nanoasset.com.br

atendimento@nanoasset.com.br
11 97250- 8045

Rua George Ohm, 230
Cidade Monções – SP

POLÍTICA DE COMPLIANCE, CONTROLES INTERNOS E CIBERSEGURANÇA

NanoAsset

COMPLIANCE E CONTROLES INTERNOS

Versão Atualizada: Julho/2024

Objetivo

Formalizar os procedimentos para gerenciamento dos riscos de compliance e controles internos na NanoAsset GESTÃO DE RECURSOS LTDA ("NanoAsset").

A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a NanoAsset (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de Risco, Compliance e PLD.

Estrutura e Responsabilidades

Cabe à NanoAsset garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento à legislação, regulação, autorregulação e políticas internas vigentes.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à NanoAsset contidas nesta Política, zelando para que todas as normas éticas, legais, regulatórias e autorregulatórias sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ou indício de violação ao Diretor de Risco, Compliance e PLD.

Cabe à alta administração da NanoAsset:

1. A responsabilidade pelos controles internos e o gerenciamento dos riscos de compliance;

2. Indicar um diretor estatutário responsável por compliance e controles internos, devendo tal profissional ter acesso a todas as informações e pessoas na NanoAsset quando do exercício de suas atribuições;

3. Aprovar, estabelecer e divulgar esta Política; e

4. Garantir a efetividade do gerenciamento do risco de compliance.

O Diretor de Risco, Compliance e PLD deve:

1. Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e Compliance da NanoAsset, atuando no gerenciamento efetivo de tais atividades no seu dia a dia;

2. Gerenciar o Comitê de Compliance e o Conselho de Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;

3. Designar os secretários das reuniões do Comitê de Compliance e do Conselho de Ética;

4. Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas.

É responsabilidade de todos os Colaboradores o cumprimento das normas legais, regulatórias e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da NanoAsset.

Qualquer suspeita, indício e/ou evidência de desconformidade por eles verificada deve ser imediatamente comunicada ao Diretor de Risco, Compliance e PLD.

O Diretor de Risco, Compliance e PLD se reporta apenas à alta administração da NanoAsset, com autonomia e independência para indagar a respeito de práticas e procedimentos adotados nas suas operações/atividades, devendo adotar medidas que coíbam ou mitiguem as eventuais inadequações, incorreções e/ou inaplicabilidades.

Os controles e monitoramentos determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de Compliance da NanoAsset, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade: o Diretor de Risco, Compliance e PLD tem poder de veto – mas não de voto – nos Comitês de negócios da NanoAsset.

A Área de Compliance é formada pelo diretor estatutário responsável e por mais um profissional, e se dedicam ao exercício das atividades de cumprimento de regras, políticas,

procedimentos e controles internos, incluindo o cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção (além de também acumular a função de controle de risco).

Revisão e Atualização

Este Código deverá ser revisado e atualizado a cada 2 (dois) anos, ou em prazo inferior, caso necessário em função de mudanças legais, regulatórias, autorregulatórias ou estruturais da NanoAsset.

Escopo e Atribuições do Compliance

A atuação do Diretor de Risco, Compliance e PLD tem por escopo:

Temas Normativos

• Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à NanoAsset e às suas atividades, e apresentar o resultado de suas verificações no Comitê de Compliance;

• Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção, renovação e/ou manutenção junto às autoridades reguladoras/autorreguladoras competentes;

• Auxiliar a alta administração da NanoAsset no relacionamento com órgãos reguladores, e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;

• Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação, regulação e autorregulação em vigor.

Boas Práticas

• Disseminar e promover as informações necessárias para o cumprimento das políticas internas e das normas legais, regulatórias e de autorregulação aplicáveis;

• Exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;

• Disponibilizar aos novos Colaboradores as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;

• Estabelecer controles para que todos os Colaboradores da NanoAsset que desempenhem funções ligadas à gestão de fundos de investimento ou de carteiras administradas, atuem com independência;

• Garantir que os controles internos sejam compatíveis com os riscos da NanoAsset em suas atividades;

• Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Comitê de Compliance e/ou no Conselho de Ética;

• Orientar previamente e/ou acompanhar o responsável pela comunicação à imprensa em contatos telefônicos, entrevistas, publicação de artigos ou qualquer outra forma de manifestação de opinião através de veículo público (inclusive na internet).

Governança

• Aprovar novas políticas internas no Comitê de Compliance, ou a sua revisão, por força de mudanças na legislação, regulação ou autorregulação aplicáveis, ou ainda, de decisões internas da NanoAsset;

• Aprovar a oferta de novos produtos e prestação de novos serviços pela NanoAsset, a partir de inputs técnicos do Comitê de Investimento;

• Atuar para que haja efetividade na segregação física de atividades conflitantes;

• Apresentar o resultado de seus controles e verificações no Comitê de Compliance;

• Monitorar e buscar a efetiva aplicação dos documentos de compliance e controles internos abaixo listados;

• Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da NanoAsset e às suas demais políticas;

• Convocar, gerenciar, organizar e secretariar o Comitê de Compliance, registrando suas decisões em atas;

• Implementação de Regras e Guarda de Evidências – monitoramento da implementação de procedimentos, de cumprimento das normas e políticas internas, bem como de mecanismos de guarda de evidências;

• Salvaguarda de Informações - devem ser mantidos, pelo prazo mínimo de 5 (cinco) anos, os documentos e informações exigidos pela regulação aplicável.

• Informar, de forma clara e transparente, qualquer potencial conflito de interesse entre a NanoAsset e empresas do grupo , junto ao mercado e clientes.

