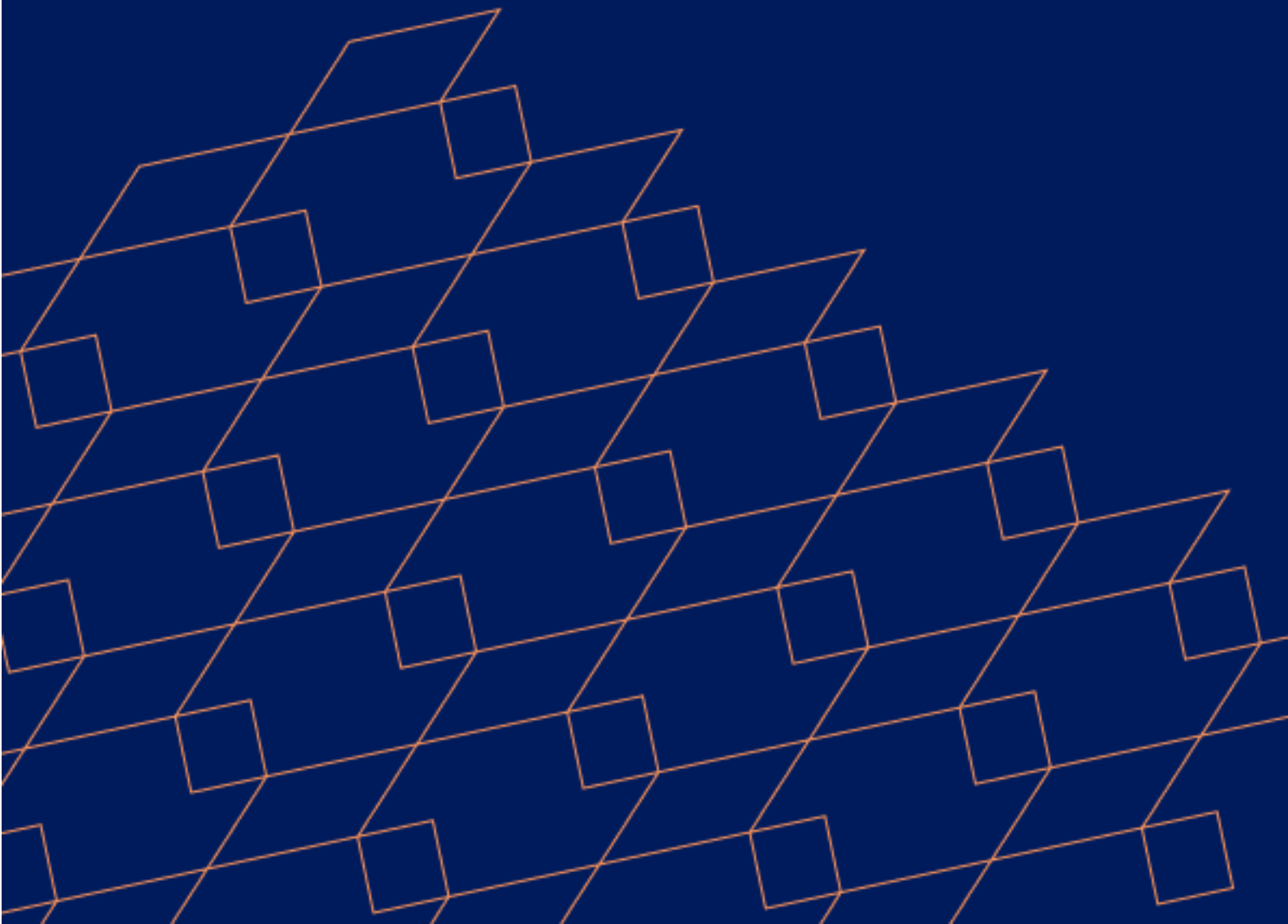
MANUAL DE COMPLIANCE E CONTROLES INTERNOS

JUNHO/2026



SUMÁRIO

1. INTRODUÇÃO

Este Manual de Compliance e Controles Internos ("Manual") torna público os princípios, as regras, os valores e os procedimentos que norteiam a atuação da Netz Holding Ltda. ("Netz Holding") e de todas as empresas do Grupo Econômico.

O Grupo Econômico da Netz Holding exerce diversas atividades, visando sempre um atendimento personalizado, de qualidade e integridade para todos os seus clientes. Os serviços atualmente prestados pelo grupo, incluem, entre outros: (i) Consultoria[1]; (ii) Câmbio, Seguros e Banking[2]; (iii) Securitizadora[3]; (iv) Distribuição de Títulos de Securitização de Emissão Própria[4]; e (iv) Gestão de Fundos de Investimentos, Gestão de Patrimônio e Distribuição de Fundos Próprios[5], sendo todo o Grupo Econômico doravante denominado "Netz" ou "Grupo Netz". 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 do Grupo Netz 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[6], de modo a assegurar a conformidade com as normas regulatórias, autorregulatórias e as melhores práticas de mercado, garantindo integridade, ética, mitigação de riscos, prevenção de conflitos de interesse e adequada condução dos negócios.

