SUMÁRIO

1. Apresentação 3
1.1 Objetivo da Política 3
1.2 Abrangência e Princípios 3
1.3 Vigência 3
1.4 Área técnica responsável pela política 3
2. Conceitos e Definições 4
3. Referencial 5
3.1. Combate à Corrupção e Suborno (Anticorrupção): 5
3.2. Prevenção à Lavagem de Dinheiro (PLD): 6
3.3. Proteção de Dados e Privacidade: 6
3.4. Concorrência e Defesa do Consumidor: 6
3.5. Legislação Trabalhista e Segurança: 6
3.6. Demais Referências: 7
3.7. Código de Ética e Conduta: 7
4. DIRETRIZES (Foco nos Mecanismos de Prevenção e Detecção) 7
4.1. Due Diligence de Integridade (DDI) e Gestão de Terceiros 7
4.2. Controles Internos e Monitoramento de Risco 8
4.4. Segurança da Informação e LGPD 8
5. DIVULGAÇÃO E DISSEMINAÇÃO 9
6. RESPONSABILIDADES 9
6.1 Primeira Linha (Operação): 9
6.2 Segunda Linha (Controle): 9
6.3 Terceira Linha (Garantia): 9
7. PROCESSO DE INVESTIGAÇÃO INTERNA 9
7.1. Delimitação de Objeto e Escopo: 9
7.2. Coleta e Preservação de Evidências: 10
7.3. Entrevistas: Planejamento e Imparcialidade: 10
7.4. Relatório Conclusivo: 10
8. MONITORAMENTO, AUDITORIA E INDICADORES 10
8.1. Monitoramento e Testes de Conformidade 11
8.2. Auditoria e Análise Crítica Periódica 11
8.3. Indicadores de Desempenho (Key Performance Indicators - KPI) 11
9. CANAL DE DENÚNCIA 12

10. CONSEQUÊNCIAS 12
11. MELHORIA CONTÍNUA 12
12. GESTÃO DE DOCUMENTOS E REGISTROS 12
12.1. Armazenamento Seguro e Confidencialidade 13
12.2. Rastreabilidade e Retenção 13
13. EXCEÇÕES 13

1. Apresentação

A presente Política Corporativa de Compliance e Integridade estabelece princípios, diretrizes, responsabilidades e procedimentos destinados a promover o cumprimento das leis, regulamentos e normas internas aplicáveis às atividades da Organização, assegurando uma atuação íntegra, ética, transparente e responsável.

1.1 Objetivo da Política

1.1.1 Geral: Assegurar a observância das diretrizes para uma atuação ética, transparente e com tolerância zero à fraude e à corrupção. O Programa visa prevenir, detectar e remediar desvios de conduta, garantindo a conformidade com as leis nacionais e internacionais (LAC, FCPA) e, de forma específica, com as políticas de integridade e os requisitos Legais , bem como com as diretrizes do Programa de Compliance.

1.1.2 Específico: Garantir o cumprimento integral de leis, regulamentos e normativos internos, além de prevenir, detectar e responder a desvios éticos, fraudes, irregularidades e atos lesivos, promovendo um ambiente organizacional baseado em integridade e ética.

1.2 Abrangência e Princípios

Aplica-se a todos os públicos de interesse da INACE: administradores, colaboradores, fornecedores, prestadores de serviços, parceiros, terceiros, intermediários (brokers), subcontratados e demais parceiros de negócio, com utilização de mecanismos de monitoramento em toda a cadeia de valor, são salvaguardados os princípios do Programa de Compliance: Integridade, Transparência, Proporcionalidade, Boa Governança, Responsabilização e Sustentabilidade.

1.3 Vigência

Esta Política entra em vigor na data de sua publicação e terá prazo indeterminado, com revisão periódica a cada 12 meses ou sempre que necessário.

1.4 Área técnica responsável pela política

A Alta Administração assume o compromisso de demonstrar conduta exemplar, garantir os recursos necessários ao Programa e assegurar a independência funcional da área de Compliance. Ressalta-se que o sucesso do Programa de Compliance e Integridade é responsabilidade de toda a Companhia, sendo indispensável a liderança e o suporte incondicional da Alta Administração.