Escopo e Atribuições do Compliance

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo Compliance - deve ser submetida ao Conselho de Ética da NanoAsset para conclusão e deliberação dos passos a serem dados a tal respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de Risco, Compliance e PLD deve comunicar os respectivos órgãos competentes, nos prazos regulatórios, como seguem:

• A CVM deve ser comunicada no prazo máximo de 10 (dez) dias da verificação da respectiva ocorrência ou sua identificação, ou em prazo menor, se assim exigido pela regulação aplicável;

• O COAF deve ser comunicado no prazo de 24 (vinte e quatro) horas da verificação da respectiva ocorrência ou sua identificação.

Os demais prazos aplicáveis à NanoAsset encontram-se previstos no Anexo I a esta Política, bem como na planilha de controle interno detalhada, intitulada “Quadro de Rotinas”.

Documentos de Compliance e Controles Internos

O Sistema de Compliance e Controles Internos da NanoAsset está previsto em seus documentos internos, que englobam todas as suas políticas, manuais e Código de Ética e Conduta Profissional, além de procedimentos e organismos internos.

Documentos Específicos Disponibilizados no Website da NanoAsset

Cabe ao Diretor de Risco, Compliance e PLD preencher os respectivos Formulários de Referência da NanoAsset e mantê-los em seu website. Tais formulários devem ser atualizados obrigatoriamente até o dia 31 de março de cada ano.

Adicionalmente, cabe ao Diretor de Risco, Compliance e PLD manter no website da NanoAsset, em suas versões atualizadas, ao menos os documentos abaixo assinalados com asteriscos (obrigatórios pela regulamentação em vigor). Os demais documentos, poderão ser disponibilizados, a critério da gestora:

• Código de Ética e Conduta Profissional*;

• Formulários de Referência da NanoAsset *;

• Política de Compliance e Controles Internos*;

• Política de Gestão de Riscos*;

• Política de Investimentos Pessoais e da Empresa*;

• Política de Rateio de Ordens de Investimento*;

• Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;

• Plano de Contingência e Continuidade de Negócios;

Testes e Relatórios Anuais

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pela NanoAsset, é realizado um teste anual de aderência, o qual deve ser formalizado em relatório.

Os relatórios relativos aos controles internos e à prevenção à lavagem de dinheiro são de responsabilidade do Diretor de Risco, Compliance e PLD: os relatórios, após ratificação pelo Comitê de Compliance, são encaminhados à alta administração da NanoAsset anualmente, até o último dia útil de ABRIL de cada ano.

Os Relatórios Anuais em questão ficam disponíveis para consulta da CVM, através de sistema de arquivamento em nuvem NanoAsset.

Organismos Relacionados a Compliance e Controles Internos

Comitê de Compliance

O Comitê de Compliance é responsável por avaliar o descumprimento das normas legais, regulatórias, autorregulatórias e das políticas, manuais e procedimentos internos da NanoAsset.

Ademais, cabe ao Comitê de Compliance avaliar, do ponto de vista normativo, as atividades da NanoAsset e dos veículos de investimento sob sua responsabilidade, a fim de

garantir a aderência à legislação e normas regulatórias e autorregulatórias em vigor, bem como aprovar ações de correção nestas matérias, além de:

• Avaliar os processos internos da NanoAsset do ponto de vista de melhores práticas, bem como avaliar as ocorrências do período;

• Concluir por eventuais apontamentos de situações irregulares ao Conselho de Ética e/ou à alta administração da NanoAsset;

• Analisar eventuais situações ocorridas de desenquadramento de mandato no mês anterior, procedimentos adotados, e recomendações de controle futuro;

• Elaborar e distribuir a Lista Restrita de Ativos da NanoAsset fazendo seu acompanhamento e monitoramento; e

• Monitorar mudanças regulatórias e coordenar ajustes e adaptações necessárias na NanoAsset e seus produtos. Periodicidade: trimestral.

Participantes: composto pelos diretores da NanoAsset e pela equipe de Compliance, sempre com a presença do Diretor de Risco, Compliance e PLD.

Convidados: podem ser convidados outros Colaboradores da NanoAsset, porém sem direito a voto.

Quórum mínimo: Necessária a presença de ao menos três membros, sendo obrigatória a presença do Diretor de Risco, Compliance e PLD (ou representante por ele designado).

Tem direito a voto no Comitê apenas os sócios e diretores, cabendo sempre ao Diretor de Risco, Compliance e PLD, voto de minerva ou veto.

Formalização das decisões: atas do Comitê sob responsabilidade da Área de Compliance.

Comitê de Risco

O Comitê de Risco tem suas atribuições descritas na forma definida na Política de Gestão de Riscos da NanoAsset.

Conselho de Ética

O Conselho de Ética tem suas atribuições descritas na forma definida no Código de Ética e Conduta Profissional da NanoAsset.

Segregação de Atividades e Conflitos de Interesse

Cabe ao Diretor de Risco, Compliance e PLD assegurar e verificar que sejam devidamente segregadas das atividades de gestão de quaisquer outras atividades eventualmente desempenhadas pela NanoAsset (ou empresas na qual a NanoAsset, seus sócios, diretores ou colaboradores possuam participação acionária ou interesses econômicos), que com aquelas guardem qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma: a segregação em questão deverá se dar tanto física quanto logicamente, com restrição de acesso a dependências, sistemas, diretórios e arquivos apenas aos Colaboradores autorizados de cada área pertinente da NanoAsset - e, se for o caso, entre estes e colaboradores de empresas de seu grupo econômico -, nos termos de suas Políticas.

Todas e quaisquer atribuições de controle na NanoAsset – notadamente, mas sem limitação, o próprio compliance e o gerenciamento de riscos – não dependem nem estão sujeitas às suas áreas de negócios, de forma a assegurar a total autonomia de tais controles frente a cogitações de ordem comercial, ou de gestão de fundos ou carteiras de valores mobiliários.

O bom uso de instalações, equipamentos e informações comuns é obrigatório para todos os funcionários. As estações de trabalho, incluindo as autônomas e os equipamentos portáteis, devem ter, sem exceção, senha de inicialização tendo seu acesso bloqueado após minutos de inatividade, liberado apenas com senha do usuário da própria estação.