2. OBJETIVO E APLICABILIDADE

Este Manual tem por objetivo consolidar os princípios, regras, procedimentos e controles internos necessários à adequada condução das atividades das empresas do Grupo Netz, assegurando o cumprimento das normas legais, regulatórias, autorregulatórias e internas aplicáveis, bem como a observância das melhores práticas de mercado.

Este Manual possui caráter corporativo e aplica-se a todas as empresas do Grupo Netz. Sem prejuízo da adoção de diretrizes comuns, cada empresa deverá observar

[1] Netz Solutions Ltda., CNPJ/MF nº 60.408.897/0001-19.
[2] Netz Select Corretora de Seguros Ltda., CNPJ/MF nº 39.151.020/0001-07 e Netz Corretora de Seguros Ltda., CNPJ/MF nº 61.734.108/0001-00.
[3] Netz Securitizadora S.A., CNPJ/MF nº 61.833.005/0001-90.
[4] Netz Securitizadora S.A., CNPJ/MF nº 61.833.005/0001-90.
[5] Netz Asset Gestão de Recursos Ltda., CNPJ/MF nº 48.638.617/0001-63.
[6] Considera-se "Colaborador" qualquer pessoa que trabalhe em toda e qualquer empresa Grupo Netz, independentemente do tipo de regime de contratação, ou seja, celetista, associado, pessoa jurídica e terceiros que atuem em nome do Grupo Netz.

integralmente as exigências específicas aplicáveis à sua atividade, inclusive quanto à segregação de funções, independência de áreas, certificações exigidas, controles regulatórios e deveres de reporte.

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 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 responsável pela elaboração, revisão, atualização e monitoramento deste Manual, garantindo que seu conteúdo reflita a regulamentação vigente, as políticas corporativas do Grupo e os procedimentos internos aplicáveis. A Área de GRC é compartilhada com as demais empresas do Grupo Netz e atualmente composta por 5 (cinco) colaboradores, sob a coordenação da Diretora de Governança, Risco e Compliance, observada a segregação funcional e operacional aplicável às atividades reguladas da Companhia.

Este Manual deverá ser interpretado em conjunto com o Código de Ética e Conduta, as Políticas de PLDFTP, de Segurança da Informação e Cibersegurança, de Proteção de Dados Pessoais, de Investimentos Pessoais, o Plano de Continuidade de Negócios (PCN) e os demais normativos internos do Grupo Netz, conforme aplicável.

As políticas, normativos internos e demais documentos referidos neste Manual são disponibilizados aos colaboradores em repositório interno controlado pela Área de Governança, Risco e Compliance, sendo de acesso permanente e atualizado. As atualizações relevantes serão comunicadas aos colaboradores pelos canais internos de comunicação, observadas as obrigações de assinatura do Termo de Recebimento e Compromisso (Anexo I) e a participação obrigatória nos treinamentos periódicos sobre os temas previstos neste Manual.

3. BASE LEGAL

Este Manual observa, conforme aplicável à atividade desempenhada por cada empresa do Grupo Netz, a legislação e regulamentação pertinente, incluindo, sem limitação:

(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 60, de 23 de dezembro de 2021 ("Resolução CVM 60");

(iv) Resolução CVM nº 175, de 23 de dezembro de 2022 ("Resolução CVM 175");

(v) Código da ANBIMA de Ofertas Públicas ("Código de Ofertas Públicas") e demais disposições acessórias a este Código de Ofertas Públicas, conforme alterados;

(vi) Código ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código AGRT") e demais disposições acessórias a este Código AGRT, conforme alterados;

(vii) Código ANBIMA de Distribuição de Produtos de Investimento ("Código de Distribuição") e demais disposições acessórias a este Código de Distribuição (quando aplicável);

(viii) Regras e Procedimentos de Certificação ANBIMA, conforme alterado ("RP Certificação ANBIMA");

(ix) Código da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("ANBIMA") de Ética ("Código de Ética") e demais disposições acessórias a este Código de Ética, conforme alterados;

(x) Lei nº 12.846, de 1º de agosto de 2013, e Decreto nº 11.129, de 11 de julho de 2022 ("Normas Anticorrupção");

(xi) Lei nº 9.613, de 03 de março de 1998 ("Lei de Lavagem de Dinheiro");

(xii) Lei nº 13.709, de 14 de agosto de 2018 ("Lei Geral de Proteção de Dados" ou "LGPD");

(xiii) Lei nº 14.430, de 3 de agosto de 2022 ("Marco Legal da Securitização");

(xiv) Lei nº 11.076, de 30 de dezembro de 2004, no que aplicável a operações de securitização do agronegócio;

(xv) Lei nº 9.514, de 20 de novembro de 1997, no que aplicável a operações de securitização imobiliária;

(xvi) normas expedidas pelo Banco Central do Brasil aplicáveis às atividades de câmbio, banking e correlatas, quando aplicável;

(xvii) normas expedidas pela SUSEP aplicáveis às atividades de seguros, quando aplicável; e

(xviii) demais manifestações, ofícios, orientações e normas dos órgãos reguladores e autorreguladores aplicáveis às atividades das empresas do Grupo Netz.

