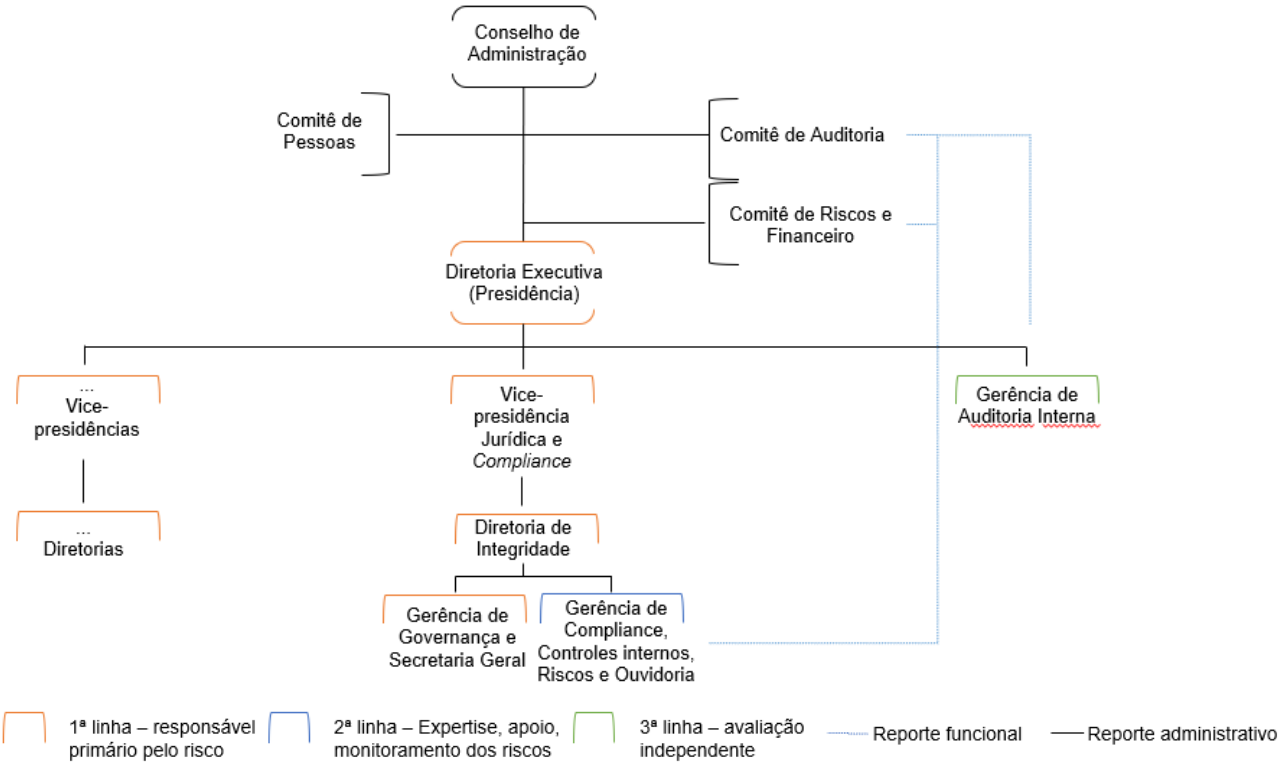
5 CONCEITOS (DEFINIÇÕES E PRECEITOS METODOLÓGICOS)