As áreas de negócios possuem acesso restrito a seus profissionais, para garantir segurança e segregação física da área da área responsável pela administração de carteiras de valores mobiliários e de eventuais demais atividades conflitantes (a título de exemplo, caso sejam futuramente desenvolvidos negócios relacionados à intermediação ou distribuição de valores mobiliários ou outra atividade qualquer de cunho conflitante).

A segregação física é monitorada pela área de Compliance mediante a governança e monitoramento de pessoas com acesso (físico e lógico) a suas áreas de competência, onde cada um possui acesso eletrônico específico para as respectivas áreas.

Vale destacar aqui que as atividades secundárias que serão desempenhadas pela gestora estão totalmente relacionadas a gestão de investimento, tais como: estruturação de fundos exclusivos para clientes profissionais e qualificados; análise de portfólio de clientes; assessoria para construção de regulamento de fundos junto a administradores e custodiantes; orientação/assessoria junto a clientes de carteira administradas com relação aos seus investimentos financeiros.

Portanto, nesses casos, esses serviços secundários estão englobados nas taxas de administração e performance cobrados pelo serviço de gestão de ativos mobiliários.

Com relação à segregação de informações, há procedimentos internos relacionados à confidencialidade de informações devidamente classificadas, conforme detalhado nos termos da Política de Segurança de Informação. Além disso, os arquivos estão em nuvem com acessos restritos às suas áreas. E no caso da Nano Capital, esta tem um backup em nuvem próprio em outro prestador de serviço e com acessos próprios e restritos a equipe.

Como regra geral, os Colaboradores detentores de Informações Confidenciais, em função de seu cargo ou função, devem estabelecer barreiras de acesso a dados e informações aos demais colaboradores, cujo acesso seja dispensável e/ou não autorizado/essencial.

Essas barreiras servem para atender a diversos propósitos, incluindo a conformidade com leis e regulamentos que governam o tratamento e a utilização de certos tipos de informações, evitar situações que possam suscitar um potencial conflito de interesses e coibir a má utilização de dados e/ou informações.

A análise de produtos ou serviços oferecidos pela NanoAsset deve sempre privilegiar o melhor interesse do investidor, e, caso envolva a oferta de produtos ou serviços da NanoAsset deve se dar por atributos técnicos e de melhor benefício ao investidor.

Deve se mitigar, especialmente potenciais conflitos de interesse, sempre na busca das melhores alternativas ao investidor, de forma transparente, quando envolver:

• a atividade de gestão que eventualmente envolva a alocação em fundos geridos pela própria NanoAsset; e

• a atividade de gestão e outras atividades quaisquer que venham a ser desenvolvidas pela NanoAsset, e que envolva o investimento por parte dos veículos sob gestão da NanoAsset ou de clientes.

Tais hipóteses devem considerar não apenas produtos e serviços ofertados pela NanoAsset, mas também empresas do grupo, ou nas quais a NanoAsset, sócios, diretores ou colaboradores tenham participação acionária ou interesses econômicos ou pessoais, parcerias estratégicas, etc.

No caso da outra empresa que faz parte do grupo econômico, a Nano Capital, a segregação física é feita por acesso eletrônico, onde só quem tem acesso às dependências da NanoAsset são seus colaboradores e sócios.

E caso haja alocação em algum ativo originado pela Nano Capital, o mesmo deverá ser informado do potencial conflito de interesse. Também deverá ter um limite de acordo com o perfil de risco do cliente/fundo e deverá demonstrar as razões técnicas da escolha do produto.

No caso de haver atividades que tenham potencial conflito de interesse entre as atividades da NanoAsset com a da Nano Capital, tem de ser respeitar as seguintes condições:

• Primeiramente, o time de alocação e gestão tem de provar o benefício econômico e financeiro dos ativos junto a seus investidores e suas respectivas carteiras e fundos

• Ser aprovado pelo comitê de Risco & Compliance, com aprovação obrigatória do Diretor de Risco & Compliance.

• O formato de alocação será sempre via Fundo de Investimento, e não via carteira administrada diretamente.

• Informar, no regulamento do fundo, que a NanoAsset poderá adquirir títulos de emissão pública de ofertas em plataforma eletrônicas de investimento coletivo (Equity Crowdfunding), sejam da Nano ou de outras plataformas.

• Disclaimer em materiais de divulgação, tais como prospectos e lâminas, informando o potencial conflito de interesse, para conhecimento do cliente.

• Aprovação expressa dos clientes, com a ciência desses casos.

Contratações Externas

Em sua atividade de gestão de carteiras, a NanoAsset não realiza quaisquer contratações de prestadores de serviço em nome dos fundos sob sua gestão, seja de atividades reguladas pela CVM ou autorreguladas pela ANBIMA, cabendo tais contratações aos respectivos administradores dos referidos fundos.

Assim, esta Política se aplica somente às contratações feitas pela própria NanoAsset, em seu próprio nome e benefício.

A contratação de serviços de terceiros deve ser precedida das seguintes providências:

• Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção; Portanto, não são previstas neste documento regras de Supervisão Baseada em Risco, conforme previstas na autorregulação da ANBIMA.

• O Compliance poderá demandar medidas adicionais pré-contratação, tais como visita às dependências do prestador de serviço, clippings de mídia impressa/internet, além de outras medidas reputadas cabíveis/convenientes à contratação.

• De acordo com a avaliação de conveniência dos profissionais envolvidos, solicitar a assinatura, pelos terceiros a serem contratados, de "Acordo de Não Divulgação" (Non-Disclosure Agreement ou "NDA"); e

• Nos processos de negociação de qualquer contrato a ser celebrado pela NanoAsset, o Colaborador envolvido na negociação deverá informar ao Comitê de Compliance sobre qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negociais, que tenha com membros do potencial contratado.

