OUTUBRO 2025

Netz

Manual de Compliance e Controles Internos

Sumário

1. INTRODUÇÃO

Este Manual de Compliance e Controles Internos ("Manual") torna públicos princípios, regras, valores e procedimentos que norteiam a atuação da Netz Asset Ltda. ("Netz", "Netz Asset" ou "Asset").

Cumpre salientar que a Netz Asset faz parte da Netz Holding, é um Grupo Econômico que exerce diversas atividades, visando sempre um atendimento personalizado, de qualidade e integridade para todos os seus clientes. Os serviços atualmente prestados são os de: (i) Consultoria[1]; (ii) Câmbio, Seguros e Banking[2]; (iii) Securitizadora[3]; e (iv) Gestão de Fundos de Investimentos e Gestão de Patrimônio[4]. Todas as atividades observam as normas regulatórias e autorregulatórias, melhores práticas do mercado, mitigando conflitos de interesse e prestando de um serviço de excelência e alto impacto.

O propósito da Netz Holding é cuidar do patrimônio para que pessoas extraordinárias possam dedicar sua energia ao que realmente importa.

O Manual consolida as práticas e controles internos adotados, estabelecendo diretrizes que orientam a conduta de todos os colaboradores[5], de modo a assegurar a conformidade com as normas regulatórias, autorregulatórias e as melhores práticas de mercado, garantindo a integridade, a ética e a excelência na condução dos negócios.

Todas as atividades são conduzidas em estrita observância às normas legais, regulatórias e autorregulatórias aplicáveis, em conformidade com os princípios de governança corporativa, gestão de riscos e compliance, buscando mitigar conflitos de interesse e a prestação de serviços de alto padrão ético e técnico.

2. OBJETIVO E APLICABILIDADE

Este Manual torna público os princípios, regras e valores, além de consolidar as regras, procedimentos e controles internos necessários à adequada condução das atividades da Netz Asset assegurando o cumprimento das normas regulatórias, autorregulatórias e internas, bem como a observância das melhores práticas de mercado.

Todos os colaboradores deverão, ao receber este Manual, assinar o Termo de Recebimento e Compromisso (anexo I) declarando que leram, compreenderam e se comprometem a observar integralmente as regras aqui estabelecidas. Sempre que o Manual for atualizado, os colaboradores serão notificados quanto às

[1] Netz Solutions LTDA, CNPJ nº 60.408.897/0001-19
[2] Netz Select Corretora de Seguros LTDA., CNPJ nº 39.151.020/0001-07 e Netz Corretora de Seguros LTDA., CNPJ nº 61.734.108/0001-00
[3] Netz Securitizadora de Créditos, CNPJ nº 61.833.005/0001-90
[4] Netz Asset Gestão de Recursos LTDA., CNPJ nº 48.638.617/0001-63
[5] Tal como previsto no Código de Ética da Netz Holding

alterações relevantes e deverão assinar um novo Termo, ratificando sua ciência e adesão à versão vigente.

A Área de Governança, Risco e Compliance (GRC), sob responsabilidade de sua Diretora é a área responsável pelas regras aqui previstas, bem como pela atualização e monitoramento das regras deste Manual, garantindo que o conteúdo reflita as normas regulatórias e autorregulatórias em vigor, além das políticas internas e procedimentos operacionais da Netz.

3. BASE LEGAL

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021 ("Resolução CVM 21");
(ii) Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM 50");
(iii) Resolução CVM nº 175, de 23 de dezembro de 2022 ("Resolução CVM 175");
(iv) Código de Administração e Gestão de Recursos de Terceiros ("Código AGRT Anbima");
(v) Regras e Procedimentos de Deveres Básicos Anbima ("RP Deveres Básicos Anbima")
(vi) Lei nº 12.846/13 e Decreto nº 11.129/22 ("Normas Anticorrupção");
(vii) Lei nº 9.613, de 03 de março de 1998 ("Lei de Lavagem de Dinheiro");
(viii) Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD); e
(ix) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorregulados aplicáveis às atividades da Netz Holding.