- **Abordagem Top down**: Consiste na identificação, na avaliação e no monitoramento dos principais riscos que afetam os objetivos e direcionadores estratégicos.
- **Abordagem bottom-up**: Consiste na identificação, na avaliação e no monitoramento dos riscos que afetam os processos relacionados na cadeia de valor da VIBRA.
- **Análise de Riscos**: Consiste em compreender a natureza do risco e suas características e determinar o seu potencial de influenciar, positiva ou negativamente, a realização de objetivos estabelecidos pela Companhia (Guia 73 - ISO - Adaptado).
- **Apetite a riscos**: É a diretriz de o quanto de risco a companhia está disposta a incorrer, de forma qualitativa, para atender seus objetivos estratégicos.
- **Auditoria Interna**: A auditoria interna é uma atividade independente e objetiva de avaliação com abordagem sistemática e disciplinada à avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, controle e governança.” (Instituto dos Auditores Internos – IIA Brasil - adaptado)
- **Avaliação de Riscos**: Consiste na identificação e na análise dos eventos que, potencialmente, comprometem o atendimento dos objetivos da Companhia.
- **Catálogo de riscos**: É a base de informações que concentra e padroniza as categorias e subcategorias de riscos.
- **Dono do risco**: Tem como responsabilidade a gestão, como executores do processo de gerenciamento de riscos e dos sistemas de controles internos da organização, representando a 1º linha no modelo das 3 linhas.
- **Estrutura de Gerenciamento de Riscos**: Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua do gerenciamento de riscos através de toda a organização (Guia 73 - ISO).
- **Evento**: Ocorrência ou mudança em um conjunto específico de circunstâncias. (ISO 31.000/2018).
- **Gerenciamento de Riscos**: Conjunto de atividades coordenadas para direcionar e controlar uma organização ou área de negócio em relação aos seus riscos (ISO - Adaptado).
- **Gestão de crises**: Gerenciamento de comunicações, externas e internas, e das atividades da alta administração que estão sendo tomadas para reverter os impactos do desastre. Inclui a definição de métricas para caracterizar quais cenários constituem uma crise e mecanismos de resposta necessários.” (GTAG - Gestão de Continuidade de Negócios - Adaptado)
- **Governança Corporativa**: É o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (Código das Melhores Práticas de Governança Corporativa do IBGC – 5° Edição).
- **Identificação de Riscos**: Consiste em identificar, compreender o contexto externo e interno e descrever os riscos que podem influenciar e impactar os objetivos e atividades da organização (ISO 31.000/2018).
- **Indicador-chave de risco**: Utilizado para evidenciar e mensurar certos eventos ou condições propensas a desencadear eventos de riscos que surgiram ou ocorreram” (The Institute of Internal Auditors – The IIA Global - livre tradução e adaptado).

- **Impacto**: Resultado ou efeito de um evento.
- **Incerteza**: É o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade (Guia 73 - ISO).
- **Matriz de Risco**: É definida e preenchida a partir da combinação entre a probabilidade e o impacto dos riscos, propiciando comparações entre os eventos de risco potencial e permitindo a priorização para tratamento dos riscos.
- **Modelo das 3 linhas**: Ajuda as organizações a identificar estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos (IIA - Instituto dos auditores internos, 2020).
- **Monitoramento de Riscos**: Verificação, supervisão e observação crítica, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado (Guia 73 - ISO).
- **Objetivo**: Declarações concisas sobre situações futuras a serem alcançadas. Os objetivos podem se referir a diferentes aspectos empresariais tais como negócios, segurança e meio ambiente e financeiro. Podem também ser classificados em diferentes categorias, tais como estratégica, conformidade e operacional (Guia 73 - ISO - Adaptado).
- **Oportunidade**: Situação ou evento que influencie favoravelmente a realização dos objetivos previamente estabelecidos pela Companhia (COSO-ERM).
- **Plano de Continuidade dos Negócios**: Plano de continuidade para retomar as atividades operacionais normais o mais rápido possível, com o mínimo de interrupção, depois de um evento catastrófico (The Institute of Internal Auditors – The IIA Global - livre tradução e adaptado).
- **Probabilidade**: Representa a possibilidade de que um determinado evento ocorra (COSO-ERM).
- **Risco**: É o efeito das incertezas nos objetivos (ISO 31.000/2018).
- **Risco Básico**: Risco decorrente do desdobramento do Risco Empresarial, a ser realizado conforme critério definido pelo dono do risco associado ao Risco Empresarial.
- **Risco Empresarial**: Abrange os principais eventos de risco de negócio, operacional, cibernético, sustentabilidade, financeiro, regulatório, que impactam as atividades ou o atendimento aos objetivos da Companhia.
- **Severidade**: É o resultado da combinação da probabilidade e do impacto dos riscos (COSO - ERM 2017 - Adaptado).
- **Tolerância a Risco**: É a quantificação de risco, alinhado ao apetite a risco, que a companhia está disposta a tolerar para atender seus objetivos estratégicos. Pode ser entendido também como uma variação aceitável do apetite a riscos medido com base nos indicadores-chave de risco.
- **Tratamento dos Riscos**: Posteriormente à avaliação de riscos, é definido o tratamento que será dado aos riscos e como estes devem ser monitorados e comunicados às diversas partes envolvidas. Tratar os riscos consiste, basicamente, em decidir entre aceitá-lo, mitigá-lo, transferi-lo ou eliminá-lo. A decisão depende principalmente do grau de apetite ao risco da Companhia.

