TÍTULO

GESTÃO DE RISCOS E OPORTUNIDADES EMPRESARIAIS (ERM)

1. OBJETIVO

A Política de Gestão de Riscos e Oportunidades Empresariais da ENGIE Brasil estabelece os princípios, diretrizes e responsabilidades para a gestão estruturada de riscos e oportunidades empresariais no âmbito das companhias.

O propósito da Gestão de Riscos e Oportunidades Empresariais – ERM é de continuamente manter e melhorar o valor, a reputação e a implementação da estratégia das companhias, encorajando uma tomada de risco razoável em termos legais, e que seja considerada aceitável e economicamente viável. O alcance desse objetivo requer o adequado conhecimento dos riscos aos quais as companhias estão expostas, bem como a capacidade de identificá-los, avaliá-los e gerenciá-los de forma estruturada. Busca-se, com isso, fortalecer a gestão de riscos e oportunidades empresariais como parte da cultura organizacional e contribuir para a resiliência, continuidade e a sustentabilidade dos negócios das companhias.

2. DEFINIÇÕES

2.1 ADMINISTRADORES
Membros do Comitê Executivo da ENGIE Brasil (COMEX), membros responsáveis pelas GBUs, Diretoria das empresas operacionais e, no caso de empresas listadas em bolsa de valores, o Conselho de Administração e outros órgãos de governança.

2.2 APETITE A RISCO
Grau de risco que as companhias estão dispostas a aceitar para alcance de seus objetivos estratégicos e resultados, servindo como referência para a tomada de decisão em todos os níveis.

2.3 BUSINESS PARTNER
Consultor interno que integra a gestão de riscos aos objetivos de negócio da Companhia, colaborando ativamente com líderes e gestores para identificar, avaliar e mitigar ameaças que possam surgir de mudanças estratégicas, novos projetos ou ambiente de negócios.

2.4 CATÁLOGO DE RISCOS
Documento que traz a relação dos principais riscos, organizada em famílias de risco e numerados para permitir a consolidação pelo controlador, ENGIE S.A.

2.5 COSO ERM - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION
Framework internacional que orienta a identificação, avaliação, gerenciamento e monitoramento dos riscos de negócios para aumentar o valor da empresa, alinhando a gestão de riscos à estratégia e ao desempenho. Visa proteger o patrimônio, melhorar a tomada de decisão e garantir que os objetivos estratégicos sejam alcançados.

2.6 DONO DO RISCO (RISK OWNER)
Todos os gestores da ENGIE são donos dos riscos relacionados a suas atribuições ou autoridades, e assumem a responsabilidade pela exposição ao risco incorrido por suas decisões. Todo gestor é um Gestor de Riscos.

2.7 ERM – ENTERPRISE RISK MANAGEMENT
Sigla em inglês para Enterprise Risk Management que significa Gestão de Riscos Empresariais.

2.8 GBU – GLOBAL BUSINESS UNIT
Corresponde a um segmento operacional cujo desempenho operacional e financeiro é regularmente revisado pelo Comitê Executivo do Grupo.

Cópia não controlada

2.9 GESTÃO DE RISCOS E OPORTUNIDADES EMPRESARIAIS (ERM)
Exercício estruturado e multidisciplinar, com objetivo de identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos e oportunidades que possam impactar os objetivos estratégicos da Companhia. O ERM é um processo contínuo, com ciclos anuais e visão de curto, médio e longo prazo, alinhado a metodologia do Grupo ENGIE e fundamentado em normas internacionais como ISO 31000 e COSO ERM.

2.10 IMPACTO
Representação quantitativa e/ou qualitativa do efeito positivo ou negativo que a materialização do risco/oportunidade traz em relação ao projetado no caso base financeiro (PMT V1), ou no atingimento dos objetivos empresariais.

2.11 ISO 31000
Norma internacional que foca em lidar com a incerteza de forma estruturada para aumentar a resiliência organizacional. Seu objetivo é fornecer diretrizes estruturadas para que organizações de qualquer porte integrem a gestão de riscos em todas as atividades, estratégias e operações, visando proteger o valor, melhorar o desempenho, aumentar a confiança na tomada de decisões e garantir a perenidade do negócio.

2.12 PRM – PROJECT RISK MANAGEMENT
Sigla em inglês para Project Risk Management que significa Gestão de Riscos em Projetos. A Gestão de Riscos em Projetos é uma abordagem sistemática e interativa para a identificação, avaliação, mitigação e revisão dos riscos envolvidos em um projeto, que possibilita alcançar os objetivos do projeto com consciência e aceitação dos fatores aleatórios que podem ocorrer. A gestão de riscos em projetos visa coordenar as etapas individuais, independentemente de sua natureza, e as formas como essas etapas interagem, considerando os objetivos do projeto.