A observância das normas acima deverá ocorrer conforme a natureza da atividade exercida por cada empresa do Grupo, sem prejuízo da aplicação de outros normativos específicos que venham a ser exigidos por reguladores, autorreguladores ou pela legislação aplicável.

4. RESPONSABILIDADES E DIRETRIZES

A coordenação das atividades relacionadas a este Manual é atribuição da Diretora de Governança, Risco e Compliance, que atua com independência funcional e autoridade compatível com o exercício de suas atribuições, sem prejuízo da interação necessária com a Alta Administração e com as demais áreas do Grupo.

A Área de Governança, Risco e Compliance possui atuação corporativa e centralizada no âmbito do Grupo Netz, sendo responsável pela implementação, monitoramento e aprimoramento contínuo das políticas, controles e procedimentos internos que asseguram a conformidade das atividades do Grupo com as normas legais, regulatórias, autorregulatórias e internas.

A atuação centralizada da Área de GRC não afasta a necessidade de observância das peculiaridades regulatórias de cada empresa do Grupo, devendo ser assegurados, quando exigidos, segregação de atividades, independência funcional, controles específicos e reporte adequado aos órgãos competentes.

A atuação da Área de GRC em fóruns, comitês e instâncias de governança observará os respectivos regimentos internos e normativos corporativos, sempre que existentes.

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, movimentações e eventos relevantes para fins de prevenção à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, conforme normativos internos e regulamentação aplicável;
- 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, bem como a elaboração de relatórios regulatórios e internos relacionados a compliance, riscos, controles internos e PLDFTP;
- 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 do Grupo 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 dos fóruns e comitês internos do Grupo Netz, nos termos dos respectivos regimentos, contribuindo para o fortalecimento da governança corporativa e da aderência regulatória;
- 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 atualizadas, quando aplicável, as informações cadastrais e regulatórias em sistemas internos e em bases de órgãos reguladores e autorreguladores;
- Supervisionar a adequação das informações de *suitability*;
- 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.

4.2. Treinamento GRC

As empresas do Grupo Netz mantêm Programa de Treinamentos em compliance, ética, prevenção à lavagem de dinheiro, segurança da informação, proteção de dados pessoais, anticorrupção e demais temas regulatórios e autorregulatórios aplicáveis às atividades do Grupo. O Programa é estruturado com treinamentos periódicos, com periodicidade mínima anual, e treinamentos extraordinários sempre que houver alterações regulatórias relevantes, identificação de risco ou indicação da Área de GRC.

São destinatários obrigatórios do Programa todos os colaboradores, administradores e estagiários do Grupo, observado o conteúdo aplicável a cada função. A Área de GRC mantém registro de presença, conteúdo programático, instrutor e avaliação dos participantes, conservando as evidências pelo prazo mínimo de 5 (cinco) anos ou pelo prazo exigido pela regulamentação aplicável. A ausência injustificada nos treinamentos obrigatórios sujeita o colaborador às medidas disciplinares cabíveis, observado o regramento interno do Grupo.

5. KYC, KYP, KYE E KYS

O Grupo Netz 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*): procedimentos de identificação, qualificação, classificação e monitoramento de clientes, investidores e contrapartes, conforme aplicável;
- KYP (*Know Your Partner*): diligência sobre parceiros comerciais e estratégicos, com avaliação de histórico, reputação, integridade e conformidade;

- KYE (*Know Your Employee*): diligência sobre colaboradores, incluindo verificação de antecedentes, conflitos de interesse e monitoramento compatível com a função exercida; e
- KYS (*Know Your Supplier*): diligência sobre fornecedores e prestadores de serviços, com avaliação de idoneidade, reputação, capacidade técnica e aderência a padrões éticos e regulatórios.

Para a realização das diligências, poderão ser utilizadas fontes públicas, bases cadastrais, sistemas de terceiros e demais mecanismos compatíveis com a natureza da análise. Todos os processos observarão a legislação aplicável, os normativos internos do Grupo Netz e as diretrizes dos órgãos reguladores e autorreguladores competentes.

O Grupo Netz mantém matriz interna de risco para classificação das partes avaliadas e definição da periodicidade de monitoramento.