6 COMPETÊNCIAS E RESPONSABILIDADES

Escala	Proposta de tratamento (Aceitar/mitigar/transferir/eliminar)	Alçada de aprovação	Informados
Muito Alto	Diretoria Executiva	Conselho de Administração, precedida de avaliação no CAE	Comitê de Riscos e Financeiro
Alto	Vice-Presidente	Diretoria Executiva	Comitê de Auditoria Estatutário, Conselho de Administração e Comitê de Riscos e Financeiro
Médio	Gerente Executivo ou Diretor	Vice-Presidente	Diretoria Executiva
Baixo	Gerente/Coordenador	Gerente Executivo ou Diretor	Vice-Presidente
Muito Baixo			



6.1 Do Conselho de Administração (CA)

- Aprovar o apetite e indicadores de tolerância a risco da Vibra proposto pela Diretoria Executiva.
- Acompanhar de forma sistemática a gestão de riscos.
- Aprovar a Política e a Metodologia de Gestão de Riscos Corporativos, assim como suas revisões.
- Aprovar os riscos com severidade muito alta, após avaliação realizada pelo CAE.

6.2 Do Comitê de Auditoria Estatutário (CAE)

- Assessorar o Conselho de Administração no estabelecimento de políticas globais relativas à gestão de riscos, assim como quaisquer revisões submetidas à sua aprovação.
- Avaliar e monitorar as exposições de risco da Companhia.
- Supervisionar a estrutura e as atividades de gerenciamento de riscos pela gestão da organização, em linha com as diretrizes e políticas estabelecidas pelo conselho de administração.
- Avaliar, monitorar e emitir recomendações sobre riscos corporativos.
- Apreciar a metodologia de gestão de riscos corporativo para aprovação do Conselho de Administração.
- Revisar e monitorar os indicadores de tolerância a riscos propostos pela Diretoria Executiva para aprovação do Conselho de Administração.
- Revisar a declaração do apetite a riscos proposta pela Diretoria Executiva para aprovação do Conselho de Administração.

6.3 Do Comitê de Riscos e Financeiro (CORF)

- Assessorar o Conselho de Administração em assuntos estratégicos e financeiros, tais como a análise e a emissão de recomendações sobre os riscos concernentes à gestão financeira e demais diretrizes definidas em seu regimento interno.
- Avaliar, monitorar e emitir recomendações sobre riscos externos prospectivos associados ao planejamento estratégico .

6.4 Da Auditoria Interna

- Avaliar, de forma sistemática, o processo de gerenciamento de riscos e recomendar melhorias.

6.5 Da Diretoria Executiva (DE)

- Propor o apetite a risco da Vibra Energia, principalmente, mas não limitado, ao momento da definição do plano estratégico (PE) e do Business Plan (BP).
- Propor os indicadores de tolerância aos riscos bem como opinar sobre a necessidade de mudança/revisão.
- Possibilitar que as medidas necessárias para o alinhamento entre o apetite a risco e as estratégias da Vibra Energia sejam executadas e monitoradas continuamente.
- Monitorar as exposições de risco estratégicos e operacionais.
- Analisar a Política de Gestão de Riscos Corporativos, assim como suas revisões, submetendo-as a apreciação do Comitê de Auditoria Estatutário e aprovação do Conselho de Administração.
- Validar a avaliação dos riscos com os diretores e gestores e, quando a alçada de aprovação do tratamento do risco exigir, informar o Comitê de Auditoria Estatutário, o Comitê de Riscos e Financeiro e o Conselho de Administração.
- Avaliar o impacto e probabilidade de ocorrência dos riscos estratégicos e operacionais propostos pelos diretores e gestores.
- Elaborar proposta da declaração do apetite a risco bem como opinar sobre a necessidade de mudança/revisão.

