POLÍTICA DE GESTÃO DE RISCOS

GRUPO EQUATORIAL

GRUPO equatorial ENERGIA

SUMÁRIO

SUMÁRIO

SUMÁRIO

1.0 - FINALIDADE

Estabelecer diretrizes para assegurar as melhores práticas da Gestão de Riscos Corporativos, relacionadas à identificação, avaliação, monitoramento e reporte dos riscos, que possam afetar os objetivos estratégicos do Grupo Equatorial.

2.0 - CAMPO DE APLICAÇÃO

Aplica-se ao Grupo Equatorial Energia e suas controladas.

No caso de sociedades nas quais o Grupo Equatorial exerça influência significativa, tais como joint ventures e sociedades que a Companhia detenha participação minoritária, o conteúdo desta Política deverá ser levado ao conhecimento do(s) stakeholders, permitindo a incorporação, sempre que possível, das diretrizes por ela preconizadas.

3.0 - RESPONSABILIDADES

3.I Conselho de Administração

a) Definir as estratégias para alcance dos objetivos de negócio;

b) Aprovar a Política de Gestão de Riscos e suas revisões quando necessário;

c) Avaliar e aprovar a matriz de riscos corporativos, estabelecendo os limites aceitáveis ao apetite a riscos do Grupo Equatorial;

d) Aprovar os planos de resposta aos riscos com grau de exposição extrema ou riscos priorizados pela alta administração.

3.2 Comitê de Auditoria e Riscos

a) Garantir que o Grupo Equatorial mantenha uma cultura voltada à Gestão de Riscos, incentivando o cumprimento da Política e da Norma de Procedimento de Gestão de Riscos;

b) Analisar a Política de Gestão de Riscos, metodologia e os documentos chave a serem utilizados no processo de gestão de riscos do Grupo e submetê-los à aprovação do Conselho de Administração;

c) Analisar o apetite a riscos e submetê-lo à aprovação do Conselho de Administração;

d) Reportar periodicamente o nível de exposição dos riscos prioritários ao Conselho de Administração;

e) Avaliar a efetividade do processo de gestão de riscos e sugerir melhorias, quando necessário;

f) Aprovar o Plano Anual de Riscos.

3.3 Área de Gestão de Riscos e Controles Internos (GRC)

a) Definir a estrutura e a metodologia, e executar a estratégia de Gestão de Riscos Corporativos do Grupo Equatorial;

b) Avaliar e monitorar as exposições a riscos, acompanhando a implantação das ações de mitigação das áreas de negócio e reportando o cenário periodicamente à Alta Administração e ao Comitê de Auditoria e Riscos;

c) Assessorar a Alta Administração na proposição do Apetite a Risco, bem como auxiliar as áreas de negócio na identificação de

riscos, avaliação de Impacto e direcionamento das Respostas aos Riscos (aceitar, compartilhar, evitar e reduzir);

d) Apoiar o Comitê de Auditoria e Riscos na avaliação contínua da Estrutura da Gestão e Riscos Corporativos, mantendo a base atualizada com os registros de perdas que se materializarem na Companhia;

e) Desenvolver em conjunto com as áreas de negócio os indicadores para monitoramento dos riscos, bem como proposta dos limites de tolerância;

f) Apoiar as áreas de negócio no desenho e na melhoria de Controles Internos para tratamento das não-conformidades identificadas nos trabalhos de Auditoria Interna e mapeamento de riscos.

3.4 Presidentes e Superintendentes

a) Fomentar a cultura da Gestão de Riscos junto as áreas de negócio;

b) Incorporar a Gestão de Riscos, no planejamento e gestão de processos críticos;

c) Acompanhar os Indicadores de Risco (KRI's), que ultrapassem os limites de tolerância ou necessitem de ações mitigadoras.