6. POLÍTICA DE CERTIFICAÇÃO PROFISSIONAL

As empresas do Grupo Netz que aderirem a códigos de autorregulação ou estiverem sujeitas a exigências específicas de certificação profissional deverão assegurar que os colaboradores que desempenhem atividades elegíveis estejam devidamente certificados, atualizados e em conformidade com a regulamentação aplicável, observadas as particularidades de cada atividade.

Este capítulo estabelece os critérios de exigência, elegibilidade, enquadramento funcional, monitoramento, atualização, dispensa, equivalência e afastamento relacionados às certificações exigidas no âmbito das atividades reguladas e autorreguladas do Grupo Netz, com foco especial nas exigências da ANBIMA aplicáveis à gestora e às atividades de distribuição, quando cabíveis.

6.1. Atividades Elegíveis e Princípios Gerais

A certificação exigida para cada Colaborador será definida com base nos seguintes critérios, cumulativamente:

- nas funções efetivamente exercidas;
- no grau de autonomia e responsabilidade; e
- na existência ou não de alçada ou poder discricionário final de investimento.

É vedado a qualquer Colaborador:

- exercer atividade elegível sem a certificação correspondente, dispensa ou equivalência formalmente reconhecida; ou
- atuar além dos limites conferidos pela certificação obtida.

A Equipe de Governança, Risco e Compliance é responsável por:

- validar o correto enquadramento das funções;
- monitorar a validade e o status das certificações; e
- impedir o exercício irregular de atividades elegíveis.

6.2. Certificações Aplicáveis à Gestão de Recursos (CGA e CGE)

São consideradas certificações aplicáveis às atividades de gestão discricionária de recursos de terceiros:

- CGA – Certificação de Gestores ANBIMA, exigida para a gestão de fundos regulados pela Resolução CVM nº 175 e carteiras administradas;
- CGE – Certificação de Gestores ANBIMA para Fundos Estruturados, exigida para a gestão de fundos estruturados, incluindo FIDCs, FIPs, FIIs, ETFs, FIAGROs estruturados e demais veículos previstos nas Regras da ANBIMA.

São elegíveis à CGA e/ou CGE exclusivamente os Colaboradores que:

- integrem a equipe técnica de gestão; e
- detenham, de fato, alçada e poder discricionário final para ordenar a compra ou venda de ativos, sem necessidade de aprovação prévia.

A CFG – Certificação ANBIMA Fundamentos de Gestão constitui requisito prévio para a obtenção da CGA ou CGE, não conferindo, por si só, alçada ou poder decisório de investimento.

6.3. Certificação C-Pro R (Profissional de Relacionamento)

A certificação C-Pro R é aplicável aos colaboradores que atuem em atividades de relacionamento com clientes, investidores ou cotistas, observados os limites, atribuições e permissões previstos nas regras vigentes da ANBIMA.

São elegíveis à C-Pro R os Colaboradores que:

- prestem informações institucionais, operacionais ou comerciais;

- prospectem clientes e realizem acompanhamento comercial ou pós-venda; e
- não participem da análise, recomendação ou decisão de investimentos.

A obtenção da C-Pro R exige, obrigatoriamente, a prévia certificação CPA (Certificação Profissional ANBIMA), a qual possui caráter de fundamentos e não confere, por si só, autorização para o exercício de atividades elegíveis nem alçada decisória.

A atuação do profissional certificado pela C-Pro R deverá observar os limites e atribuições previstos nas regras vigentes da ANBIMA, não lhe sendo conferido, por si só, poder discricionário final de investimento.

6.4. Certificação C-Pro I (Profissional de Investimentos)

A certificação C-Pro I é aplicável aos Colaboradores que atuem em atividades de análise, avaliação, recomendação ou indicação de investimentos, sem poder discricionário final.

São elegíveis à C-Pro I os Colaboradores que:

- realizem análises técnicas ou de produtos;
- elaborem recomendações ou sugestões de investimento; e
- participem do processo decisório de forma consultiva.

A obtenção da C-Pro I exige, obrigatoriamente, a prévia certificação CPA, a qual não confere alçada decisória.

A C-Pro I não substitui as certificações CGA ou CGE e não confere poder final de decisão, sendo obrigatória a validação por profissional devidamente certificado, conforme aplicável.

6.5. Validade, Atualização e Manutenção das Certificações

As certificações ANBIMA estão sujeitas a prazos de validade e procedimentos periódicos de atualização, conforme as Regras vigentes.

A Gestora assegurará que:

- nenhum Colaborador exerça atividade elegível com certificação vencida;
- os prazos e status sejam continuamente monitorados pela Equipe de Governança, Risco e Compliance; e
- os procedimentos de atualização sejam cumpridos tempestivamente.

Os critérios relativos a pagamento, subsídio, reembolso, incentivos ou exceções encontram-se definidos em documento interno específico, podendo exceções ser estabelecidas mediante deliberação da Diretoria Executiva, a ser oportunamente formalizada.