1.4.1 Comprometimento da Alta Gestão (Tone at the Top)

O Conselho de Administração e a Diretoria Executiva devem demonstrar apoio visível e inequívoco ao Programa, assegurando que a ética e a integridade prevaleçam sobre as metas de negócio e garantindo que atos lesivos resultem em responsabilização.

1.4.2 Obrigações de Compliance

Identificar e monitorar continuamente as leis, normas e regulamentos aplicáveis.

1.4.3 Provisão de Recursos

A INACE deve prover recursos financeiros, tecnológicos e humanos adequados e suficientes para que a função de Compliance opere de forma efetiva.

1.4.4 Independência

A Companhia deve garantir a independência e a autonomia da Área de Compliance, assegurando que seus pareceres e ações não sejam obstruídos ou indevidamente influenciados.

1.4.5 Promoção da Cultura

A Companhia deve liderar pelo exemplo, promovendo e exigindo uma cultura de conformidade e integridade em todos os níveis e junto a todos os públicos de interesse.

2. *Conceitos e Definições*

Para fins desta Política, serão considerados para a Programa de Compliance

- **Integridade:** Conjunto de princípios e valores éticos que definem a cultura da Companhia e guiam a conduta de todos os públicos de interesse, assegurando que as ações sejam transparentes, responsáveis e em conformidade com as leis.
- **Conformidade (Compliance):** Refere-se à obrigação de cumprir todas as leis, regulamentos, normas setoriais e políticas internas aplicáveis às atividades da Organização.
- **Fraude:** Qualquer ato intencional de omissão ou manipulação com o objetivo de obter vantagem indevida, causando prejuízo à Companhia ou a terceiros.
- **Corrupção:** Ato de oferecer, prometer, dar ou autorizar, direta ou indiretamente, qualquer vantagem indevida a **Agente Público** ou a outra pessoa em troca de influência ou decisão favorável.
- **Agente Público:** Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nas entidades da Administração Pública, nacional ou estrangeira.
- **Públicos de Interesse (Stakeholders):** Pessoas e entidades que interagem com a Companhia e estão sujeitas a esta Política, incluindo administradores, colaboradores, fornecedores, prestadores de serviços, parceiros, terceiros, intermediários (*brokers*), subcontratados e parceiros de negócio, monitorados em toda a **Cadeia de Valor**.
- **Controles Internos:** Mecanismos, regras, procedimentos e ações estabelecidas pela Alta Administração para assegurar a execução eficiente das operações e o cumprimento dos objetivos do *Compliance*, prevenindo erros e fraudes.

- **Segregação de Funções:** Princípio fundamental de Controle Interno que estabelece que nenhuma pessoa deve ter controle completo sobre todas as etapas de uma transação ou processo crítico, visando mitigar o risco de fraude.
- **Risco de Integridade (GRI):** Risco de ocorrência de atos de corrupção, fraude, suborno, lavagem de dinheiro ou outros atos lesivos contra a Administração Pública ou a própria Companhia.
- **Prevenção à Lavagem de Dinheiro (PLD):** Conjunto de medidas e procedimentos para prevenir que a Companhia seja utilizada, de forma não intencional, para ocultar ou dissimular a origem, movimentação ou propriedade de bens, direitos ou valores provenientes de atividades criminosas.
- **Conheça Seu Cliente (KYC - Know Your Client):** Procedimento obrigatório de PLD que visa a identificação e verificação da identidade dos clientes, parceiros e fornecedores, e a análise da compatibilidade das transações com o perfil de risco apurado.
- **Canal de Conduta (Denúncias):** Ferramenta sigilosa e independente, administrada por terceiros ou pela área de *Compliance*, que permite aos públicos de interesse reportar, de boa-fé e com garantia de não retaliação, suspeitas de violação ao Código de Ética, à lei ou a esta Política.
- **Modelo das Três Linhas de Defesa:** Modelo de governança que estabelece papéis e responsabilidades claras para a gestão de riscos e controles, dividindo-os em: Primeira Linha (Operação/Gestão de Riscos), Segunda Linha (*Compliance*/Controle) e Terceira Linha (Auditoria Interna/Garantia).
- **Litigation Hold:** Procedimento formal de suspensão imediata da rotina de descarte de documentos e registros (físicos ou digitais) assim que a Companhia toma conhecimento de uma investigação, litígio ou processo regulatório, garantindo a preservação das evidências.