3.5 Gestores das Áreas de Negócios (Donos dos Riscos – Risk Owners)

a) Efetuar o monitoramento dos riscos, direta ou indiretamente, envolvidos nas operações sob sua gestão, a partir da identificação das causas e consequências associadas à materialização;

b) Assumir e garantir que os riscos estejam dentro dos limites de tolerância definidos pelo Conselho de Administração;

c) Reporte periódico ao Comitê de Auditoria e Riscos ou Área de GRC dos eventos relevantes, que afetem o grau de exposição do

Grupo Equatorial a riscos, incluindo os resultados dos indicadores de riscos prioritários;

d) Garantir a operacionalização da gestão de riscos, sendo parte integrante do processo de identificação, avaliação e mensuração, bem como, a implementação de ações e planos de resposta, relativos aos riscos envolvidos nas operações sob sua gestão, de acordo com as deliberações tomadas em conjunto com a Área de GRC e Comitê de Auditoria e Riscos.

3.6 Auditoria interna

a) Avaliar a adequação e eficácia dos controles internos das unidades que compõem o Grupo Equatorial;

b) Apresentar recomendações para minimizar riscos através do aprimoramento das estruturas de controle existentes;

c) Apontar ao Comitê de Auditoria e Riscos a ocorrência de não conformidades, oportunidades de melhorias nos processos e nos controles, falhas, desvios, irregularidades e/ou ilegalidades observadas.

4.0 - DEFINIÇÕES

4.I Auditoria

Processo de exame e validação de um sistema, atividade ou informação.

4.2 Apetite a Risco

Nível de risco que uma organização está disposta a aceitar para atingir seus objetivos.

4.3 Avaliação de Risco

Significância do risco identificado, relacionado ao impacto e à vulnerabilidade dos controles internos.

4.4 CAD

Conselho de Administração.

4.5 COAUD

Comitê de Auditoria Interna.

4.6 Controle Interno

Conjunto de atividades, métodos ou rotinas destinadas a assegurar confiabilidade aos processos do negócio, atender às leis e regulamentos aplicáveis, proteger os ativos e ajudar a administração no alcance dos objetivos da Companhia.

4.7 Criticidade

Nível de risco implícito em um processo ou atividade. Quanto maior o risco intrínseco, mais crítico se torna o processo ou atividade.

4.8 Dano

Perda ou prejuízo sofrido em razão de ação, omissão ou influência de alguém.

4.9 Evento

Ocorrência ou mudança em um conjunto específico de circunstâncias, que materializadas possam representar risco aos objetivos do processo ou da política da Companhia.

4.10 Gestão de Riscos

Atividade coordenada que visa identificar, avaliar, priorizar e monitorar a organização no que se refere a riscos.

4.11 Impacto

Nível de severidade dos efeitos causados por certa ação ou acontecimento. É a magnitude do dano levando-se em consideração a gravidade das consequências aos negócios da Companhia.

4.12 Matriz de Riscos Corporativos

Ferramenta que permite à Alta Administração mensurar, avaliar e ordenar os eventos de riscos estratégicos que podem afetar o alcance dos objetivos de suporte do Grupo, tipificando os riscos em baixo, médio, alto ou muito alto.

4.13 Processo

Conjunto de macroatividades interdependentes e intergadas, objetivando desempenhar uma função corporativa.

4.14 Probabilidade

Possibilidade de materialização de um determinado Risco.

4.15 Resposta ao Risco

Decisões tomadas pela Companhia para desenvolver uma série de medidas a fim de alinhar os riscos com o respectivo apetite ao risco.

4.16 Risco

São as incertezas no alcance dos objetivos, é a combinação de impacto e probabilidade de ocorrência.

4.17 Risco Corporativo

Riscos que podem afetar a Companhia como um todo, impactando diretamente os objetivos estratégicos da organização.

4.18 Risco Inerente

Riscos sempre presentes no ramo do negócio, nos processos ou na atividade, independente dos controles internos administrativos adotados.

4.19 Risco Residual

Risco remanescente após a mitigação por controles internos.

