MANUAL DE COMPLIANCE E CONTROLES INTERNOS

CASA RIO CONSULTORIA DE VALORES MOBILIARIOS LTDA.

VERSÃO	**DATA**
01	MAIO/2026

MANUAL DE COMPLIANCE E CONTROLES INTERNOS

Manual de Compliance e Controles Internos ("**Manual**") da **CASA RIO CONSULTORIA DE VALORES MOBILIARIOS LTDA.**, sociedade empresária limitada, inscrita no CNPJ sob o nº CNPJ: 66.100.211/0001-04, com sede na cidade de Niterói, Estado do Rio de Janeiro, à Rua Ator Paulo Gustavo, nº 222, sala 202, CEP: 24.230-063 ("**Consultoria**").

I. INTRODUÇÃO

Este Manual visa estabelecer as diretrizes, normas, valores e princípios essenciais para orientar a conduta pessoal e profissional dos "Colaboradores" da Consultoria, incluindo sócios, funcionários, e indivíduos em posições de liderança ou responsabilidade.

O propósito deste Manual é definir os procedimentos, as normas de Compliance e os controles internos da Consultoria, incluindo aspectos como confidencialidade e segregação de atividades. Este Manual foi elaborado de acordo com os requisitos estabelecidos pela Comissão de Valores Mobiliários ("**CVM**").

O programa de Compliance da Consultoria é destinado a instituir, bem como a manter atualizados e efetivos, os controles internos, em linha com a complexidade das atividades desenvolvidas. O objetivo é garantir conformidade (Compliance) contínua com as leis e regulamentações em vigor.

Em consonância com a sua política interna, a Consultoria espera que cada um de seus Colaboradores execute seu trabalho de maneira ética, legal e honesta, respeitando sempre o dever fiduciário devido aos clientes, potenciais clientes e outros participantes do mercado.

O(a) Diretor(a) de Compliance será responsável por atualizações periódicas deste Manual, conforme necessário, garantindo sua conformidade com novas leis ou práticas de mercado.

A versão mais recente do Manual estará sempre disponível para os Colaboradores no website da Consultoria.

II. CONFLITOS DE INTERESSE E PRESENTES

Política de Conflitos de Interesse

A Consultoria estabelece nesta seção a sua Política de Conflitos de Interesse, visando gerenciar, mitigar e, idealmente, eliminar quaisquer conflitos de interesse reais ou potenciais que possam surgir entre as atividades da Consultoria e seus Colaboradores.

Um conflito de interesse ocorre quando as atividades ou relações pessoais de um Colaborador podem interferir, em qualquer medida, com as obrigações para com a Consultoria. Em tais situações, é fundamental que os Colaboradores evitem se envolver em qualquer atividade ou transação que possa gerar conflitos, comprometendo sua objetividade ou a eficácia de suas

ações.

A Consultoria e seus Colaboradores devem agir com vigilância para prevenir situações de conflito de interesse, protegendo os interesses da empresa e de seus clientes. Quando um conflito for inevitável, o(a) Diretor(a) de Compliance será responsável por avaliá-lo e adotar medidas cabíveis para sua mitigação. Todo conflito identificado deve ser prontamente comunicado ao(à) Diretor(a) de Compliance.

Em casos complexos, o(a) Diretor(a) de Compliance convocará uma reunião com a Alta Administração para deliberar sobre o conflito.

São exemplos de possíveis conflitos de interesse: (a) Colaborador (ou um parente próximo) ser proprietário ou administrador de uma empresa que negocia diretamente com a Consultoria; (b) Colaborador ter um emprego ou interesses comerciais externos que possam interferir em sua capacidade de desempenhar seu trabalho na Consultoria; (c) Colaborador (ou um parente próximo) ter influência significativa como acionista, diretor, funcionário, consultor ou agente de uma empresa, organização ou entidade concorrente da Consultoria ou que tenha negócios atuais ou futuros, seja como cliente, fornecedor ou contratado da Consultoria.

Os Colaboradores devem evitar o uso indevido de informações confidenciais ou recursos da Consultoria. Qualquer atividade externa, remunerada ou não, deve ser comunicada e aprovada pelo(a) Diretor(a) de Compliance para evitar conflitos.