Após a contratação dos respectivos serviços, a Área de Compliance poderá, a seu critério, supervisionar os contratados.

Qualquer eventual exceção às normas acima deverá ser reportada ao Comitê de Compliance.

A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:

• O critério principal para escolha e contratação de terceiros será a modalidade menor preço, mediante a obtenção de orçamentos em número determinado pelo Diretor de

Risco, Compliance e PLD para escolha do fornecedor ou prestador de serviços;

• Em casos excepcionais em que um fornecedor mais caro seja escolhido, a contratação deverá ser justificada com os outros critérios (por exemplo: prazo, qualidade, expertise, menor impacto ambiental etc.);

• Não haverá exigência de concorrência:

• Nas compras e contratações para valores inferiores a R$ 5.000,00 (cinco mil reais), desde que os pagamentos não se refiram a parcelas de um mesmo serviço;

• Quando já houver um contrato com prestadores de serviços recorrentes, não sendo, neste caso, necessário realizar concorrência a cada contratação ou compra;

• Em compras e contratações em casos de especialidade do fornecedor/prestador;

• Em compras e contratações em casos emergenciais, caracterizados pela urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer as atividades da NanoAsset, e que não pôde ser previsto antecipadamente.

Contratação de Corretoras

A supervisão poderá ser realizada mediante procedimentos diversos a critério do Compliance, tais como visitas in loco, clippings de mídia impressa/internet, requisição periódica de certidões administrativas/judiciais, além de outras medidas reputadas cabíveis/convenientes à contratação.

O processo de seleção deve ser respaldado por análise criteriosa e objetiva de aspectos qualitativos da corretora de valores mobiliários ("Corretora ou Corretoras"). Dentre os aspectos qualitativos analisados, devem ser avaliados principalmente a reputação, o porte, a posição no ranking da B3, os selos de certificação que a corretora possui por meio do programa de qualificação da B3 e os custos.

O Diretor responsável pela gestão das carteiras dos fundos de investimentos ou o membro da equipe de gestão por ele autorizado, indicará ao Diretor de Compliance o nome da Corretora que pretende recomendar para contração.

A Área de Compliance da NanoAsset realizará um processo de due diligence da Corretora indicada, por meio do Questionário ANBIMA de due diligence para Contratação de Corretoras, disponível através do link:

(https://www.anbima.com.br/data/files/66/46/EF/AD/CB1F561086B1AE5678A80AC2/QDD_se rvicos_qualificados_e_corretoras.pdf).

A Área de Compliance manterá uma lista de Corretoras aprovadas no processo de due diligence e os membros da equipe de gestão executarão ordens exclusivamente através das Corretoras constantes desta lista. O Diretor de Compliance atualizará a lista de Corretoras aprovadas conforme as novas relações forem estabelecidas ou relações existentes forem terminadas ou modificadas.

No que diz respeito a contratações em nome dos fundos de investimentos sob sua gestão, a NanoAsset se limita à contratação apenas de Corretoras - sempre que possível - pertencentes a uma lista previamente apontada pelo administrador dos fundos sob sua gestão (caso a contratação não seja realmente feita pelo próprio administrador fiduciário).

Requisitos ligados à reputação no mercado das Corretoras são avaliados, com o objetivo de identificação de eventuais atividades ilícitas ou de lavagem de dinheiro, corrupção e financiamento do terrorismo, bem como se a Corretora também tem práticas de prevenção à lavagem de dinheiro e anticorrupção: para tal, estes são analisados em sistemas de clipping, verificação de PEPs, listas restritivas e outras investigações internas da NanoAsset, tais como serviços equivalentes às consultas Serasa, SPC e processos judiciais (cíveis e/ou criminais, inclusive ambientais), com vistas a atestar a sua idoneidade e reputação.

Requisitos Contratuais

Os contratos estabelecidos com as Corretoras devem estabelecer:

• As obrigações e deveres das partes envolvidas;

• A relação e as características dos serviços que serão contratados e exercidos por cada uma das partes;

• A obrigação de cumprir suas atividades em conformidade com as disposições previstas nas normas aplicáveis da ANBIMA e da CVM, especificamente, no que aplicável, para cada tipo de fundo de investimento; e

• Que os terceiros contratados devem, no limite de suas atividades, deixar à disposição do administrador fiduciário todos os documentos e informações exigidos pela regulação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da regulação vigente.

As contratações de Corretoras necessariamente devem ser aprovadas no Comitê de Risco e Compliance, em processo de análise prévia coordenado pelo Diretor responsável por Compliance e PLD. A avaliação deve considerar, ao menos:

• Tempo de existência da corretora e composição acionária;

• Políticas internas e governança;

• Preço e qualidade dos serviços;

• Estrutura tecnológica, operacional, sistemas, controles etc.; ü Atendimento aos programas de capacitação e excelência da B3;

• Processos eventualmente existentes (CVM, B3, BACEN, ANBIMA, etc.);

• Solidez patrimonial, estrutura operacional, corpo de funcionários e capacitação técnica;

• Aspectos reputacionais e experiência anterior de profissionais da NanoAsset com a Corretora;

• Qualificação das áreas de execução, research, prêmios recebidos etc.

Classificação e Supervisão por Nível de Risco

A partir dos atributos acima, as Corretoras serão classificadas, pelo Comitê de Risco, em 3 níveis de risco, a saber: (i) baixo; (ii) médio e (iii) alto.

As Corretoras classificadas como de baixo risco, passam por processo de revisão/atualização a cada 24 (vinte e quatro) meses; as de médio risco, a cada 18 (dezoito) meses; e, as de alto risco, a cada 12 (doze) meses.