4.20 Stakeholder

Público estratégico e descreve uma pessoa ou grupo que tem interesse em uma empresa, negócio ou indústria, podendo ou não ter feito um investimento neles.

4.21 Vulnerabilidade

Refere-se à disposição da empresa a um evento de risco em termos de critérios relacionados à agilidade e adaptabilidade, bem como às Atividades de Controles exercidas em cada risco.

4.22 Indicadores de Risco (KRI's)

Componentes do processo de monitoramento de riscos utilizados para verificar a evolução de um risco ou condições de risco em potencial, informando o perfil do risco em relação ao apetite ao risco (nível de risco tolerável), sinalizando aos gestores a necessidade de ações a serem tomadas em relação ao apetite ao risco (nível de risco tolerável), sinalizando aos gestores a necessidade de ações a serem tomadas.

5.0 - DIRETRIZES DA GESTÃO DE RISCOS

5.I Estabelecer, disseminar e cultivar uma cultura voltada à Gestão de Riscos

a) Identificar os riscos inerentes ao negócio, priorizá-los, avaliar e responder de acordo com o apetite a riscos do Grupo Equatorial;

b) Prover que todos os colaboradores compreendam os objetivos, papéis, funções e as responsabilidades atribuídas para cada agente envolvido no processo de gestão de riscos;

c) Estabelecer planos de resposta aos riscos tempestivamente monitorados pelas instâncias responsáveis no Grupo;

d) Reportar os KRI's de acordo com os limites de tolerância a riscos, previamente aprovados pelo Conselho de Administração e as estratégias de mitigação dos riscos.

6.0 - OBJETIVOS DA GESTÃO DE RISCO

a) Atuar em sintonia com as melhores práticas de mercado quanto à gestão de riscos;

b) Proteção contra perda de valor;

c) Identificação e tratamento de riscos que possam ameaçar a execução dos objetivos estratégicos do Grupo;

d) Reconhecimento e reputação. Melhorar a confiança das partes interessadas;

e) Redução da possibilidade de ocorrência de fraudes e erros em processos operacionais;

f) Identificação de oportunidades de melhorias, objetivando a redução de atividades manuais, morosidades e gargalos em processos;

g) Maior alinhamento e sinergia entre gerências e processos dentro da empresa;

h) Garantir o alinhamento das diretrizes da Alta Administração com os processos operacionais.

7.0 - CATEGORIA DOS RISCOS

O Dicionário de Riscos Corporativos considera as características e o ambiente de negócio da empresa, classificando em cinco categorias os riscos:

7.I Estratégicos

Possível impacto decorrente de práticas frágeis governança, decisões não baseadas em um planejamento estratégico, investimentos indevidos e falta de capacidade de resposta às mudanças no ambiente, ou de publicidade negativa sobre práticas e/ou negócios da organização.

7.2 Financeiros

Possível impacto derivado de operações financeiras incoerentes com boas práticas de mercado, ou em desacordo com os valores da Companhia.

7.3 Compliance (ou conformidade)

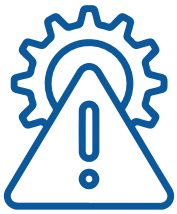
Possível impacto originário do descumprimento de leis/regulamentos, ou processos movidos por clientes ou contrapartes, ou denúncias.

7.4 Operacionais

Possível impacto decorrente de problemas operacionais, como falhas nos controles internos.