3. Referencial

3.1. Combate à Corrupção e Suborno (Anticorrupção):

Este é o pilar fundamental do Compliance em qualquer empresa que se relaciona com o poder público ou que atua em nível internacional.

3.1.1 Lei nº 12.846/2013 (Lei Anticorrupção Brasileira - LAC):

3.1.1.1 Foco: Responsabiliza civil e administrativamente empresas (pessoas jurídicas) por atos de corrupção, fraude em licitações e outros atos lesivos contra a administração pública nacional ou estrangeira.

3.1.1.2 Impacto no Compliance: É a lei que define os Programas de Compliance como critério de atenuação de penalidades (art. 7º, VIII). A política de Compliance deve, obrigatoriamente, focar na prevenção, detecção e remediação dos atos listados na LAC.

3.1.2 Decreto nº 8.420/2015:

3.1.2.1 Foco: Regulamenta a LAC, detalhando os parâmetros para avaliação dos programas de integridade (Compliance) e as regras para a celebração de Acordos de Leniência.

3.1.3 Foreign Corrupt Practices Act (FCPA- EUA):

3.1.3.1 Foco: Lei americana que proíbe o suborno a funcionários públicos estrangeiros. É crucial para a INACE, que busca a internacionalização, pois qualquer empresa que faça negócios nos EUA ou utilize o dólar pode ser responsabilizada.

3.2. Prevenção à Lavagem de Dinheiro (PLD):

Especialmente relevante no setor de bens de alto valor, como INACE IATES LTDA.

3.2.1 Lei nº 9.613/98 (Lei de Lavagem de Dinheiro):

3.2.1.1 Foco: Define o crime de lavagem de dinheiro, estabelece penalidades e, o mais importante para o Compliance, obriga determinados setores (como o de bens de luxo e o financeiro) a adotarem medidas de Prevenção à Lavagem de Dinheiro (PLD).

3.2.1.2 Impacto no Compliance: Requer políticas de "Conheça seu Cliente" (KYC- Know Your Client) e monitoramento de transações atípicas, especialmente no fechamento de grandes vendas de INACE IATES LTDA.

3.3. Proteção de Dados e Privacidade:

Essencial para a gestão de informações de clientes e colaboradores. Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD):

3.3.1 Foco: Regula o tratamento de dados pessoais no Brasil, impondo regras rigorosas sobre coleta, armazenamento, processamento e descarte de informações.

3.3.2 Impacto no Compliance: A política deve incluir um pilar de **Compliance Digital/LGPD**, garantindo a segurança dos dados e o consentimento dos titulares, evitando multas e danos à reputação.

3.4. Concorrência e Defesa do Consumidor:

Garantem a ética nas relações comerciais.

3.4.1 Lei nº 8.884/94 (Lei da Concorrência):

3.4.1.1 Foco: Previne e reprime infrações contra a ordem econômica (cartéis, dumping, etc.).

3.4.1.2 Impacto no Compliance: As políticas devem incluir diretrizes claras sobre antitruste, especialmente em parcerias ou relações com fornecedores e concorrentes internacionais.

3.4.2 Lei nº 8.078/90 (Código de Defesa do Consumidor- CDC):

3.4.2.1 Foco: Proteção e defesa dos direitos do consumidor.

3.4.2.2 Impacto no Compliance: Garante que a comunicação, os contratos e o pós-venda (serviços de refit e manutenção) sigam padrões de ética e transparência.

3.5. Legislação Trabalhista e Segurança:

Garantem a integridade da relação com a mão de obra especializada do estaleiro. **Consolidação das Leis do Trabalho (CLT) e Normas Regulamentadoras (NRs):**

3.5.1 Foco: Saúde, segurança e direitos dos trabalhadores.

3.5.2 Impacto no Compliance: O Compliance Trabalhista garante que o estaleiro cumpra integralmente as leis de segurança do trabalho (especialmente em um ambiente de construção naval) e evite passivos e multas trabalhistas.