A metodologia da NanoAsset para aferição do nível de risco segue os seguintes critérios:

Alto Risco - são consideradas de "alto risco" as Corretoras que, individual ou cumulativamente:

• Tenham quaisquer apontamentos verificados no processo de pré-contratação da NanoAsset, sem oferecer, ou tendo se recusado a dar, justificativa para as ocorrências constatadas;

• Não estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;

• Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, sem oferecer, ou tendo se recusado a dar, as devidas explicações para tanto;

• Tenham apontamentos verificados no processo de screening da NanoAsset, via mídia impressa ou na internet, sem justificativa plausível para tal;

• Se recusem a permitir o acesso de Colaboradores do Compliance da NanoAsset às suas dependências, quando do procedimento de pós-contratação;

• Tenham, em seus quadros PEPs, conforme definidas na política da NanoAsset;

• Falhem em atender, sem justificativa, outros critérios reputados convenientes pela NanoAsset na verificação de suas atividades/idoneidade.

Médio Risco - são consideradas de "médio risco" as Corretoras que, individual ou cumulativamente:

• Tenham apontamentos verificados no processo de pré-contratação da NanoAsset, oferecendo, porém, justificativa plausível para tanto;

• Estejam em processo de regularização de suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou de suas obrigações autorregulatórias, quando aplicáveis;

• Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, oferecendo, porém, as devidas explicações para tanto;

• Tenham apontamentos verificados no processo de screening da NanoAsset, via mídia impressa ou na internet, justificando a contento da NanoAsset a ocorrência verificada;

• Falhem em atender, mas remediando posteriormente, outros critérios reputados convenientes pela NanoAsset na verificação de suas atividades/idoneidade.

Baixo Risco - são consideradas de "baixo risco" as Corretoras que:

• Não tenham quaisquer apontamentos verificados no processo de pré-contratação da NanoAsset;

• Estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;

• Não tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores;

• Não tenham apontamentos verificados no processo de screening da NanoAsset, via mídia impressa ou na internet, sem justificativa plausível para tal;

• Atendam, com sucesso, outros critérios reputados convenientes pela NanoAsset na verificação de suas atividades/idoneidade.

A contagem de prazo é válida a partir do efetivo uso das Corretoras em operações, e, para aquelas em que houver uso frequente de operações (ao menos 4 – quatro – vezes ao mês). A mera aprovação da Corretora, sem seu uso efetivo, não dá início à contagem de prazo.

As revisões precisam ser apresentadas ao Comitê de Risco, com a manifestação do Diretor de Gestão a respeito da efetividade e qualidade dos serviços prestados pela Corretora.

No caso de eventos extraordinários, como falhas na execução de ordens, aquisições ou alterações societárias e notícias ou fatos relevantes divulgados ao público e ao mercado, que justifiquem fiscalização em prazo menor, tal procedimento deve ser realizado e documentado com a urgência necessária.

Soft Dollar

Em relacionamentos comerciais é comum que sejam recebidos e oferecidos presentes, hospitalidades ou entretenimento de/para parceiros de negócios. Porém é importante que tais brindes não facilitem a tomada de decisão ou a troca de favores que configurem conflitos de interesses. Desta forma, nenhum colaborador deve dar ou aceitar qualquer tipo de gratificação, presentes ou benefícios que possa gerar conflito de interesses, ainda que potencial, com a

NanoAsset, especialmente nos casos de clientes, fornecedores, agentes ou entidades públicas, ou até concorrentes, salvo com expressa autorização do Departamento de Compliance.

Não estão abrangidos pela vedação ao recebimento de presentes, hospitalidades ou entretenimento de/para parceiros de negócios, os brindes que (i) não tenham valor comercial; ou (ii) que sejam distribuídos de forma generalizada a título de cortesia, propaganda, divulgação habitual ou por ocasião de eventos especiais ou datas comemorativas, desde que não ultrapassem, cumulativamente e dentro do período de um ano, o valor de R$1.000,00 (mil reais), em relação a um mesmo terceiro.

Treinamentos e Reciclagens

A Área de Compliance, será responsável por difundir as melhores práticas dentro da NanoAsset, por meio de treinamentos, sempre que houver uma atualização nas diretrizes de segurança ou demais políticas internas.

A frequência e renovação destes treinamentos presenciais dependerá da velocidade de crescimento e novas contratações da gestora, e será considerado pela diretoria.

Independentemente de novos treinamentos, cada novo colaborador tem acesso a todas as políticas e manuais internos para aculturamento das regras definidas pela gestora.

Sempre que houver mudanças significativas nas políticas (motivadas por decisão interna, ou adaptação a novos normativos), ou tópicos de segurança, serão promovidos treinamentos de reciclagem, mesmo se não houver novos colaboradores contratados.

A NanoAsset pode fazer uso de suas consultorias externas para apoio profissional em treinamentos e reciclagens. Os treinamentos contam com lista de presença. Os treinamentos têm periodicidade anual, caso haja mudança nos quadros de colaboradores, ou, atualizações significativas de políticas e procedimentos.

O programa de treinamento deve incluir em sua agenda anual os temas relacionados a PLDFT, e ser obrigatório a todos os Colaboradores com linguagem clara e que aborde as especificidades de cada função desempenhada.

Os treinamentos ministrados para os Colaboradores internos devem atender aos seguintes critérios:

• Ser aplicado no ingresso de todo novo Colaborador;

• Ser ministrado anualmente a todos os Colaboradores;

• Prover insumos para reciclagem das áreas e pessoas com deficiência de aprendizado.

O Programa de Treinamentos de PLDFT da NanoAsset deve considerar os Terceiros Relevantes. Nesse sentido, conforme acordo entre as partes, o Diretor de Risco, Compliance e PLD poderá considerar a apresentação, pelo Terceiro Relevante, de evidência de realização de treinamento de PLDFT, âmbito interno do referido Terceiro Relevante, de forma satisfatória a critério da Diretoria. Sendo, portanto, dispensado da participação nos treinamentos oferecidos pela Gestora.