4. RESPONSABILIDADES E DIRETRIZES

A coordenação direta das atividades relacionadas a este Manual é uma atribuição da Diretora de Governança, Risco e Compliance[6], que atua com independência funcional e autoridade plena para o desempenho de suas funções, sem subordinação hierárquica a outras áreas operacionais ou comerciais da Netz.

A Área de Governança, Risco e Compliance (GRC) responde diretamente à Alta Administração e desempenha papel essencial na implementação, monitoramento e aprimoramento contínuo das políticas, controles e procedimentos internos que asseguram a conformidade das atividades da Netz com as normas regulatórias, autorregulatórias e internas.

É importante destacar que na estrutura da Netz Holding, a Área de Governança, Risco e Compliance ("GRC") são coordenadas pela mesma Diretora[7], assim, os profissionais podem atuar de forma conjunta, observando as regras de cada atividade, como a Política de Gestão de Riscos e a Política de Investimentos Pessoais

[6] Conforme artigo 4º, inciso IV, da Resolução 21 CVM.
[7] Compreendendo também a responsabilidade das questões relacionadas a Controles Internos, PLD/FTP, LGPD, ESG e Qualidade.

4.1. Responsabilidade da Área de GRC

- Elaborar, revisar e atualizar políticas, manuais, códigos e procedimentos internos, garantindo aderência às normas regulatórias e autorregulatórias vigentes e às melhores práticas de mercado;
- Monitorar e acompanhar alterações normativas e regulatórias, avaliando os impactos sobre os negócios e propondo as adaptações necessárias;
- Coordenar e ministrar treinamentos periódicos de compliance, PLD/FTP, ética, segurança da informação e demais temas relevantes, bem como treinamentos extraordinários, quando necessário;
- Atuar de forma consultiva junto às demais áreas, prestando orientações sobre a correta interpretação e aplicação das normas e políticas internas;
- Conduzir testes periódicos de controles internos e de segurança da informação, avaliando a eficácia dos procedimentos implementados;
- Apoiar a Alta Administração na identificação e mitigação de conflitos de interesse, inclusive no que se refere a acessos físicos e digitais, processos internos e comunicações externas;
- Coordenar e acompanhar incidentes de segurança da informação, atuando para mitigar riscos e implementar planos de ação corretiva;
- Implementar e supervisionar as diretrizes de privacidade e proteção de dados pessoais, em conformidade com a LGPD, incluindo a revisão de contratos, cláusulas e termos de confidencialidade;
- Realizar o monitoramento anual dos investimentos pessoais dos colaboradores e partes relacionadas, conforme a Política de Investimentos Pessoais, prevenindo conflitos de interesse;
- Zelar pelo correto uso, tratamento e compartilhamento de informações confidenciais, em conformidade com as normas internas e regulatórias;
- Verificar e monitorar operações e movimentações para fins de prevenção à lavagem de dinheiro e financiamento ao terrorismo (PLD/FTP);
- Conduzir diligências cadastrais e reputacionais para verificação de clientes, contrapartes, colaboradores, prestadores de serviços e parceiros, mitigando riscos regulatórios, reputacionais, dentre outros;
- Assegurar a guarda e manutenção de informações cadastrais e de diligências pelo prazo mínimo de 5 (cinco) anos, ou conforme exigido pela regulamentação aplicável;
- Coordenar os reportes obrigatórios ao COAF, quando cabíveis, e a elaboração de relatórios regulatórios e internos relacionados a compliance, risco e PLD/FTP;
- Acompanhar o cumprimento das certificações exigidas para o exercício das atividades reguladas e autorreguladas;
- Avaliar e monitorar a qualidade dos serviços prestados por terceiros, garantindo que estejam em conformidade com as normas aplicáveis e os padrões internos da Netz;