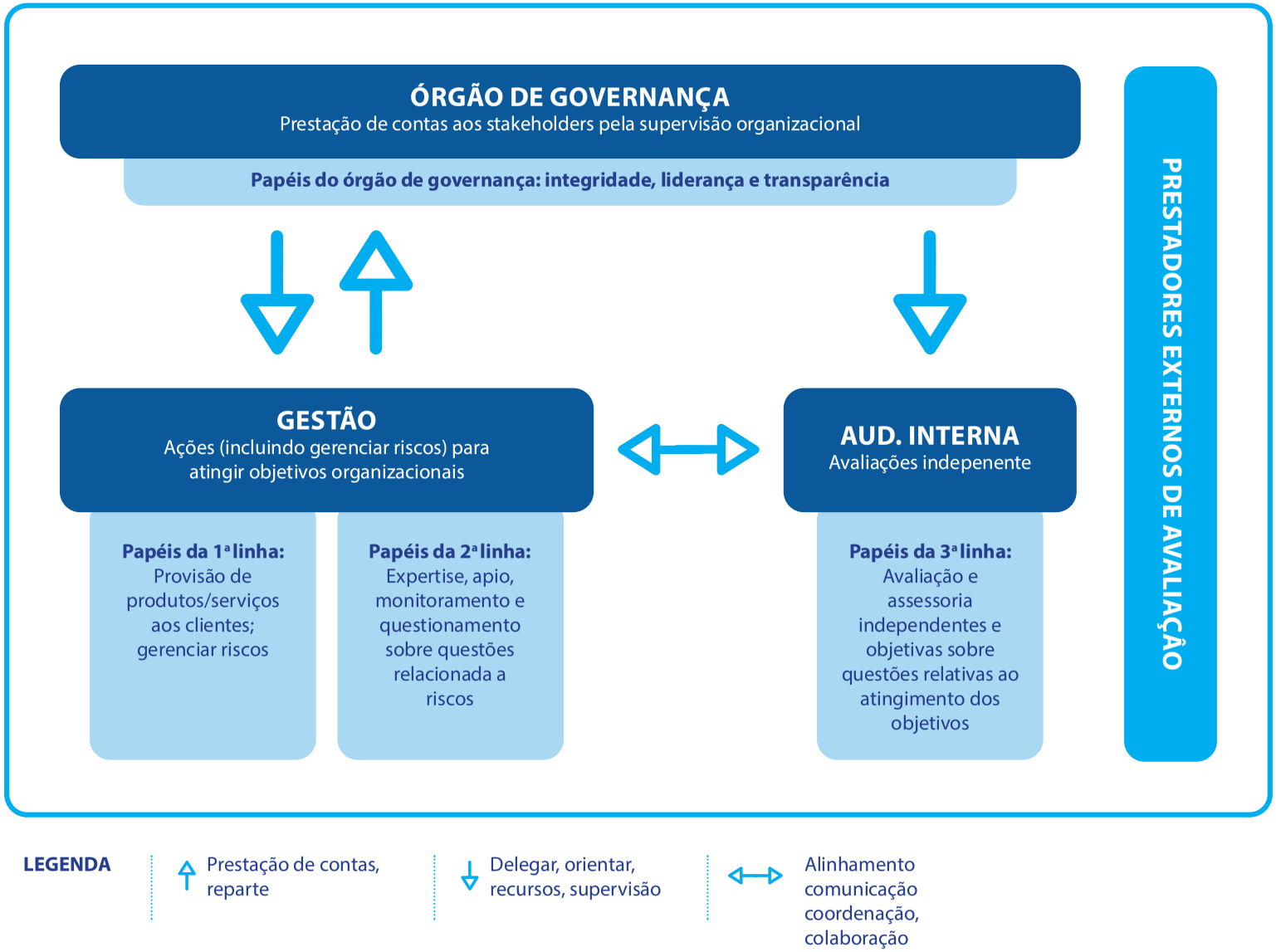
7.5 Cibernéticos

Possível impacto decorrente do desalinhamento estratégico da tecnologia da informação com os objetivos do negócio, ataques cibernéticos e comprometimento da segurança das informações, indisponibilidade de sistemas e perda de integridade



8.0 - ESTRUTURA DE GESTÃO DE RISCOS

A definição da estrutura de Gestão de Riscos do Grupo Equatorial considera o contexto atual da companhia, boas práticas de mercado e a integração dos riscos aos processos do Grupo, reforçando a responsabilidade de todos os colaboradores para gestão dos riscos corporativos, permitindo que os objetivos estratégicos do Grupo sejam alcançados, conforme adotado no modelo das três linhas:


ÓRGÃO DE GOVERNANÇA
Prestação de contas aos stakeholders pela supervisão organizacional
Papéis do órgão de governança: integridade, liderança e transparência
PRESTADORES EXTERNOS DE AVALIAÇÃO
GESTÃO
Ações (incluindo gerenciar riscos) para atingir objetivos organizacionais
AUD. INTERNA
Avaliações indepenente
Papéis da 1ª linha: Provisão de produtos/serviços aos clientes; gerenciar riscos
Papéis da 2ª linha: Expertise, apio, monitoramento e questionamento sobre questões relacionada a riscos
Papéis da 3ª linha: Avaliação e assessoria independentes e objetivas sobre questões relativas ao atingimento dos objetivos
LEGENDA
Prestação de contas, reparte
Delegar, orientar, recursos, supervisão
Alinhamento comunicação coordenação, colaboração

8.I Modelos das Três Linhas

8.1.1 Como 1ª linha, as Áreas e Unidades de negócio da Companhia são responsáveis pela gestão contínua dos riscos e exploração de oportunidades, propagando uma cultura de desenvolvimento dos processos, sistemas e controles internos, para atingimento das metas e objetivos estratégicos do Grupo Equatorial.

8.1.2 Como 2ª linha, tem o intuito de fornecer conhecimento complementar, de apoio a implantação e manutenção dos planos de resposta associados aos riscos e controles internos, assim como o desenvolvimento da melhoria contínua das práticas do gerenciamento de riscos.

8.1.3 Como 3ª linha, a Área de Auditoria Interna, atua no assessoramento da administração, voltada para o exame e avaliação da adequação, eficiência e eficácia dos sistemas de controles, baseado nos conceitos de gerenciamento de riscos do negócio.

9.0 - ETAPAS DA GESTÃO DE RISCOS

O processo de gestão de riscos do Grupo Equatorial considera as seguintes etapas:

9.I Identificação e Análise de Riscos

9.1.1 Identificação de Risco e Fatores de Risco

Os riscos identificados devem ser mapeados para detectar os fatores de riscos e permitir um melhor entendimento das principais causas, que potencialmente levam à sua materialização, assim como, principais agravantes e atenuantes relacionados, que servem de insumo para avaliação de riscos. Essa atividade deve ser coordenada e consolidada pela Área de GRC junto às unidades e áreas de negócio, responsáveis primários pelos riscos.

9.1.2 Análise Geral de Riscos (AGR)

A AGR reflete, de maneira estruturada, as percepções da Alta Administração, bem como os executivos (áreas e unidades de negócio) em relação aos principais aspectos de gestão e riscos envolvidos nas operações, áreas/processos de negócio e características da Companhia;

A Área de GRC auxiliará as Áreas e unidades de negócio da Companhia na identificação dos riscos, sendo necessário ter em vista os possíveis cenários de perda para o Grupo Equatorial, ligando a estes suas respectivas causas e consequências relacionadas à materialização do risco.

9.2 Avaliação de Riscos

A avaliação de riscos tem como objetivo atribuir um nível de exposição aos riscos com base em vetores e critérios definidos. Os vetores principais utilizados pelo Grupo Equatorial são: Impacto e Vulnerabilidade.

9.2.1 Impacto

O impacto refere-se à extensão que um evento de risco pode afetar à Companhia. A classificação de impacto do Grupo Equatorial considera um vetor principal financeiro e vetores auxiliares qualitativos;

A avaliação do impacto poderá ser realizada exclusivamente de forma qualitativa ou quantitativa, dependendo do risco que está sendo avaliado. É preferível a aplicação de método qualitativo caso a Companhia não possua dados confiáveis, íntegros ou não exista modelo reconhecido capaz de quantificar o risco ou cujo, modelo seja demasiado complexo e que o retorno da quantificação não supere o esforço do cálculo.