6.6. Identificação, Monitoramento e Banco de Dados ANBIMA

Antes da contratação, admissão, promoção ou transferência de qualquer Colaborador, a Equipe de Governança, Compliance e Risco deverá:

- validar as funções a serem exercidas;
- identificar eventual Atividade Elegível; e
- verificar certificações existentes no Banco de Dados da ANBIMA.

Todas as informações deverão ser atualizadas até o último dia útil do mês subsequente ao evento que ensejou a alteração.

6.7. Afastamento e Medidas Corretivas

A constatação de atuação em atividade elegível sem certificação válida implicará:

- afastamento imediato do Colaborador das respectivas atividades;
- apuração de responsabilidades; e
- definição e implementação de plano de adequação, quando aplicável.

Compete à Diretora de Governança, Risco e Compliance determinar o afastamento, avaliar eventual falha de supervisão e definir as medidas corretivas cabíveis.

6.8. Dispensa e Equivalência de Certificações

A Gestora observará estritamente as regras de dispensa de exame e de equivalência de certificações previstas no Código de Certificação da ANBIMA e nas orientações técnicas divulgadas pela entidade.

6.8.1. Dispensa por experiência profissional

A dispensa de exame poderá ser solicitada por profissionais que comprovem experiência profissional conforme critérios da ANBIMA, independentemente da posse de certificações externas, mediante decisão do Conselho de Certificação. O próprio profissional interessado deverá fazer a solicitação de dispensa à ANBIMA.

6.8.2. Equivalência por certificação (CFA® e CAIA®)

Profissionais com certificação ativa CFA® e/ou CAIA® poderão solicitar equivalência para certificações da ANBIMA, inclusive CGA e CGE, mediante solicitação formal e aprovação expressa do Conselho de Certificação, não sendo o reconhecimento automático.

A certificação CFP® poderá ser considerada para fins de equivalência ou dispensa em relação à trilha C-Pro R, nos termos das regras aplicáveis. O próprio profissional interessado deverá fazer a solicitação de dispensa à ANBIMA.

6.9. Limites, Restrições e Rastreabilidade

As certificações da trilha C-Pro possuem escopos próprios e não são intercambiáveis, devendo sua utilização observar estritamente as atividades autorizadas conforme a regulação vigente e as normas de autorregulação da ANBIMA aplicáveis.

Nesse sentido:

- as certificações da trilha C-Pro devem ser utilizadas em conformidade com seus respectivos escopos, limites, requisitos e permissões previstos nas regras vigentes da ANBIMA, não sendo admitida a substituição ou equivalência automática entre certificações sem previsão normativa específica; e
- a certificação C-Pro R não habilita o profissional para atividades privativas de análise ou recomendação de investimentos, permanecendo tais atribuições restritas aos profissionais devidamente certificados para essas funções, nos termos da regulação aplicável.

Adicionalmente, o Grupo Netz manterá controles que assegurem a rastreabilidade das certificações dos profissionais e a aderência entre as atividades desempenhadas e as habilitações exigidas, incluindo registros atualizados, evidências de certificação válida e mecanismos de verificação periódica.

Nenhuma certificação, dispensa ou equivalência:

- confere, por si só, poder discricionário final de investimento; ou
- substitui automaticamente as certificações CGA ou CGE, quando exigidas.

Toda decisão deverá ser documentada e mantida disponível para fins de auditoria, supervisão e fiscalização pela ANBIMA e pela CVM.

7. CONFLITO DE INTERESSES E SEGREGAÇÃO DE ATIVIDADES

O Grupo Netz adota controles destinados a identificar, avaliar, prevenir, mitigar e, quando necessário, administrar situações de conflito entre interesses pessoais, profissionais e institucionais, bem como a assegurar a segregação física, lógica, informacional e funcional entre as empresas do Grupo Netz e entre atividades potencialmente conflitantes.

Considerando a atuação do Grupo Netz em múltiplas frentes, incluindo gestão, estruturação de operações, consultoria, securitização e distribuição própria, deverão ser observados controles específicos de segregação de atividades, acessos, fluxos de informação e tomada de decisão, conforme a natureza da atividade e a regulamentação aplicável.

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*.

As informações digitais serão segregadas por meio de sistemas eletrônicos com perfis de acesso restritos, trilhas de auditoria e controles de autenticação compatíveis com a criticidade da informação, sendo a liberação e revisão de acessos realizada em conjunto pelas Áreas de Tecnologia da Informação e GRC.

As diretrizes deste item deverão ser observadas em conjunto com o Código de Ética, a Política de Negociação de Valores Mobiliários e a Política de Investimentos Pessoais e os demais normativos internos relacionados à prevenção de conflitos de interesse no âmbito do Grupo.