O programa de Treinamentos é aplicável a administradores, empregados e colaboradores que possuam acesso a informações confidenciais, participem do processo de decisão de investimento ou participem da prospecção de novos negócios. O treinamento deve abranger as políticas e procedimentos adotados pela NanoAsset e será sempre compatível com a atividade desempenhada pelo administrador, sócio ou funcionário.

A NanoAsset promoverá a conscientização e difusão de melhores práticas sobre proteção dos Dados na empresa, através de ações educativas e treinamentos periódicos.

Licenças e Desligamentos

No caso de licenças e desligamentos, o Diretor de Risco, Compliance e PLD deve verificar se o Colaborador está vinculado à NanoAsset no site da ANBIMA, e, nesse caso, desvincular o profissional, o que deve ocorrer impreterivelmente no mesmo mês de licença e/ou desligamento.

Os profissionais em licença não devem continuar vinculados no período em que estiverem de licença. Quando retornarem, deverá ser efetuado o vínculo novamente.

Banco de Dados da ANBIMA

O Diretor de Risco, Compliance e PLD é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

O controle de admissão, licença e demissão consta na agenda regulatória do Comitê de Compliance, onde são formalizados tais registros, devendo as eventuais atualizações junto à entidade ocorrer até o último dia do mês subsequente ao evento.

Código de Ética e Conduta Profissional

Cabe ao Diretor de Risco, Compliance e PLD requerer dos novos Colaboradores a assinatura formal do Termo de Conhecimento e Adesão ao Código de Ética e Conduta Profissional e das demais políticas da NanoAsset, até o último dia do mês subsequente à sua contratação.

POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Versão Atualizada: Julho/2024

Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da NANO GESTAO DE RECURSOS LTDA ("NanoAsset").

A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a NanoAsset (doravante, "Colaboradores").

Contexto Operacional e de Negócios

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da NanoAsset:

• A NanoAsset não possui sistemas desenvolvidos internamente, executando suas atividades utilizando sistemas de terceiros, todos apenas acessíveis via web, não possuindo nenhum sistema que necessite de instalações locais para ser executado;

• Os fornecedores dos sistemas utilizados pela NanoAsset se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da NanoAsset;

• Os colaboradores da NanoAsset estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;

• A NanoAsset aloca recursos sob gestão mediante a utilização de corretoras/plataformas de investimento acessíveis pela WEB e disponíveis para qualquer dispositivo eletrônico (laptops, smartphones, tablets ou computadores de mesa);

• O sistema de consolidação de carteiras utilizado pela NanoAsset identifica os clientes por meio de siglas ou identificação alfanumérica, dispensando a identificação mediante o preenchimento de cadastro com informações pessoais;

• Os arquivos contendo informações pessoais e financeiras dos clientes da NanoAsset são armazenados em nuvem, com backups periódicos não superiores a 7 (sete) dias corridos, podendo ser recompostos solicitando tais informações aos próprios clientes;

• Os dispositivos eletrônicos (laptops, smartphones, tablets) utilizados no exercício das atividades da NanoAsset possuem senha de acesso e criptografia;

• A NanoAsset utiliza redes sem fio para fornecer acesso à web para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à web, os Colaboradores utilizam redes/roteadores de redundância. Neste caso, e em caso de trabalho remoto, os Colaboradores da NanoAsset comprometem-se a utilizar redes sem fio seguras para desempenhar suas atividades;

• O espaço físico/escritório da NanoAsset deve ser o local preferencialmente utilizado para as suas atividades, reuniões com clientes, comitês e reuniões com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da NanoAsset estão parametrizados para serem passíveis de desempenho remoto.

Responsabilidades

Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de Risco, Compliance e PLD, que deverá avaliá-las e submetê-las ao Comitê de Compliance e/ou Conselho de Ética, conforme o caso.

O Diretor de Risco, Compliance e PLD deve garantir o atendimento a esta Política, sendo o responsável na NanoAsset por temas de segurança da informação/cibernética.

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/regulatórias/autorregulatórias.]

Informações Confidenciais

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

• Identifiquem dados pessoais ou patrimoniais (da NanoAsset ou de clientes);

• Sejam objeto de acordo de confidencialidade celebrado com terceiros;

• Identifiquem ações estratégicas – dos negócios da NanoAsset, seus clientes ou dos portfólios sob gestão;

• Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da NanoAsset, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;

• Sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que

• O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que são de uso pessoal e intransferível.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de Risco, Compliance e PLD,(ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, bem como (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de Risco, Compliance e PLD acerca da possibilidade de compartilhamento da Informação Confidencial.

Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na NanoAsset:

• Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

• Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

• Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da NanoAsset:

• As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;

• A informação deve ser utilizada apenas para os fins sob os quais foi coletada;

• A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

• A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

• Segregação de instalações, equipamentos e informações comuns, quando aplicável;

• A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de Risco, Compliance e PLD.

Identificação, Classificação e Controle da Informação

O Colaborador que recebe ou prepara uma informação pode, se eventualmente necessário, classificá-la como “Confidencial”. Para tal conclusão, devem ser consideradas as questões de natureza legal e regulatória, de estratégia negocial, os riscos do compartilhamento, as necessidades de restrição de acesso e os impactos no caso de utilização indevida das informações.

Caso haja informação de natureza “Confidencial”, o acesso a mesma deve ser restrito e controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de Risco, Compliance e PLD, e, se reputado necessário, da assessoria jurídica da NanoAsset.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de Risco, Compliance e PLD.

Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando trabalhando remotamente. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na NanoAsset são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares.

A NanoAsset poderá, a qualquer momento, mediante prévia aprovação do Diretor de Risco, Compliance e PLD, e sem obrigação de cientificação prévia:

• inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários; ü disponibilizar esses recursos a terceiros, caso entenda necessário;

• solicitar aos usuários justificativas pelo uso efetuado;

• monitorar acesso a sites, aplicativos etc.;

• bloquear acesso a sites.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é cancelada, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à NanoAsset.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede em nuvem da NanoAsset, mediante segregação física e lógica.