2.13 MATRIZ DE RISCOS E OPORTUNIDADES EMPRESARIAIS
Documento que sintetiza o resultado da análise de riscos e oportunidades empresariais, contendo identificação dos riscos e oportunidades, causas, consequências, evolução do risco, cenários, planos de mitigação e a representação gráfica (matriz de linhas e colunas) da exposição aos riscos, com base na combinação entre impacto e probabilidade, utilizada para priorização e tratamento, que é o Mapa de Calor (Heatmap).

2.14 MODELO DE TRÊS LINHAS
Criado pelo Institute of Internal Auditors - IIA, é uma estrutura de governança que estabelece papéis e responsabilidades para a gestão de riscos em três níveis: áreas de negócio (1ª linha), funções de gestão de riscos, controles internos e conformidade (2ª linha) e auditoria interna (3ª linha).

2.15 OPORTUNIDADE
Qualquer evento incerto, com probabilidade de exercer impacto positivo sobre a sustentabilidade ou a reputação da empresa, ou a consecução de seus objetivos estratégicos, financeiros ou operacionais.

2.16 RISCO
Qualquer evento incerto, com probabilidade de exercer impacto negativo sobre a sustentabilidade ou a reputação da empresa, ou a consecução de seus objetivos estratégicos, financeiros ou operacionais.

2.17 RISK REGISTER
Compilação estruturada dos riscos que foram identificados e gerenciados ao longo do ciclo de vida do projeto (em PRM) e/ou durante a revisão de riscos corporativos (em ERM). Deve ser criado no início do projeto, na fase de Desenvolvimento de Negócios e deve ser mantido atualizado durante toda a duração do projeto e entregue em cada etapa fundamental, sempre que houver uma

Cópia não controlada

mudança de participantes. Para cada risco corporativo, deve ser desenvolvido um registro de riscos específico.

2.18 RISK OFFICER
Profissional responsável pela gestão de riscos e oportunidades empresariais, alinhado com a metodologia do grupo ENGIE e normas aplicáveis.

2.19 PLANO DE AÇÃO
Conjunto de medidas adotadas para reduzir o impacto e/ou a probabilidade de materialização de um risco, com o objetivo de alinhá-lo ao apetite a risco definido pela Companhia.

2.20 PROBABILIDADE
Chance de ocorrência de um evento de risco, devendo ser expressa de forma quantitativa, conforme critérios definidos pelo Grupo ENGIE.

3. DISPOSIÇÕES

3.1 APLICAÇÃO E ABRANGÊNCIA

Esta política aplica-se a todas as empresas operacionais, controladas e sugerido para as não controladas da ENGIE no Brasil.

Abrange todos os tipos de riscos aos quais a ENGIE Brasil está exposta, independentemente de sua origem ou natureza. Deve ser observada em qualquer atividade ou decisão que possa impactar os objetivos estratégicos, operacionais, financeiros, ambientais, sociais, reputacionais ou de conformidade da Companhia.

4. PRINCÍPIOS

4.1 GERAIS

4.1.1 Confidencialidade

4.1.1.1 A identificação, avaliação de riscos, estratégias de mitigação e os planos de ação são informações altamente estratégicas, sensíveis, classificadas como “restrita/internas”, conforme regras do Grupo ENGIE, pois destacam vulnerabilidades exploráveis por concorrentes e ações que geram vantagens competitivas.

4.1.1.2 Essas informações estão sujeitas a comunicação controlada e devem atender às obrigações legais, especialmente no contexto de divulgações financeiras.

4.1.1.3 A implementação do ERM respeita as obrigações de governança e obrigações legais das entidades do Grupo. Uma correta implementação da proteção a essas informações deverá ser condizente com a difusão específica de informações entre gestores para que possam implementar ações de gestão de risco.

4.1.2 Framework

4.1.2.1 A gestão de riscos e oportunidades empresariais da ENGIE Brasil está alinhada à metodologia do Grupo ENGIE, que é baseada nas melhores práticas de gestão internacionalmente reconhecidas, como a ISO 31000 e COSO ERM, considerando a legislação aplicável. A metodologia abrange

Cópia não controlada

documentação de apoio (catálogo de riscos, manuais etc.) e ferramentas de gestão (sistemas corporativos).

4.1.2.2 Os valores do Grupo ENGIE são considerados no processo de gestão de riscos e oportunidades da ENGIE Brasil, bem como a conformidade com as obrigações legais e regulatórias.