3.6. Demais Referências:

- ISO 37001, ISO 37301, COSO ERM, IIA, ABRAPP, CGU demais órgão reguladores.
- MANUAL DE COMPLIANCE: Os Pilares do programa de Compliance, LEC – Legal Ethics Compliance. São Paulo em 06/09/2021
- GUIA PRATICO COMPLIANCE – Certificação Compliance Livro KPMG Business School. São Paulo em novembro/2020
- Guia de compliance [livro eletrônico] / [organização] ABRAPP- Associação Brasileira das Entidades Fechadas e Previdência Complementar, Comissão Técnica Sul de Governança e Riscos da Abrapp.--São Paulo : ABRAPP Associação Brasileira das Entidades Fechadas de Previdência Complementar,2021.
- CICLO PDCA - DEMMING, W. Edwards. Out of the Crisis. Cambridge, MA: Massachusetts Institute of Technology – Center for Advanced Engineering Study, 1986

3.7. Código de Ética e Conduta:

Define valores, comportamentos aceitáveis, relacionamento com agentes públicos, conflitos de interesse e proibição de suborno.

4. DIRETRIZES (Foco nos Mecanismos de Prevenção e Detecção)

4.1. Due Diligence de Integridade (DDI) e Gestão de Terceiros

4.1.1 Obrigatoriedade da DDI: É obrigatória a realização da Due Diligence de Integridade (DDI) para todos os terceiros que representem risco de integridade para a INACE, incluindo subcontratados em projetos com estatais.

4.1.2 Classificação de Risco: Os terceiros serão classificados em Baixo, Médio ou Alto Risco de Integridade (GRI), sendo a extensão das medidas de controle proporcional a essa classificação.

4.1.3 Cláusulas de Conformidade: Todos os contratos de fornecimento, parcerias e subcontratações devem conter cláusulas específicas de Compliance, permitindo a auditoria da INACE sobre a conformidade do parceiro e prevendo sanções em caso de violação das leis anticorrupção.

4.2. Controles Internos e Monitoramento de Risco

4.2.1 Gestão de Riscos de Compliance: Adoção das metodologias COSO ERM e ISO 37301 para identificação, avaliação, definição de controles, análise de riscos residuais e implementação de ações mitigatórias.

4.2.2 Gestão de Riscos entes públicos: O Comitê de Compliance deve realizar análises periódicas dos riscos de integridade, com foco em áreas de maior exposição, como licitações, compras, transações financeiras e relacionamento com Agentes Públicos.

4.2.3 Segregação de Funções: Devem ser mantidos Controles Internos robustos, incluindo a segregação de funções em processos críticos (por exemplo: pagamentos, contratação de fornecedores), a fim de evitar que uma única pessoa detenha controle total sobre uma transação.

4.2.4 Auditoria Contínua: A INACE manterá um processo de monitoramento e auditoria contínua para verificar a aderência e a efetividade dos Controles Internos e do Programa de Integridade.

4.3. Regras de Relacionamento com Agentes Públicos e Contratações

4.3.1 Presentes, Brindes e Hospitalidade (Densidade): As regras sobre Presentes, Brindes e Hospitalidade devem ser formalizadas em diretriz específica, estabelecendo limites de valor, a necessidade de registro e a exigência de aprovação prévia, de modo a evitar qualquer percepção de influência indevida em processos de licitação ou tomada de decisão.

4.3.2 Processos de Licitação: A participação em licitações com empresas estatais ou órgãos da Administração Pública deve ser conduzida sob a estrita supervisão da área de Compliance, garantindo lisura, transparência e o compromisso de não frustrar o caráter competitivo do processo.

4.3.3 Uso de Intermediários: A contratação de intermediários para atuação perante a Administração Pública é desestimulada e, quando estritamente necessária, estará sujeita à Due Diligence de Integridade (DDI) de Alto Risco.

4.4. Segurança da Informação e LGPD

A INACE deve garantir que possui políticas e procedimentos específicos para a preservação da privacidade e segurança de dados, assegurando a conformidade com a LGPD e com os altos padrões de segurança da informação incluindo também as adequações legais a Administração Pública.

5. DIVULGAÇÃO E DISSEMINAÇÃO

O Comitê de Compliance deve garantir que os treinamentos são obrigatórios e periódicos para todos os colaboradores, incluindo a Alta Administração. O conteúdo dos treinamentos deve ser adequado ao risco da função (ex: foco para a área comercial; foco em Anticorrupção para a equipe de licitações). Este modelo servirá de base para o estabelecimento, acompanhamento e análise crítica dos Objetivos da Qualidade, assegurando que as melhorias sejam sustentáveis e orientadas a agregar valor.