8. POLÍTICA ANTICORRUPÇÃO

As empresas do Grupo Netz estão sujeitas às normas anticorrupção aplicáveis, inclusive a Lei nº 12.846/2013 e o Decreto nº 11.129/2022, comprometendo-se a prevenir, identificar e reprimir atos lesivos à administração pública, nacional ou estrangeira, bem como quaisquer práticas incompatíveis com padrões éticos e de integridade.

Considera-se agente público e, portanto, sujeito à esta Política, sem limitação: (i) qualquer indivíduo que exerce, mesmo que temporariamente e/ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de

investidura ou vínculo, mandato, cargo, emprego ou função em órgão público, entidade governamental ou controlada pelo governo; (ii) qualquer indivíduo que seja candidato a 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[7].

Ainda que as atividades das empresas do Grupo Netz não estejam diretamente ligadas 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 de qualquer das empresas do Grupo Netz; e
- Manter relacionamento comercial com terceiros que não observem padrões éticos, legais e reputacionais compatíveis com os do Grupo Netz.

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.

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

Conforme previsto na Política Corporativa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (“Política de PLDFTP”) e na respectiva Metodologia ABR, o Grupo Netz mantém controles destinados à mitigação do risco de utilização de suas estruturas para práticas ilícitas, observadas a legislação e a regulamentação aplicáveis, tais 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 ao COAF, quando cabível, nos termos da legislação e regulamentação aplicáveis;
- Treinamentos periódicos para conscientização; e
- Atualização anual do relatório de PLDFTP.

[7] 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).

Cabe à Área de GRC a análise, o monitoramento e o tratamento das informações relacionadas ao tema, bem como a supervisão dos controles adotados pelas áreas envolvidas. Os registros, relatórios, comunicações e evidências relacionadas ao PLDFTP deverão ser armazenados pelo prazo mínimo exigido pela regulamentação aplicável, observado, em qualquer hipótese, o prazo mínimo de 5 (cinco) anos, quando cabível.

10. 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:

- Dados de clientes, investidores, contrapartes, parceiros e colaboradores;
- Estratégias de investimento, planos de negócio, projetos internos e deliberações ainda não públicas;
- Dados pessoais e dados pessoais sensíveis; e
- Modelos, sistemas, bases de dados e códigos internos.

O tratamento e o compartilhamento dessas informações deverão observar sua respectiva classificação, conforme a Política de Segurança da Informação e Cibersegurança do Grupo, bem como os critérios de necessidade, proporcionalidade e acesso restrito.

Os meios de comunicação e dispositivos utilizados para fins profissionais poderão ser monitorados, na forma da legislação aplicável e das políticas internas do Grupo. Em caso de suspeita de violação às diretrizes previstas neste Manual ou no Código de Ética, os registros e arquivos pertinentes poderão ser analisados para fins de apuração, observados os princípios de necessidade, proporcionalidade e confidencialidade.

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

O Grupo Netz mantém controles e políticas específicas para assegurar a integridade, disponibilidade e confidencialidade das informações corporativas e pessoais, em conformidade com as normas regulatórias e autorregulatórias aplicáveis, especialmente as Políticas de Segurança da Informação e Cibersegurança e de Proteção de Dados Pessoais do Grupo.
A Área de Tecnologia e Segurança da Informação, em conjunto com a Área de GRC, é responsável por, dentre outros:

- Controlar acessos físicos e lógicos;
- Garantir o uso adequado de equipamentos, sistemas e credenciais;
- Implementar controles de segurança, testes e medidas de contingência;
- Responder a incidentes de segurança da informação e comunicar à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável, observados os fluxos internos de reporte e comunicação; e
- Apoiar o cumprimento das diretrizes corporativas de proteção de dados pessoais.

O Grupo promoverá treinamentos periódicos sobre segurança da informação e proteção de dados pessoais, de modo a disseminar as diretrizes aplicáveis e reforçar a cultura de integridade e proteção da informação.

A segurança da informação é responsabilidade compartilhada entre as áreas de GRC e Tecnologia da Informação, observadas as respectivas atribuições, as políticas corporativas do Grupo e a regulamentação aplicável. O Grupo mantém procedimentos de backup, recuperação de dados, controle de acesso e contingência compatíveis com a criticidade de suas operações.

Os controles, sistemas e procedimentos de segurança da informação, de privacidade e de segurança cibernética são objeto de testes e validação periódicos, no mínimo anuais, ou em prazo inferior quando exigido pela regulamentação aplicável, em atendimento ao artigo 16 das Regras e Procedimentos de Deveres Básicos da ANBIMA. Os resultados dos testes, incluindo eventuais não conformidades e os respectivos planos de ação, serão reportados à Área de GRC e à Alta Administração e mantidos à disposição dos órgãos reguladores e autorreguladores.