Comunicação e aceite do cliente em situações de conflito de interesse: Uma vez identificado um potencial conflito, o(a) Diretor(a) de Compliance organizará o envio de uma comunicação escrita aos clientes afetados, detalhando o conflito e as medidas propostas para sua gestão. A comunicação incluirá uma solicitação de aceite, dando ao cliente um prazo mínimo de 5 dias úteis para resposta. A falta de resposta será considerada como um aceite tácito. Em caso de discordância, serão buscadas alternativas para resolver o impasse, priorizando os interesses do cliente, devendo todas as comunicações e respostas serão arquivadas para futura referência.

Em situações em que o cliente manifeste discordância, a Consultoria buscará alternativas para resolver a situação, priorizando sempre os melhores interesses do cliente.

Presentes, Brindes e Entretenimento

Os Colaboradores são proibidos de aceitar vantagens (presentes, brindes, etc.) que possam influenciar suas decisões. A aceitação de presentes de valor inferior a R$ 200,00 é permitida, mas qualquer valor superior requer análise e aprovação do(a) Diretor(a) de Compliance.

Os brindes promocionais personalizados com a identificação do fornecedor ou cliente estão excluídos dessas normas. Refeições ocasionais e brindes de valor razoável também podem estar isentos dessas normas. Em caso de dúvida, o Colaborador deve buscar a aprovação do(a) Diretor(a) de Compliance.

III. ESTRUTURA ORGANIZACIONAL

Alta Administração da Consultoria

A Alta Administração, conforme conceito dado pela Res. CVM 50, é o órgão decisório máximo da Consultoria, responsável pelos assuntos estratégicos da Consultoria, pela atividade de consultoria de valores mobiliários e pelo cumprimento de regras, políticas, procedimentos e controles da Consultoria, comprometendo-se com a efetividade e adequação da presente Política PLD/FTP e demais políticas, manuais, protocolos e dos controles internos da Consultoria.

Os membros da Alta Administração são profissionais com profunda expertise e competência técnica, responsáveis pela eleição da Diretoria da Consultoria, incluindo o(a) Diretor(a) de Compliance que tem a responsabilidade de estabelecer diretrizes para prevenir a Lavagem de Dinheiro e Financiamento ao Terrorismo e a Proliferação de Armas de Destruição em Massa ("**LD/FTP**") na Consultoria de Valores Mobiliários.

A Alta Administração é formada por (i) Cristian da Cunha Menezes; (ii) Fabrício de Albuquerque e Vasconcelos Rocha (iii) Carlos Augusto Varella Francisco; e (iv) Alessandra Zagury.

Diretor de Compliance – responsável pela PLD/FTP

O diretor indicado pela Consultoria para ser a responsável pelo combate e prevenção à LD/FTP, inclusive perante a CVM, é a Sra. Alessandra Zagury ("**Diretor de PLD/FTP**"). O diretor de PLD/FTP tem total independência, autonomia e conhecimento para o pleno cumprimento dos seus deveres, assim como tem pleno acesso a todas as informações que julgar necessárias para que a respectiva governança de riscos, bem como autonomia para garantir o exercício da Política PLD/FTP pela Consultoria.

As principais responsabilidades do(a) Diretor(a) de Compliance são:

- Servir como o ponto de contato principal para consultas internas e externas sobre PLD/FTP.
- Supervisionar e aprimorar os procedimentos e controles estabelecidos para prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
- Comunicar ao Conselho de Controle de Atividades Financeiras (COAF), em até 24 horas, quaisquer transações ou propostas que sugiram a ocorrência de crimes de lavagem de dinheiro ou ocultação de bens.

O diretor de Compliance desempenha um papel crucial na manutenção e no fortalecimento do programa de Compliance da Consultoria, garantindo a conformidade com as leis, regulamentações e políticas internas, devendo:

- Realizar auditorias periódicas do programa de Compliance, preservando registros e

evidências dessas auditorias.