- Acompanhar o cumprimento das normas regulatórias e autorregulatórias em contratos, documentos, materiais de divulgação e demais comunicações externas;
- Participação no Comitê de Ética, em conjunto com a Alta Administração, para análises de condutas e possíveis infrações, sugerindo as sanções cabíveis;
- Atuar de forma preventiva e corretiva na análise de potenciais conflitos de interesse, orientando as áreas quanto às providências adequadas;
- Participar ativamente dos Comitês Internos da Netz, com direito a voto e veto, contribuindo para o fortalecimento da governança corporativa e aderência às normas regulatórias e autorregulatórias;
- Supervisionar e manter atualizado o Plano de Continuidade de Negócios (PCN), conduzindo planos de ação e relatórios de contingência sempre que necessário;
- Revisar e aprovar materiais publicitários, técnicos ou institucionais, garantindo conformidade com as normas da CVM, ANBIMA e demais órgãos;
- Manter as informações atualizadas nos bancos de dados da ANBIMA, bem como nos sistemas e cadastros oficiais da Netz;
- Supervisionar a adequação das informações de suitability para gestão de patrimônio;
- Elaboração e manutenção dos documentos internos e externos e publicidade conforme necessidade e obrigações regulatórias e autorregulatórias; e
- Estruturar e monitorar planos de ação para mitigação de riscos operacionais e falhas em processos internos.

5. KYC, KYP, KYE E KYS

A Netz Asset adota controles estruturados para conhecer seus clientes, parceiros e colaboradores, garantindo a integridade das relações comerciais e a mitigação de riscos reputacionais e de integridade.

- KYC (*Know Your Client*): identificação, qualificação e monitoramento contínuo de clientes e investidores;
- KYP (*Know Your Partner*): diligência sobre fornecedores e parceiros estratégicos, verificando histórico, reputação e compliance, além do monitoramento contínuo de clientes e investidores;
- KYE (*Know Your Employee*): verificação de antecedentes, histórico profissional e eventual conflito de interesse de colaboradores, realizando devido monitoramento; e
- KYS (*Know Your Supplier*): diligência sobre prestadores de serviço, verificando histórico, reputação e monitoramento contínuo.

Para a realização das diligências são utilizadas fontes públicas de consulta, além de sistema terceiro. Todos os processos observam as normas legais e diretrizes dos

órgãos reguladores e autorreguladores. A Netz possui matriz de risco interna para definição de risco de cada parte de acordo com o escopo da diligência, indicando qual periodicidade de monitoramento.

6. CONFLITO DE INTERESSES E SEGREGAÇÃO DE ATIVIDADES

A Netz adota controles para identificar, avaliar e mitigar situações de conflito entre interesses pessoais e profissionais, além de garantir a segregação física e digital entre as empresas da Netz Holding[8]. As regras de segregação de atividades observam as normas regulatórias e autorregulatórias[9].

As informações digitais são segregadas através de sistemas eletrônicos utilizados com acesso restrito e protegidos por senha[10], sendo que a liberação dos acessos é feita em conjunto pelas Áreas de Tecnologia da Informação e GRC.

É vedado aos colaboradores:

- Participar de decisões em que tenham interesse direto ou indireto;
- Utilizar informações privilegiadas para benefício próprio ou de terceiros;
- Atuar em atividades externas sem autorização prévia da Diretoria; e
- Negociar valores mobiliários em períodos de restrição ou blackout.

7. POLÍTICA ANTICORRUPÇÃO

A Netz Asset está sujeita às normas e Leis de Anticorrupção[11], incluindo, mas não se limitando, as quais estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo de responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito a Política, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político. Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais[12].

---

[8] Conforme item 1 deste Manual.
[9] Tal como indicado no Código de Ética.
[10] Tal como detalhado na Política de Segurança da Informação e Código de Ética.
[11] Em complemento as Políticas de PLDFTP e KYC e a Matriz Interna de Risco.
[12] As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Ainda que a atividade da Netz Asset não esteja diretamente ligada aos agentes públicos, aos colaboradores é vedado:

- Oferecer, prometer, solicitar ou receber vantagem indevida;
- Financiar ou patrocinar atos ilícitos;
- Utilizar intermediários para disfarçar ou mascarar atos de corrupção;
- Realizar contribuições políticas em nome da Asset; e
- Manter relacionamento com terceiros que não observem padrões éticos compatíveis com os da Netz Asset.