6. RESPONSABILIDADES

As responsabilidades são alocadas conforme o Modelo das Três Linhas de Defesa (Recomendação de Boas Práticas da CGU):

6.1 Primeira Linha (Operação):

Áreas de negócio (Comercial, Compras, Jurídico) – Responsáveis por identificar e gerenciar os riscos em suas atividades diárias.

6.2 Segunda Linha (Controle):

Comitê de Compliance / Compliance Officer – Responsáveis por estabelecer políticas, monitorar os riscos e realizar a DDI.

6.3 Terceira Linha (Garantia):

Auditoria Interna – Responsável por avaliar, de forma independente, a efetividade das duas primeiras linhas.

7. PROCESSO DE INVESTIGAÇÃO INTERNA

O Processo de Investigação Interna é o mecanismo de resposta da Companhia para apurar as denúncias recebidas por meio do Canal de Conduta, garantindo a lisura, a imparcialidade e a conformidade legal do procedimento.

7.1. Delimitação de Objeto e Escopo:

A delimitação de objeto e escopo é a fase inicial e estruturante de qualquer investigação interna, pois define com clareza o que será investigado, por que, de que forma e até onde o processo irá se estender. Essa etapa garante que a investigação seja conduzida com precisão, imparcialidade, foco e eficiência, evitando excessos, omissões ou desvios de finalidade.

7.1.1 Recebimento e Análise Preliminar: A Área de Compliance (ou o Comitê) realizará a triagem e a classificação inicial da denúncia. Será feita a delimitação precisa dos fatos, das pessoas e do período a ser investigado.

7.1.2 Designação da Equipe: A investigação será conduzida por uma equipe interna devidamente treinada, ou por terceiros independentes, garantindo a imparcialidade, confidencialidade e o

conhecimento técnico. A equipe deve assinar um termo de confidencialidade e isenção de conflito de interesses.

7.2. Coleta e Preservação de Evidências:

Princípio da Preservação: Todas as informações e documentos potencialmente relevantes devem ser coletados de maneira sistemática e segura, garantindo a integridade da cadeia de custódia (digital e física) das evidências, evitando contaminação ou adulteração.

7.2.1 Tipos de Evidências: A coleta pode incluir e-mails, registros de acesso, dados de sistemas financeiros, documentos de compras e licitações, e-mails corporativos, mensagens e quaisquer outros registros que possam comprovar ou refutar a denúncia. O tratamento de dados pessoais durante a coleta deve seguir estritamente os preceitos da LGPD.

7.3. Entrevistas: Planejamento e Imparcialidade:

As entrevistas serão conduzidas de maneira estruturada, com base nas evidências coletadas, e com o objetivo de obter informações relevantes e esclarecer os fatos. O entrevistador deve manter a neutralidade e assegurar que o entrevistado se sinta seguro e protegido de retaliação.

7.3.1 Direito de Defesa: Em respeito ao direito de defesa, os entrevistados sobre os quais recaiam suspeitas de má conduta (sujeitos da investigação) terão o direito de serem acompanhados por um advogado particular, se assim o desejarem, e serão formalmente notificados sobre as acusações para que possam apresentar sua versão.

7.4. Relatório Conclusivo:

Estrutura: Ao término da apuração, a equipe de investigação elaborará um relatório minucioso, contendo: (a) o resumo dos fatos investigados; (b) a metodologia utilizada; (c) as evidências coletadas; (d) as conclusões e a materialidade da violação; e (e) a recomendação de medidas disciplinares (se for o caso) e planos de ação corretivos e preventivos para a Área de Compliance.

7.4.1 Decisão e Ação: O relatório será apresentado ao Comitê de Auditoria Estatutário ou à Alta Administração, que deliberará sobre as medidas a serem aplicadas, garantindo que as ações sejam proporcionais à gravidade da violação e estejam em conformidade com o Código de Conduta e a legislação vigente.

8. MONITORAMENTO, AUDITORIA E INDICADORES

Auditorias, testes de conformidade, monitoramento e análise crítica periódica conforme ISO 37301. O monitoramento e a auditoria são fundamentais para **garantir a efetividade** do Programa de *Compliance* ao longo do tempo. Conforme a **ISO 37301**, o sistema de gestão de *compliance* deve ser dinâmico e estar sujeito à análise e à melhoria contínua.

