POLITICA DE GESTÃO DE RISCOS DA COMGÁS

REV 1 – 14/07/23

1. OBJETIVO

A presente Política de Gestão de Riscos tem por objetivo estabelecer as diretrizes para identificação, avaliação, tratamento e monitoramento dos riscos inerentes às atividades da organização, bem como definir princípios e responsabilidades a serem observados por todos os colaboradores, contribuindo para a consecução dos objetivos estratégicos da Comgás.

2. APLICAÇÃO

Esta Política é aplicável a Comgás, devendo ser observada por todos os seus Administradores, Conselheiros, empregados, colaboradores, independentemente do nível hierárquico do cargo ou função ocupada, bem como a terceiros que se relacionam ou que atuem em nome da Comgás.

3. FUNDAMENTOS LÓGICOS

3.1. Considerações

A estrutura de Gestão de Riscos da Comgás considera uma atuação em conjunto de todos os seus membros, de acordo com o nível hierárquico dos cargos e funções ocupados, sendo de responsabilidade de todos identificar e comunicar eventuais riscos com o intuito de municiar à Alta Administração da Companhia com as melhores informações, apoiando o negócio no atingimento dos objetivos definidos, auxiliando a tomada de decisão. Conforme os objetivos do trabalho, assuntos envolvidos e relevância das deficiências identificadas, podem ser utilizados níveis variados para a discussão dos riscos e suas ramificações.

A Gestão de Riscos da Comgás será realizada de forma contínua, com reporte periódico à Alta Administração da Companhia, considerando a estrutura, modelo de negócio e complexidade das operações, priorizando os riscos de suborno identificados durante a análise e avaliação.

A Gestão de Riscos também deverá incluir o processo de análise e avaliação da eficácia dos controles internos implementados pela Comgás.

3.2. Definição e tipos de riscos

Risco é todo evento potencial que pode impactar negativamente o alcance dos objetivos da Comgás ou de processos de negócio específicos.

Os riscos são categorizados da seguinte forma:

i. Origem dos eventos

É determinante para a definição da abordagem a ser empregada na resposta ao risco.

- *Riscos externos* são ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a organização opera, porém, em geral, não é possível intervir diretamente sobre estes eventos que terão, portanto, uma ação predominantemente reativa.
- *Riscos internos* são eventos originados na própria estrutura da organização, pelos seus processos, seu quadro de pessoal ou de seu ambiente tendo como resposta uma ação proativa.

i. Natureza dos Riscos

É o que permite uma consolidação dos riscos de uma forma organizada e de acordo com a sua natureza - estratégica, operacional, financeira e de compliance em função da(s) área(s) da organização que é(são) afetada(s) pelos eventos. Os riscos podem pertencer a naturezas distintas e em alguns casos poderão se encaixar em duas ou até mesmo em todas as naturezas simultaneamente.

- *Riscos Estratégicos* estão associados à tomada de decisão da Alta Administração e podem gerar perda substancial no valor econômico da organização.
- *Riscos Operacionais* estão associados à possibilidade de ocorrência de perdas (de produção, ativos, clientes, receitas) 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. Os

riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impacto negativo na reputação da sociedade, além da potencial geração de passivos contratuais, regulatórios e ambientais.

- *Riscos Financeiros* são aqueles associados à exposição das operações financeiras da organização, segregados em:
  i. Câmbio: associado à volatilidade do mercado e pode afetar a Companhia quando tiver ativos ou passivos atrelados à moeda estrangeira.
  ii. Juros: também associado à volatilidade do mercado. A Companhia pode, eventualmente, contratar dívidas e derivativos indexados a taxas de juros fixos ou flutuantes, porém, alterações na percepção de risco dos agentes do mercado podem gerar volatilidade nas curvas de juros e, desta forma, aumentar as despesas financeiras da Companhia.
  iii. Liquidez: Situação em que a Companhia encontra dificuldades em cumprir com as obrigações associadas com seus passivos financeiros.
  iv. Crédito: associado às contrapartes da Companhia que podem, eventualmente, deixar de honrar seus compromissos e obrigações.
- *Riscos de Conformidade (Compliance)* aqueles associados à exposição a 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 a prevenção de lavagem de dinheiro, integridade etc.
- *Riscos de Suborno* aqueles associados à oferta, promessa, aceitação ou solicitação de qualquer vantagem indevida, ainda que não seja financeira, direta ou indiretamente, com o objetivo de influenciar uma pessoa a praticar ou deixar de praticar determinado ato em troca de benefícios ilegais.

i. Tipo

As naturezas dos riscos podem ter diversos tipos de riscos associados a ela, variando de acordo com a origem, ambiente e reposta ao risco. Ex.: Risco de origem interna, de natureza financeira do tipo SOx.

3.3. Identificação de riscos

O processo de identificação de riscos tem por objetivo principal reduzir seus eventos de ocorrência com impactos negativos à Comgás. Dessa forma, o limite temporal para o processo de reavaliação de riscos das áreas de negócios deve ser definido em conjunto com os respectivos gestores das áreas, não podendo ser superior a 2 (dois) anos, a depender da criticidade dos riscos identificados no ciclo anterior.