9.2.2 Vulnerabilidade

A Vulnerabilidade refere-se à quão preparada es-tão as defesas da organização frente aos eventos de riscos. A classificação da vulnerabilidade no Grupo Equatorial considera três vetores auxiliares: Controles Internos, Planos de Ação e/ou Resposta e Eventos Externos, logo será obtido o valor residual do risco.

9.2.3 Exposição ao Risco e Priorização

O resultado dos vetores de impacto e vulnerabilidade será a exposição ao risco, conforme demonstração gráfica abaixo:

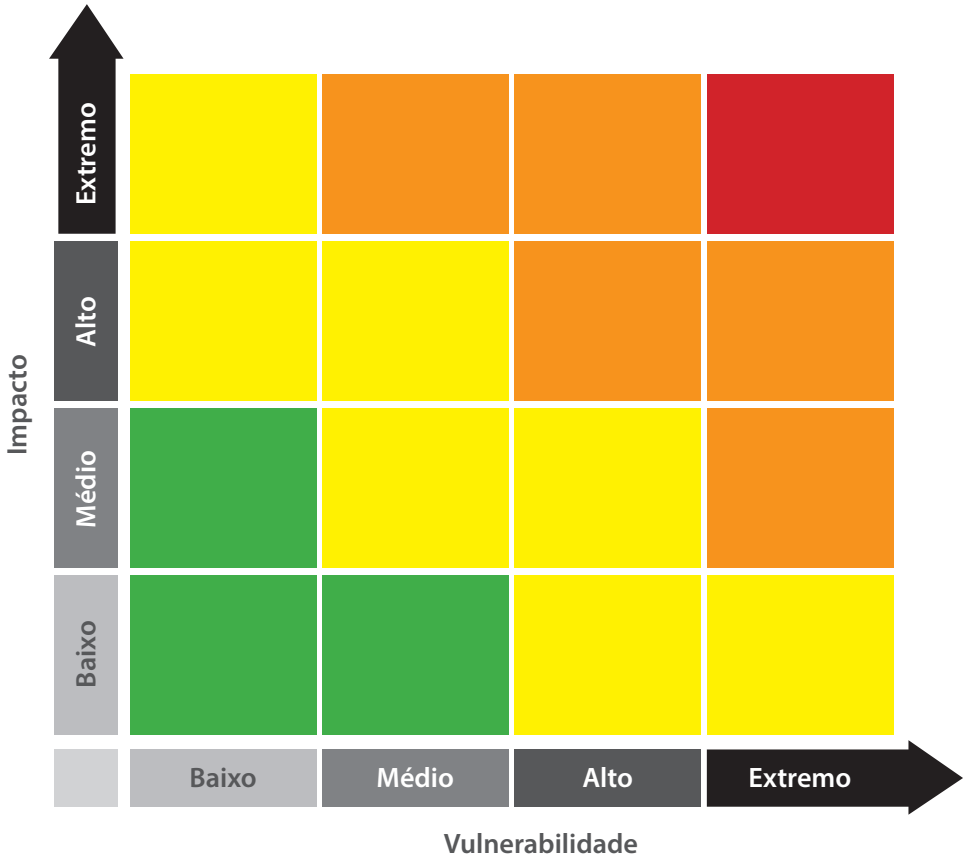


Figura 2: Mapa de Risco

A partir do resultado obtido na avaliação dos vetores de Impacto e Vulnerabilidade, os riscos devem ser classificados, conforme o grau abaixo:

a) EXTREMO: Representa extrema ameaça em potencial, é um evento intolerável, essa atividade não deve ser iniciada ou prossegui-la até que o risco seja reduzido. Em caso de não ser possível a redução do risco, mesmo utilizando recursos elevados, a atividade deve ser proibida.