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e Backups

Os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de Risco, Compliance e PLD, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços fornecidos por terceiros deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. O Diretor de Risco, Compliance e PLD deve solicitar o resultado de tais testes aos fornecedores de tais sistemas, bem como acompanhar a solução de eventuais deficiências apontadas em tais testes.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de Risco, Compliance e PLD deverá ser imediatamente comunicado, para a tomada das medidas cabíveis.

Testes de Controles

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de Risco, Compliance e PLD e reportados ao Comitê de Compliance.

Os testes devem verificar se:

• Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;

• Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que têm acesso a estas informações;

• Há segregação física e lógica;

• Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;

• A manutenção de registros permite a realização de auditorias e inspeções.

Riscos de Cibersegurança

As principais ameaças e riscos aos ativos cibernéticos da NanoAsset são:

• Malwares – softwares desenvolvidos para corromper os computadores e redes, como:

• vírus: software que causa danos às máquinas, redes, softwares e bancos de dados;

• cavalos de tróia: aparecem dentro de outro software, criando uma entrada para invasão da máquina;

• spywares: software maliciosos que coletam e monitoram as atividades das máquinas invadidas;

• ransomware: softwares maliciosos que bloqueiam o acesso a sistemas e bases de dados, solicitando resgates para restabelecimento do uso/acesso.

• Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como, por exemplo:

• pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

• phishing: links veiculados por e-mails simulando pessoas ou empresas confiáveis que enviam comunicação eletrônica aparentemente oficial para obter informações confidenciais;

• vishing: simulação de pessoas ou empresas confiáveis para, por meio de ligações telefônicas, obtenção de informações confidenciais;

• smishing: simulação de pessoas ou empresas confiáveis para, por meio de mensagens de texto, obtenção de informações confidenciais; ü ataques de DDOS (distributed denial of services) e botnets – ataques visando a negar ou atrasar o acesso aos serviços ou sistemas da instituição;

• invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Obrigações de Cibersegurança

Na prestação de seus serviços, a NanoAsset obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos.

O responsável por tais questões na NanoAsset é o Diretor de Risco, Compliance e PLD.

São itens obrigatórios de cibersegurança (empresa):

◦ A adequada proteção dos ativos cibernéticos da NanoAsset, aí incluídos sua rede, sistemas, softwares, websites, equipamentos, serviços de arquivamento em nuvem e arquivos eletrônicos.

◦ Restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de colaboradores da NanoAsset;

◦ Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;

◦ Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;

◦ Excluir ou desabilitar contas inativas;

◦ Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;

◦ Garantir o cumprimento do procedimento de backup para os servidores em nuvem e ativos cibernéticos, eletrônicos e computacionais da NanoAsset;

◦ Detectar, identificar, registrar e comunicar ao Diretor de Risco, Compliance e PLD as violações ou tentativas de acesso não autorizadas;

◦ Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;

◦ Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;

◦ Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;

◦ A NanoAsset dispõe de segurança nos serviços de nuvem do qual utiliza para o acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado;

◦ É realizado backup de arquivos de forma sistemática. Os dados de backup atualizados são armazenados em local seguro, com monitoramento.

São itens OBRIGATÓRIOS de cibersegurança (Colaboradores):

◦ Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;

◦ Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para evitar vírus ou códigos maliciosos;

◦ No caso de recebimento de mensagens que contrariem as regras estabelecidas pela NanoAsset, NUNCA as repassar, alertando o responsável da sua área e o Diretor de Risco, Compliance e PLD, se for o caso;

◦ Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;

◦ Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;

◦ Utilizar equipamentos, aplicativos, impressoras, acesso a sites, e e-mail (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da NanoAsset;

◦ Tecnologias, marcas, metodologias e quaisquer informações que pertençam à NanoAsset não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;

◦ Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens VEDADOS de cibersegurança (Colaboradores):

◦ Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais;

◦ Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;

◦ Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da NanoAsset;

◦ Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da NanoAsset;

◦ Alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de Risco, Compliance e PLD;

◦ Contratar provedores de acesso sem autorização prévia ou ciência do Diretor de Risco, Compliance e PLD;

◦ Uso de compartilhadores de informações, tais como redes Peer-toPeer (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da NanoAsset.

Exceções a esta Política de Cibersegurança (Colaboradores):

◦ Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos colaboradores para desempenhar suas atividades na NanoAsset, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da NanoAsset, seus clientes e parceiros de negócio, podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;

◦ É facultado ao Diretor de Risco, Compliance e PLD autorizar exceções à esta política, devendo estar formalizadas por e-mail.

ANEXO I

Quadro de Obrigações Periódicas

Norma	Artigo	Tema	Obrigação	Período
RCVM 21	25, caput e I a III	Relatório Anual	Entrega do relatório à administração	Último dia útil de abril a cada ano (data base 31/12)
RCVM 21	17, caput e II	Formulário de Referência	Envio do FR pelo CVMWeb	Anualmente, até 31/03 (data base 31/12)
RCVM 51	1.º, II	Declaração Eletrônica de Conformidade	Envio pelo CVMWeb	Anualmente, até 31/03 (data base 31/12)
RCVM 50	4.º, III	Política de PLD	Atualização dos dados cadastrais dos clientes/investidores e/ou verificação da efetiva atualização	No máximo a cada 5 (cinco) anos

			dos citados dados pelo administrador/ distribuidor	
RCVM 50	6.º, I a VII, e §§	Relatório Anual de PLD	Entrega do relatório à administração da NanoAsset (obs: pode estar compreendido no Relatório Anual de Compliance, em vez de ser apresentado em separado)	Anualmente, até o último dia útil do mês de abril
RCVM 50	23, caput e Parágrafo Único	Política de PLD	Declaração Negativa de PLD à CVM	Anualmente, até o último dia útil do mês de abril
RCVM 51	1.º, I	Atualização de dados cadastrais	Atualização via CVMWeb	7 (sete) dias úteis contados do evento que deu causa à alteração