A Área de GRC é responsável por supervisionar a aderência às normas anticorrupção e reportar imediatamente à Alta Administração qualquer suspeita de violação de tais regras.

8. PREVENÇÃO À LAVAGEM DE DINHEIRO, FINANCIAMENTO DO TERRORISMO E AFINS (PLDFTP)

Tal como previsto na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa ("Política de PLD/FTP), a Netz Asset possui diversos controles para mitigação de envolvimento com práticas ilícitas e de lavagem de dinheiro, tal como:

- Identificação e diligência de clientes, parceiros, colaboradores e fornecedores (KYC, KYP, KYE e KYS);
- Monitoramento contínuo de operações, movimentações e de diligências;
- Comunicação de operações suspeitas à CVM e COAF;
- Treinamentos periódicos para conscientização;
- Atualização anual do relatório de PLDFTP.

Cabe à Área de GRC a análise, monitoramento e tratamento das informações recebidas e relacionadas com o tema, além do monitoramento das movimentações da gestão de patrimônio[13]. Os registros de informações relacionadas são armazenados por, no mínimo, 5 anos.

9. CONFIDENCIALIDADE E PROTEÇÃO DE INFORMAÇÕES

Os colaboradores devem preservar o sigilo de todas as informações obtidas em razão do exercício de suas funções, no âmbito pessoal ou profissional. É expressamente vedado divulgar, compartilhar ou utilizar informações estratégicas, financeiras, operacionais ou pessoais sem autorização formal, tal como exemplificado no Código de Ética. Para tanto, são consideradas informações confidenciais, dentre outras:

[13] Como aportes, dados patrimoniais e reputacionais, dentre outros.

- Dados de clientes, investidores e contrapartes;
- Estratégias de investimento, planos de negócio e projetos internos;
- Dados pessoais e sensíveis;
- Modelos, sistemas e códigos internos.

Todos os meios de comunicação e dispositivos utilizados para fins profissionais serão monitorados, assim, em caso de suspeita de violação às diretrizes previstas neste Manual e no Código de Ética, os arquivos poderão ser acessados pela Diretora de GRC para apuração da situação. Em caso de violação, o Comitê de Ética fará a análise da situação e deliberará pela sanção cabível.

9.1. Segurança da Informação e Proteção de Dados (LGPD)

A Netz Asset mantém controles e políticas[14] para assegurar a integridade, disponibilidade e confidencialidade das informações corporativas e pessoais, em conformidade com as normas regulatórias e autorregulatórias, além da LGPD.

A Área de Tecnologia e Segurança da Informação, em conjunto com a Área de GRC, é responsável por, dentre outros:

- Controlar acessos físicos e digitais;
- Garantir o uso adequado de equipamentos e sistemas;
- Implementar testes e planos de contingência;
- Responder a incidentes de segurança e comunicar à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável; e
- Garantir que os titulares de dados exerçam seus direitos de acesso, retificação, exclusão e portabilidade.

Com o intuito de divulgar as informações relacionadas e disseminar o conteúdo para todos os colaboradores, um treinamento anual sobre LGPD é ministrado aos colaboradores.

A segurança da informação, tal como previsto na Política é responsabilidade das Áreas de GRC e Tecnologia da Informação em conjunto, observando as normas regulatórias e autorregulatórias, além de monitoramentos e treinamentos periódicos que são realizados.

A Netz possui procedimentos de backup[15] e recuperação de dados para situações de falha ou contingência, observando princípios de confidencialidade, integridade, conformidade e proporcionalidade, dentre outros.

10. FATOS RELEVANTES

[14] Políticas de LGPD e Segurança da Informação.
[15] Em tempo real através de arquivos em nuvem.

Em que pese seja responsabilidade do administrador fiduciário do fundo a operacionalização da divulgação de qualquer fato relevante ocorrido ou relacionado ao funcionamento do fundo, da classe ou aos ativos integrantes da carteira, assim que dele tiver conhecimento, é responsabilidade dos demais prestadores de serviços, incluindo as Gestoras, informar imediatamente ao administrador fiduciário sobre os fatos relevantes de que venham a ter conhecimento, para a devida divulgação.