4.1.2.3 *A tomada de risco é intrínseca a qualquer empresa:* a realização de negócios implica na tomada de um nível razoável de risco e deve levar em conta a sustentabilidade do negócio a longo prazo, por meio de identificação e monitoramento contínuo dos riscos.

4.1.2.4 *Não existe risco zero:* não é economicamente viável mitigar um risco a ponto de que seu impacto seja zero. Entretanto, é essencial implementar procedimentos de gestão e planos de mitigação que controlem os riscos dentro do apetite definido pelo Grupo ENGIE, equilibrando custo e benefício.

4.1.2.5 *Gerir melhor nossos riscos, de forma a assegurar nossa performance:* Gerir os riscos dá maior garantia de que os objetivos estratégicos e operacionais serão atingidos, em um contexto de mudança do ambiente de negócios. Essa abordagem promove conhecimento aprofundado dos riscos, fomentando decisões conscientes e reflexivas para escolhas mais seguras.

4.1.2.6 *O pior risco é aquele que não se conhece:* risco que não é identificado não é mitigado.

4.1.2.7 A cultura de gestão de riscos e oportunidades empresariais deve ser promovida continuamente por meio de treinamentos, orientações e engajamento das lideranças, assegurando capacitação adequada aos envolvidos em suas responsabilidades.

4.1.2.8 Esta Política deve ser revisada em consonância com a Política de Gestão de Riscos e Oportunidades do Grupo ENGIE.

4.2 ESTRUTURA DA GESTÃO DE RISCOS E OPORTUNIDADES EMPRESARIAIS

4.2.1 A ENGIE Brasil adota o Modelo das Três Linhas, conforme diretrizes do Institute of Internal Auditors (IIA):

a) **1ª linha** – composta pelos gestores das áreas de negócio, responsáveis por identificar, avaliar e gerenciar os riscos relacionados ao seu âmbito de atuação. Devem implementar planos de ação para adequada mitigação dos riscos, além de acompanhar a efetividade dessas iniciativas;

b) **2ª linha** – composta pelas áreas de Compliance, Controles Internos e Gestão de Riscos e Oportunidades Empresariais. A área de Gestão de Riscos e Oportunidades Empresariais é responsável por apoiar e orientar a 1ª linha na aplicação da metodologia corporativa de gestão de riscos, promovendo aderência à política e procedimentos, à consolidação das informações e à cultura de riscos na organização;

c) **3ª linha** – composta pela área de Auditoria Interna que atua com independência funcional para avaliar a eficácia da gestão de riscos e oportunidades empresariais, dos controles internos e da governança. Nas empresas listadas em bolsa de valores, a Auditoria Interna reporta diretamente ao Comitê de Auditoria Estatutário e ao Conselho de Administração, contribuindo com recomendações para o aprimoramento contínuo dessas práticas.

Cópia não controlada

No processo de gestão de riscos e oportunidades empresariais, os planos de ação e controles definidos no âmbito do Programa de Controle Interno do Grupo (INCOME) são mitigadores de riscos. A Matriz de Riscos e Oportunidades Empresariais orienta o plano anual de trabalho da auditoria interna. A gestão de riscos e oportunidades empresariais trabalha de forma coordenada com outras linhas funcionais, como Ética, TI, entre outros.

4.3 PROCESSO DE GESTÃO DE RISCOS E OPORTUNIDADES EMPRESARIAIS

4.3.1 A gestão de riscos e oportunidades empresariais da ENGIE Brasil deve ser implementada de forma estruturada, sistemática e contínua, com emissão bianual da Matriz de Riscos e Oportunidades Empresariais (versão preliminar e final), alinhada as melhores práticas internacionais, incluindo as diretrizes da ISO 31000 e do COSO ERM, conforme apresentado a seguir:



Figura 1: Ciclo de Gestão de Riscos e Oportunidades Empresariais

a) Consideração do contexto
Análise do ambiente de negócios em que a Companhia atua.

b) Análise dos riscos
Compreende a identificação, análise de causas e consequências, avaliação de cenários, com quantificação/qualificação de impacto e probabilidade do risco inerente (risco bruto) e do risco residual (risco após mitigação). As empresas podem estabelecer Fórum de Gerenciamento de Riscos para promover e ampliar a discussão do tema.

c) Mitigação
Mitigação de risco por meio de planos de ação contínuos e planos de ação específicos com períodos definidos (data de início e data de fim).

d) Monitoramento
Os riscos identificados, as materializações relevantes e os planos de mitigação estabelecidos são monitorados pelos donos dos riscos com o apoio da área de gestão de riscos e oportunidades empresariais.