- Atualizar e manter o Manual de Compliance, o Código de Ética e outras políticas internas.
- Disponibilizar uma cópia atualizada do Manual de Compliance no site da Consultoria e fornecer uma cópia a cada colaborador anualmente ou sempre que atualizações ocorrerem.
- Assegurar a coleta do Formulário - Conheça seu Colaborador, diretamente ou através de terceiros competentes.
- Coordenar treinamentos internos em Compliance, mantendo-os atualizados conforme as leis e regulamentações vigentes.
- Coordenar e acompanhar inspeções regulatórias.
- Responder a dúvidas dos colaboradores sobre Compliance de maneira ágil.
- Monitorar a adesão às políticas internas e regulamentações aplicáveis.
- Comunicar à Alta Administração e órgãos reguladores quaisquer irregularidades detectadas.
- Manter a guarda de evidências de análises de Compliance relevantes para futuras auditorias ou inspeções.
- Elaborar o Relatório Anual de Compliance ("**Relatório**"). O Relatório, uma vez concluído, será apresentado à Alta Administração da Consultoria, contendo as seguintes considerações: (a) conclusões dos exames efetuados; (b) propostas de correções para eventuais falhas identificadas, com o respectivo cronograma para solução destas, se for o caso; e (c) obter a opinião do diretor consultor de valores mobiliários, sobre as deficiências constatadas nas verificações e as ações planejadas de acordo com cronograma específico ou as medidas já adotadas para resolvê-las.

Respeitando as normas aplicáveis, o diretor de Compliance tem a prerrogativa de delegar algumas responsabilidades e obrigações de compliance para outros Colaboradores, desde que devidamente qualificados e sempre em conformidade com a legislação pertinente.

O diretor de Compliance detém plena autonomia e independência em suas decisões, sendo capaz de questionar os riscos assumidos nas operações realizadas e aplicar as devidas sanções disciplinares, independente de nível hierárquico, sem a necessidade de validação prévia dos administradores ou sócios da Consultoria.

IV. POLÍTICA DE CONFIDENCIALIDADE

A Política de Confidencialidade da Consultoria tem como objetivo assegurar a proteção das informações confidenciais da Consultoria e de seus clientes. Reconhecendo a importância da confidencialidade nos mercados financeiro e de capitais, esta política abrange todas as informações não públicas relacionadas à Consultoria, obtidas em suas atividades, ou recebidas de clientes e potenciais clientes.

Definição de Informações Confidenciais: Engloba todas as formas de comunicação, sejam elas orais ou escritas, transmitidas por qualquer meio.

Diretrizes para os Colaboradores:

Proteção da Confidencialidade: Os Colaboradores devem salvaguardar as informações confidenciais, evitando a sua divulgação sem autorização.

Restrições de Acesso e Divulgação: É proibido compartilhar informações confidenciais com terceiros não autorizados, salvo quando exigido por lei ou com consentimento expresso do cliente ou parceiro.

Acessos Remotos: Permitidos somente via VPN segura ou mecanismos similares, utilizando dispositivos e autenticação seguros. Todos os acessos são registrados e monitorados.

Uso de Dispositivos Móveis: Restrito a dispositivos fornecidos pela Consultoria, salvo aprovação do departamento de Compliance para uso de dispositivos pessoais sob políticas de segurança específicas.

Plataformas de Comunicação Externas: Deve-se utilizar apenas plataformas e sistemas autorizados e monitorados pela Consultoria para tratar de informações confidenciais.

Formação e Conscientização: É mandatório para todos os colaboradores participar de treinamentos regulares sobre segurança da informação e estar ciente das consequências de violações.

Violações: Resultarão em medidas disciplinares, podendo incluir rescisão contratual e desligamento.

Monitoramento e Revisão: A Consultoria se reserva o direito de monitorar as comunicações para assegurar a conformidade com esta política.

Comunicação de Incidentes: Obrigatória a notificação imediata de qualquer suspeita ou confirmação de comprometimento de informações confidenciais ao departamento de Compliance.

Proteção de Informações dos Clientes: É fundamental a segurança e uso apropriado das informações dos clientes, seguindo a legislação aplicável e as normas internas para compartilhamento de dados.

Compartilhamento de Informações Confidenciais: Limitado a situações necessárias para a condução dos negócios, com afiliadas ou conforme a lei permite, sempre sob a prévia aprovação do(a) Diretor(a) de Compliance ou do Comitê de Risco e Compliance.