6.6 Da área de Integridade responsável pela gestão dos riscos corporativos (ERM)

- Definir metodologia corporativa de gestão de riscos pautada em uma visão integrada e sistêmica que possibilite um ambiente de contínuo monitoramento dos riscos nos mais diversos níveis hierárquicos da empresa.
- Estimular a integração e capturar a sinergia das ações de gestão de riscos dentre as diversas unidades organizacionais, assim como dentre os demais processos de negócio, gestão e serviços corporativos.
- Disseminar conhecimentos em gerenciamento de riscos.
- Elaborar, mensurar e reportar os indicadores de tolerância aos riscos, e as suas atualizações.
- Monitorar e reportar periodicamente à Diretoria Executiva, ao Comitê de Auditoria Estatutário, ao Comitê de Riscos e Financeiro e ao Conselho de Administração o efeito dos principais riscos nos resultados integrados da Vibra Energia.
- Avaliar a necessidade de tratamento aos riscos em desconformidade com o apetite a riscos.
- Propor, quando necessário, a responsabilização do dono do risco para eventual descumprimento de planos de ação oriundos das recomendações desta área e da Diretoria Executiva, no tocante a riscos.
- Monitorar e reportar a aderência ao apetite a riscos.
- Revisar as categorias (nível 1) e riscos empresariais (nível 2) a cada dois anos e/ou a qualquer mudança relevante na estrutura da Companhia e/ou revisão do planejamento estratégico.
- Elaborar matriz de riscos corporativos, com base nas fontes externas e internas de informação, bem como proceder às atualizações periódicas.
- Analisar, validar e comunicar a lista de riscos que afetam os objetivos e

direcionadores estratégicos (abordagem Top down) e de riscos que afetam os processos (abordagem Bottom-up).

6.7 Dos titulares da estrutura geral da companhia (Vice-Presidentes)

- Coordenar, promover e acompanhar as ações de gestão de risco na sua área de atuação.
- Contribuir, avaliar e validar a matriz de riscos, com o apoio da unidade organizacional responsável pela gestão dos riscos corporativos.
- Contribuir, avaliar e validar os indicadores de tolerância a riscos e os seus resultados, com o apoio da unidade organizacional responsável pela gestão dos riscos corporativos.
- Estabelecer e implementar protocolos de Gestão de Crise e planos de Continuidade de Negócio para os riscos sob sua responsabilidade, considerados como de impacto Muito Alto e Alto (severidade), e, para os demais riscos, sempre que aplicável. Tais protocolos e planos devem ser testados periódica e adequadamente, inclusive com simulações.

6.8 Dos titulares de unidades organizacionais (Diretores/Gestores)

- Identificar riscos preventivamente e fazer sua necessária gestão, avaliar a probabilidade de ocorrência e adotar medidas para sua prevenção e minimização, em consonância com essa política, com as diretrizes e com as normas corporativas de gestão de riscos, em articulação com a unidade organizacional responsável pela gestão dos riscos corporativos.
- Fornecer, tempestivamente, à unidade organizacional responsável pela gestão dos riscos corporativos todas as informações necessárias para a avaliação integrada dos riscos, o monitoramento e o reporte a Diretoria Executiva, ao Comitê de Auditoria Estatutário, ao Comitê de Riscos e Financeiro e ao Conselho de Administração.
- Identificar e contribuir com a elaboração dos indicadores de tolerância aos riscos apropriados aos seus processos operacionais.
- Fornecer os dados à unidade organizacional responsável pela gestão dos riscos corporativos para mensuração dos indicadores de tolerância aos riscos.
- Definir o tratamento dos riscos em desconformidade com o apetite a riscos, bem como cumprir os prazos estabelecidos nos planos de ação.