Nesse sentido, são considerados relevantes, nos termos do artigo 64, §1º da Parte Geral da Resolução CVM 175, quaisquer fatos que possam influir de modo ponderável no valor das cotas ou na decisão dos investidores de adquirir, resgatar, alienar ou manter cotas.

A seguinte lista não é exaustiva e apresenta exemplos de fatos potencialmente relevantes:

- alteração no tratamento tributário conferido ao fundo, à classe ou aos cotistas;
- contratação de formador de mercado e o término da prestação desse serviço;
- contratação de agência de classificação de risco, caso não estabelecida no regulamento do fundo ou no anexo da classe;
- mudança na classificação de risco atribuída ao fundo, à classe ou à subclasse de cotas;
- alteração de prestador de serviço essencial;
- fusão, incorporação, cisão ou transformação do fundo ou da classe de cotas;
- alteração do mercado organizado em que seja admitida a negociação de cotas do fundo;
- cancelamento da admissão das cotas do fundo ou da classe à negociação em mercado organizado; e
- emissão de cotas de fundo fechado.

Os fatos relevantes podem, de formar excepcional, deixar de ser divulgados, caso seja entendido pela Asset e pelo administrador fiduciário do fundo que sua revelação põe em risco interesse legítimo dos fundos ou de seus cotistas. Neste caso, tais informações serão tratadas como confidenciais até a Netz julgar como oportuno o momento para sua divulgação.

Por outro lado, o administrador fiduciário fica obrigado a divulgar imediatamente fato relevante na hipótese de a informação escapar ao controle ou se ocorrer oscilação atípica na cotação, preço ou quantidade negociada de cotas, em havendo negociação em mercado regulado. A Netz Asset deverá notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

A Netz disponibilizará os fatos relevantes relativos aos fundos sob sua gestão em seu website.

11. CANAL DE DENÚNCIAS

A Netz mantém um canal de denúncias independente, confidencial e acessível, destinado ao relato de condutas suspeitas, violações éticas ou descumprimentos regulatórios. Todos os relatos serão tratados com confidencialidade, segurança e boa fé.

A apuração dos casos reportados é conduzida pela Diretora de GRC e avaliará as informações no Comitê de Ética[16].

12. GERENCIAMENTO DE RISCOS OPERACIONAIS

O risco operacional é a possibilidade de ocorrência de perdas resultantes de equívoco, deficiência ou inadequação de processos internos, pessoas, sistemas ou de eventos externos. Ocorre ainda, pela imprecisão e/ou inadequação dos sistemas de informação, processamento de operações, falhas nos controles internos ou na execução de ordens.

Podem ocorrer por conta das fragilidades nos processos, que podem ser gerados por falta de regulamentação interna e/ou documentação referente a políticas e procedimentos, ou ainda de problemas em sistemas terceiros.

Para os fins estabelecidos nesta Política, risco operacional contempla também o risco legal associado à inadequação ou deficiência dos contratos firmados pela instituição, bem como as sanções sofridas em razão de descumprimento de dispositivos legais e as indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Netz.

A responsabilidade pelo tratamento dos riscos operacionais é da Área de GRC, através de estrutura de gerenciamento capacitada para identificar, avaliar, monitorar, controlar e mitigar riscos, inclusive aqueles decorrentes de serviços terceirizados, entretanto, todos os colaboradores estão plenamente capacitados para mitigar as situações de risco e administrá-las, se necessário, em conjunto com a Área de GRC.

A estrutura de Gerenciamento de Riscos Operacionais contempla uma gama de atividades e controles, tal como treinamentos, identificação conjunta de riscos, categorização, testes, avaliação, planos de ação, monitoramento de testes e incidentes, controle de prazos e responsáveis, aprovação, comunicação à hierarquia responsável, reporte ao Comitê de GRC, dentre outros.