Uso de Informações: Estritamente para fins profissionais e proibida a utilização para vantagens pessoais ou divulgação a partes não autorizadas.

Segurança de E-mail e Dados: Utilização da solução Office 365 Business da Microsoft para e-

mails, com segurança reforçada por dispositivos de firewall e antivírus, além de procedimentos de backup externo para continuidade operacional.

V. POLÍTICA DE TREINAMENTO

O presente Manual dispõe sobre a política de treinamento de Compliance ("**Política de Treinamento de Compliance**"), que tem como objetivo estabelecer as condições, a frequência e a importância da realização de treinamentos junto aos Colaboradores da Consultoria.

O(a) Diretor(a) de Compliance da Consultoria é encarregado de organizar, ou garantir a organização, de treinamentos, anuais e obrigatórios, de Compliance, observados os seguintes temas: Prevenção à Lavagem de Dinheiro; Anticorrupção e Confidencialidade; Práticas de mercado, produtos disponíveis e regulamentação aplicável; Insider Trading; outros temas que julgar necessários e adequados para a Consultoria

Os treinamentos serão disponibilizados aos Colaboradores de diversas formas, como acesso online, palestras presenciais, seminários ou materiais escritos. Esses treinamentos podem ser desenvolvidos e realizados por Colaboradores capacitados ou por escritórios de advocacia/terceiros qualificados contratados pela Consultoria.

O(a) Diretor(a) de Compliance deve manter, ou delegar a responsabilidade de manter, o registro de todos os treinamentos realizados, incluindo os materiais utilizados e a lista de Colaboradores que participaram e concluíram os treinamentos no tempo estipulado. A não conclusão dos treinamentos pode resultar em medidas disciplinares.

Todo novo Colaborador da Consultoria deverá receber ou ter acesso a todos os manuais, políticas e procedimentos internos da Consultoria, que passarão a fazer parte de suas atividades diárias.

VI. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação da Consultoria define as diretrizes para a proteção de informações valiosas acessadas ou geradas pelos colaboradores. O compromisso com a segurança das informações é fundamental, abrangendo dados armazenados nos equipamentos da Consultoria e assegurando a integridade, confidencialidade e disponibilidade dessas informações.

Diretrizes Principais:

Responsabilidade dos Colaboradores: Cada membro da equipe é responsável por proteger as informações pertinentes à sua função, tratando-as com ética e profissionalismo.

Programa de Segurança Cibernética: Inclui avaliação de riscos, medidas de prevenção e proteção, monitoramento e testes, planos de resposta a incidentes, testes de contingência e governança.

Identificação de Riscos: Avaliação regular para identificar riscos e vulnerabilidades internas e externas, considerando impactos financeiros, operacionais e de reputação.

Ações de Prevenção: Controle de acesso, autenticação multifatorial, limitação de acesso a recursos essenciais e serviço de backup.

Monitoramento e Testes: Monitoramento contínuo e testes de invasão e phishing para detectar ameaças e reforçar controles.

Resposta a Incidentes: Comunicação e ação imediata em caso de incidentes de segurança.

Governança: Atualização contínua do programa de segurança, promoção da cultura de segurança e definição de indicadores de desempenho.

Protocolos Específicos:

Assinatura de Documentos de Confidencialidade: Todos os colaboradores devem assinar um documento de confidencialidade para reforçar a proteção das informações.

Barreiras de Informação: Implementação de barreiras entre departamentos para preservar a confidencialidade de informações sensíveis.

Proteção Contra Código Malicioso: Todos os ativos de informação devem ser verificados contra códigos maliciosos antes de serem introduzidos no ambiente de produção.

Disposições Finais

Comunicação de Incidentes: Deve ser feita imediatamente ao(à) Diretor(a) de Compliance, seguindo o procedimento estabelecido nesta Política.

Descarte Seguro de Informações: As informações confidenciais devem ser descartadas de forma segura para impedir recuperação ou leitura indevida.

Controle de Acesso: Segregação de funções e controle rigoroso de acessos para minimizar riscos e garantir a auditoria eficaz.