Em relação aos riscos de Conformidade ou de Suborno, definidos no item 4.2 desta política, a periodicidade de reavaliação será definida de acordo com a criticidade dos processos avaliados, conforme definido na Planilha de Controle da Matriz de Riscos de Compliance.

O processo de identificação de riscos da Comgás deve ser precedido de uma análise da empresa e de seus contextos, interno e externo, como tamanho, estrutura, modelo de negócios aplicado, parceiros e fornecedores que se relacionam com as organizações, obrigações e deveres estatutários, regulatórios e legais.

O processo de Gestão de Riscos da Companhia é baseado na Matriz Impacto versus Probabilidade, de acordo com os critérios estabelecidos a seguir:

3.3.1. Cálculo do impacto

O impacto deve ser analisado nas dimensões financeira, reputacional, jurídica, operacional, saúde e segurança, social e meio ambiente, em níveis classificados como muito baixo, baixo, médio, alto e muito alto.

O impacto financeiro informa os limites aceitáveis que a Companhia está disposta a colocar em risco em troca de valor. Deve estar alinhado com a missão, a visão, os valores fundamentais e a estratégia adotada. Fatores qualitativos e quantitativos, tais como: volatilidade de resultados, dependência de capital, reputação, rigores regulatórios, entre outros, podem ser utilizados no cálculo

para ajuste da classificação para um perfil mais agressivo ou conservador, conforme o caso.

Uma vez definido o impacto financeiro, será utilizado como referência o montante envolvido no processo em questão para uma base de 12 meses.

3.3.2. Definição da probabilidade

A probabilidade trata das chances do impacto negativo apurado se materializar e é calculada da seguinte forma:

PROBABILIDADE			
Peso	**Classificação**	**Quantitativo**	**Qualitativo**
1	Muito Baixa	O evento repete uma vez por ano ou menos	Hipótese muito restrita de ocorrência, pois as circunstâncias pouco indicam a possibilidade. O evento nunca ocorreu anteriormente na empresa e/ou é extremamente raro no setor.
2	Baixa	O evento repete mais de uma vez por ano	Evento pode ocorrer em algum momento, mas as circunstâncias pouco indicam essa possibilidade. O evento nunca ocorreu na empresa e/ou já ocorreu esporadicamente no setor.
3	Média	O evento repete uma vez por mês	Evento pode ocorrer em algum momento, pois as circunstâncias indicam moderadamente essa possibilidade. O evento pode ter ocorrido anteriormente na empresa e/ou ocorre periodicamente no setor.
4	Alta	O evento repete mais do que uma vez ao mês, porém menos do que semanalmente	Evento pode ocorrer em algum momento, pois as circunstâncias indicam essa possibilidade. O evento ocorreu na empresa no último ano e/ou regularmente ocorre para muitas organizações do setor.
5	Muito Alta	O evento repete uma vez por semana ou mais	Evento esperado que ocorra, as circunstâncias indicam claramente essa possibilidade. O evento ocorreu na empresa pelo menos uma vez ao ano e/ou ocorre para quase todas as organizações do setor.

Figura 1 – Situação e probabilidade

3.3.3. Definição do nível de risco

Após o cálculo do impacto e da probabilidade de ocorrência de riscos identificados, serão definidos os respectivos níveis de riscos, a partir da combinação dos pesos atribuídos aos cálculos de impacto versus probabilidade, a fim de determinar a ordem de prioridade de tratamento desses riscos.

3.3.4. Análise da maturidade dos controles existentes

Após a definição do nível do risco inerente, isto é, o nível de risco antes de aplicados os controles mitigatórios, deverão ser analisados na Matriz de Riscos e Controles todos os controles existentes e implementados formalmente para mitigar a ocorrência e o impacto negativo desse risco.

3.3.5. Avaliação do Risco Residual

Após a avaliação da maturidade dos controles mitigatórios implementados, será possível definir o nível de risco residual, ou seja, o nível de risco remanescente após a aplicação dos controles implementados pela Companhia.

4. IMPLEMENTAÇÃO

4.1. Resposta ao Risco

A Comgás mantem estruturas à gestão dos riscos operacionais e estratégicos, como Controles Internos, SSMA (Saúde, Segurança e Meio Ambiente), Gestão de Crises e Gestão de Riscos, e as utiliza como instrumento para proteção. Tais áreas operam concomitantemente a sistemas operacionais sofisticados com recursos de segurança específicos, tais como bloqueio de acessos a sistemas chave da Companhia, parametrizações pré-determinadas de segregação de função na execução das atividades, log de atividades dentro do sistema, entre outros que buscam a mitigação desses riscos.

A Gestão de Riscos deve estar integrada aos processos de planejamento estratégico da Comgás, sendo realizada de forma gradual, priorizando os processos internos que porventura estejam mais expostos ao risco de suborno e que possam impactar diretamente no atingimento de objetivos definidos pela Alta Administração.