b) ALTO: Representa grande ameaça em potencial, portanto, a atividade não deve ser iniciada até que o risco seja reduzido. Esforços e recursos devem ser alocados para mitigá-lo. Para atividade em andamento, ação urgente deve ser tomada.

c) MÉDIO: Realizar esforços para reduzir o risco, mas o custo de prevenção deve ser avaliado e limitado, possuí menor o nível de criticidade quanto ao impacto nos negócios do Grupo. As medidas de redução de riscos devem ser implementadas em período de tempo definido.

d) BAIXO: Não requer controles adicionais aos que já existem. É necessário monitoramento e informação existentes. Há necessidade de instrução e monitoramento pelos responsáveis das atividades.

Os riscos priorizados devem entrar em um fluxo diferenciado de tratamento, considerando:

Maior criticidade na implantação dos planos de resposta e ações de remediação de gaps de controle;

Definição de Indicadores de Risco para monitoramento;

Maior frequência de reporte do status do risco e dos planos de resposta ao CAR e CAD.

9.3 Resposta aos Riscos

Após os riscos priorizados na etapa anterior, é definido pela Companhia as estratégias para a tomadade decisão, desenvolvendo uma série de medidas para mitigar as ameaças aos objetivos do Grupo Equatorial, a fim de alinhar os riscos com o respectivo apetite ao risco, desenvolvendo planos de respostas formais definidos pelo Dono do Risco com apoio da Área de GRC. As possibilidades de resposta ao risco são aceitar, compartilhar, evitar e reduzir:

a) Aceitar: a Alta Administração concorda em enfrentar o risco, se e quando ele se materializar. Um plano de solução, ou contingência pode ser desenvolvido para essa eventualidade. Estratégiautilizada quando não é possível ou prático responder ao risco, ou uma resposta não se justifica pela importância do risco;

b) Compartilhar: transferência ou compartilhamento de uma porção do risco, visando a redução da probabilidade ou do impacto (Exemplo: No risco de incêndio, onde o custo do sinistro poderia ser transferido para Seguradoras);

c) Evitar: está relacionada a uma ação que elimina totalmente a fonte de um risco específico (Exemplo: Venda de determinada operação);

d) Reduzir: são adotadas medidas para reduzir o nível de exposição de um evento de risco adverso para um limite aceitável pelo Grupo Equatorial Energia;

Os Planos de Resposta devem definir também ações corretivas ou planos de emergência no caso de materialização de riscos, mesmo que a resposta tenha sido aceitar.

9.4 Monitorar os Riscos

O monitoramento dos riscos é um processo contínuo da Gestão de Riscos, consiste em definir, acompanhar e atualizar periodicamente os Indicadores de Riscos, que estão diretamente relacionados aos fatores de risco, assim como o acompanhamento e atualização do status de implementação dos planos de resposta e/ou de ação em conjunto com as partes interessadas no gerenciamento de riscos.

Periodicamente, os resultados dos indicadores devem ser reportados para a Diretoria primária, conforme frequência estabelecida para cada risco, ao Comitê de Auditoria e Riscos e Conselho de Administração, de acordo com os respectivos calendários de reuniões e regimentos.

10 - REFERÊNCIAS

10.1 Gerenciamento de Riscos Corporativos – Enterprise Risk Management – Aligning Risk with Strategy and Performance – COSO 2017;

10.2 Risk Assessment in Practice by Deloitte Touche Tohmatsu Services, Inc. – COSO 2012;

10.3 Developing Key Risk Indicators to Strengthen Enterprise Risk Management – COSO 2010;

10.4 Implementing Enterprise Risk Management – John R.S. Fraser – 2015;

10.5 Gerenciamento de Riscos Corporativos - Risk Assessment in Practice - COSO 2013;

10.6 Regulamento do Novo Mercado da B3;

10.7 ABNT NBR 31.000 ISO - Technical Management Board Working Group on Risk Management.

GRUPO equatorial ENERGIA