Backup e Recuperação: Implementação de backups diários e sistemas de recuperação para proteger a integridade e disponibilidade dos dados.

Monitoramento de Logs: Manutenção de logs de sistemas por um período de cinco anos para garantir a integridade e a capacidade de auditoria.

Cada computador utilizado pelos colaboradores será fornecido com senhas individuais que permitem a identificação do usuário recente.

O controle de acesso à informação centralizada é realizado pelo departamento de Compliance, que mantém o registro de contas e senhas. Os computadores, também, são configurados com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, inclusive, mas não se limitando, a segregação das funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Todos os arquivos armazenados nos servidores da Consultoria são protegidos por um backup diário, firewall de última geração e sistema antivírus atualizado.

Os backups são realizados automaticamente todos os dias, utilizando ferramentas de armazenamento em nuvem da Microsoft. A Consultoria tem um sistema de backup e recuperação de arquivos que visa garantir a segurança das informações, a recuperação em caso de desastres e a integridade, confiabilidade e disponibilidade dos dados armazenados.

Todos os logs de sistemas são mantidos pela Consultoria por um período de 5 anos. A empresa verifica regularmente os padrões de todos os computadores, arquivos em rede, softwares, hardwares ou acessos não autorizados. Dessa forma, por meio dos logs, a Consultoria consegue garantir a integridade, autenticidade e capacidade de auditoria das informações e sistemas. Todas as declarações de imprensa (envolvendo ou não a Consultoria) devem ser aprovadas previamente pelo(a) Diretor(a) de Compliance. Este poderá, a qualquer momento e sem aviso prévio, verificar o conteúdo das ligações telefônicas gravadas, os arquivos disponíveis no diretório interno e os e-mails enviados e recebidos. O descarte de informações confidenciais armazenadas digitalmente deve ser realizado de maneira a impossibilitar sua recuperação. Documentos físicos contendo informações confidenciais que não precisam ser arquivados devem ser descartados imediatamente após seu uso, impedindo sua recuperação ou leitura.

A Política de Segurança da Informação da Consultoria é um compromisso com a proteção das informações contra ameaças, garantindo sua integridade, confidencialidade e disponibilidade. É essencial que todos os colaboradores compreendam suas responsabilidades dentro deste contexto e atuem de acordo com as diretrizes estabelecidas.

VII. PROCEDIMENTO DE TESTES PERIÓDICOS

O(a) Diretor(a) de Compliance deve realizar ou assegurar que sejam realizados testes de Compliance ao longo do ano fiscal. O objetivo desses testes é identificar e mitigar possíveis riscos aos quais a Consultoria possa estar exposta, e garantir a conformidade com as leis, regulamentações, políticas e procedimentos internos da Consultoria. Além disso, ele deve realizar um teste periódico específico de segurança para os sistemas de informações, especialmente os mantidos eletronicamente.

VIII. PROCEDIMENTO INTERNO DE REPORTE DE VIOLAÇÕES À CVM

Este Manual estabelece o Procedimento Interno de Reporte de Violações à Comissão de Valores Mobiliários (CVM), delineando as normas e procedimentos específicos para os colaboradores da Consultoria. O objetivo é assegurar a comunicação efetiva à CVM de qualquer violação às regulamentações por ela emitidas.

Diretrizes Principais

Responsabilidade dos Colaboradores: Todos que tiverem acesso a informações relevantes sobre a Consultoria são obrigados a reportar imediatamente ao(à) Diretor(a) de Compliance a identificação ou a suspeita de qualquer violação regulatória.

Análise pelo(a) Diretor(a) de Compliance: O(a) Diretor(a) de Compliance é responsável por analisar os registros, operações ou transações apontadas como potenciais violações. Essa análise deve ser conduzida com rigor e objetividade, visando a identificação precisa da existência de não conformidades.

Regularização e Confirmação de Suspeitas: Após o prazo concedido para a regularização de eventuais situações de não conformidade, ou caso a suspeita de violação se confirme após as análises, o(a) Diretor(a) de Compliance deve elaborar um relatório detalhado sobre o caso.