8.1. Monitoramento e Testes de Conformidade

8.1.1 Monitoramento Contínuo: A Área de *Compliance* realizará o monitoramento de forma contínua, visando identificar transações, eventos ou padrões de comportamento atípicos ou de alto risco. Isso inclui a verificação de **Controles Internos** e a análise de dados financeiros para identificar possíveis desvios.

8.1.2 Testes de Conformidade (*Compliance Testing*): Serão realizados testes periódicos e pontuais, focados nas áreas de maior risco (ex: despesas com Agentes Públicos, processos de DDI, compras e licitações), para avaliar se os controles estão funcionando conforme o esperado e se os colaboradores estão aderindo às políticas.

8.2. Auditoria e Análise Crítica Periódica

8.2.1 Auditoria Interna (Terceira Linha de Defesa): A Auditoria Interna é responsável por **avaliar de forma independente** a adequação e a eficácia do Programa de *Compliance*, testando os controles estabelecidos pela Segunda Linha e a aderência das operações (Primeira Linha).

8.2.2 Análise Crítica (Alta Administração): A Alta Administração deve realizar, anualmente ou mediante eventos relevantes, uma **Análise Crítica** do Programa de Integridade, garantindo:

8.2.2.1 O Programa continua adequado ao contexto e aos riscos da Companhia.

8.2.2.2 Os objetivos de *Compliance* estão sendo alcançados.

8.2.2.3 Há provisão de recursos suficientes para a manutenção do Programa.

8.3. Indicadores de Desempenho (Key Performance Indicators - KPI)

A efetividade do Programa será medida por indicadores quantitativos e qualitativos, tais como:

8.3.1 KPIs de Prevenção e Detecção:

8.3.1.1 Percentual de colaboradores treinados em Compliance.

8.3.1.2 Número e taxa de aprovação de Due Diligence de terceiros (DDI).

8.3.1.3 Tempo médio para atualização de políticas internas.

8.3.2 KPIs de Resposta e Remediação:

8.3.2.1 Volume de denúncias recebidas e taxa de denúncias procedentes.

8.3.2.1 Tempo médio de conclusão das investigações internas.

8.3.2.2 Taxa de aplicação de medidas disciplinares em casos de violação comprovada.

8.3.3 KPIs Culturais (Percepção): Resultados de pesquisas internas sobre a percepção da cultura de integridade e do conhecimento do Canal de Conduta.

9. CANAL DE DENÚNCIA

Independente, seguro, com anonimato e proteção contra retaliação. A inserção de um Canal de Denúncias permite a comunicação de irregularidades de forma anônima e tem como intuito proteger o colaborador contra represálias. O Canal é um sistema que auxilia no tratamento e análise de dados de não-conformidade. Sanções Disciplinares: Se a falha for detectada, ela deve ser corrigida de imediato e, se for o caso, uma medida disciplinar pertinente deve ser aplicada prontamente. A INACE IATES LTDA disponibiliza um Canal de Denúncia independente, seguro e confidencial, destinado ao recebimento de relatos de suspeitas ou indícios de violações ao Código de Ética e Conduta, a esta Política de Compliance e Integridade, à legislação vigente ou a quaisquer normas internas da Companhia.

O Canal de Denúncia pode ser acessado por meio do seguinte link: www.contatoseguro.com.br/inace

O canal está disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, permite a realização de denúncias de forma anônima, se assim desejar o denunciante, e assegura a confidencialidade das informações, bem como a proteção contra qualquer forma de retaliação aos denunciantes que atuem de boa-fé.

10. CONSEQUÊNCIAS

A violação desta política, especialmente em atos lesivos contra os instrumentos normativos internos, bem como contra os ditames que regem a Administração Pública, resultará em sanções disciplinares severas, podendo incluir a rescisão imediata do contrato de trabalho e o acionamento das autoridades competentes. O Canal de Conduta (Denúncias) deve garantir proteção contra qualquer forma de retaliação àqueles que, de boa-fé, reportarem não conformidades, reforçando um dos principais indicadores de eficácia dos processos institucionais.