Informações Periódicas

Norma	**Artigo**	**Tema**	**Obrigação**	**Período**
RCVM 50	22 e §§	Política de PLD	Comunicar ao COAF todas as situações e operações detectadas, ou	24 (vinte e quatro) horas a contar conclusão análise

			propostas de operações que possam constituir-se em sérios indícios de LDFT	caracterizou atipicidade operação, respectiva proposta, mesmo da situ atípica detectada
RCVM 21	18, VIII	Violação à regulação	Informar à CVM a ocorrência ou indícios de violação da sua regulação	10 (dez) dias úteis da ocorrência ou sua identificação
Ofício Circular CVM/SIN 10/15	Item 37	Atualização cadastral	Envio à CVM do contrato social atualizado, no caso de mudança de denominação social ou de substituição de diretor responsável pela gestão	7 (sete) dias úteis do fato que deu causa à alteração

ANEXO II

Modelo de Relatório de Aderência

Ilmos. Srs.

Sócios e Diretores da

NANO GESTAO DE RECURSOS LTDA

Ref.: Relatório Anual – Resolução CVM nº 21, de 25 de fevereiro de 2021 (“RCVM 21”)

Ano Base: [•]

Prezados Senhores,

Em cumprimento ao disposto no art. 25 da RCVM 21, vimos apresentar a V.Sas. o relatório pertinente às atividades da NANO GESTAO DE RECURSOS LTDA, (“NanoAsset”) no ano de [•] (“Relatório”).

De acordo com a RCVM 21, o mencionado Relatório contém:

• As conclusões dos exames efetuados;

• As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e

• A manifestação do diretor responsável pela administração de carteiras de valores mobiliários, ou, quando for o caso, pelo diretor responsável pela gestão de risco, a respeito das eventuais deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las (cf. art. 25, I, II e III, da RCVM 21).

Este relatório ficará à disposição da Comissão de Valores Mobiliários (“CVM”) na sede da NanoAsset, para eventuais posteriores checagens, verificações e/ou fiscalizações por parte da CVM.

Além dos aspectos acima, V.Sas. encontrarão também, no corpo do presente Relatório, os resultados do Teste de Aderência determinado na Política de Compliance e Controles Internos da NanoAsset, e o correspondente parecer final do Diretor de Risco Compliance e PLD, que assina o presente documento.

Assim sendo, passamos abaixo à exposição dos elementos pertinentes do presente

Relatório.

I. Conclusão dos Exames Efetuados (RCVM 21, art. 25, I)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

II. Recomendações sobre as Deficiências Encontradas e Cronogramas de Saneamento

(RCVM 21, art. 25, II)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo estimativas de datas de acompanhamento e conclusão das soluções)

III. Manifestações dos Diretores Correspondentes de Gestão e de Risco sobre as Verificações Anteriores e Respectivas Medidas Planejadas (RCVM 21, art. 25, III) (enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo os resultados esperados e os efetivamente alcançados)

IV. Parecer Final do Diretor de Risco, Compliance e PLD (enumerar detalhadamente)

Sendo então o que nos cumpria para o momento, aproveitamos o ensejo desta correspondência para nos colocarmos à disposição de V.Sas. para os eventuais esclarecimentos porventura reputados necessários.

Atenciosamente,

[•]

NANO GESTAO DE RECURSOS LTDA Diretor de Risco, Compliance e PLD

ANEXO III

Orientações Gerais sobre o Conteúdo Técnico do Teste de Aderência

A Diretoria de Risco, Compliance e PLD deve estruturar registro e controle ativo, ao longo do ano, para composição do Relatório Anual (descrito no Anexo I), ao menos sobre as seguintes matérias relacionadas abaixo.

Tais temas devem – ao longo do ano – ser endereçados e monitorados no Comitê de Compliance, e, quando necessário, ser objeto de acompanhamento próximo da alta gestão (sócios e diretores) da NanoAsset.

Tal controle deve ser feito em planilhas específicas, servindo como ferramenta de compliance e controle de risco operacional.

O controle ao longo do ano dos eventos abaixo, e seu registro é uma das obrigações centrais do Comitê de Compliance.

I. Conclusão dos Exames Efetuados (RCVM 21, art. 25, I)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

-> Deve constar em planilha de controle o registro dos seguintes eventos (ao menos) ocorridos ao longo do ano, suas consequências / perdas e as atitudes corretivas adotadas:

• erros operacionais atinentes a operações dos fundos; erros relativos à movimentação financeira de clientes;

• falhas em pagamentos de remuneração de distribuidores ou corretagem de fundos pagas a corretoras ou quaisquer prestadores de serviço;

• desenquadramentos de carteiras, comunicação com administrador e reenquadramento; ü qualquer outro descumprimento de norma legal constatado;

• eventos de liquidez dos fundos;

• falhas operacionais relativas à infraestrutura tecnológica e plano de correção implementado;

• acionamentos do plano de contingência e continuidade de negócios;

• falhas de fornecedores; falhas relativas a quaisquer políticas internas ou normas legais e plano de correção implementado;

• mudanças expressivas em parâmetros de liquidez dos fundos; eventos relacionados ao gerenciamento de risco, com especial atenção a risco de crédito e liquidez;

• ofícios ou qualquer outro alerta e comunicação recebidos de reguladores, ou processos administrativos junto à CVM, ANBIMA e demais reguladores aplicáveis, ou em alçadas do poder judiciário;

• descumprimento de contratos quaisquer; ü quebra de dever de sigilo contratual; ü quaisquer eventos adicionais considerados relevantes pelo compliance e que tenham colocado em risco a empresa, seus colaboradores, clientes, carteiras sob gestão ou as boas práticas de mercado.