Cópia não controlada

e) Aprovação
O processo de gestão de riscos e oportunidades empresariais segue o cronograma definido pelo Grupo ENGIE a cada ano. A Matriz de Riscos e Oportunidades Empresariais deve ser aprovado nas instâncias aplicáveis: empresas operacionais (Diretoria Executiva), ENGIE Brasil (Comitê Executivo com a participação dos representantes das GBUs). Além disso, em empresas listadas em bolsa de valores, a Matriz de Riscos e Oportunidades Empresariais deve ser discutida no Comitê de Auditoria Estatutário e deve ser apresentada ao Conselho de Administração e ao Conselho Fiscal.

f) Comunicação
A Matriz de Risco e Oportunidades Empresariais deve ser comunicada aos níveis apropriados de gestão das empresas operacionais, GBUs, ao Grupo ENGIE, Auditoria Interna, área Jurídica e área de Controles Internos. Os riscos e oportunidades empresariais também serão comunicados aos demais stakeholders de acordo com a legislação aplicável e orientações do Grupo ENGIE.

4.3.2 A gestão de riscos e oportunidades empresariais no desenvolvimento de projetos deve observar a metodologia de PRM (Project Risk Management) definida pelo Grupo ENGIE. Quando os projetos são aprovados e seguem para a fase de implantação, passam a ter seus riscos geridos de acordo com a metodologia ERM.

4.4 RESPONSABILIDADES E ATRIBUIÇÕES

4.4.1 A ENGIE Brasil mantém uma estrutura organizada responsável pela aplicação da gestão de riscos e oportunidades empresariais descrita nesta Política, em diferentes níveis da organização, conforme detalhado nos itens subsequentes.

4.4.2 Dono/Gestor do Risco

4.4.2.1 São atribuições do Dono/Gestor do Risco:

a) Identificar, avaliar e monitorar os riscos associados as suas atividades e processos;
b) Desenvolver, acompanhar e atualizar regularmente os planos de ação;
c) Manter atualizadas as informações de riscos junto a área de Gestão de Riscos e Oportunidades Empresariais;
d) Atuar como referência na gestão dos riscos da sua área, promovendo a comunicação e a prevenção.

4.4.3 Área de Gestão de Riscos e Oportunidades Empresariais

4.4.3.1 São atribuições da Área de Gestão de Riscos e Oportunidades Empresariais:

a) Coordenar, monitorar e reportar o risco empresarial à Administração, para subsidiar a tomada de decisão estratégica;
b) Atuar na elaboração do Risk Register de projetos de expansão, conforme as diretrizes do Grupo ENGIE;
c) Contribuir para os reportes relacionados à gestão de riscos e oportunidades empresariais para stakeholders externos;
d) Secretariar o Fórum de Gerenciamento de Riscos, no caso de empresas listadas em bolsa de valores;
e) Dar suporte à Diretoria Executiva na tomada de decisão estratégica relacionada a riscos;

Cópia não controlada

f) Disseminar conhecimento sobre riscos e boas práticas de gestão de riscos, contribuindo para o fortalecimento da cultura de prevenção e responsabilidade corporativa.

4.4.4 **Fórum de Gerenciamento de Riscos** [1]

4.4.4.1 São atribuições do Fórum de Gerenciamento de Riscos:

a) Analisar e propor contribuições à minuta da Matriz de Riscos e Oportunidades Empresariais preparada pela área de gestão de riscos e oportunidades empresariais com base nas propostas encaminhadas pelas áreas de negócio donas dos riscos;
b) Contribuir com a identificação de outros riscos e oportunidades empresariais;
c) Validar proposta de Matriz de Riscos e Oportunidades (draft) a ser encaminhada para aprovação da Diretoria Executiva;
d) Promover a cultura de gerenciamento dos riscos, reforçando a conduta alinhada aos valores da Companhia.

4.4.5 **Diretoria Executiva**

4.4.5.1 São atribuições da Diretoria Executiva:

a) São responsáveis pela gestão dos riscos de suas áreas de atuação ou sobre as quais têm autoridade. São os donos dos riscos de suas companhias, e podem delegar a propriedade e a gestão para outros gestores. “Todo Gestor é um Gestor de Risco”;
b) Definir o nível geral de risco (apetite a risco) que deve ser alcançado dentro de um período de tempo específico com base na orientação do Grupo ENGIE;
c) Garantir a execução da Política de Gestão de Riscos e Oportunidades Empresariais;
d) Integrar a análise de riscos à tomada de decisão estratégica e operacional;
e) Assegurar recursos, estrutura e capacitação adequados à gestão de riscos e oportunidades empresariais nas áreas sob sua responsabilidade;
f) Promover a cultura do gerenciamento de riscos e reforçar condutas alinhadas aos valores organizacionais;
g) Aprovar as alterações propostas quanto ao tratamento dos riscos e monitoramento dos planos de mitigação.