11. MELHORIA CONTÍNUA

Uso do ciclo PDCA — Planejar, Fazer, Checar, Agir — para aprimoramento contínuo. O aprimoramento contínuo é fundamental, pois o sistema de gestão de compliance deve estar preparado para constantes adequações. Os negócios estão em constante mudança por força de vários fatores como tecnológicos, sociais, comportamentais, econômicos, políticos e ambientais.

12. GESTÃO DE DOCUMENTOS E REGISTROS

Armazenamento seguro, rastreabilidade e sigilo a Gestão de Documentos e Registros é um pilar essencial para a governança e para a demonstração da efetividade do Programa de Compliance perante órgãos reguladores e em eventuais investigações internas ou externas. O objetivo é assegurar que todas as ações e decisões tomadas estejam devidamente registradas e possam ser recuperadas.

12.1. Armazenamento Seguro e Confidencialidade

Segurança Física e Digital: A Companhia deve implementar sistemas de armazenamento que garantam a segurança física (acesso restrito, controle de cópias) e a segurança digital (criptografia, firewalls, backups regulares e redundantes) de todos os documentos e registros de Compliance.

12.1.1 Sigilo e Acesso Restrito: Será estabelecida uma política rigorosa de acesso baseado na necessidade de saber (need-to-know), garantindo que apenas o Comitê de Compliance, o Compliance Officer e a equipe de Investigação Interna (quando aplicável) tenham acesso aos registros mais sensíveis (ex: denúncias, relatórios de DDI de alto risco e processos de investigação).

12.1.2 Conformidade com a LGPD: Os documentos que contenham dados pessoais de colaboradores, terceiros, clientes ou partes relacionadas deverão ser tratados e armazenados em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD) e as políticas internas de Segurança da Informação.

12.2. Rastreabilidade e Retenção

12.2.1 Rastreabilidade: Todos os registros de ações de Compliance (ex: aprovações de brindes, relatórios de DDI, atas de reuniões do Comitê, comprovantes de treinamento e ações corretivas) devem conter metadados que permitam sua rastreabilidade imediata, incluindo data, responsável pela criação/aprovação e versão do documento.

12.2.2 Política de Retenção de Documentos: Será instituída uma Política de Retenção e Descarte que define, em alinhamento com a legislação aplicável (ex: prazos fiscais, trabalhistas e da Lei Anticorrupção), o período mínimo de guarda obrigatória para cada tipo de registro. Após o prazo legal, os documentos serão descartados de forma segura para evitar vazamentos.

12.2.3 Preservação em Caso de Investigação: Em caso de conhecimento ou suspeita de uma investigação (interna ou externa) ou litígio, a retenção de documentos e a rotina de descarte serão suspensas imediatamente (conforme o procedimento de Litigation Hold), garantindo a preservação de todas as evidências potenciais.

13. EXCEÇÕES

Para todas as situações excepcionais e/ou não contempladas nesta política, caberá ao **Comitê de Auditoria Estatutário** ou ao **Conselho de Administração** tomar a decisão final, mediante recomendação do *Compliance Officer*, garantindo que a decisão está devidamente registrada e fundamentada no interesse da integridade da Companhia.

Revisão Documental

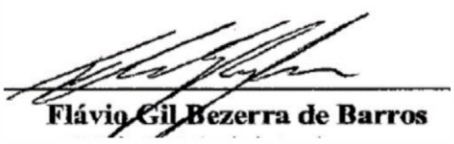
Versão	Data da Revisão	Descrição da Alteração	Data da Aprovação

1.1	02/09/2025	Inclusão dos Dados do Revisor Campo inicial da Política.	02/09/2025
1.1	02/09/202	Inclusão 3.1. Combate à Corrupção e Suborno (Anticorrupção)	02/09/2025
1.1	02/09/2025	Inclusão 3.2. Prevenção à Lavagem de Dinheiro (PLD)	02/09/2025
1.1	02/09/2025	Revisão Geral da Estrutura e Atualização de Nomes de Cargos.	02/09/2025
1.1	02/09/2025	Conceitos e Definições Anticorrupção e Lavagem de Dinheiro	02/09/2025
...	...	...	...

Cientifique-se e cumpra-se.

Fortaleza, 02 de setembro de 2025.

Aprovação

Nome	Assinatura	Data
Flávio Gil Bezerra Barros		02/09/2025
Flávia Maria Gradvohl Bezerra de Barros		02/09/2025
Robert Gil Gradvohl Bezerra		02/09/2025