[16] Composto pela Diretora de GRC e a Alta Administração.

Neste contexto, a mitigação do risco operacional se dá por meio de procedimentos de validação contínua dos diferentes sistemas utilizados, inclusive a organização da Área de Tecnologia da Informação e Segurança da Informação, com a possibilidade de conexão via nuvem através de VPN, data center equipado com no-break's, ar-condicionado e servidores de alto desempenho, com capacidade e disponibilidade que garantem a continuidade dos negócios.

As principais medidas de controles internos para prevenção ligadas ao risco operacional são:

- Inventário de processos;
- Mapeamento de processos;
- Reconfirmação de todos os negócios e "entrada" de dados;
- Reconciliação diária dos extratos;
- Backup diário em servidor externo da base de dados e arquivos;
- Acesso remoto aos sistemas utilizados;
- Report e de incidentes operacionais, com o intuito de monitorar e identificar as falhas nos processos, aprimorando-os continuamente.

Ainda que sejam praticadas todas as medidas que mitiguem o risco de vazamento de informações sensíveis ou confidenciais, especialmente no caso de envio de e-mail ou documento a destinatário diverso daquele pretendido, os colaboradores têm ciência de que caso aconteça tal hipótese, as Áreas de GRC, TI e responsável pela área deverão ser informados, incluindo: (i) conteúdo do e-mail e anexos; (ii) data e horário do envio; (iii) destinatário original; e (iv) dados do destinatário.

Após o recebimento da ocorrência, a Diretora de GRC tomará as medidas cabíveis. Vale ressaltar que o envio do e-mail não exime o colaborador de reportar o incidente através de outra ferramenta operacional utilizada na troca da referida informação.

13. AUDITORIA, MONITORAMENTO E MELHORIAS CONTÍNUAS

A Netz realiza auditorias internas e externas periódicas para verificar a eficácia dos controles internos e o cumprimento das normas.

As auditorias podem abranger:

- Revisão de processos e políticas;
- Verificação de conformidade regulatória;
- Avaliação de riscos e planos de mitigação;
- Acompanhamento de planos de ação.

Os resultados são reportados à Alta Administração e, quando aplicável, aos órgãos regulatórios e autorregulatórios.

Todas as conclusões apresentadas pela auditoria serão avaliadas e tratadas pela Área de GRC para aplicação das melhorias necessárias e aplicáveis.

14. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente ou em prazo inferior caso necessário.

Histórico das atualizações		
Data	Versão	Tópicos
janeiro/2025	1ª	Constituição da Gestora
abril/2025	2ª	Atualização – conflitos de interesse
outubro/2025	3ª	Atualização – Netz Holding

ANEXO I
TERMO DE CONFIDENCIALIDADE E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº_____, DECLARO para os devidos fins:

1. Ter recebido, na presente data, o Manual de Compliance e Controles Internos da Netz Asset Gestão de Recursos LTDA.;
2. Cumprir integralmente as disposições do Manual e das políticas internas correlatas, zelando pela ética, integridade, transparência e observância das normas legais, regulatórias e autorregulatórias aplicáveis;
3. Manter absoluto sigilo e confidencialidade sobre todas as informações obtidas em decorrência do meu vínculo com a Netz Asset, incluindo dados estratégicos, operacionais, financeiros, de clientes, fornecedores, parceiros, sócios, colaboradores ou quaisquer terceiros;
4. Não divulgar, reproduzir, copiar, transferir, armazenar ou utilizar tais informações para fins distintos dos autorizados, sob qualquer meio (físico, digital, verbal ou outro);
5. Comunicar imediatamente à Diretoria de Governança, Risco e Compliance qualquer fato, incidente, irregularidade ou suspeita de violação às normas deste Manual ou às políticas internas da Gestora; e
6. O dever de confidencialidade subsiste mesmo após o término do vínculo com a Netz Asset;

Declaro, por fim, que o descumprimento das disposições deste termo poderá resultar em penalidades administrativas ou legais.

[local], [data].

_____

[**COLABORADOR**]