4.4.6 **Comitê de Auditoria Estatutária** [2]

4.4.6.1 São atribuições do Comitê de Auditoria Estatutária:

a) Monitorar a eficácia do processo de gestão de riscos e oportunidades, o cumprimento de leis e regulamentos;
b) Confirmar se o risco divulgado em comunicação externa se baseia em metodologia de avaliação de risco e se está em conformidade com as normas e leis aplicáveis;
c) Assessorar o Conselho de Administração na supervisão da gestão de riscos e oportunidades empresariais e na melhoria contínua das práticas de governança;
d) Avaliar e monitorar as exposições de risco da Companhia;
e) Tomar conhecimento e supervisionar as matrizes de riscos e oportunidades empresariais, bem como suas revisões.

4.4.7 **Conselho de Administração**[3]

[1] Não obrigatório, porém recomendável.
[2] No caso de empresas listadas em bolsas de valores
[3] No caso de empresas listadas em bolsas de valores

Cópia não controlada

4.4.7.1 São atribuições do Conselho de Administração:

a) Aprovar a Política de Gestão de Riscos e Oportunidades Empresariais e suas revisões;
b) Monitorar a eficácia do processo de gestão de riscos e oportunidades empresariais;
c) Tomar conhecimento e supervisionar as matrizes de riscos e oportunidade empresariais, bem como suas revisões;
d) Assegurar que a diretoria possua mecanismos e controles internos para identificar, avaliar, priorizar, mitigar, relatar e monitorar os riscos, de forma a mantê-los em níveis compatíveis com o apetite a riscos da organização;
e) Promover a cultura de gestão de riscos e oportunidades empresariais, integridade, responsabilidade e prevenção no nível mais alto da Companhia.

4.4.8 **Comitê Executivo (COMEX)**

4.4.8.1 São atribuições do Comitê Executivo (COMEX):

a) Aprovar a Política de Gestão de Riscos e Oportunidades Empresariais e suas revisões;
b) Tomar conhecimento e supervisionar as matrizes de risco e oportunidade empresariais, bem como suas revisões.

4.4.9 **Suporte à Gestão de Riscos e Oportunidades Empresariais** (linha funcional ERM)

4.4.9.1 São atribuições do Suporte à Gestão de Riscos e Oportunidades Empresariais (linha funcional ERM):

a) A linha funcional de ERM é composta por todos os Risk Officers das entidades;
b) A linha funcional ERM é supervisionada pelo Risk Officer da ENGIE Latam e pelo Chief Risk Officer (CRO) de cada entidade;
c) O Chief Risk Officer (CRO) é membro do Comitê Executivo (COMEX) de cada entidade e é responsável pela gestão de riscos no seu perímetro, por definir o apetite ao risco e apoiar a consecução dos planos de ação.

4.4.10 **Risk Officer**

4.4.10.1 São atribuições do Risk Officer:

a) Conduzir a revisão anual de riscos do seu âmbito de atuação de acordo com a metodologia do ERM, sob a supervisão e validação do CRO;
b) Implementar as diretrizes do Grupo em conjunto com as áreas de apoio;
c) Assessorar na identificação, análise e avaliação dos riscos e planos de ação;
d) Como Business Partner, deve assessorar os gestores sobre como reduzir ou aumentar a tomada de riscos, tanto nas operações diárias quanto em projetos, em conformidade com as leis, regulamentos e políticas do Grupo;
e) O Risk Officer integra na revisão anual de riscos do seu âmbito de atuação uma avaliação da consistência entre as avaliações de gestão de riscos e oportunidades empresariais e as apresentadas na seção de riscos do PMT;
f) Atuar na revisão de riscos de projetos (PRM);
g) Interagir com a área de Auditoria Interna para apoiá-la no estabelecimento de um Plano Anual de Auditoria baseado em riscos;
h) Interagir com a área de Controle Interno para definir os planos de ação do Programa de Controles Internos do Grupo (INCOME), que servem como medidas de mitigação de riscos para a Gestão de Riscos e Oportunidades Empresariais (ERM);
i) Contribuir para a melhora do conhecimento dos riscos da sua entidade, assim aumentando a credibilidade, melhorando a avaliação da tomada de risco e, portanto,

Cópia não controlada

mantendo e criando valor, atuando para subsidiar a tomada de decisões estratégicas e operacionais;

j) Certificar-se de que a Política, procedimentos e metodologias sejam implementados corretamente.

Cópia não controlada