O risco nunca pode ser eliminado por completo, no entanto, para definição das tratativas, a avaliação dos riscos é feita de forma conjunta, envolvendo tanto as áreas mencionadas, como também a Diretoria responsável pelo processo em que o risco foi identificado, avaliando o grau de impacto *versus* probabilidade de ocorrência para cada risco identificado, para então definir-se o melhor instrumento de proteção, que podem ser:

- Evitar: Quando se elimina o fato gerador do risco, por exemplo, descontinuando determinado processo ou saindo de mercado específico. Dessa forma, são estabelecidas ações que eliminam a probabilidade do risco se materializar.
- **Mitigar**: Quando são aplicáveis os controles internos (ex.: aprovação, revisão, segregação de funções, reconciliação, perfis de

acesso etc.) ou barreiras para que o dano potencial e/ou probabilidade do risco sejam substancialmente reduzidos.

- Transferir: Quando o risco é dividido ou transferido para uma contraparte externa à Empresa. Exemplos de compartilhamento de riscos são as operações de *hedge* (moeda estrangeira, preços, juros) e apólices de seguro.
- Aceitar: Quando o impacto *versus* probabilidade do risco é considerado irrelevante, toma-se a decisão de aceitar o risco, pois o custo da ação de controle seria maior do que o próprio risco potencial envolvido.

O entendimento dos riscos e adoção de ações como resposta é de responsabilidade de todos os gestores da Comgás.

Todos os assuntos ou dúvidas relacionadas a riscos, relevância e controles devem ser esclarecidos junto as áreas de Auditoria Interna da Cosan, Riscos, Controles Internos e Compliance da Comgás.

5.2. Papéis e Responsabilidades

A Companhia possui uma área específica de Gerenciamento de Riscos e atua com o direcionamento e apoio do Comitê de Auditoria e da Diretoria Financeira, que acompanham e monitoram as atividades relativas ao processo de gestão de riscos da Comgás.

O Conselho de Administração é responsável por analisar e aprovar esta Política de Gestão de Riscos, definindo as diretrizes necessárias para a sua correta execução, bem como o apetite ao risco, que consiste na definição do nível de risco que a Comgás está disposta a aceitar.

Os *risk owners* (proprietários dos riscos) são responsáveis por recomendar ajustes na matriz de riscos quando julgar necessário, garantindo o registro dos riscos nas hipóteses em que não se enquadrem nos fatores de riscos existentes na matriz vigente. Possuem as atribuições de avaliar e propor melhorias dos mecanismos de gestão de riscos e controles internos em sua área/negócio, além de garantir os recursos necessários para a implementação e execução dos planos de ação para mitigação dos riscos identificados.

Os diretores devem atuar de forma comprometida no gerenciamento e cultura de riscos, por meio do engajamento, conhecimento, compreensão e acompanhamento dos principais riscos da Companhia, além de ratificar a

priorização dos riscos a serem tratados/gerenciados nos processos e áreas de sua supervisão.

As gerências de Controles Internos e Compliance são responsáveis pela supervisão e monitoramento dos riscos de Compliance, em especial os riscos de suborno identificados, sendo responsáveis pela elaboração e condução dos eventuais planos de ação para mitigação de tais ocorrências, realizando o reporte periódico à Função Antissuborno por meio de indicadores.

O Comitê de Auditoria da Companhia desempenha a função de verificar a adequação da estrutura operacional de Gestão de Riscos de forma a garantir a efetividade desta Política, reportando-se, periodicamente, ao Conselho de Administração.

1. Monitoramento

Para que o processo de Gestão de Riscos esteja adequado e seja realizado de forma eficiente, é fundamental que o processo de avaliação seja periódico, devendo ser realizado o monitoramento contínuo dos riscos identificados e dos planos de ação que tenham sido executados. Dessa forma, caberá à Alta Administração da Companhia, o monitoramento e análise crítica por meio de indicadores dos resultados obtidos.

Todo o processo de supervisão, acompanhamento, análise crítica e monitoramento deverá ser devidamente documentado, permitindo, assim, um maior controle e um fluxo eficaz de informações para identificar eventuais necessidades de ajustes.

2. Considerações Finais

Todos os casos omissos, exceções e necessidades de alteração no presente documento deverão ser submetidos à análise do Comitê de Auditoria e Conselho de Administração.

A não observância às regras e diretrizes previstas nesta Política poderá ensejar na aplicação de sanções disciplinares previstas na "Política de Medidas Disciplinares PLT-033" e no Código de Conduta, sem prejuízo de a Comgás adotar as medidas administrativas, civis e penais cabíveis conforme o caso.

1. Revisão e Aprovação

Esta Política será revisada periodicamente, nos termos das regras internas de governança normativa, ou sempre que houver advento de mudanças significativas em processos, normas ou leis que possam afetar a adequação desta Política às necessidades da Comgás, ou, ainda, por determinação da Diretoria emitente. Eventuais modificações significativas nesta Política serão prontamente divulgadas.

A presente Política revoga todas as disposições em contrário.

Conforme disposto no Estatuto Social da Companhia, a presente Política foi aprovada pelo Conselho de Administração.

comgas