Procedimentos de Reporte:

Comunicação Inicial: O colaborador deve reportar imediatamente ao(à) Diretora de Compliance qualquer suspeita ou identificação de violação.

Análise Preliminar: O(a) Diretor(a) de Compliance realizará uma análise preliminar para avaliar a validade da suspeita reportada.

Investigação Detalhada: Caso necessário, uma investigação detalhada será conduzida para apurar a extensão da violação.

Elaboração de Relatório: Com base nas análises e investigações realizadas, o(a) Diretor(a) de Compliance elaborará um relatório sobre a violação, incluindo recomendações e medidas corretivas.

Comunicação à CVM: Se a violação se confirmar e for de natureza significativa, o relatório será submetido à CVM, seguindo os procedimentos e prazos regulamentares.

Compromisso com a Transparência e Ética:

A Consultoria se compromete a manter a transparência e a ética em todas as suas operações e relações. A aderência estrita a este Procedimento de Reporte de Violações é essencial para a manutenção da integridade e da confiança no ambiente regulatório.

Este Procedimento reflete o compromisso da Consultoria com a conformidade regulatória e a transparência, assegurando que todas as violações sejam prontamente identificadas, analisadas e reportadas à CVM conforme necessário.

IX. SEGREGAÇÃO DE ATIVIDADES

O(a) Diretor(a) de Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos Diretores ou demais sócios da Consultoria. A Área de Compliance atua de forma autônoma e independente, se reportando ao(à) Diretor(a) de Compliance.

A Consultoria manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros, sendo um requisito essencial para que seja dado o efetivo cumprimento das atividades de consultoria de valores mobiliários.

A Consultoria adota um conjunto de procedimentos estabelecidos pelo(a) Diretor(a) de Compliance, com o objetivo de proibir e impedir o fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou Colaboradores, da instituição que não estejam diretamente envolvidos na atividade de consultoria de valores mobiliários.

A Consultoria realizará os melhores esforços para que a segregação das informações e suas atividades sejam sempre preservadas. Com o intuito de assegurar a completa segregação, os seguintes procedimentos operacionais serão adotados: (a) Instalação física com limitação de acesso de terceiros. Essas medidas incluem a delimitação de áreas para discussões confidenciais e a aplicação de políticas rígidas que proíbem tais discussões em espaços compartilhados; (b) segregação informacional absoluta e inviolável da Consultoria e qualquer sociedade que os Colaboradores tenham relacionamento, os equipamentos devem ser utilizados apenas por aqueles autorizados e em circunstâncias específicas. Adicionalmente, a gestão e proteção das informações comuns serão reforçadas através do uso de tecnologia segura e práticas de gerenciamento de dados; (c)preservação de informações confidenciais por todos os seus Colaboradores, proibindo a transferência de tais informações a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente; e (d) a implantação e manutenção de programa de treinamento de Colaboradores que tenham acesso a informações confidenciais e/ou participem de processo de consultoria de valores mobiliários.

O programa incluirá orientações claras sobre as políticas de confidencialidade, expectativas de comportamento e as consequências para o não cumprimento dessas políticas. A participação de todos os Colaboradores relevantes será obrigatória e registrada para garantir a conformidade.

X. CONSIDERAÇÕES FINAIS

Este Manual não substitui a obrigação que cada Colaborador tem de usar o bom senso,

discernimento e de, sempre que necessário, em caso de dúvidas, contatar o(a) Diretor(a) de Compliance diretamente ou através do seu e-mail.

Quaisquer solicitações de exceções às regras descritas neste Manual devem ser encaminhadas ao(à) Diretor(a) de Compliance, que possui amplos poderes para aprovar exceções a este Manual, desde que a razão, natureza, prazo, e outras informações importantes sobre a decisão sejam devidamente formalizadas, sempre respeitando as leis e regulamentações aplicáveis.

Este Manual será revisado anualmente ou em períodos menores caso necessário. Eventuais alterações acontecerão caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Após a contratação e, anualmente, todos os Colaboradores deverão aderir a esta Política através do preenchimento e assinatura do Formulário "Conheça seu Colaborador" que será disponibilizada pelo(a) Diretor(a) de Compliance

* * * * *