11. FATOS RELEVANTES

Este item aplica-se às atividades exercidas no âmbito da gestão de fundos de investimento e demais estruturas sujeitas à regulamentação da CVM, em especial a Resolução CVM 175, quando aplicável. Embora a divulgação de fatos relevantes seja operacionalizada, conforme o caso, pelo administrador fiduciário ou pelo responsável legalmente competente, cabe à Netz, na qualidade de prestadora de serviços essenciais ou participante da estrutura, comunicar tempestivamente os fatos de que tenha conhecimento e que possam demandar divulgação, nos termos da regulamentação aplicável.

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.

Em caráter excepcional, a divulgação poderá ser temporariamente postergada quando, de forma fundamentada e em conformidade com a regulamentação aplicável, sua revelação puder comprometer interesse legítimo do fundo, da classe ou de seus cotistas, hipótese em que as informações deverão ser mantidas sob confidencialidade até que cesse a justificativa para o sigilo.

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 deverá notificar o administrador fiduciário caso tenha conhecimento de qualquer situação neste sentido.

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

12. 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 preliminar dos casos reportados será conduzida pela Diretora de GRC, com posterior submissão ao Comitê de Ética[8], quando cabível, nos termos dos normativos internos do Grupo.

13. 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, avaliação, planos de ação, monitoramento de testes e incidentes, controle de prazos e responsabilidades, aprovação, comunicação à hierarquia responsável, reporte ao Comitê de GRC, dentre outros.

A mitigação do risco operacional se dá por meio da adoção de controles estruturados, incluindo governança de processos, definição de responsabilidades, validações sistêmicas e manuais, monitoramento contínuo, gestão de incidentes, planos de ação corretiva, controles de contingência e supervisão periódica dos riscos identificados.

Os controles relacionados à continuidade operacional, contingência tecnológica e tratamento de incidentes deverão ser observados em conjunto com o Plano de

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

Continuidade de Negócios (PCN), com a Política de Segurança da Informação e com o Manual de Gestão de Incidentes do Grupo, quando aplicáveis.

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

- Inventário e mapeamento de processos;
- Definição de controles preventivos e detectivos;
- Reconciliações e conferências periódicas;
- Monitoramento de sistemas e acessos;
- Backup e controles de contingência tecnológica;
- Acesso remoto aos sistemas utilizados;
- Registro e tratamento de incidentes operacionais, por meio de formulário; e
- Implementação e acompanhamento de planos de ação.

Na hipótese de ocorrência de incidente operacional ou vazamento de informação, o colaborador deverá comunicar imediatamente as Áreas de GRC, Tecnologia da Informação e a liderança da área envolvida, por meio dos canais internos definidos pelo Grupo, informando, sempre que possível, a descrição do evento, a data e horário da ocorrência, os envolvidos, o conteúdo impactado e as medidas já adotadas.

O reporte imediato não afasta a necessidade de registro formal do incidente na ferramenta corporativa aplicável, quando existente, para fins de rastreabilidade, apuração, plano de ação e auditoria.

14. AUDITORIA, MONITORAMENTO E MELHORIAS CONTÍNUAS

O Grupo realizará monitoramentos, testes e, quando aplicável, auditorias internas e externas com o objetivo de verificar a eficácia dos controles internos, a aderência aos normativos internos e o cumprimento das exigências legais, regulatórias e autorregulatórias.

As avaliações poderão abranger, entre outros aspectos, a revisão de processos, a verificação de conformidade regulatória, a análise de riscos e controles, a implementação de planos de ação e a efetividade das medidas corretivas adotadas.

Os resultados dessas avaliações deverão ser reportados à Alta Administração e, quando cabível, aos fóruns de governança competentes, servindo de base para o aprimoramento contínuo do ambiente de controles internos do Grupo. Os planos de ação decorrentes dessas avaliações deverão ser formalizados, acompanhados e revisados até sua conclusão, com definição de responsáveis e prazos.

No âmbito específico das atividades de securitização, o Diretor Responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos da Netz Securitizadora encaminhará aos órgãos de administração da companhia, até o último dia útil do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior, contendo: (i) as conclusões dos exames efetuados; (ii) as recomendações a respeito de eventuais deficiências, com cronograma de saneamento, quando for o caso; e (iii) a manifestação do Diretor Responsável pelas Atividades de Securitização sobre as deficiências encontradas em verificações anteriores e sobre as medidas planejadas ou efetivamente adotadas, nos termos do artigo 21 da Resolução CVM nº 60. O relatório alcança todas as subsidiárias integrais referidas no §1º do artigo 3º da Resolução CVM nº 60 e fica disponível à CVM na sede da companhia.

15. VIGÊNCIA E ATUALIZAÇÃO

Este Manual será revisado, no mínimo, anualmente, ou em prazo inferior sempre que houver alterações relevantes na legislação, na regulamentação, na estrutura do Grupo ou nos processos internos que justifiquem sua atualização.

Histórico das atualizações		
Data	**Versão**	**Tópicos**
janeiro/2025	V1.0	Constituição da Gestora
abril/2025	V2.0	Atualização – conflitos de interesse
outubro/2025	V3.0	Atualização – Netz Holding
junho/2026	V4.0	Atualização – Netz Securitizadora

ANEXO I
Termo de Recebimento e Compromisso

TERMO DE RECEBIMENTO E COMPROMISSO

1. IDENTIFICAÇÃO DO DECLARANTE

Nome completo: _____
CPF/MF nº: _____
RG nº: _____
Cargo/Função:_____
Departamento/Área: _____
Empresa do Grupo Netz: _____
Data de admissão/Início do vínculo: ____/____/____
E-mail corporativo: _____

2. DECLARAÇÕES E COMPROMISSOS

Pelo presente Termo, eu, acima qualificado(a), na condição de integrante do Grupo Netz, na qualidade de colaborador(a), administrador(a), estagiário(a), prestador(a) de serviços ou parceiro(a) de negócio, declaro, sob as penas da lei, o quanto segue:

(i) Que recebi, nesta data, uma via – em meio físico e/ou eletrônico – do Manual de Compliance e Controles Internos do Grupo Netz, doravante denominado simplesmente "Manual";

(ii) Que li integralmente o conteúdo do Manual, tive a oportunidade de esclarecer todas as dúvidas junto à área de Compliance do Grupo Netz e compreendi plenamente o seu conteúdo, alcance, finalidade e aplicabilidade às minhas atividades;

(iii) Que me comprometo a observar, cumprir e fazer cumprir, integral e permanentemente, todas as regras, diretrizes, políticas, procedimentos, vedações e controles estabelecidos no Manual, bem como na legislação vigente, nas normas regulatórias aplicáveis e nas demais políticas internas do Grupo Netz;

(iv) Que atuarei sempre com ética, integridade, transparência, lealdade, boa-fé e diligência no desempenho de minhas atividades, abstendo-me de praticar qualquer ato que possa configurar conflito de interesses, fraude, corrupção, lavagem de dinheiro, financiamento ao terrorismo, discriminação, assédio ou qualquer outra conduta vedada pelo Manual e pela legislação aplicável;

(v) Que manterei absoluto sigilo e confidencialidade sobre todas as informações de natureza profissional, técnica, comercial, financeira, estratégica,

operacional ou de qualquer outra natureza a que tiver acesso em razão do meu vínculo com o Grupo Netz, inclusive sobre dados pessoais de clientes, colaboradores e parceiros, observando integralmente a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e demais normas aplicáveis;

(vi) Que comunicarei imediatamente à área de Compliance do Grupo Netz, por meio dos canais oficiais disponibilizados, inclusive pelo canal de denúncias, qualquer suspeita, indício ou conhecimento de descumprimento das disposições do Manual, das normas legais ou regulatórias aplicáveis, ou de qualquer ato ilícito, irregular ou antiético praticado por integrantes do Grupo Netz ou por terceiros;

(vii) Que estou ciente de que o canal de denúncias garante a confidencialidade das informações reportadas e a proteção do denunciante de boa-fé contra qualquer forma de retaliação;

(viii) Que estou ciente de que o Manual de Compliance e Controles Internos poderá ser revisado, atualizado e complementado periodicamente, comprometendo-me a tomar conhecimento das novas versões disponibilizadas pelo Grupo Netz e a observar as atualizações como se neste Termo estivessem expressamente reproduzidas;

(ix) Que me comprometo a participar dos treinamentos, capacitações e eventos de reciclagem em compliance promovidos pelo Grupo Netz, sempre que convocado(a);

(x) Que estou ciente e expressamente concordo que o descumprimento, total ou parcial, das regras, políticas e procedimentos estabelecidos no Manual, na legislação aplicável ou nas demais normas internas do Grupo Netz poderá ensejar a aplicação das medidas disciplinares cabíveis, incluindo, conforme a gravidade do caso, advertência verbal ou escrita, suspensão, rescisão do vínculo contratual ou empregatício por justa causa, sem prejuízo da apuração das responsabilidades civis, administrativas, regulatórias e criminais aplicáveis;

(xi) Que este Termo é firmado em caráter irrevogável e irretratável, produzindo efeitos a partir desta data e perdurando pelo prazo de vigência do meu vínculo com o Grupo Netz, bem como, no que for cabível, após o seu término, especialmente quanto às obrigações de sigilo e confidencialidade.

São Paulo/SP, _____ de _____ de _____

_____

Assinatura do(a) Declarante

3. CIÊNCIA DA ÁREA DE COMPLIANCE

Atesto o recebimento do presente Termo, devidamente assinado pelo(a) Declarante acima qualificado(a), que passa a integrar o respectivo dossiê funcional/contratual, na forma do Manual de Compliance e Controles Internos do Grupo Netz.

_____

Área de Governança, Risco e Compliance – Grupo Netz

Nome do responsável: _____

Data: ____/____/_____